Cyber Authentication Technology Solutions: Deployment Profile of SAML 2.0

Table of Contents

Version

3.x

Date

2019-11-06

Status

Implementer’s Draft

Required Information

Document identifier: TBD

1. Introduction

SAML V2.0 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 for SAML 2.0

This deployment profile of SAML 2.0 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.

This deployment profile is based on the draft SAML V2.0 Interoperability Deployment Profile V1.0 [SAML2Iop] published by the Kantara Initiative, which in turn is based on the SAML 2.0 specifications created by the Security Services Technical Committee (SSTC) of the Organization for the Advancement of Structured Information Standards (OASIS).

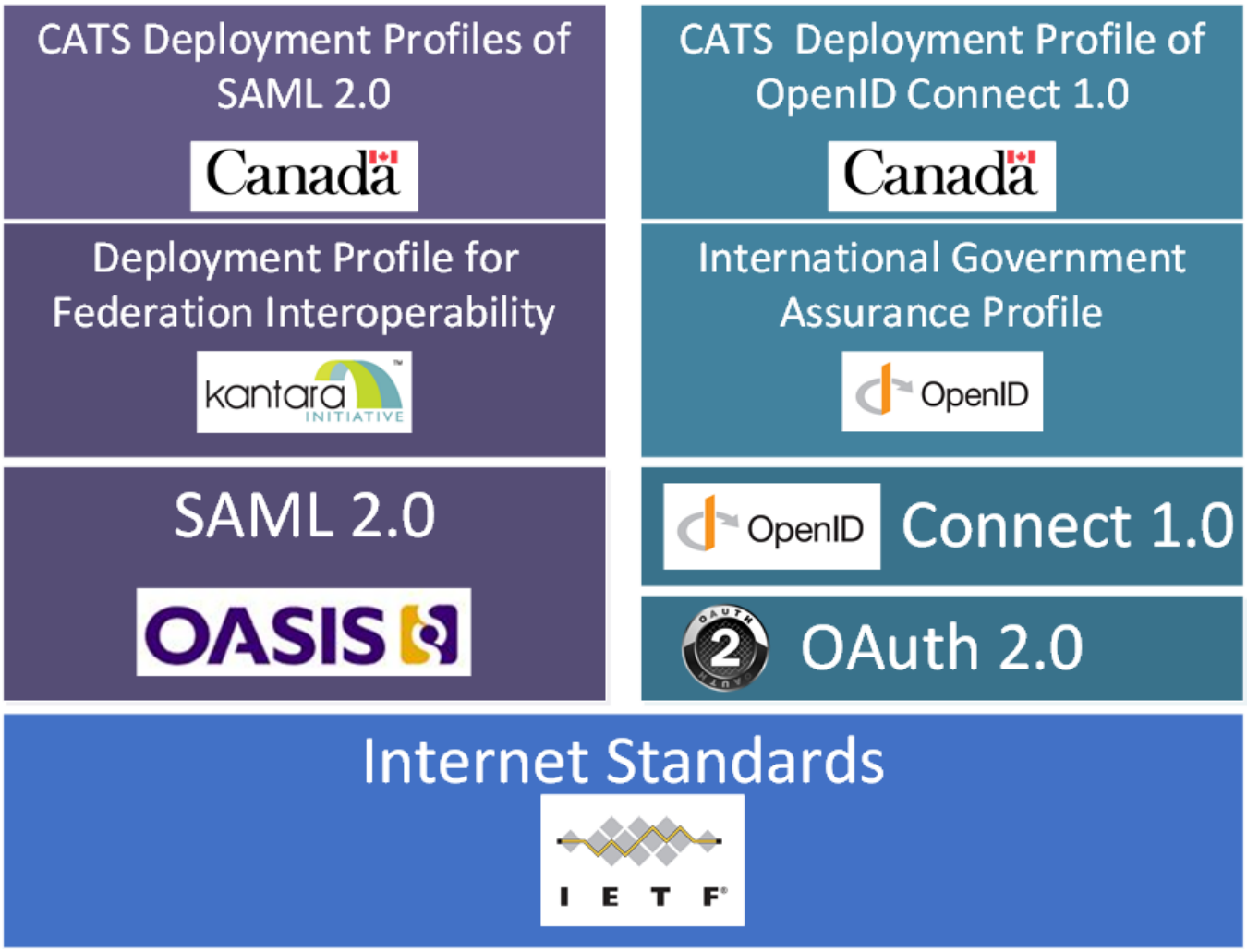

Figure 1. CATS Profile Building Blocks

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: `<ns:Element>`, `Attribute`, **Datatype**, `OtherCode`. The normative requirements of this specification are individually labeled with a unique identifier in the following form: **[SDP-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. References to SAML 2.0 specification

When referring to elements from the SAML 2.0 core specification [SAML2Core], the following syntax is used:

- `<samlp:ProtocolElement>` - for elements from the SAML 2.0 Protocol namespace.
- `<saml:AssertionElement>` - for elements from the SAML 2.0 Assertion namespace.

When referring to elements from the SAML 2.0 metadata specification [SAML2Meta], the following syntax is used:

- `<md:MetadataElement>`

When referring to elements from the SAML 2.0 Metadata Extensions for Login and Discovery User Interface specification [MetaUI], the following syntax is used:

- `<mdui:MetadataElement>`

When referring to elements from the SAML 2.0 Metadata Extension for Entity Attributes specification [MetaAttr], the following syntax is used:

- `<mdattr:MetadataElement>`

When referring to elements from the SAML V2.0 Asynchronous Single Logout Protocol Extension specification [SAML2ASLO], the following syntax is used:

- `<aslo:Element>`

When referring to elements from the XML-Signature Syntax and Processing Version 1.1 WWWC Recommendation [XMLSig], the following syntax is used:

- `<ds:Element>`

2.2. Terminology

The following SAML standard terms and abbreviations are used in a manner consistent with the SAML Browser SSO Profile and Single Logout profiles described in [SAML2Prof]. Formal definitions of these terms can be found in the SAML2 Glossary [SAML2Gloss]:

- **Service Provider (SP)**
- **Session Authority**
- **Session Participant**
- **Subject**
- **Identity Provider (IdP)**
- **Proxying Identity Provider**

In addition, the following terms are used:

Anonymous Credential

A Credential that, while still making an assertion about some property, status, or right of the person, does not reveal the person's identity.

Assurance

A measure of certainty that a statement or fact is true.

Credential Assurance

The assurance that an individual, organization or device has maintained control over what has been entrusted to him or her (e.g., a password, key, token, document or identifier) and that the credential has not been compromised (e.g., tampered with, modified or stolen).

Identity Assurance

A measure of certainty that an individual, organization or device is who or what it claims to be.

Authoritative Party

A federation member that provides credential and/or identity assurance to other federation members (i.e. "Relying Parties").

Credential

A unique physical or electronic object (or identifier) issued to, or associated with, a person, organization, or device (e.g. key, token, document, program identifier).

Credential Service Provider (CSP)

An Identity Provider that provides anonymous credential authentication services.

Federation

A cooperative agreement between autonomous entities that have agreed to relinquish some of their

autonomy in order to work together effectively to support a collaborative effort. The federation is supported by trust relationships and standards to support interoperability.

Level of Assurance

A level of confidence that may be relied on by others.

Relying Party (RP)

A federation member who relies on credential and/or identity assurance from other federation members (i.e. “Authoritative Parties”).

Sign in Canada Acceptance Platform

A Government of Canada service that acts as a trusted intermediary between Credential Service Providers / Trusted Digital Identity Providers and Government of Canada Relying Parties. The Acceptance Platform operates as a Proxying Identity Provider and centralized Session Authority.

Sign in Canada Federation

A Federation whose members include the Sign in Canada Acceptance Platform and all Relying Parties who use it.

Sign in Canada Federation Operator

The department or agency responsible for overseeing operation of the Sign in Canada Federation.

Trusted Digital Identity

An electronic representation of a person, used exclusively by that same person, to receive valued services and to carry out transactions with trust and confidence.

Trusted Identity Provider

An Identity Provider that authenticates Trusted Digital Identities and provides Verified Claims about their owner.

User Agent

Software that is acting on behalf of a user. For example, a web browser or native mobile application.

Verified Claim

a qualification, achievement, quality, or piece of information about a person’s background such as a name, government ID, payment provider, home address, or university degree. Such a claim describes a quality or qualities, property or properties of a person which establish their existence and uniqueness.

Whether explicit or implicit, all the requirements in this document are meant to apply to deployments of SAML profiles and may involve explicit support for requirements by SAML-implementing software and/or supplemental support via application code. Deployments of a Service Provider may refer to both stand-alone implementations of SAML, libraries integrated with an application, or any combination of the two. It is difficult to define a clear boundary between a Service Provider 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 of SAML 2.0

The requirements specified are in addition to all normative requirements of the underlying Web Browser SSO and Single Logout profiles [SAML2Prof], as modified by the Approved Errata [SAML2Err], and 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 SAML 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.

The normative requirements of this CATS Deployment Profile in terms of the applicable sections of the Kantara Profile are detailed in Sections 4 through 6 of this document. The requirements of [SAML2Iop] are repeated word-for-word in the same order as they appear in the upstream profile. Each requirement is then annotated with the support required by this profile: typically this is either “Supported” or “Constrained” or “Not Applicable”. Whenever further details are required to fully explain the CATS requirement, they are provided.

This profile also has requirements which are additional to the [SAML2Iop] requirements. These are specified at the end of each applicable section, as well as in section 7.

Compliance with all requirements labed "REQUIRED" "MANDATORY", "MUST", and "MUST NOT" is required for all members of the Sign in Canada Federation. Federation members who wish to seek an exemption to one or more MANDATORY requirements may do so via the Government of Canada Trusted Digital Identity Committee (TDIC). The TDIC may, at its discretion, direct adjustments to this specification that strengthen or relax requirements as warranted.

Government of Canada departments and agencies who choose not to implement any requirements labelled with the key words "SHOULD", "SHOULD NOT", "RECOMMENDED" or "NOT RECOMMENDED" must document the implications and their reasons for doing so in a Security Assessment and a Privacy Impact Assessment.

4. Common Requirements

This section includes material of general significance to both IdPs and SPs. Subsequent sections provide guidance specific to those roles.

4.1. General

4.1.1. Clock Skew

Kantara Requirement: ***[SDP-G01]***

> Deployments MUST allow between three (3) and five (5) minutes of clock skew — in either direction — when interpreting `xsd:dateTime` values in assertions and when enforcing security policies based thereupon.
>
> *The following is a non-exhaustive list of items to which this directive applies:* `NotBefore`, `NotOnOrAfter`, *and* `validUntil` *XML attributes found on* `<saml:Conditions>`, `<saml:SubjectConfirmationData>`, `<samlp:LogoutRequest>`, `<md:EntityDescriptor>`, `<md:EntitiesDescriptor>`, `<md:RoleDescriptor>`, *and* `<md:AffiliationDescriptor>` *elements.*

CATS Support: *Supported*

4.1.2. Data Size

Kantara Requirement: ***[SDP-G02]***

> Unless otherwise specified, deployments MUST limit the size of each string-valued XML element and attribute they produce to 256 characters.
>
> *This requirement is generic, but is primarily targeted at the content of the* `<saml:NameID>` *and* `<saml:AttributeValue>` *elements.*

CATS Support: *Supported*

4.1.3. Document Type Definitions

Kantara Requirement: ***[SDP-G03]***

Deployments MUST NOT produce any SAML protocol message that contains a (DTD) Document Type Definition.

CATS Support: *Supported*

4.1.4. SAML entityIDs

Kantara Requirement: ***[SDP-G04]***

Deployments MUST be named via an absolute URI whose total length MUST NOT exceed 256 characters.

An entityID should be chosen in a manner that minimizes the likelihood of it changing for political or technical reasons, including for example a change to a different software implementation or hosting provider.

CATS Support: *Supported*

4.2. Metadata and Trust Management

4.2.1. Metadata Consumption and Use

Kantara Requirement: ***[SDP-MD01]***

> Deployments MUST provision their behavior in the following areas based solely on the consumption of SAML Metadata [SAML2Meta] on an automated, periodic or real-time basis using (where applicable) the processing rules defined by the SAML Metadata Interoperability profile [SAML2MDIOP]:
>
> - indications of support for Web Browser SSO and Single Logout profiles
> - selection, determination, and verification of SAML endpoints and bindings
> - determination of the trustworthiness of XML signing keys and TLS client and server certificates
> - selection of XML Encryption keys
> - determination of subject identifier SAML Attribute(s) to provide (per `[SAML2SubjId]`)
> - optional signing of assertions via the `WantAssertionsSigned` flag
> - optional enforcement of request signing via the `AuthnRequestsSigned` flag
>
> Deployments MUST NOT require out of band communication or coordination for the management of any behavior by peers included within the enumerated areas identified above. Deployments MAY of course rely on additional sources of policy, including other metadata content, in order to make determinations whether to successfully interact with peers or refuse to do so.

CATS Support: *Constrained*

Deployments MUST NOT use SAML metadata to provision their behaviour in the following areas:

- determination of the trustworthiness of TLS client and server certificates
- determination of subject identifier SAML Attribute(s) to provide

---

Kantara Requirement: ***[SDP-MD02]***

> Consumption of metadata MUST be contingent on verification of a signature (STRONGLY RECOMMENDED) or TLS server certificate. It MUST be possible to communicate changes to the keys within the metadata without also changing the key used to establish trust in the metadata.
>
> *In most cases, this requirement implies that a key communicated via metadata will not also be used to sign and verify the same metadata, but it is possible to construct scenarios in which this may happen if metadata verification relies on a chain of certificates signed by an ultimately trusted Certificate Authority. The details of such an approach are beyond the scope of this document.*

CATS Support: *Constrained*

Consumption of metadata by the Sign in Canada acceptance platform and all deployments federating

with it MUST be contingent on verification of a signature applied by the Sign in Canada Federation Operator.

4.2.1.1. Metadata Validity

Kantara Requirement: ***[SDP-MD03]***

> Metadata without a `validUntil` attribute on its root element MUST be rejected. Metadata whose root element's `validUntil` attribute extends beyond a deployer- or community-imposed threshold MUST be rejected.
>
> *These are critical (but very simple to implement) requirements for secure application of* `[SAML2MDIOP]` *because it is the method by which keys are revoked and the window of revocation is established.*

CATS Support: *Supported*

4.2.2. Metadata Production

Kantara Requirement: ***[SDP-MD04]***

> Deployments MUST have the ability to provide SAML metadata capturing their requirements and characteristics in the areas identified above in a secure fashion, the specifics of which will necessarily vary by context and community. The use of services offering third-party validation, curation, signing, and publishing of metadata is a recommended practice.
>
> An entity's metadata MUST NOT contain content that advertises profile support or features that aren't supported by that entity's deployment, but it MAY include content indicating support for profiles or features beyond the scope of this profile.
>
> *As an example, deployments that lack support for, or have not tested and integrated an implementation's support for the HTTP-Artifact binding [SAML2Bind] must omit such endpoints.*
>
> *This profile does not mandate any specific automated support for the production of metadata by a deployment. In fact, automatic generation of metadata has a strong tendency to undermine the correct functioning of peer deployments in the face of key rollover or changes to endpoints or other software features because it tends to change too suddenly to accommodate a graceful transition between states.*

CATS Support: *Constrained*

Members of the Sign in Canada Federation MUST provide their metadata to the Sign in Canada

---

Federation Operator who performs third-party validation, curation, signing, and publishing of metadata.

4.2.2.1. Keys and Certificates

Kantara Requirement: ***[SDP-MD05]***

> Public keys used for signing, encryption, and TLS client and server authentication MUST be expressed via X.509 certificates included in metadata via `<md:KeyDescriptor>` elements.
>
> *By virtue of [SAML2MDIOP], this profile (and SAML in general) does not place requirements on the non-key material contained in X.509 certificates in metadata. However, the following are suggested practices to avoid interoperability issues with deployments outside the scope of this profile:*
>
> - *use long-lived certificates*
> - *use self-signed certificates*
> - *do not use expired certificates*
> - *do not sign certificates with MD5- or SHA1-based signature algorithms*

CATS Support: *Constrained*

Deployments owned by Government of Canada departments and agencies MUST use X.509 certificates issued by the Government Shared Services (GSS) Certificate Authority for signing and encryption of SAML messages.

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

Deployments MUST NOT accept expired certificates.

Deployments SHOULD NOT perform runtime path validation or revocation checking of X.509 certificates used for signing or encryption of SAML messages.

Using revocation checking mechanisms such as certificate revocation lists (CRLs) and the Online Certificate Status Protocol (OCSP) during runtime creates a dependency that can reduce the availability of a deployment. In the event of a private key compromise, the Sign in Canada Federation Operator will revoke the affected deployment's SAML metadata.

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

This profile does not contain any requirement for using TLS client authentication.

Kantara Requirement: ***[SDP-MD06]***

> RSA public keys MUST be at least 2048 bits in length. At least 3072 bits is RECOMMENDED for new deployments.

CATS Support: *Supported*

Kantara Requirement: ***[SDP-MD07]***

> EC public keys MUST be at least 256 bits in length.

CATS Support: *Supported*

Kantara Requirement: ***[SDP-MD08]***

> By virtue of the profile's overall requirements, an IdP's metadata MUST include at least one signing certificate (that is, an `<md:KeyDescriptor>` with no `use` attribute or one set to `signing`), and an SP's metadata MUST include at least one encryption certificate (that is, an `<md:KeyDescriptor>` with no `use` attribute or one set to `encryption`).

CATS Support: *Constrained*

The metadata of IdPs and SPs MUST contain at least one signing certificate with the `use` attribute set to `signing` and at least one encryption certificate with the `use` attribute set to `encryption`.

4.2.2.2. Discovery and User Interface Elements

Kantara Requirement: ***[SDP-MD09]***

Metadata MUST include an `<mdui:UIInfo>` element as defined in [MetaUI] containing at least the child elements `<mdui:DisplayName>` and `<mdui:Logo>`. An SP's metadata MUST include the child element `<PrivacyStatementURL>`

CATS Support: *Constrained*

Metadata MAY include a `<mdui:UIInfo>` element with any child elements.

Kantara Requirement: ***[SDP-MD10]***

The content of the `<mdui:Logo>` element MUST be either an `https` URL or an in-line image embedded in a `data` URI element. The size of the `data` URI used in a `<mdui:Logo>` element is not limited to 256 characters.

Specific details around logo formats including image size, encoding and aspect ratio should be coordinated with the common practice of the entity's community of SAML peers.

CATS Support: *Supported*

Kantara Requirement: ***[SDP-MD11]***

Metadata MUST include an `<md:ContactPerson>` element within the `<md:EntityDescriptor>` element, with a contactType of `technical` and an `<md:EmailAddress>` element.

CATS Support: *Supported*

Kantara Requirement: ***[SDP-MD12]***

An IdP's metadata MUST include the `errorURL` attribute on its `<md:IDPSSODescriptor>` element. The content of the `errorURL` attribute MUST be an https URL resolving to an HTML page.

The errorURL HTML page should be suitable for referral by SPs if they receive insufficient attributes from the IdP to successfully authenticate or authorize the user's access. The page should provide information targeted at the end user explaining how to contact the operator of the IdP to request addition of the necessary attributes to the assertions.

CATS Support: *Supported*

4.3. Cryptographic Algorithms

Kantara Requirement: ***[SDP-ALG01]***

Deployments MUST support, and use, the following XML Signature and Encryption algorithms when communicating with peers in the context of this profile. Where multiple choices exist, any of the listed options may be used. The profile will be updated as necessary to reflect changes in government and industry recommendations regarding algorithm usage.

This profile does not impose specific algorithm or version requirements regarding the use of TLS between clients and servers and defers to existing industry best practices or other deployment guidance in that area.

- Digest
  - `http://www.w3.org/2001/04/xmlenc#sha256` [XMLEnc]
- Signature
  - `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256` [RFC4051]
  - `http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256` [RFC4051]
- Block Encryption
  - `http://www.w3.org/2009/xmlenc11#aes128-gcm` [XMLEnc]
  - `http://www.w3.org/2009/xmlenc11#aes256-gcm` [XMLEnc]
- Key Transport
  - `http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p` [XMLEnc]
- Key Transport Digest
  - `http://www.w3.org/2000/09/xmldsig#sha1` [XMLSig]

This profile cannot preclude the use of other algorithms when communicating with peers outside the scope of this profile, but the other algorithms in common use are generally considered to be weakening (e.g., SHA-1) or broken outright (e.g., RSA PKCS#1.5). Note that the use of AES-CBC block encryption algorithms remains widespread at the time of authoring, but are known to be broken [XMLEncBreak].

The key transport requirement is defined in the interest of avoiding interoperability problems without a compelling security benefit. The original OAEP padding method defaults to the use of SHA-1 as a digest algorithm (as mandated above) and assumes the use of the "MGF1 with SHA-1" mask generation function.

CATS Support: *Constrained*

IdP deployments MUST also support the use of `http://www.w3.org/2001/04/xmlenc#aes128-cbc` [XMLEnc]

to encrypt Assertions for any SP that has specified this algorithm in its metadata.

The use of block encryption algorithms using the Galois/Counter Mode (GCM) mode of option is RECCOMMENDED for SP deployments, however `http://www.w3.org/2001/04/xmlenc#aes128-cbc` MAY be used if the SP software does not support GCM algorithms.

As per [ITSP.40.111], these encryption and signature algorithms are approved for use to protect the confidentiality of PROTECTED A and PROTECTED B information and the integrity of information to the medium injury level.

Deployments MUST configure TLS according to [ITSP.40.062] and [ITPIN-2018-01].

5. Service Provider Requirements

This section provides requirements specific to SPs, in addition to the Common Requirements above.

5.1. Web Browser SSO

Kantara Requirement: ***[SDP-SP01]***

> SPs MUST support the Web Browser SSO profile [SAML2Prof], as updated by the Approved Errata [SAML2Err], with behavior, capabilities, and options consistent with the additional constraints specified in this section.

CATS Support: *Supported*

5.1.1. Requests

5.1.1.1. Binding

Kantara Requirement: ***[SDP-SP02]***

> The HTTP-Redirect binding [SAML2Bind] MUST be used for the transmission of `<samlp:AuthnRequest>` messages.

CATS Support: *Supported*

Kantara Requirement: ***[SDP-SP03]***

> Requests MUST NOT be issued inside an HTML frame or via any mechanism that would require the use of third-party cookies by the IdP to establish or recover a session with the User Agent. This will typically imply that requests will involve a full-frame redirect, in order that the top level window origin be associated with the IdP.

CATS Support: *Supported*

5.1.1.2. Request Content

Kantara Requirement: ***[SDP-SP04]***

> The `<samlp:AuthnRequest>` message MUST either omit the `<samlp:NameIDPolicy>` element (RECOMMENDED), or the element MUST contain an `AllowCreate` attribute of "true" and MUST NOT contain a `Format` attribute.

CATS Support: *Constrained*

`<samlp:NameIDPolicy>` MAY contain a `Format` attribute, in which case its value MUST be `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.

An `SPNameQualifier` attribute MAY also be present to request that the assertion subject's identifier be returned (or created) in the namespace of a service provider other than the requester, or in the namespace of an affiliation group of service providers.

`SPNameQualifier` *provides critical functionality that supports changes in the topology of a federation. This is why this profile has not adopted [SAML2SubjAttr] as it does not currently provide equivalent functionality.*

Kantara Requirement: ***[SDP-SP05]***

> The message SHOULD contain an `AssertionConsumerServiceURL` attribute and MUST NOT contain an `AssertionConsumerServiceIndex` attribute (i.e., the desired endpoint MUST be the default, or identified via the `AssertionConsumerServiceURL` attribute).

CATS Support: *Supported*

Kantara Requirement: ***[SDP-SP06]***

> The `AssertionConsumerServiceURL` value, if present, MUST match an endpoint location expressed in the SP's metadata exactly, without requiring URL canonicalization/normalization.
>
> *As an example, the SP cannot specify URLs that include a port number (e.g., https://sp.example.com:443/acs) in its requests unless it also includes that port number in the URLs specified in its metadata, and vice versa.*

CATS Support: *Supported*

5.1.1.3. Authentication Contexts

Kantara Requirement: ***[SDP-SP07]***

> An SP that does not require a specific `<saml:AuthnContextClassRef>` value MUST NOT include a `<samlp:RequestedAuthnContext>` element in its requests.
>
> An SP that requires specific `<saml:AuthnContextClassRef>` values MUST specify the allowable values in a `<samlp:RequestedAuthnContext>` element in its requests, with the `Comparison` attribute set to `exact`.
>
> *An SP should not request a `<saml:AuthnContextClassRef>` value in the absence of a shared understanding between itself and the IdP regarding its definition.*

CATS Support: *Constrained*

SP deployments MUST include `<samlp:RequestedAuthnContext>`. The optional `Comparison` attribute MAY be included, in which case it MUST have the value `exact`.

The `<samlp:RequestedAuthnContext>` MUST include a Level of Assurance as specified in [SAML2Assur].

The SP MAY indicate a willingness to accept more than one level of assurance, by including multiple `<samlp:RequestedAuthnContext>` elements.

This is useful when a certain minimum level of assurance is required, but the SP is willing to accept a higher level of assurance.

The AuthnContext Schema for the Sign in Canada levels of assurance are published at https://github.com/canada-ca/CATS-STAE/tree/master/SAML/src/schemas.

5.1.2. Responses

5.1.2.1. Binding

Kantara Requirement: ***[SDP-SP08]***

> SPs MUST support the HTTP-POST binding for the receipt of `<samlp:Response>` messages. Support for other bindings is OPTIONAL.

CATS Support: *Supported*

Kantara Requirement: ***[SDP-SP09]***

The endpoint(s) at which an SP supports receipt of `<samlp:Response>` messages MUST be protected by TLS/SSL.

CATS Support: *Constrained*

TLS MUST be configured according to [ITSP.40.062] and [ITPIN-2018-01].

5.1.2.2. XML Encryption

Kantara Requirement: ***[SDP-SP10]***

SPs MUST support decryption of `<saml:EncryptedAssertion>` elements. Support for other encrypted constructs is OPTIONAL.

CATS Support: *Constrained*

SPs MUST NOT implement other encrypted constructs.

5.1.2.3. Error Handling

Kantara Requirement: ***[SDP-SP11]***

SPs MUST gracefully handle error responses containing `<samlp:StatusCode>` other than `urn:oasis:names:tc:SAML:2.0:status:Success`.

CATS Support: *Supported*

Kantara Requirement: ***[SDP-SP12]***

If a successful authentication response lacks sufficient or appropriate SAML Attributes (including subject identifiers) for successful SP operation, the SP MUST display a meaningful status message to the user. This message MUST direct the user to appropriate support resources offered by the SP or, alternatively, to the `errorURL` attribute in an IdP's metadata.

There are many reasons an SP may be unable or choose not to provide service to a user based on an given authentication response. IdPs failing to release the necessary SAML Attributes is the most prevalent interoperability issue encountered in larger, general purpose federations, which is why this scenario is singled out here.

CATS Support: *Constrained*

The response to such errors MUST direct users to appropriate support resources offered by the SP.

5.1.3. Subject Identification

5.1.3.1. NameID Formats

Kantara Requirement: ***[SDP-SP13]***

SPs MUST NOT require the presence of a `<saml:NameID>` element.

Use of `<saml:NameID>` elements in this profile is restricted to their role in the Single Logout profile, and not for long term identification of subjects. Standardized SAML Attributes are used instead, as described below.

CATS Support: *Constrained*

SP deployments MUST support `<saml:NameID>` and the `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` name identifier format as described in [SAML2Core]. `<saml:Attribute>` elements MUST NOT be used for this purpose.

The `NameQualifier` and `SPNameQualifier` attributes of the `<saml:NameID>` element allow for the qualification of the element value, which provides critical functionality to support changes in the topology of a federation. This profile has not adopted [SAML2SubjAttr] as it does not currently provide equivalent functionality.

5.1.3.2. Subject Identifiers

Kantara Requirement: ***[SDP-SP14]***

If an SP requires persistent tracking/identification of its users (as most do), then it MUST support one or both of the SAML Attributes defined by [SAML2SubjId] for this purpose.

SPs MAY support legacy or historical `<saml:NameID>` and `<saml:Attribute>` identifier content for compatibility reasons but MUST NOT require their use.

If an SP requires coordination and/or correlation of user activity between itself and other SPs, then the SAML Attribute named `urn:oasis:names:tc:SAML:attribute:subject-id` *is appropriate. Otherwise the SAML Attribute named* `urn:oasis:names:tc:SAML:attribute:pairwise-id` *can be used.*

CATS Support: *Constrained*

SP deployments MUST NOT implement [SAML2SubjId].

SP deployments MUST support `<saml:NameID>` and the `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` name identifier format as described in [SAML2Core].

5.1.3.3. Subject Identifier Requirements Signaling

Kantara Requirement: ***[SDP-SP15]***

An SP MUST represent its identifier requirements in its SAML metadata, consistent with the Requirements Signaling mechanism defined in [SAML2SubjId].

CATS Support: *Not Applicable*

5.1.3.4. Identifier Scoping

Kantara Requirement: ***[SDP-SP16]***

SPs MUST prevent unintended identifier collisions in the values asserted by different IdPs, and the required identifier types, per [SAML2SubjId], are "scoped" via a DNS-like syntax to help fulfill this requirement.

CATS Support: *Not Applicable*

Kantara Requirement: ***[SDP-SP17]***

SPs MUST associate identifier scopes with IdPs such that only authorized IdPs may assert identifiers with particular scopes for particular purposes.

It is RECOMMENDED that the `<shibmd:Scope>` metadata extension defined in [SAML2SubjId] be supported for this purpose. SPs MAY ignore any such extension elements whose `regexp` attribute is `true` or `1`. SPs MUST NOT rely on this extension unless the metadata is verifiably obtained from a third party that is trusted to supply it.

In the event that this extension cannot be used, then SPs MUST apply policy established in some other manner.

Note that scopes and IdPs do not necessarily have a 1:1 relationship; it may well be legitimate for multiple IdPs to assert a given scope, or for an IdP to assert identifiers in multiple scopes, but the rules for this should be explicit and enforced.

CATS Support: *Not Applicable*

5.1.3.5. Displayable Identifiers

The required identifier types above are opaque, unknown to users in most cases, and unsuitable for display.

Kantara Requirement: ***[SDP-SP18]***

SPs requiring the display of identifiers to users, the identification of other users via searching, selection, etc., and similar use cases SHOULD rely on additional suitable SAML Attributes such as:

- `urn:oid:0.9.2342.19200300.100.1.3` (mail)
- `urn:oid:2.16.840.1.113730.3.1.241` (displayName)
- `urn:oid:2.5.4.42` (givenName)
- `urn:oid:2.5.4.4` (sn)

Note that most standardized SAML Attributes of this sort tend to be defined as multi-valued.

CATS Support: *Not Applicable*

5.1.4. Attribute Value Constraints

Kantara Requirement: ***[SDP-SP19]***

> When consuming SAML Attributes with standardized definitions in external specifications, SPs MUST NOT impose constraints beyond the definitions of those attributes.
>
> *For example, the definition of the `mail` attribute (in SAML, `urn:oid:0.9.2342.19200300.100.1.3`) explicitly allows for multiple values, so an SP that consumes it for some purpose must necessarily allow for that possibility.*

CATS Support: *Supported*

5.1.5. Usability

Silo-oriented, multi-tenant approaches to federated application deployment create an inherent friction with the intended design of the web, user behavior and experience, and the needs of collaboration inherent in many applications. SSO, when integrated poorly, can negatively impact usability, and the following sections, while not strictly matters of SAML interoperability, have a significant effect on the perception of the system as a whole and on the successful adoption of SSO, regardless of the protocol.

The web inherently operates on the basis of *addressability* of resources; that is, users expect to be able to access a piece of information or an application function directly, without regard for their identity, current level of access, or what is convenient for an application developer to support. This leads naturally to the ability to create bookmarks to what matters to them, and users will consistently route around attempts to force them through proxies, portals, and other artificial access paths.

At a high level, these issues fall under the term `deep linking`.

For a wide range of applications in the collaborative space, this notion is not merely convenient, but utterly essential, because such applications presume the sharing of resources with peers between organizations.

For the purposes of the following requirements, we will refer to applications that rely on the exposure of resource URLs that may be shared between users from multiple organizations as "collaborative" applications, even if their purpose may not specifically align with that term.

5.1.5.1. Support for Multiple IdPs

Kantara Requirement: ***[SDP-SP20]***

SPs MUST allow for the possibility that any given request requiring authentication may be potentially satisfied by more than one IdP. That is, any scenario in which a piece of content, policy, configuration, or decision on the part of an application is bound to an IdP MUST be constructed in a fashion such that more than one IdP may be so bound.

This requirement flows from both the inherent requirements of collaborative applications described above, and from the simple reality that enterprises vary in their structure. Some organizations rely on more than one IdP due to administrative boundaries, but frequently contract for or access services as a single body. Thus, any presumed mapping between a contract or set of access policies and a single SAML IdP is too constraining. This constraint imposes a need for complex proxying of SSO by many organizations and SPs are cautioned to avoid it.

CATS Support: *Supported*

5.1.5.2. Deep Linking

Kantara Requirement: ***[SDP-SP21]***

Applications SHOULD, and collaborative applications MUST, support deep linking. Deep linking implies maintaining support for such links across the boundary of a Web Browser SSO profile interaction involving any IdP 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 Web Browser SSO profile exchange.

Deep linking implies support for SP-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. Deep linking may co-exist with support for unsolicited responses (so-called IdP-initiated SSO), but precludes its requirement.

CATS Support: *Supported*

Kantara Requirement: ***[SDP-SP22]***

It is RECOMMENDED that SPs support the preservation of POST bodies across a successful Web Browser SSO profile exchange, subject to size limitations dictated by policy or implementation constraints.

CATS Support: *Supported*

5.1.5.3. Discovery

Deep linking also implies support for some form of IdP "discovery", the process by which an SP establishes which IdP to use on behalf of a subject. Use of IdP-initiated SSO is a common workaround for supporting discovery, but cannot be required when deep linking is supported, in addition to having other drawbacks.

A common means of discovery is the mapping of resource/application URL (typically virtual host, sometimes path) to a specific IdP. This is strongly discouraged, and is disallowed for collaborative applications, since it makes the sharing of URLs between users from multiple organizations at best inconvenient, and in some cases, impossible.

Kantara Requirement: ***[SDP-SP23]***

> SPs that support deep linking MUST support some form of Identity Provider discovery that accomodates all, or at least the vast majority, of their user base. Support for caching mechanisms such as cookies or other persistence solutions is encouraged.

CATS Support: *Constrained*

SP deployments participating in the Sign in Canada federation MUST NOT support [IDPDisco].

Discovery services are provided by the Sign in Canada Acceptance Platform as part of authentication request processing.

5.2. Single Logout

Kantara Requirement: ***[SDP-SP24]***

> SPs MAY support the Single Logout profile [SAML2Prof], as updated by the Approved Errata [SAML2Err]. The following requirements apply in the case of such support.

CATS Support: *Constrained*

SPs MUST support the Single Logout Profile for the sending of `<samlp:LogoutRequest>` messages and SHOULD support the receipt of `<samlp:LogoutRequest>` messages.

5.2.1. Requests

5.2.1.1. Binding

Kantara Requirement: ***[SDP-SP25]***

> The HTTP-Redirect binding [SAML2Bind] MUST be used for the transmission of `<samlp:LogoutRequest>` messages.

CATS Support: *Supported*

Kantara Requirement: ***[SDP-SP26]***

> SPs MUST support the HTTP-Redirect [SAML2Bind] binding for the receipt of `<samlp:LogoutRequest>` messages, in the event that inbound `<samlp:LogoutRequest>` messages are supported.

CATS Support: *Constrained*

SPs SHOULD support the SOAP [SAML2Bind] binding for the the receipt of `<samlp:LogoutRequest>` messages.

An SP MAY support the HTTP-Redirect binding in the event that their implementation does not support the SOAP binding, in which case the SP MUST support cross-origin resource sharing [CORS] so that the IdP can send `<samlp:LogoutRequest>` messages without giving up control of the user agent.

Kantara Requirement: ***[SDP-SP27]***

> Requests MUST NOT be issued inside an HTML frame or via any mechanism that would require the use of third-party cookies by the IdP to establish or recover a session with the User Agent. This will typically imply that requests must involve a full-frame redirect, in order that the top level window origin be associated with the IdP.
>
> *The full-frame requirement is also necessary to ensure that full control of the user interface is released to the IdP.*

CATS Support: *Supported*

5.2.1.2. Request Content

Kantara Requirement: ***[SDP-SP28]***

> Requests MUST be signed (via a signature created in accordance with the HTTP-Redirect binding [SAML2Bind]).

CATS Support: *Supported*

Kantara Requirement: ***[SDP-SP29]***

> The `<saml:NameID>` element included in `<samlp:LogoutRequest>` messages MUST exactly match the corresponding element received from the IdP, including its element content and all XML attributes included therein.

CATS Support: *Supported*

Kantara Requirement: ***[SDP-SP30]***

> The `<saml:NameID>` element in `<samlp:LogoutRequest>` messages MUST NOT be encrypted.
>
> *The normative requirement for the use of transient identifiers is intended to obviate the need for XML Encryption.*

CATS Support: *Constrained*

The `<saml:NameID>` element SHOULD be encrypted via the `<saml:EncryptedID>` element.

This profile uses persistent identifiers which should be protected.

Note that encrypting the NameID increases the size of the SAML message significantly, which has historically caused problems with very old browsers that do not support long URLs. SP software should be configured to not include unnecessary elements such as `<ds:X509Data>` *in* `<saml:EncryptedID>`.

5.2.2. Responses

5.2.2.1. Binding

Kantara Requirement: ***[SDP-SP31]***

The HTTP-Redirect binding [SAML2Bind] MUST be used for the transmission of `<samlp:LogoutResponse>` messages.

CATS Support: *Constrained*

The SOAP [SAML2Bind] binding SHOULD be used for the transmission of <samlp:LogoutResponse> messages.

The HTTP-Redirect binding MAY be used if the SP implementation does not support the SOAP binding.

Kantara Requirement: ***[SDP-SP32]***

SPs MUST support the HTTP-Redirect [SAML2Bind] binding for the receipt of `<samlp:LogoutResponse>` messages, in the event that they do not include the `<aslo:Asynchronous>` extension [SAML2ASLO] in all of their requests.

CATS Support: *Supported*

5.2.2.2. Response Content

Kantara Requirement: ***[SDP-SP33]***

Responses MUST be signed (via a signature created in accordance with the HTTP-Redirect binding [SAML2Bind]).

CATS Support: *Supported*

5.2.3. Behavioral Requirements

Kantara Requirement: ***[SDP-SP34]***

SPs MUST terminate a subject's local session before issuing a `<samlp:LogoutRequest>` message to the IdP.

This ensures the safest possible result for subjects in the event that logout fails for some reason, as it often will.

CATS Support: *Supported*

Kantara Requirement: ***[SDP-SP35]***

> SPs MUST NOT issue a `<samlp:LogoutRequest>` message as the result of an idle activity timeout.
>
> *Timeout of a single application/service must not trigger logout of an SSO session because this imposes a single service's requirements on an entire IdP deployment. Applications with sensitive requirements should consider other mechanisms, such as the* `ForceAuthn` *attribute, to achieve their goals.*

CATS Support: *Supported*

5.2.4. Logout and Virtual Hosting

Kantara Requirement: ***[SDP-SP36]***

> An SP that maintains distinct sessions across multiple virtual hosts SHOULD identify itself by means of a distinct entityID (with associated metadata) for each virtual host.
>
> *A single entity can have only one well-defined* `<SingleLogoutService>` *endpoint per binding. Cookies are typically host-based and logout cannot typically be implemented easily across virtual hosts. Unlike during SSO, a* `<samlp:LogoutRequest>` *message cannot specify a particular response endpoint, so this scenario is generally not viable.*

CATS Support: *Supported*

5.3. Metadata and Trust Management

5.3.1. Support for Multiple Keys

The ability to perform seamless key migration depends upon proper support for consuming and/or leveraging multiple keys at the same time.

Kantara Requirement: ***[SDP-SP37]***

> SP deployments MUST support multiple signing certificates in IdP metadata and MUST support validation of XML signatures using a key from any of them.

CATS Support: *Constrained*

SP deployments SHOULD support multiple signing certificates in IdP metadata.

Kantara Requirement: ***[SDP-SP38]***

> SP deployments MUST be able to support multiple decryption keys and MUST be able to decrypt `<saml:EncryptedAssertion>` elements encrypted with any configured key.

CATS Support: *Constrained*

SP deployments SHOULD support multiple decryption keys.

5.3.2. Metadata Content

Kantara Requirement: ***[SDP-SP39]***

By virtue of this profile's requirements, an SP's metadata MUST contain:

- an `<md:SPSSODescriptor>` role element containing
  - at least one `<md:AssertionConsumerService>` endpoint element
  - at least one `<md:KeyDescriptor>` element whose `use` attribute is omitted or set to `encryption`
  - an `<md:Extensions>` element at the role level containing
    - an `<mdui:UIInfo>` extension element containing the child elements `<mdui:DisplayName>`, `<mdui:Logo>`, and `<mdui:PrivacyStatementURL>`
    - an `<mdattr:EntityAttributes>` extension element for signaling Subject Identifier requirements with previously prescribed content
- an `<md:ContactPerson>` element with a `contactType` of `technical` and an `<md:EmailAddress>` element

If the SP supports the Single Logout profile, then its metadata MUST contain (within its `<md:SPSSODescriptor>` role element):

- at least one `<md:KeyDescriptor>` element whose `use` attribute is omitted or set to `signing`
- at least one `<md:SingleLogoutService>` endpoint element (this MAY be omitted if the SP solely issues `<samlp:LogoutRequest>` messages containing the `<aslo:Asynchronous>` extension [SAML2ASLO])

CATS Support: *Constrained*

The metadata of SPs MUST contain at least one signing certificate with the `use` attribute set to `signing` and at least one encryption certificate with the `use` attribute set to `encryption`.

SP metadata MAY include an `<md:Extensions>` element containing an `<mdui:UIInfo>` extension element, but it MUST NOT include an `<mdattr:EntityAttributes>` extension element.

The `<md:SPSSODescriptor>` element of an SP's metadata MUST also include an `AuthnRequestsSigned` attribute set to `true` or `1` and a `WantAssertionsSigned` attribute set to `true` or `1`.

An SP's metadata SHOULD include two `<md:SingleLogoutService>` elements, one with the `Binding` attribute value of `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`, the other with the `Binding` attribute value of `urn:oasis:names:tc:SAML:2.0:bindings:SOAP`.

The `<md:SPSSODescriptor>` element of SP metadata MAY contain 0, 2 or more `<md:AttributeConsumingService>` elements that specify collections of attributes required or desired by the service provider. Each `<md:AttributeConsumingService>` MUST include two `<md:ServiceName>` elements, one in english and one in french. `<md:ServiceDescription>`, if present, MUST also be included for both english and french.

If an SP metadata includes any `<md:AttributeConsumingService>` elements, exactly one of them must

have the `isDefault` attribute set to `true` or `1`. This default `<md:AttributeConsumingService>` must contain exactly one `<md:RequestedAttribute>` element that specifies a "null" attribute as follows:

```
<RequestedAttribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                    Name="data:,null" FriendlyName="null" isRequired="false"/>
```

This provides a mechanism to prevent unecessary disclosure of personal information, whereby the IDP will not return any attributes unless explicitly requested by the SP using the `AttributeConsumingServiceIndex` *attribute of the* `<samlp:AuthnRequest>`.

5.4. CATS-Specific Requirements

5.4.1. Authentication Requests

[CDP-SP01]

`<samlp:AuthnRequest>` messages MUST be signed using the SHA-256 algorithm.

[CDP-SP02]

`<samlp:AuthnRequest>` messages MAY include the `AttributeConsumingServiceIndex` attribute with a value specifying the index of an `<md:AttributeConsumingService>` defined in the service provider's metadata.

This provides the mechanism whereby a service provider can explicitly request a defined set of attributes, only when required.

6. Identity Provider Requirements

This section provides requirements specific to IdPs, in addition to the Common Requirements above.

6.1. Web Browser SSO

Kantara Requirement: ***[SDP-IDP01]***

> IdPs MUST support the Web Browser SSO profile [SAML2Prof], as updated by the Approved Errata [SAML2Err], with behavior, capabilities, and options consistent with the additional constraints specified in this section.

CATS Support: *Supported*

6.1.1. Requests

6.1.1.1. Binding

Kantara Requirement: ***[SDP-IDP02]***

> IdPs MUST support the HTTP-Redirect binding [SAML2Bind] for the receipt of `<samlp:AuthnRequest>` messages.

CATS Support: *Supported*

Kantara Requirement: ***[SDP-IDP03]***

> The endpoint(s) at which an IdP supports receipt of `<samlp:AuthnRequest>` messages MUST be protected by TLS/SSL.

CATS Support: *Constrained*

TLS MUST be configured according to [ITSP.40.062].

6.1.1.2. Signing

Kantara Requirement: ***[SDP-IDP04]***

> IdPs MUST support unsigned requests generally but MUST reject unsigned requests in the event that an SP's metadata includes an `AuthnRequestsSigned` attribute set to `true` or `1`.

CATS Support: *Supported*

Kantara Requirement: ***[SDP-IDP05]***

> If a request is signed, IdPs MUST successfully verify the signature or fail the request. An IdP MAY handle a signature verification failure locally rather than via an error response to the SP.

CATS Support: *Supported*

6.1.1.3. Endpoint Selection/Verification

Kantara Requirement: ***[SDP-IDP06]***

> IdPs MUST verify the `AssertionConsumerServiceURL` supplied in an SP's `<samlp:AuthnRequest>` (if any) against the `<md:AssertionConsumerService>` elements in the SP's metadata. In the absence of such a value, the default endpoint from the SP's metadata MUST be used for the response.
>
> When verifying the `AssertionConsumerServiceURL`, it is RECOMMENDED that the IdP perform a case-sensitive string comparison between the requested value and the values found in the SP's metadata. It is OPTIONAL to apply any form of URL canonicalization.
>
> *The Web Browser SSO profile [SAML2Prof] notes that validation of the response endpoint is required but does not mandate a specific approach, primarily due to metadata being an optional portion of the original standard. The above is the most common and interoperable approach to meeting this requirement.*

CATS Support: *Supported*

6.1.1.4. Forced Re-Authentication

Kantara Requirement: ***[SDP-IDP07]***

IdPs MUST ensure that any response to a `<samlp:AuthnRequest>` that contains the attribute `ForceAuthn` set to `true` or `1` results in an authentication challenge that requires proof that the subject is present. If this condition is met, the IdP MUST also reflect this by setting the value of the `AuthnInstant` value in the assertion it returns to a fresh value.

If an IdP cannot prove subject presence, then it MUST fail the request and SHOULD respond to the SP with a SAML error status.

Due to the potential for confusion over more frequent authentication challenges, the IdP may wish to indicate when this feature is being used on the login user interface it presents to the user.

CATS Support: *Supported*

6.1.2. Responses

6.1.2.1. Binding

Kantara Requirement: ***[SDP-IDP08]***

IdPs MUST support the HTTP-POST binding [SAML2Bind] for the transmission of `<samlp:Response>` messages.

CATS Support: *Supported*

6.1.2.2. Response Content

Kantara Requirement: ***[SDP-IDP09]***

Successful responses MUST be directly signed using a `<ds:Signature>` element within the `<samlp:Response>` element. Error responses MAY be unsigned.

CATS Support: *Constrained*

Responses MUST NOT be signed.

Kantara Requirement: ***[SDP-IDP10]***

> Successful responses MUST contain exactly one SAML assertion. The assertion MUST contain exactly one `<saml:AuthnStatement>` element and MUST contain zero or one `<saml:AttributeStatement>` elements. The assertion within the response MAY be directly signed.

CATS Support: *Constrained*

The assertion within the response MUST be directly signed.

The `<saml:AuthnStatement>` MUST include exactly one `<saml:AuthnContext>` element that specifies the level of assurance [SAML2Assur] to which the subject was authenticated.

Kantara Requirement: ***[SDP-IDP11]***

> In the event the HTTP-POST binding [SAML2Bind] is used, assertions MUST be encrypted and transmitted via a `<saml:EncryptedAssertion>` element. Information intended for the consumption of the SP MUST NOT be further encrypted via `<saml:EncryptedID>` or `<saml:EncryptedAttribute>` constructs.
>
> *While encryption is viewed in some quarters as onerous or unnecessary, interoperability is enhanced by uniformity. Moreover, a spate of recent vulnerabilities across the industry would have been almost entirely mitigated by its use, demonstrating that it is no longer acceptable to view it as an optional part of front-channel delivery of assertions, if it ever was.*

CATS Support: *Supported*

6.1.3. Subject Identifiers

Kantara Requirement: ***[SDP-IDP12]***

> Assertions MUST contain a `<saml:NameID>` element with the `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` Format, as defined in [SAML2Core], for the purposes of logout.

CATS Support: *Constrained*

The `<saml:NameID>` Format MUST be `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.

Kantara Requirement: ***[SDP-IDP13]***

IdPs MUST support one or both of the SAML Attributes defined by [SAML2SubjId] for non-transient identification of subjects. Support for both is RECOMMENDED.

CATS Support: *Constrained*

IdP deployments MUST NOT implement [SAML2SubjId].

Kantara Requirement: ***[SDP-IDP14]***

IdPs MUST enumerate the scope(s) of the subject identifiers they support in their metadata by means of the `<shibmd:Scope>` extension element, as defined in [SAML2SubjId]. They MUST NOT contain a regular expression (i.e., each element's `regexp` attribute MUST be set to `false` or `0`).

The element(s) may be positioned as an extension of either the `<md:EntityDescriptor>` or `<md:IDPSSODescriptor>` as deemed appropriate.

Note that while common, it is not a requirement for the scope(s) to be contained within the IdP's entityID, nor for it to bear any relationship to other data asserted by the IdP, such as email addresses.

CATS Support: *Constrained*

IdP deployments MUST NOT implement [SAML2SubjId].

6.1.3.1. Subject Identifier Requirements Signaling

Kantara Requirement: ***[SDP-IDP15]***

IdPs MUST support the metadata-based identifier requirement signaling mechanism defined in [SAML2SubjId].

The purpose of this requirement is to provide a level of confidence to a signaling SP that a compliant IdP which fails to do as instructed is unwilling or unable to fulfill the requirements rather than merely oblivious to them.

CATS Support: *Not Applicable*

Kantara Requirement: ***[SDP-IDP16]***

If an IdP cannot or will not satisfy the requirements of an SP in this respect, then it MAY return an assertion without the data it is unable to provide or return an error as it sees fit.

CATS Support: *Not Applicable*

Kantara Requirement: ***[SDP-IDP17]***

In the absence of any signaling by an SP, an IdP MAY supply either, both, or neither of the SAML Attributes defined in [SAML2SubjId], or return an error as it sees fit.

CATS Support: *Not Applicable*

6.1.4. Attributes

Kantara Requirement: ***[SDP-IDP18]***

`<saml:Attribute>` elements MUST contain a NameFormat of `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.

This requirement ensures unique, non-conflicting naming of SAML Attributes even in cases involving custom requirements for which no standard SAML Attributes may exist.

CATS Support: *Not Applicable*

Kantara Requirement: ***[SDP-IDP19]***

It is RECOMMENDED that the content of each `<saml:AttributeValue>` element be limited to a single child text node (i.e., a simple string value).

Note that this refers to `<saml:AttributeValue>` *elements, not* `<saml:Attribute>` *elements, and refers to the form of each individual value. It discourages the use of complex XML content models within the value of a SAML Attribute.*

CATS Support: *Not Applicable*

Kantara Requirement: ***[SDP-IDP20]***

> Multiple values of a `<saml:Attribute>` MUST be expressed as individual `<saml:AttributeValue>` elements rather than embedded in a delimited form within a single `<saml:AttributeValue>` element.

CATS Support: *Supported*

6.2. Single Logout

Kantara Requirement: ***[SDP-IDP21]***

> IdPs MUST support the Single Logout profile [SAML2Prof], as updated by the Approved Errata [SAML2Err], with behavior, capabilities, and options consistent with the additional constraints specified in this section.
>
> *The term "IdP session" is used to refer to the ongoing state between the IdP and its clients allowing for SSO. Support for logout implies supporting termination of a subject's IdP session in response to receiving a `<samlp:LogoutRequest>` or upon some administrative signal.*

CATS Support: *Supported*

Kantara Requirement: ***[SDP-IDP22]***

> IdPs MAY allow a subject the option to maintain their IdP session rather than unilaterally terminating it.

CATS Support: *Constrained*

IdP deployments participating as a session authority MUST always terminate the subject's IdP session.

At all times, a `<samlp:LogoutRequest>` will generate a global logout for the subject's session.

Kantara Requirement: ***[SDP-IDP23]***

> IdPs MAY support the propagation of logout signaling to SPs.

CATS Support: *Constrained*

IdP deployments participating as a session authority MUST support the propagation of logout.

6.2.1. Requests

6.2.1.1. Binding

Kantara Requirement: ***[SDP-IDP24]***

> The HTTP-Redirect binding [SAML2Bind] MUST be used for the transmission of `<samlp:LogoutRequest>` messages, in the event that propagation is supported.

CATS Support: *Constrained*

The SOAP binding [SAML2Bind] MUST be used for the transmission of <samlp:LogoutRequest> messages to SPs that have included a `<md:SingleLogoutService>` SOAP endpoint in their metadata.

The HTTP-Redirect binding [SAML2Bind] MUST be used for the transmission of <samlp:LogoutRequest> messages to those SPs that have not included a `<md:SingleLogoutService>` SOAP endpoint in their metadata, but have included an HTTP-Redirect endpoint.

In cases where multiple SPs are participating in a session, identity providers MUST first use the SOAP binding to send `<samlp:LogoutRequest>` messages to all SPs that support SOAP before using the HTTP-Redirect binding to send `<samlp:LogoutRequest>` messages to any SPs that do not support SOAP.

Notwithstanding the above, in cases where multiple session participants support the same binding, an IdP MAY send `<samlp:LogoutRequest>` messages to multiple SPs concurrently using the same binding.

Doing so can improve the response time perceived by the user.

When using the HTTP-Redirect binding to transmit <samlp:LogoutRequest> messages, an IdP SHOULD NOT employ mechanisms that could lead to loss of control of the user agent in situations where an SP fails to respond to the <samlp:LogoutRequest>.

For example, if the IdP employs a full-frame browser redirect to an SP that fails to respond, control of the browser will not return to the IdP and it will not be able to respond to the SP that initiated the logout.

Kantara Requirement: ***[SDP-IDP25]***

IdPs MUST support the HTTP-Redirect [SAML2Bind] binding for the receipt of `<samlp:LogoutRequest>` messages.

CATS Support: *Supported*

6.2.2. Request Content

Kantara Requirement: ***[SDP-IDP26]***

Requests MUST be signed (via a signature created in accordance with the HTTP-Redirect binding [SAML2Bind]).

CATS Support: *Supported*

Kantara Requirement: ***[SDP-IDP27]***

The `<saml:NameID>` element in `<samlp:LogoutRequest>` messages MUST NOT be encrypted.

The normative requirement for the use of transient identifiers is intended to obviate the need for XML Encryption.

CATS Support: *Constrained*

The `<saml:NameID>` element of `<samlp:LogoutRequest>` messages transmitted via the HTTP-Redirect binding [SAML2Bind] MUST be encrypted via the `<saml:EncryptedID>` element.

This profile uses persistent identifiers which should be protected.

`<saml:EncryptedID>` MUST NOT include any optional elements that unnecessarily increase the size of the `<samlp:LogoutRequest>` message.

This is to avoid issues with older browsers that do not support long URLs.

6.2.3. Responses

6.2.3.1. Binding

Kantara Requirement: ***[SDP-IDP28]***

> The HTTP-Redirect binding [SAML2Bind] MUST be used for the transmission of `<samlp:LogoutResponse>` messages.

CATS Support: *Supported*

Kantara Requirement: ***[SDP-IDP29]***

> IdPs MUST support the HTTP-Redirect [SAML2Bind] binding for the receipt of `<samlp:LogoutResponse>` messages, in the event that `<samlp:LogoutRequest>` propagation is supported.

CATS Support: *Supported*

6.2.3.2. Response Content

Kantara Requirement: ***[SDP-IDP30]***

> Responses MUST be signed (via a signature created in accordance with the HTTP-Redirect binding [SAML2Bind]).

CATS Support: *Supported*

Kantara Requirement: ***[SDP-IDP31]***

> The `<samlp:StatusCode>` in the response issued by the IdP MUST reflect whether the IdP session was successfully terminated.

CATS Support: *Supported*

6.3. Metadata and Trust Management

6.3.1. Support for Multiple Keys

The ability to perform seamless key migration depends upon proper support for consuming and/or

leveraging multiple keys at the same time.

Kantara Requirement: ***[SDP-IDP32]***

> IdP deployments MUST support multiple signing certificates in SP metadata and MUST support validation of signatures using a key from any of them.

CATS Support: *Supported*

6.3.2. Metadata Content

Kantara Requirement: ***[SDP-IDP33]***

> By virtue of this profile's requirements, an IdP's metadata MUST contain:
>
> - an `<md:IDPSSODescriptor>` role element containing
>   - at least one `<md:SingleSignOnService>` endpoint element
>   - at least one `<md:SingleLogoutService>` endpoint element
>   - at least one `<md:KeyDescriptor>` element whose `use` attribute is omitted or set to `signing`
>   - an `errorURL` attribute
>   - an `<md:Extensions>` element at the role level containing
>   - an `<mdui:UIInfo>` extension element containing the child elements `<mdui:DisplayName>` and `<mdui:Logo>`
>   - at least one `<shibmd:Scope>` element
>   - alternately, the `<shibmd:Scope>` element(s) MAY instead reside in an `<md:Extensions>` element at the root (`<md:EntityDescriptor>`) level
> - an `<md:ContactPerson>` element with a `contactType` of `technical` and an `<md:EmailAddress>` element

CATS Support: *Constrained*

The metadata of IdPs MUST contain at least one signing certificate with the `use` attribute set to `signing` and at least one encryption certificate with the `use` attribute set to `encryption`.

IdP metadata MAY include an `<md:Extensions>` element containing an `<mdui:UIInfo>` extension element, but it MUST NOT include an `<mdattr:EntityAttributes>` extension element.

IdP metadata SHOULD NOT include an `ErrorURL` attribute.

IdP metadata MUST NOT contain a <shibmd:Scope> extension element.

6.4. CATS-Specific Requirements

6.4.1. Metadata Content

[CDP-IDP01]

In addition to the requirements of **[SDP-IDP31]**, an IdP's metadata MUST also contain the levels of assurance to which it conforms, as specified by the Identity Assurance Certification Attribute Profile [SAML2Assur].

6.4.2. Responses

[CDP-IDP02]

IdP deployments MUST support the issuance of `<saml2p:Response>` messages (with appropriate status codes) in the event that a user indicates they wish to cancel/exit or if an error condition occurs, provided that the user agent remains available.

6.4.3. Session Management and Timeouts

[CDP-IDP03]

`<saml:AuthnStatement>` elements MUST NOT include a `SessionNotOnOrAfter` attribute.

[CDP-IDP04]

IdPs MUST NOT issue a `<saml:Assertion>` with an `IssueInstant` attribute value that exceeds the value of the `AuthnInstant` attribute of the included `<saml:AuthnStatement>` by more than 20 minutes.

This effectively prohibits the passive fulfilment of authentication requests (single sign-on) for a subject after 20 minutes have passed since their most recent authentication event.

Once 20 minutes have passed since the most recent authentication event, IDPs MUST issue a `<saml:Repsonse>` with a second-level `<samlp:StatusCode>` of `urn:oasis:names:tc:SAML:2.0:status:NoPassive` in response to any `<samlp:AuthnRequest>` with an `IsPassive` attribute value of `true` or `1`.

[CDP-IDP05]

IdPs participating as a session authority MUST include the `SessionIndex` attribute of `<saml:AuthnStatement>`.

[CDP-IDP06]

Once an IdP participating as a session authority has issued the first `<saml:AuthnStatement>` containing the `SessionIndex` for a new session, it MUST retain sufficient session state to successfully process `<samlp:LogoutRequest>` messages that specify a matching `<samlp:SessionIndex>` value for no less than 8 hours.

This ensures that the IdP will be able to propagate single-logout of a subject's session for up to 8 hours after issuing the first assertion for that session.

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

The IdP MAY discard all state associated with a `SessionIndex` after processing a `<samlp:LogoutRequest>` for the session.

[CDP-IDP07]

IdPs participating as a session authority MUST administratively perform a global logout of any current subject's session whenever an authentication event within that session results in the authentication of a different subject.

For example, say the IdP has issued the first `<saml:AuthnStatement>` for subject A within the last 8 hours, and subsequently receives a `<samlp:AuthnRequest>` from the same user agent triggering a new authentication event. If the end-user authenticates with a different credential (subject B) than the one originally used by subject A, then the IdP must peform a global logout of subject A's session, before starting a new session for subject B.

6.4.4. Security

[CDP-IDP08]

The private keys of an IdPs signing certificates MUST be protected within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module.

6.4.5. Attributes

[CDP-IDP09] Identity Provider deployments MUST be capable of determining whether or not to include specific SAML attributes (or specific values) in a response based on the presence of `<md:AttributeConsumingService>` elements (containing `<md:RequestedAttribute>` elements) found in the metadata for a relying party, including the value of the enclosed `isRequired` XML attribute. Accordingly, they MUST support the `AttributeConsumingServiceIndex` attribute in `<samlp:AuthnRequest>`` messages as a means of determining the appropriate `<md:AttributeConsumingService>` element to process.

[CDP-IDP10]

IdP deployments SHOULD prioritize the use of standard attribute name and definition profiles before defining custom attributes. Use of the following profiles are RECCOMENDED in descending order of preference:

- The standard OpenID Connect claims defined in section 5.1 of [OIDC]. (See **[CDP-IDP12]** below).
- The Identity Metasystem Interoperability claim types defined in section 7.5 of [IMI].
- The SAML V2.0 X.500/LDAP Attribute Profile [X500SAMLattr].

[CDP-IDP11]

<saml:Attribute> elements MUST use a `NameFormat` value of either `urn:oasis:names:tc:SAML:2.0:attrname-format:basic` or `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.

[CDP-IDP12]

The name and value of `<saml:Attribute>` elements with a `NameFormat` of `urn:oasis:names:tc:SAML:2.0:attrname-format:basic` MUST correspond to one of the standard claims defined in section 5.1 of [OIDC] as follows:

- The value of the `Name` attribute of `<saml:Attribute>` must match the JSON member name in [OIDC].
- The `xsi:type` attribute of `<saml:AttributeValue>` must specify the XML Schema type that corresponds to the JSON type in [OIDC]:

JSON Type	XML Schema Type
string	xs:string
boolean	xs:boolean
number	xs:decimal

- The `address` claim MUST NOT be used. *Refer to requirement **[SDP-IDP18]**.*
- The following properties of the `address` claim MAY be used as standalone attributes:
  - street_address
  - locality
  - region
  - postal_code
  - country
- The `formatted` member of the `address` claim SHOULD NOT be used.

7. CATS-Specific Proxy Requirements

[CDP-PIP01]

Proxying Identity Provider deployments MUST support the mapping of incoming to outgoing `<saml:NameID>` elements, to pass through values or map between different vocabularies as required.

[CDP-PIP02]

Proxying Identity Provider deployments MUST support the suppression/eliding of `<saml:AttributeStatement>` elements from the `<saml:Assertion>` of outgoing `<samlp:Response>` messages to allow for hiding the identity of the subject from SPs.

[CDP-PIP03]

Proxying Identity Provider deployments MUST support the mapping of incoming to outgoing `<samlp:RequestedAuthnContext>` and `<samlp:NameIDPolicy>` elements, to pass through values or map between different vocabularies as required.

[CDP-PIP04]

Proxying Identity Provider deployments MUST support the suppression/eliding of `<samlp:RequesterID>` elements from outgoing `<samlp:AuthnRequest>` messages to allow for hiding the identity of the Service Provider from proxied Identity Providers.

[CDP-PIP05]

Proxying Identity Provider deployments MUST support the mapping of incoming to outgoing `<saml:AuthnContext>` elements, to pass through values or map between different vocabularies as required.

[CDP-PIP06]

Proxying Identity Provider deployments MUST support the suppression of `<saml:AuthenticatingAuthority>` elements from outgoing `<saml:AuthnContext>` elements to allow for hiding the identity of the proxied Identity Provider from Service Providers.

[CDP-PIP07]

Proxying Identity Provider deployments MUST support the use of a `<samlp:IDPList>` containing one or more `<samlp:IDPEntry>` elements in incoming and outgoing `<samlp:AuthnRequest>` messages.

This allows one proxy in a chain of proxies to provide IdP discovery services on behalf of other proxies in the chain.

[CDP-PIP08]

`<samlp:AuthnRequest>` messages produced by Proxying Identity Provider deployments MUST include the

`ForceAuthn` attribute with a value of `true` or `1`.

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
- [RFC4051] IETF RFC 4051, Additional XML Security Uniform Resource Identifiers, April 2005. https://www.ietf.org/rfc/rfc4051.txt
- [SAML2Core] OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
- [SAML2Bind] OASIS Standard, Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
- [SAML2Prof] OASIS Standard, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
- [SAML2Meta] OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
- [SAML2Gloss] OASIS Standard, Glossary for the OASIS Security Assertion Markup Language (SAML) V2, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.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
- [SAML2MDIOP] OASIS Standard, SAML V2.0 Metadata Interoperability Profile Version 1.0, October 2019. http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop-os.pdf
- [IdPDisco] OASIS Committee Specification, Identity Provider Discovery Service Protocol and Profile, March 2008. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf
- [SAML2Err] OASIS Approved Errata, SAML Version 2.0 Errata 05, May 2012. http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf
- [XMLEnc] D. Eastlake et al. XML Encryption Syntax and Processing. W3C Recommendation, April 2013. https://www.w3.org/TR/xmlenc-core1/
- [XMLSig] D. Eastlake et al. XML-Signature Syntax and Processing, Version 1.1. W3C Recommendation, April 2013. https://www.w3.org/TR/xmldsig-core1/
- [SAML2Assur] OASIS Committee Specification, SAML V2.0 Identity Assurance Profiles Version 1.0, November 2010. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.pdf
- [SAML2SubjId] OASIS Committee Specification, SAMLV2.0 Subject Identifier Attributes Profile Version 1.0, January 2019. https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/cs01/saml-subject-id-attr-v1.0-cs01.pdf

- [SAML2ASLO] OASIS Committee Specification, SAML V2.0 Asynchronous Single Logout Profile Extension Version 1.0, November 2012. http://docs.oasis-open.org/security/saml/Post2.0/saml-async-slo/v1.0/cs01/saml-async-slo-v1.0-cs01.pdf
- [MetaUI] OASIS Standard, SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0, October 2019. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/os/sstc-saml-metadata-ui-v1.0-os.pdf
- [MetaAttr] OASIS Committee Specification, SAML V2.0 Metadata Extension for Entity Attributes Version 1.0, August 2009. http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr-cs-01.pdf
- [SAML2Iop] Kantara Initiative, SAML V2.0 Interoperability Deployment Profile V1.0 (Draft). https://kantarainitiative.github.io/SAMLprofiles/saml2int.html
- [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://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.40.062-eng_0.pdf
- [ITPIN-2018-01] - Treasury Board Canada Secretariat, Implementing HTTPS for Secure Web Connections: Information Technology Policy Implementation Notice (ITPIN). https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/policy-implementation-notices/implementing-https-secure-web-connections-itpin.html

8.2. Non-Normative

- [CATS-SAML2Id] - Treasury Board Canada Secretariat, CATS SAML 2.0 Deployment Profile for Identity Authentication. https://canada-ca.github.io/CATS-STAE/saml2id.html
- [PCTF] Identity Management Subcomittee, Pan-Canadian Trust Framework. https://github.com/canada-ca/PCTF-CCP
- [XMLEncBreak] Jager and Somorovsky, How to Break XML Encryption, October 2011. http://www.nds.rub.de/media/nds/veroeffentlichungen/2011/10/22/HowToBreakXMLenc.pdf

9. Contributors

- Canada Revenue Agency
- Communications Security Establishment
- Employment and Social Development Canada
- FedDev Ontario
- Service Canada
- Shared Services Canada
- Transport Canada
- Treasury Board of Canada Secretariat