Cyber Authentication Technology Solutions: Deployment Profile of OpenID Connect 1.0

Version	3.0.2
Date	2022-05-16
Status	Implementer's Draft

Table of Contents

1. Introduction

OpenID Connect 1.0 is a rich and extensible standard that must be profiled in order to promote interoperability, and the profiles that typically emerge from the broader standardization process usually remain fairly broad and include a number of options and features that increase the burden for implementers and make deployment-time decisions more difficult.

Implementation profiles define the features that software implementations must support such that implementers can be assured of the ability to meet their own (possibly varied) deployment requirements. Deployment profiles define specific options and constraints to which deployments are required to conform; they guide product configuration and federation operations, and provide criteria against which actual deployments may be tested. This document provides a deployment profile for use by members of a GC Federation.

1.1. Overview of the CATS Deployment Profile of OpenID Connect 1.0

The deployment profile leverages the draft International Government Assurance Profile (iGov) for OpenID Connect 1.0 [OIDC-iGov] to guide deployments of authentication, session initiation, and identity verification processes. The OpenID Connect Back Channel [OIDC-BC] and Front Channel [OIDC-FC] Logout specifications are leveraged to support session termination.

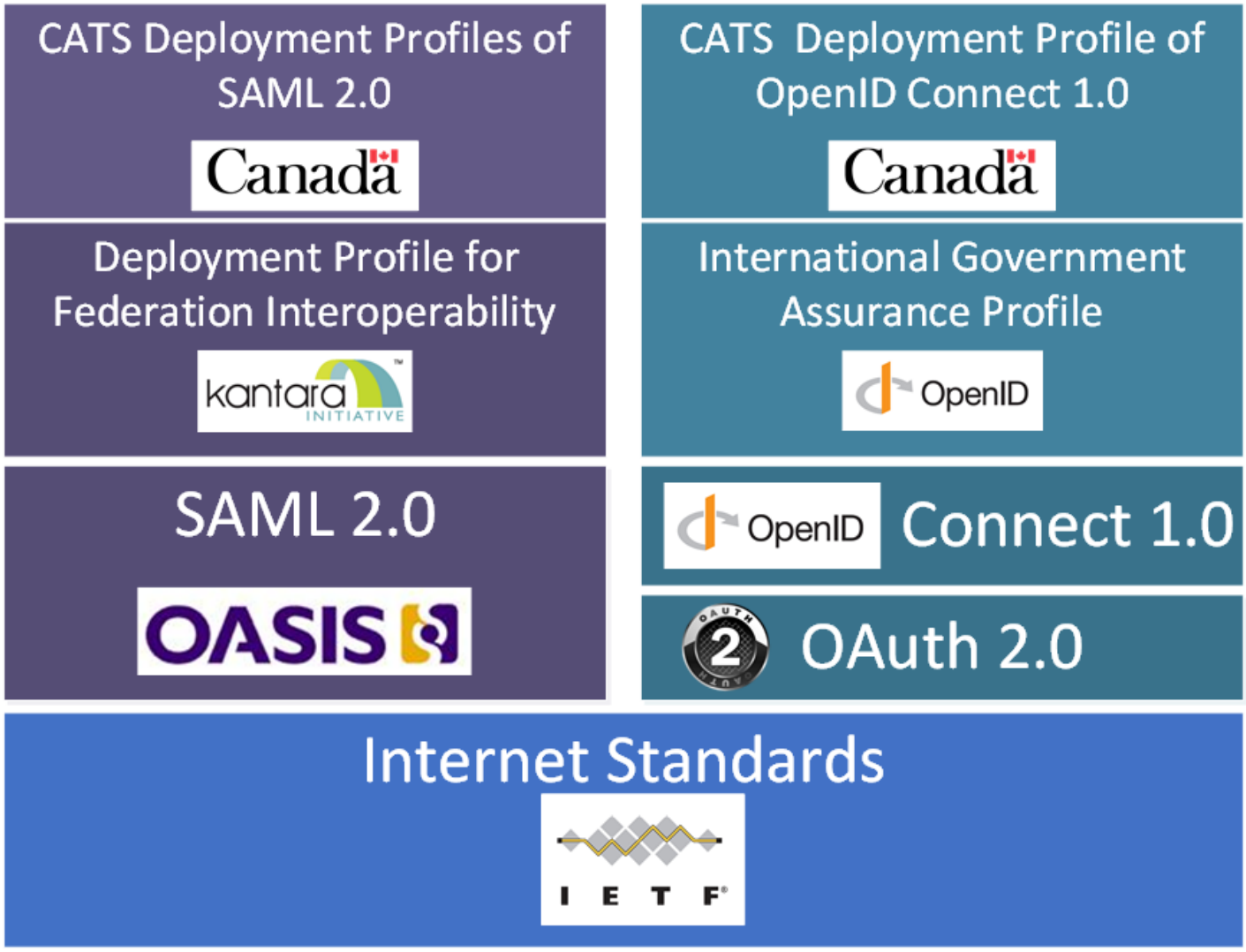

Figure 1. CATS Profile Building Blocks

2. Notation and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This specification uses the following typographical conventions in text: `ClaimName`, **Datatype**, `OtherCode`. The normative requirements of this specification are individually labeled with a unique identifier in the following form: **[ODP-EXAMPLE01]**. All information within these requirements should be considered normative unless it is set in *italic* type. Italicized text is non-normative and is intended to provide additional information that may be helpful in implementing the normative requirements.

2.1. Terminology

This specification uses the terms "Access Token", "Authorization Code", "Authorization Endpoint", "Authorization Grant", "Authorization Server", "Client", "Client Authentication", "Client Identifier", "Client Secret", "Grant Type", "Protected Resource", "Redirection URI", "Refresh Token", "Resource Owner", "Resource Server", "Response Type", and "Token Endpoint" defined by OAuth 2.0 [RFC6749], the terms "Claim Name", "Claim Value", and "JSON Web Token (JWT)" defined by JSON Web Token (JWT) [RFC7519], and the terms defined by OpenID Connect Core 1.0 [OpenID-Core].

Whether explicit or implicit, all the requirements in this document are meant to apply to deployments of OpenID Connect profiles and may involve explicit support for requirements by implementing software and/or supplemental support via application code. Deployments of a Relying Party may refer to both stand-alone implementations of OpenId Connect, libraries integrated with an application, or any combination of the two. It is difficult to define a clear boundary between an OpenID Connect client and the Relying Party application/service it represents, and unnecessary to do so for the purposes of this document.

3. Compliance to the CATS Deployment Profile for OpenID Connect 1.0

The requirements specified are in addition to all normative requirements of the underlying specifications, including the International Government Assurance Profiles (iGov) for OAuth 2.0 [iGov-OAuth2] and OpenID connect [iGov-OIDC], the OpenID Connect specifications for back-channel [OIDC-BC] and front-channel [OIDC-FC] logout, and all other specifications normatively referenced therein. Readers are assumed to be familiar with all relevant reference documents. Any such requirements are not repeated here except where deemed necessary to highlight a point of discussion or draw attention to an issue addressed in errata, but remain implied.

Note that protocol features that are optional, or lack mandatory processing rules, are assumed to be optional and out of scope of this profile if not otherwise precluded or given specific processing rules.

This specification defines requirements for the following components:

- OpenID Connect 1.0 Relying Parties (also known as OpenID Clients)
- OpenID Connect 1.0 OpenID Providers (also known as identity providers)
- OpenID Connect 1.0 proxying identity providers

The specification also defines features for interaction between these components:

- Relying party to OpenID provider
- OpenID provider to relying party

The normative requirements of this CATS Deployment Profile are detailed in Sections 4 through 7 of this document. This profile may either constrain, waive, or augment specific requirements of the underlying specifications. In such cases a reference to the source and location of the original requirement is provided, and then the requirement itself is repeated word-for-word. Each requirement is then annotated with the support required by this profile: typically this is either “Constrained”, “Not Applicable” or "Augmented". Further details are then provided to fully explain the CATS requirement.

This profile also has requirements which are specific to this profile.

Compliance with all requirements labeled "REQUIRED" "MANDATORY", "MUST", and "MUST NOT" is required for all members of a GC Federation. There are no exceptions. Requirements designated as “SHOULD”, “RECOMMENDED”, “SHOULD NOT” or “NOT RECOMMENDED” must not be interpreted to be optional. GC departments and agencies that do not implement any requirements labelled with the key words "SHOULD" or “RECOMMENDED” or choose to implement any requirements labelled "SHOULD NOT" or "NOT RECOMMENDED" must document the implications and rationale for doing so and submit this information to the applicable governance body for the purpose of seeking an exception. An exception must be granted before joining a GC Federation.

4. Common Requirements

This section includes material of general significance to both OpenID Providers and Relying Parties. Subsequent sections provide guidance specific to those roles.

4.1. Clock Skew

[ODP-G01]: Reference *[OIDC] Section 2*

exp

> REQUIRED. Expiration time on or after which the ID Token MUST NOT be accepted for processing. The processing of this parameter requires that the current date/time MUST be before the expiration date/time listed in the value. Implementers MAY provide for some small leeway, usually no more than a few minutes, to account for clock skew.

CATS Support: *Constrained*

Deployments MUST allow between three (3) and five (5) minutes of clock skew — in either direction — when interpreting the `exp` and `nbf` claims in ID tokens and when enforcing security policies based thereupon.

4.2. Security Requirements

[ODP-G02]: Reference *[iGov-OIDC] Section 6*

All transactions MUST be protected in transit by TLS as described in BCP195.

CATS Support: *Constrained*

TLS MUST be configured according to the Guidance on Securely Configuring Network Protocols [ITSP.40.062].

4.2.1. CATS-specific Requirements

[ODP-G03]

X.509 certificates used for TLS server authentication MUST be issued by a certificate authority that is recognized by all of the following:

- The Apple Trusted Root Certificate Program
- The Java Trusted Root Certificate Program
- The Microsoft Trusted Root Certificate Program
- The Mozilla Trusted Root Certificate Program

X.509 certificates used for TLS server authentication MUST comply with the following:

- Apple's Certificate Transparency policy
- Chromium Certificate Transparency Policy

Deployments MUST NOT accept expired certificates.

[ODP-G04]

Deployments MUST perform path validation and check the revocation status of X.509 certificates used for TLS server authentication.

[ODP-G05]

Deployments MUST implement HTTP Strict Transport Security (HSTS) [RFC6797].

[ODP-G06]

All cryptographic algorithms, including signing and encryption operations between RPs and OPs, MUST be implemented in conformance with [ITSP.40.111].

5. Relying Party Requirements

5.1. Requests to the Token Endpoint

[ODP-RP01] _Reference [iGov-OAuth] Section 2.3.2

Full clients, native clients with dynamically registered keys, and direct access clients as defined above MUST authenticate to the authorization server's token endpoint using a JWT assertion as defined by the JWT Profile for OAuth 2.0 Client Authentication and Authorization Grants using only the *private_key_jwt* method defined in OpenID Connect Core.

CATS Support: *Constrained*

Confidential clients (as defined in Section 2.1 of RFC 6749) SHOULD authenticate to the authorization server's token endpoint using the *private_key_jwt* method. Confidential clients that cannot support the *private_key_jwt* method MUST use either
the *client_secret_basic* or *client_secret_post* methods.

Public clients (as defined in Section 2.1 of RFC 6749), MUST use Proof Key for Code Exchange (PKCE) as described in RFC 7636, [iGov-OAuth] and [iGov-OIDC] using the S256 code challenge method. The plain code challenge method MUST NOT be used.

[ODP-RP02] _Reference [iGov-OIDC] Section 2.2

In addition to the requirements specified in Section 2.1.2 of the iGov OAuth2 profile, the following claims MUST be included:

The following parameters are specified:

```
grant_type
       MUST be set to authorization_code.
code
       The value of the code parameter returned in the
authorization response.
client_assertion_type
       MUST be set to urn:ietf:params:oauth:client-assertion-
type:jwt-bearer .
client_assertion
       The value of the signed client authentication JWT
generated as described below.
       The RP must generate a new assertion JWT for each call to
the token endpoint.
```

CATS Support: *Constrained*

Clients that do not support the *private_key_jwt* authentication method MUST NOT include *client_assertion_type* and *client_assertion*.

5.2. CATS-Specific Requirements

5.2.1. Authentication Requests

[ODP-RP03] _Reference [OIDC] Section 3.1.2.1

ui_locales

> OPTIONAL. End-User's preferred languages and scripts for the user interface, represented as a space-separated list of BCP47 [RFC5646] language tag values, ordered by preference. For instance, the value "fr-CA fr en" represents a preference for French as spoken in Canada, then French (without a region designation), followed by English (without a region designation). An error SHOULD NOT result if some or all of the requested locales are not supported by the OpenID Provider.

CATS Support: *Constrained*

The `ui_locales` parameter is REQUIRED and MUST specify the user's preferred official language.

Typically the value will be either `en-CA` *or* `fr-CA`.

[ODP-RP04] _Reference [iGov-OIDC] Section 2.4

Clients MAY optionally send requests to the authorization endpoint using the request parameter as defined by OpenID Connect. Clients MAY send requests to the authorization endpoint by reference using the request_uri parameter.

Request objects MUST be signed by the client's registered key. Request objects MAY be encrypted to the authorization server's public key.

CATS Support: *Constrained*

Clients SHOULD send requests to the authorization endpoint using the request parameter as defined by OpenID Connect.

5.2.2. Single Logout

[ODP-RP05]

RP implementations SHOULD support OpenID back-channel logout [OIDC-BC] for the receipt of logout tokens. If an RP does not support back-channel logout, support for front-channel logout [OIDC-FC] is RECOMMENDED.

[ODP-RP06]

RP implementations MUST support [OIDC-RP] for sending front-channel logout requests to the OP.

5.2.3. Usability and Official Languages

[ODP-RP07]

RP implementations SHOULD examine the value of the `locale` claim returned by the OP in order to determine whether the user changed their preferred official language while interacting with the OP. The RP application SHOULD then display all subsequent content in the newly selected language.

[ODP-RP08]

Applications SHOULD, and collaborative applications MUST, support deep linking. Deep linking implies maintaining support for such links across the boundary of an OpenID Connect profile interaction involving any OP necessary to complete the login process.

It should be possible to request a resource and (authorization permitting) have it supplied as the result of a successful OpenID Connect profile exchange.

[ODP-RP09]

It is RECOMMENDED that RPs support the preservation of POST bodies across a successful OpenID Connect profile exchange, subject to size limitations dictated by policy or implementation constraints.

Deep linking implies support for RP-initiated SSO, i.e., the direct generation of authentication request messages in response to unauthenticated or insufficiently-authenticated access attempts to an application as a whole, or to specific protected content.

6. OpenID Provider Requirements

6.1. Client Registration

[ODP-OP01]: *Reference [iGov-OAuth] Section 2.1.2*

Native applications using dynamic registration SHOULD generate a unique public and private key pair on the device and register that public key value with the authorization server. Alternatively, an authorization server MAY issue a public and private key pair to the client as part of the registration process. In such cases, the authorization server MUST discard its copy of the private key. Client credentials MUST NOT be shared among instances of client software.

CATS Support: *Constrained*

Native applications using dynamic registration MUST generate a unique public and private key pair on the device and register that public key value with the authorization server. Authorization servers MUST NOT issue a public and private key pair to the client as part of the registration process.

6.2. CATS-specific requirements

6.2.1. Claims

OP deployments SHOULD prioritize the use of the standard claim names before defining custom claims. Use of the following profiles are RECCOMENDED in descending order of preference:

- The standard OpenID Connect claims defined in section 5.1 of [OIDC].
- The claims defined in sections 3 and 4 of [OIDC-IA].
- The Identity Metasystem Interoperability claim types defined in section 7.5 of [IMI].
- Public claims that follow the URI naming convention described in the SAML V2.0 X.500/LDAP Attribute Profile [X500SAMLattr].

6.2.2. Session Management and Single Logout

[ODP-OP02]

OP deployments MUST support a default value for the `max_age` request parameter, to be enforced if `max_age` is not provided by the RP in an authentication request. This default SHOULD be separately configurable for each registered RP.

[ODP-OP03]

OpenID Provider deployments participating as a session authority MUST support both the OpenID back-channel [OIDC-BC] and front-channel [OIDC-FC] logout specifications and MUST conform to all normative requirements therein. The OP's discovery metadata must include the `backchannel_logout_supported` and `frontchannel_logout_supported` values to indicate this support. In addition, [OIDC-RP] MUST also be supported and the OP's discovery metadata MUST include the `end_session_endpoint` URL.

[ODP-OP04]

OpenID Provider deployments must support the `sid` (session ID) Claim used in ID Tokens, as a query parameter in front-channel logout URI, and as a Logout Token parameter, for those RPs that require it. The OP's discovery metadata must include the `frontchannel_logout_session_supported` and `backchannel_logout_session_supported` values to indicate this support.

[ODP-OP05]

In cases where multiple RPs are participating in a session, OpenID providers participating as a session authority MUST send a logout token to every participant who has registered a `backchannel_logout_uri` and MUST render a page containg `<iframe src="frontchannel_logout_uri">` for every participant who has registered a `frontchannel_logout_uri`.

*An OpenID Provider is obligated to fulfil its responsibilities as a session authority to notify **all** participating RPs that the user session has been terminated, regardless of any failure by one or more of those RPs. For example, if any RP fails to respond to a backchannel logout request, this must not interfere with the OPs obligation to send logout requests to all other participating RPs, or the OP's obligation to render the front-channel logout propagation page.*

An OP implementation SHOULD use non-blocking calls to send back-channel logout requests in parallel. If the OP is not able to perform both back-channel and front-channel logout concurrently, then the OP MUST perform back-channel logout first.

[ODP-OP06]

Once an OpenID Provider participating as a session authority has issued the first ID Token for a new session, it MUST retain sufficient session state to successfully propagate single-logout of a subject's session for a minimum of 8 hours.

The OP MAY retain this session state for longer than 8 hours.

6.2.3. Usability and Official Languages

[ODP-OP07]

The user interface of OpenID providers MUST respect the End-User's preferred language as indicated by the `ui_locales` request parameter, whenever the primary language subtag indicates English `en` or French `fr`.

[ODP-OP08]

If an authentication request does not include the `ui_locales` request parameter, OpenID providers SHOULD make an effort to determine the End-User's preferred language by some other means.

Examples include other technical mechanisms for obtaining the preferred language from the RP (such as 1st-party cookie, or API), accepting the user's preferred language as provide by the browser in the `Accept-Language` HTTP header, or by rendering a splash page to prompt the user for their preference.

[ODP-OP09]

The `locale` claim is REQUIRED in all ID Tokens issued by an OpenID provider. The value of this claim MUST reflect the End-User's most recently known language preference.

[ODP-OP10]

An OpenID Provider's UserInfo endpoint MUST also include the `locale` claim in all successful UserInfo responses.

6.2.4. Security Requirements

[ODP-OP11]

The private keys of the IdP MUST be stored on a FIPS 140-2 or 140-3 hardware security module that has been successfully validated at Level 2 or higher. Level 3 or higher is RECOMMENDED.

7. CATS-Specific Proxy Requirements

[ODP-PIP01]

Proxying OpenID Provider deployments MUST support the mapping of incoming to outgoing `sub` claims, to pass through values or map between different vocabularies as required.

[ODP-PIP02]

Proxying OpenID Provider deployments MUST support the mapping of incoming to outgoing `ui_loales`, `scope`, `acr_values` and `vtr` authentication request parameters, to pass through values or map between different vocabularies as required.

[ODP-PIP03]

Proxying OpenID Provider deployments MUST support the mapping of incoming to outgoing `acr` or `vot` and `vtm` claims, as well as the generation of new `acr` or `vot` and `vtm` claims using information from other claims in the ID token (such as the `iss`), to pass through values or map between different vocabularies as required.

[ODP-PIP04]

Proxying OpenID Provider deployments MUST support the consumption and production of aggregated and distributed claims as described in section 5.6.2 of [OIDC].

8. References

8.1. Normative

- [RFC2119] IETF RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997. http://www.ietf.org/rfc/rfc2119.txt
- [RFC8174] IETF RFC 8174, Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words, May 2017. http://www.ietf.org/rfc/rfc8174.txt
- [iGov-OIDC] OpenID Foundation, International Government Assurance Profile (iGov) for OpenID Connect 1.0 - Draft 03, October 2018, http://openid.net/specs/openid-igov-openid-connect-1_0-ID1.html
- [iGov-OAuth] OpenID Foundation, International Government Assurance Profile (iGov) for OAuth 2.0 - Draft 03, October 2018, http://openid.net/specs/openid-igov-oauth2-1_0-ID1.html
- [OIDC] OpenID Foundation, OpenID Connect Core 1.0 incorporating errata set 1, November 2014, https://openid.net/specs/openid-connect-core-1_0.html
- [OIDC-BC] OpenID Foundation, OpenID Connect Back-Channel Logout 1.0 - draft 06, August 2020, https://openid.net/specs/openid-connect-backchannel-1_0.html
- [OIDC-FC] OpenID Foundation, OpenID Connect Front-Channel Logout 1.0 - draft 04, August 2020, https://openid.net/specs/openid-connect-frontchannel-1_0.html
- [OIDC-RP] OpenID Foundation, OpenID Connect RP-initiated Logout 1.0 - draft 01, August 2020, https://openid.net/specs/openid-connect-rpinitiated-1_0.html

- [OIDC-IA] OpenID Foundation, OpenID Connect for Identity Assurance 1.0 - implementers draft 2, May 2020, https://openid.net/specs/openid-connect-4-identity-assurance-1_0-ID2.html
- [RFC6749] IETF RFC6749, The OAuth 2.0 Authorization Framework, October 2012, https://tools.ietf.org/html/rfc6749
- [RFC5646] IETF RFC5646, Tags for Identifying Languages, September 2009, https://tools.ietf.org/html/rfc5646
- [FETCH] Web Hypertext Application Technology Working Group (WHATWG), Fetch Standard, Living Document. https://fetch.spec.whatwg.org/ (Supersedes W3C Recommendation, Cross-Origin Resource Sharing, 2 June 2020. https://www.w3.org/TR/2020/SPSD-cors-20200602/)
- [ITSP.40.111] Communications Security Establishment, Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information. https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111
- [ITSP.40.062] Communications Security Establishment, Guidance on Securely Configuring Network Protocols. https://cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062
- [ITSP.30.031v3] Communications Security Establishment, User Authentication Guidance for Information Technology Systems. https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3
- [IMI] OASIS Standard, Identity Metasystem Interoperability Version 1.0. http://docs.oasis-open.org/imi/identity/v1.0/identity.pdf
- [X500SAMLattr] OASIS Committee Specification, SAML V2.0 X.500/LDAP Attribute Profile, March 2008. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500-cs-01.pdf

8.2. Non-Normative

- [PCTF] Identity Management Subcommittee, Pan-Canadian Trust Framework. https://github.com/canada-ca/PCTF-CCP