# adopt-saml-deployment-profile

**Jump to:**



## InCommon adopts the SAML 2.0 Deployment Profile for Federation Interoperability

*InCommon is working to adopt numerous relevant items from the SAML 2.0 Deployment Profile to improve federation interoperability. This page outlines the reasons behind this effort and provides an overview of profile requirements that have been and will be adopted.*

## Introduction

The InCommon Federation is built on the Security Assertion Markup Language (SAML), an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML is an XML-based markup language for security assertions (statements that service providers use to make access-control decisions). SAML is powerful and flexible. Yet that same flexibility also produces confusion and inconsistencies among implementations. These inconsistencies have caused numerous integration challenges due to incorrect or incompatible implementations among products that claim to support SAML.

Between 2017 and 2019, members of InCommon and other national R&E federation community, in collaboration with the Kantara Initiative, developed the Deployment Profile to clarify ambiguities when using SAML to interoperate in a federation. The Deployment Profile has been around for some time. InCommon plans to adopt specific items from the profile to form a clearer, more precise signal on what it means to be "compatible" with the federation. Some of these requirements will be enforced by the federation manager if they are metadata-related. Others will be testable. A third group of requirements will simply be community enforced and handled through the InCommon dispute resolution process.

## Why adopt Deployment Profile?

The Deployment Profile adoption effort will provide:

- clear bars for participants to measure conformance
- support for construction of testing tools
- standards for vendors participating in the IdP as a Service Program
- a potential path to future Baseline Expectation statements

## What does adopting a Deployment Profile requirement mean?

We use the word “adopt” to indicate that the InCommon Federation considers a statement integral to successful interoperation in federated transactions. These adopted statements also form components of evaluation criteria when evaluating a software’s “compatibility” with the InCommon Federation.

Participants are expected to meet the requirements described in each "adopted" statement when interacting with each other using SAML. Where applicable (for example, during metadata publishing), the Federation Operator will enforce validation rules.

To claim InCommon compatibility, software makers and service operators must meet the requirements of the "adopted" elements of the SAML 2 Deployment Profile, among other requirements.

## How does the adoption of Deployment Profile relate to Baseline Expectations?

The Deployment Profile prescribes specific SAML interaction behaviors to facilitate interoperability during federated SSO. While CTAB may choose to include some of the Deployment Profile statements in in future editions of Baseline Expectations, an adopted statement is not necessarily a part of Baseline Expectations requirements.

## About the Deployment Profile

The Kantara SAML V2.0 Deployment Profile for Federation Interoperability specifies behavior and options that deployments of the SAML V2.0 Web Browser SSO profile, and related profiles, are required or permitted to rely on. These details were not specified in the original SAML specifications. As a result, deployers made choices at their discretion and, consequently, introduced incompatible implementations. The Deployment Profile was developed by the InCommon Deployment Profile working group, enhanced and approved by the Kantara Federation Interoperability Working Group (FIWG) and later approved by Kantara All Member Ballot on 2020-02-26.

## References

**Kantara SAML V2.0 Deployment Profile for Federation Interoperability**

**SAML V2.0 Web Browser SSO profile**

# Phased Adoption

The SAML2 Deployment Profile is comprised of dozens of statements. Some of them may require substantial lead time for Participants and software makers to make the necessary changes. To help everyone get started on this journey as quickly as possible, we are choosing a phased adoption approach. The following sections outlines statements to be adopted in each phase.



## Already adopted, or "adopt now" requirements

The requirements in this section are already adopted by the InCommon Federation. They were adopted as the result of community best practices and standards established through processes like InCommon Baseline Expectations. InCommon Participants are expected to adhere to these statements today:

### General Requirements

**[SDP-G01] Clock Skew -** Deployments MUST allow between three (3) and five (5) minutes of clock skew

**[SDP-G02] Data Size -** Unless otherwise specified, deployments MUST limit the size of each string-valued XML element and attribute they produce to 256 characters.

**[SDP-G03] Document Type Definitions -** Deployments MUST NOT produce any SAML protocol message that contains a (DTD) Document Type Definition.

**[SDP-G04] SAML entityIDs -** Deployments MUST be named via an absolute URI whose total length MUST NOT exceed 256 characters.

### Metatdata Consumption and Use

**[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.

**[SDP-MD03] Metadata Validity -** 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.

### Metadata Production

**[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.

**[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>`

**[SDP-MD07] -** EC public keys MUST be at least 256 bits in length.

**[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).

**[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>.

**[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.

**[SDP-MD11] -** Metadata MUST include an <md:ContactPerson> element within the <md:EntityDescriptor> element, with a contactType of technical and an <md:EmailAddress> element.

**[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.

## Cryptographic Algorithms

**[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.

## Service Provider Requirements - Web Browser SSO

**[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.

**[SDP-SP06] -** The AssertionConsumerServiceURL value, if present, MUST match an endpoint location expressed in the SP's metadata exactly, without requiring URL canonicalization/normalization.

**[SDP-SP08] -** SPs MUST support the HTTP-POST binding for the receipt of <samlp:Response> messages. Support for other bindings is OPTIONAL.

**[SDP-SP09] -** The endpoint(s) at which an SP supports receipt of <samlp:Response> messages MUST be protected by TLS/SSL.

## Service Provider: Metadata and Trust Management

**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.

**[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.

**[SDP-SP39] -** By virtue of this profile's requirements, an SP's metadata MUST contain…*

* The Deployment Profile includes additional details. Federation Manager enforces these rules and requires any service provider registered in InCommon to meet these criteria before publishing its metadata.

## Identity Provider Requirements - Web Browser SSO

**[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.

**[SDP-IDP03] -** The endpoint(s) at which an IdP supports receipt of <samlp:AuthnRequest> messages MUST be protected by TLS/SSL.

**[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).

## Identity Provider: Metadata and Trust Management

**[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.

# Requirements planned for adoption in 2022

These requirements is slated for adoption by InCommon by December 2022. Looks for communications to InCommon participants with additional details in the coming months:

### Service Provider Requirements - Web Browser SSO

**[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).

**[SDP-SP10] -** SPs MUST support decryption of `<saml:EncryptedAssertion>` elements. Support for other encrypted constructs is OPTIONAL.

**[SDP-SP13] -** SPs MUST NOT require the presence of a `<saml:NameID>` element.

**[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.

**[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.

**[SDP-SP17] -** SPs MUST associate identifier scopes with IdPs such that only authorized IdPs may assert identifiers with particular scopes for particular purposes.

### Identity Provider Requirements - Web Browser SSO

**[SDP-IDP02] -** IdPs MUST support the HTTP-Redirect binding [SAML2Bind] for the receipt of `<samlp:AuthnRequest>` messages.

**[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.

**[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 AuthnI nstant value in the assertion it returns to a fresh value.

**[SDP-IDP08] -** IdPs MUST support the HTTP-POST binding [SAML2Bind] for the transmission of <samlp: Response> messages.

**[SDP-IDP09] -** Successful responses MUST be directly signed using a `<ds:Signature>` element within the `<samlp:Response>` element. Error responses MAY be unsigned.

**[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.

**[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.

**[SDP-IDP15] -** IdPs MUST support the metadata-based identifier requirement signaling mechanism defined in [SAML2SubjId].

### Identity Provider: Metadata and Trust Management

**[SDP-IDP33]** By virtue of this profile's requirements, an IdP's metadata MUST contain...**

** The Deployment Profile includes additional details. Federation Manager enforces these rules and requires any identity provider registered in InCommon to meet these criteria before publishing its metadata.

## Longer-term adoptions

InCommon intends to adopt statements in this section. However, doing so involve more analysis, planning, and potentially lead-time for Participants and software makers to make substantial updates. We encourage community participation to help us plot a path to adopt these items in the next one to three years:

### General Requirements

**[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]

### Service Provider Requirements - Web Browser SSO

**[SDP-SP02] -** The HTTP-Redirect binding [SAML2Bind] MUST be used for the transmission of `<samlp:AuthnRequest>` messages.

**[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.

**[SDP-SP15] -** An SP MUST represent its identifier requirements in its SAML metadata, consistent with the Requirements Signaling mechanism defined in [SAML2SubjId].

### Identity Provider Requirements - Web Browser SSO

**[SDP-IDP18] -** `<saml:Attribute>` elements MUST contain a NameFormat of `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.

**[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.

## Single Logout

SAML based Single Logout (SLO) is complex to configure, and can be difficult to execute completely across potentially hundreds of federated resources. There are valid organizational reasons for either party (Service Provider or Identity Provider) to want SLO. However, if the Service Provider is managed by one organization and the Identity Provider is managed by another, the support for SLO may not align.

At this time, InCommon's only requirement is that the IdP must support Single Logout signaling by having a logout endpoint that supports the SAML profile so that SPs can initiate a SLO request if desired.
We encourage further community discussion to determine InCommon's use of Single Logout statement within the Deployment Profile.

## Additional Deployment Profile statements

The Kantara Deployment Profile contains additional statements not mentioned above. These omitted statements do not directly relate to federation inter-operation. We generally them consider good practices to follow, although they are not required for federation interoperability.