Cyber Authentication Technology Solutions: Deployment Profile of OpenID Connect 1.0 (Draft)

Table of Contents

Version

3.x

Date

2020-06-19

Status

Work in Progress

Required Information

Document identifier: TBD

1. Introduction

OpenID Connect 1.0 is a rich and extensible standard that must be profiled to be used interoperably, 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 deployers 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 the Sign in Canada federation.

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

This deployment profile of OpenID Connect supports four of the eight trusted processes that make up the Verified Login Component of the Pan-Canadian Trust Framework [PCTF]:

- **Authentication** establishes the confidence, or Level of Assurance, that a Subject has control over their issued credential and that the credential is currently valid (i.e., not suspended or revoked).
- **Authentication Session Initiation** enables a persistent interaction between a Subject and an end-point, such as a CSP or RP, while removing the need to continuously repeat the authentication process between interactions.
- **Authentication Session Termination** an explicit logout event, session expiration due to inactivity or maximum duration, or other means.
- **Identity Verification** is the confirmation that the identity information being presented relates to the person who is making the claim.

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.

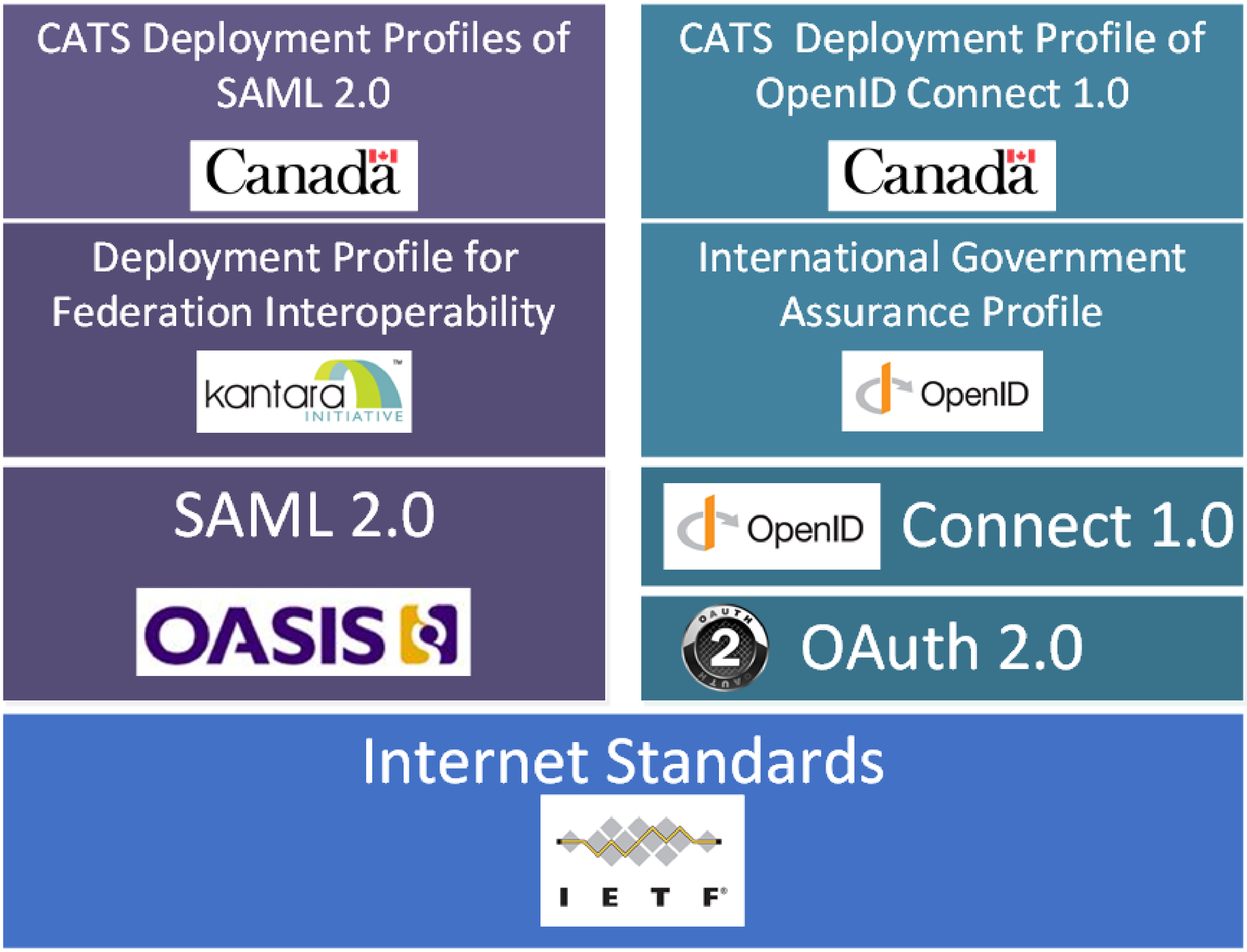
CATS Deployment Profiles of SAML 2.0
Canada
CATS Deployment Profile of OpenID Connect 1.0
Canada
Deployment Profile for Federation Interoperability
kantara INITIATIVE
International Government Assurance Profile
OpenID
SAML 2.0
OASIS
OpenID Connect 1.0
OAuth 2.0
Internet Standards
IETF

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 requiremnts of the underlying specifications. In such cases a reference to the source and location of the 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.

Deployments owned by Government of Canada departments and agencies MUST obtain approval from the Office of the Chief Information Officer, Treasury Board Secretariat before ignoring any requirements labelled with the key words "SHOULD", "SHOULD NOT", "RECOMMENDED" or "NOT RECOMMENDED".

4. Common Requirements

This section includes material of general significance to both OpernID 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.

4.1.1. TLS and Certificates

[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].

4.1.1.1. 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].

5. Relying Party Requirements

[ODP-RP01] _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`.

5.1. CATS-Specific Requirements

5.1.1. Authentication Requests

[ODP-RP02]

RP implementations MUST include the `max_age` parameter in all authentication requests. The value of `max_age` MUST be no greater than 1200 (20 minutes).

5.1.2. Single Logout

[ODP-RP03]

RP implementations SHOULD support OpenID back-channel logout [OIDC-BC] for the receipt of logout tokens. An RP MAY support the OpenID front-channel logout [OIDC-FC] in the event that their implementation does not support [OIDC-BC].

5.1.3. Usability

[ODP-RP04] RP implementations MUST include the `claims` parameter in all authentication requests that, as a minimum, requests the `locale` claim. The `claims` parameter SHOULD request that the `locale` claim be returned in the ID token. RP applications MUST examine the value of the returned `locale` claim to determine if the user changed their preferred official language while interacting with the OP, in which case the RP application MUST display all subsequent content in the newly selected language.

[ODP-RP05] 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-RP06] 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 associated with the `doc` scope described in section 4 of [iGov-OIDC].
- 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]

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.

[ODP-OP03]

In cases where multiple RPs are participating in a session, OpenID providers participating as a session authority MUST first use back-channel logout to send logout tokens to all RPs that support back-channel logout before initiating front-channel logout for any RPs that do not support back-channel logout.

[ODP-OP04]

Once an IdP participating as a session authority has issued the first authorization code 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 IdP MAY retain this session state for longer than 8 hours.

7. CATS-Specific Proxy Requirements

[ODP-PIP01]

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

[ODP-PIP03]

Proxying Identity 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 Identity 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 04, Jaqnuary 2017, https://openid.net/specs/openid-connect-backchannel-1_0.html
- [OIDC-FC] OpenID Foundation, OpenID Connect Front-Channel Logout 1.0 - draft 02, January 2017, https://openid.net/specs/openid-connect-frontchannel-1_0.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
- [CORS] W3C Recommendation, Cross-Origin Resource Sharing, January 2014. http://www.w3.org/TR/cors/
- [ITSP.40.111] Communications Security Establishment, Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information. https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.40.111-eng_0.pdf
- [ITSP.40.062] Communications Security Establishment, Guidance on Securely Configuring Network Protocols. https://cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062
- [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 Subcomittee, Pan-Canadian Trust Framework. https://github.com/canada-ca/PCTF-CCP