Cyber Authentication Technology Solutions

SAML 2.0 Deployment Profile for Identity Authentication

Table of Contents

Version

3.x

Date

2018-09-17

Status

Work In Progress

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 SAML 2.0 Deployment Profile for Identity Authentication

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).

The scope of this profile applies only to providers and consumers of trusted identity authentication services. A seperate profile [SAML2cred] supports anonymous credential authentication services.

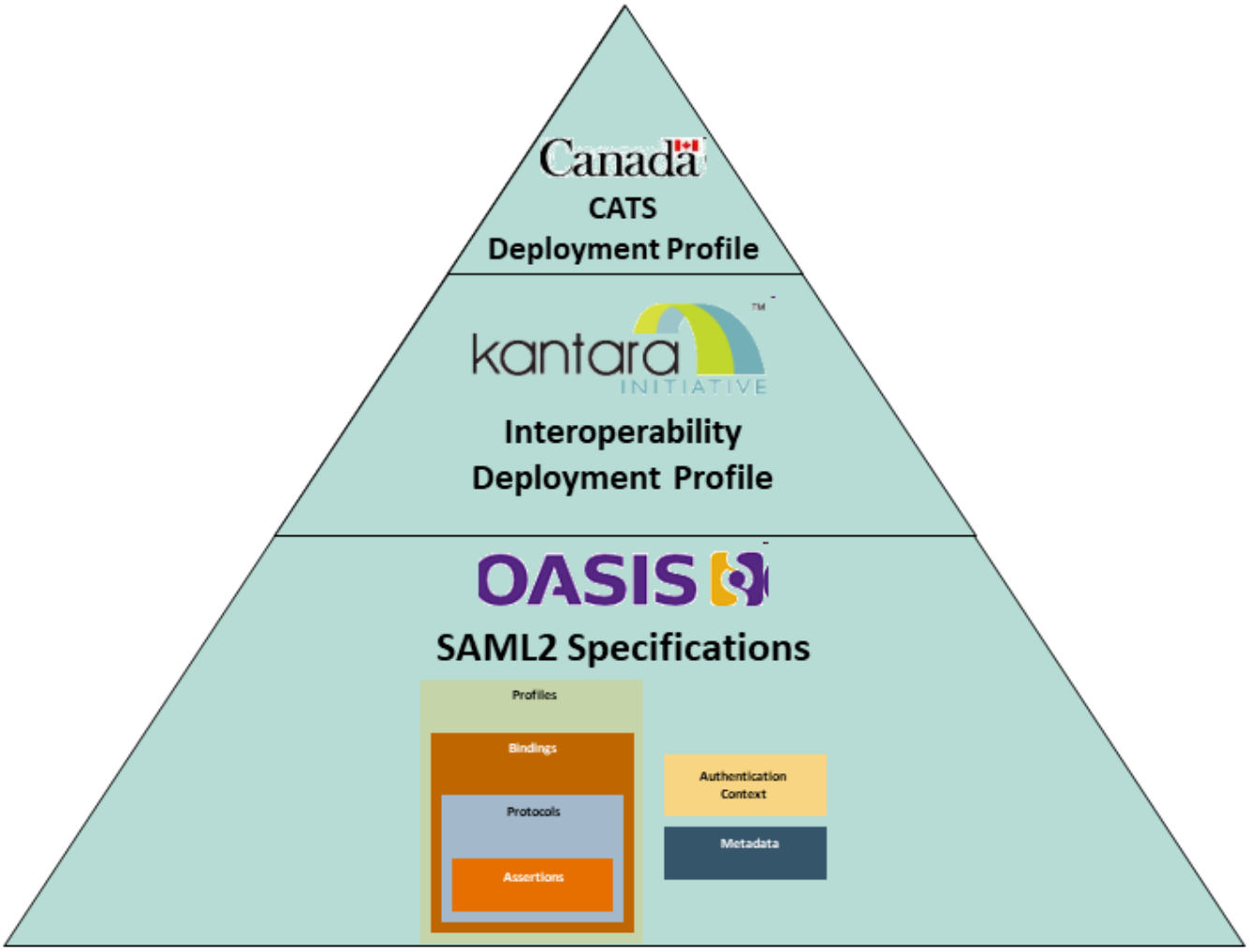

Figure 1. CATS SAML Profile Building Blocks

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.

Assurance of Credential (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).

Authoritative Party

A federation member that provides assurances of credential 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 assurances of identity 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 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.

User Agent

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

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 SAML 2.0 Deployment Profiles

The requirements specified are in addition to all normative requirements of the underlying Web Browser SSO profile [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.

Deployments owned by Government of Canada departments and agencies MUST obtain approval from the Chief Information Officer Branch of 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 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 all element and attribute content they produce to 256 characters. This applies in particular to the values within `<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. Deployments SHOULD reject messages that contain them.

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 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. The key ultimately used to establish trust in metadata MUST NOT itself appear within the same metadata in a `<md:KeyDescriptor>` element.

In most cases, the previous requirement implies that a key communicated via metadata may not also be used to sign and verify the same metadata, but it is possible to envision scenarios in which this may happen if metadata verification relies on a chain of certificates signed by an ultimately trusted Certificate Authority. However, it MUST be possible to seamlessly communicate new keys without necessarily changing the key used to establish trust in the metadata, which implies some level of indirection is required.

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 Shared Services Canada.

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.
>
> Metadata MAY include content indicating support for profiles or features beyond the bounds of this profile, but metadata MUST NOT contain content that advertises profile support or features that aren't supported by a deployment.
>
> *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*

Deployments federating with the Sign in Canada acceptance platform MUST provide their metadata to Shared Services Canada 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 requierments 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, Shared Services Canada 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`. The metadata of SPs MUST contain 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>`, `<mdui:Logo>`, and `<mdui:InformationURL>`.

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.

CATS Support: *Supported*

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

> At least one `<mdui:Logo>` element MUST have a `height` attribute of `60` and a `width` attribute of `80`.
>
> An entity SHOULD include an `<mdui:Logo>` element with a `height` attribute of `16` and a `width` attribute of `16`.
>
> Any logo referenced by an `<mdui:Logo>` element MUST be in PNG format with a transparent background.

CATS Support: *Supported*

4.3. Cryptographic Algorithms

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

Deployments MUST support, and use, the following 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.

- 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#aes192-gcm` [XMLEnc]
  - `http://www.w3.org/2009/xmlenc11#aes256-gcm` [XMLEnc]
- Key Transport
  - `http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p` [XMLEnc]
  - `http://www.w3.org/2009/xmlenc11#rsa-oaep` [XMLEnc]

The following default digest algorithm MUST be used in conjunction with the above key transport algorithms (the default mask generation function, MGF1 with SHA1, MUST be used):

- `http://www.w3.org/2001/04/xmlenc#sha256` [XMLEnc]

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].

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.

5. SP Requirements

5.1. Web Browser SSO

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

> SPs MUST support the 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 do not 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:transient`.

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 MUST NOT use a hostname with port number (such as https://sp.example.com:443/acs) in its request and without (such as https://sp.example.com/acs) in its metadata.*

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>` with the `Comparison` attribute set to `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].

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 also support decryption of `<saml:EncryptedAttribute>` elements.

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]***

> The response to such errors MUST direct users to appropriate support resources offered by the SP or, alternatively, to the `errorURL` attribute in an IdP's metadata if the cause of the error is inferred to be a lack of sufficient or appropriate attributes about the user to operate successfully.

CATS Support: *Supported*

5.1.2.4. Forced Re-Authentication

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

SPs that include a `ForceAuthn` attribute of `true` in their requests SHOULD test the currency of the `AuthnInstant` element in the received assertions to verify the currency of the authentication event.

This is necessary because clients can freely generate requests that do not specify this attribute, potentially bypassing the SP's intent.

CATS Support: *Supported*

5.1.3. Subject Identification

5.1.3.1. NameID Formats

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

SPs MUST NOT require the presence of a `<saml:NameID>` element and MUST NOT rely on the content of this element for long term identification of subjects; `<saml:Attribute>` elements MUST be used for this purpose in the manner detailed below.

CATS Support: *Supported*

5.1.3.2. Subject Identifiers

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

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.

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.*

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

CATS Support: *Constrained*

SP deployments MUST NOT use this profile for the persistent tracking/identification of users.

Persistent identification of users is accomplished by binding an identiy, authenticated using this profile, to a credential, authenticated using the [SAML2Cred] profile.

5.1.3.3. Subject Identifier Requirements Signaling

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

> 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-SP17]***

> 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-SP18]***

> SPs MUST associate identifier scopes with IdPs such that only authorized IdPs may assert identifiers with particular scopes for particular purposes.
>
> *For example, if the* `example.com` *scope is bound to the IdP named* `http://idp.example.com/saml`*, it should be generally disallowed for any other IdP to assert an identifier in that scope. Note that this is not a 1:1 relationship; it may frequently happen that multiple IdPs may assert a given scope, or an IdP may 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-SP19]***

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 ([X500SAMLattr]):

- `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 Attributes of this sort tend to be defined as multi-valued.

CATS Support: *Not Applicable*

5.1.4. Attribute Value Constraints

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

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*

5.2. Metadata and Trust Management

5.2.1. 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-SP38]***

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-SP39]***

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.

5.2.2. Metadata Content

Kantara Requirement: ***[SDP-SP40]***

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

- an `<md:SPSSODescriptor>` role element
  - at least one `<md:AssertionConsumerService>` endpoint element
  - at least one `<md:KeyDescriptor>` element whose `use` attribute is omitted or set to `encryption`
  - if the SP generates single logout requests: at least one `<md:KeyDescriptor>` element whose `use` attribute is omitted or set to `signing`
- an `<md:Extensions>` element
  - an `<mdui:UIInfo>` extension element with previously prescribed content and `<mdui:PrivacyStatementURL>`
  - an `<mdattr:EntityAttributes>` extension element for signaling Subject Identifier requirements with previously prescribed content

In addition, an SP's metadata MUST contain:

- an `<md:ContactPerson>` element with a `contactType` of `technical` and an `<md:EmailAddress>` element

An `<md:SingleLogoutService>` element MAY be omitted in the event that an SP either does not support the Single Logout Profile, or 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`.

An `<md:Extensions>` element MAY contain an `<mdui:UIInfo>` but MUST NOT include an `<mdattr:EntityAttributes>` attribute.

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`.

5.3. CATS-Specific Requirements

5.3.1. Request Signing

[CIP-SP01]

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

[CIP-SP02]

`<samlp:AuthnRequest>` messages SHOULD NOT include an `isPassive` attribute. If the SP implementation is unable to omit the `isPassive` attribute then it MUST have a value of `false` or `0`.

In all cases of identity authentication, the IdP must interact with the end-user in order to obtain their informed consent.

6. IdP Requirements

6.1. Web Browser SSO

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

> IdPs MUST support the 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. Endpoint Verification

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

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.

CATS Support: *Supported*

6.1.1.3. Signing

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

If a request is signed, IdPs MUST 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*

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

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

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.

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 signed.

CATS Support: *Needs Discussion*

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

> Successful responses MUST contain one and only one SAML assertion, and the assertion MUST contain exactly one `<saml:AuthnStatement>` element and MAY 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.

The `<saml:Assertion>` MUST contain exactly one `<saml:AttributeStatement>` element.

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, interopability 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: *Constrained*

Attriubutes contained in responses sent to a proxying identity provider that contain personal information intended for the use of a proxied service provider SHOULD be further encrypted for the proxied SP via the `<saml:EncryptedAttribute>` construct.

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*

Assertions MUST contain a `<saml:NameID>` element with the `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` Format for the purposes of interoperability. This profile does not implement session management constructs such as logout.

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].

6.1.3.1. Subject Identifier Requirements Signaling

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

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

CATS Support: *Constrained*

IdP deployments MUST NOT implement [SAML2SubjId].

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

> If an IdP cannot or will not satisfy the requirements of an SP in this respect, then it MUST fail the authentication request and SHOULD respond to the SP with a SAML error status and a second-level `<samlp:StatusCode>` of `urn:oasis:names:tc:SAML:profiles:subject-id:req`.

CATS Support: *Not Applicable*

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

> In the absence of any signaling by an SP, an IdP MAY supply either, both, or neither SAML Attribute, or return an error as it sees fit.

CATS Support: *Not Applicable*

6.1.4. Attributes

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

> `<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 Attributes even in cases involving custom requirements for which no standard Attributes may exist.*

CATS Support: *Supported*

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

> 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) and that multiple values of a `<saml:Attribute>` be expressed as individual `<saml:AttributeValue>` elements rather than embedded in a delimited form within a single element.
>
> *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 an Attribute.*

CATS Support: *Supported*

6.2. Metadata and Trust Management

6.2.1. 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-IDP30]***

> 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*

6.2.2. Metadata Content

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

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

- an `<md:IDPSSODescriptor>` role element
  - 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 `<md:Extensions>` element
  - an `<mdui:UIInfo>` extension element with previously prescribed content

In addition, an IdP's metadata MUST contain:

- an `<md:ContactPerson>` element with a `contactType` of `technical` and an `<md:EmailAddress>` element

CATS Support: *Constrained*

The `use` attribute of the `<md:KeyDescriptor>` element(s) MUST be set to `signing`.

IdP metadata MUST NOT contain a `<md:SingleLogoutService>` endpoint element.

6.3. CATS-Specific Requirements

6.3.1. 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].

6.3.2. Responses

[CIP-IDP01]

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.

6.3.3. Security

[CIP-IDP02]

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.

7. CATS-Specific Proxy Requirements

[CIP-PIP01]

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

[CIP-PIP02]

Proxying Identity Provider deployments MUST include at least one `<samlp:RequesterID>` element in the `<samlp:Scoping>` element of outgoing `<samlp:AuthnRequest>` messages that identifies the SP that originated the request.

Proxied Identity Providers must know the identity of the target relying party in order to obtain informed consent from the end-user.

[CIP-PIP03]

Proxying Identity Provider deployments MUST support the mapping of incoming to outgoing `<saml:AuthnContext>` elements as well as the generation of a new `<saml:AuthnContext>` element using information from other elements of the `<saml:Assertion>` (such as the `Issuer` or `<saml:AttributeStatement>`), to pass through values or map between different vocabularies as required.

[CIP-PIP04]

Proxying Identity Provider deployments MUST include at least one `<saml:AuthenticatingAuthority>` element in outgoing `<saml:AuthnContext>` elements to discolose the identity of the proxied Identity Provider to Service Providers.

[CIP-PIP05]

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.

[CIP-PIP06]

`<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 Committee Specification, SAML V2.0 Metadata Interoperability Profile Version 1.0, August 2009. http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.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 Working Draft, SAMLV2.0 Subject Identifier Attributes Profile Version 1.0, February 2018. https://www.oasis-open.org/committees/download.php/62438/saml-subject-id-attr-v1.0-wd04.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 Committee Specification, SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0, April 2012. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/cs01/sstc-saml-metadata-ui-v1.0-cs01.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

8.2. Non-Normative

- [SAML2Cred] Cyber Authentication Technology Solutions: SAML 2.0 Deployment Profile for Credential Authentication. https://canada-ca.github.io/CATS-STAE/saml2cred.html
- [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