## Specifying a technical profile for a SAML 2.0 claims provider

Azure AD B2C Premium provides a support for the SAML 2.0. This section outlines the specifics of a technical profile for interacting with claims provider supporting this standardized protocol.

SAML 2.0, as a token format and a protocol, is very popular in the public sector with government agencies as well as with enterprises and educational institutions.

SAML 2.0 is a suite of specifications and, as such, comprises a set of normative and non-normative documents. SAML 2.0 essentially defines XML-based **assertions** and **protocols**, **bindings**, and **profiles**.

**A prior understanding or even better a knowledge of the underlying concepts is necessary to appropriately define a technical profile in this space.**

If you’re not familiar with all of these concepts, the critical aspects of SAML 2.0 are covered in detail in the following four normative documents:

1. [Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)[[1]](#footnote-1) (SAMLCore), the core specification.
2. [Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)[[2]](#footnote-2) (SAMLBind), which maps the SAML messages onto the standard messaging or communication protocols.
3. [Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)[[3]](#footnote-3) (SAMLProf), the use cases or the “*How-to*” in regards to the use of SAML in various situations.
4. And [Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf)[[4]](#footnote-4) (SAMLConform), the operational modes for the SAML 2.0 implementations.

The term SAML Core, in relationship with the SAMLCore core specification, refers to the general syntax and semantics of SAML assertions (a.k.a. tokens) as well as the protocol used to request and transmit those assertions from one system entity to another. Most of the time, the SAML assertion you may have to consider will be the so-called "bearer" assertion, a short-lived bearer token (i.e. without a proof of possession). Such an assertion may include both an authentication statement and an attribute statement.

A SAML 2.0 protocol describes how certain SAML elements (including assertions) are packaged within SAML request and response elements, and gives the processing rules that SAML entities like an IdP in our context must follow when producing or consuming these elements. For the most part, a SAML protocol is a simple request-response protocol. It is important to keep in mind that a SAML protocol always refers to what is transmitted, and not how (the latter is determined by the choice of binding). In the context of this paper, the most interesting SAML protocols are the Authentication Request Protocol, and the Artifact Resolution Protocol,

A SAML 2.0 binding determines how SAML requests and responses map onto standard messaging or communications protocols. In other words, it’s a mapping of a SAML protocol message onto standard messaging formats and/or communications protocols. SAML 2.0 completely separates the binding concept from the underlying profile (see below).

The SAML 2.0 standard defines several bindings:

* HTTP Redirect (GET) binding,
* HTTP POST binding,
* HTTP Artifact binding,
* Etc.

A SAML 2.0 profile is a concrete manifestation of a defined use case or the “*How-to*” using a particular combination of assertions, protocols, and bindings, assertions. Indeed, it describes in detail how SAML 2.0 assertions, protocols, and bindings combine to support the considered use case. These

The SAML 2.0 standard defines several profiles:

* Web Browser SSO profile,
* Artifact Resolution profile,
* Enhanced Client or Proxy (ECP) profile,
* Etc.

The most important one is certainly the web Browser SSO profile since this is the primary SAML use case for web SSO and federation. One should also note that these profiles support various possible deployment models.

Based on the above short introduction on SAML 2.0, and the related concepts and normative documents, let’s consider how to define a suitable technical profile.

The *Name* attribute of the *Protocol* XML element has to be set to **SAML2** as per *ProtocolName* enumeration in the Azure AD B2C Premium XML schema.

The following metadata item keys must or may be present in the *Metadata* XML element:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item key | Required | | Description | |
| PartnerEntity | | True | | Allow to specify a CDATA section (ignored by the XML parser). This section contains the SAML 2.0 metadata of the SAML 2.0 claims provider. |
| IssuerUri | | False | | Specify the Issuer Uri in the SAML 2.0 assertion. |
| TreatUnsolicitedResponseAsRequest | | False | | Allow an unsolicited response to serve as an authentication request.  Value: true or false. When set to true, this allows to send an assertion to an IDP by an IDP: IDP initiated SSO. |
| WantsSignedRequests | | False | | Indicate if you want signed request.  Value: true or false. Set to false (i.e. turned that off) for testing when you don’t have the production keys from the testing environment. |
| WantsSignedAssertions | | False | | Indicate if you want signed assertions.  Value: true or false. |
| RequestsSigned | | False | | Value: true or false. |
| WantsSignedResponses | | False | | Indicate if you want signed response.  Value: true or false. |
| ResponsesSigned | | False | | Value: true or false. |
| AssertionsEncrypted | | False | | Specify that the assertion must be encrypted before being sent.  Value: true or false. |

The *Suppressions* XML element - IN SPECIAL INTERRUPT CASES - provides the ability to unblock the situation, suppress certain things in the authentication request.

The following metadata item keys may be present in the *Suppressions* XML element:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item key | Required | | Description | |
| AuthnRequest | | False | | Specify for the authentication request message a comma-separated list of optional attribute/element of the SAML message since some implementations don’t support all the optional attribute/element as per protocol and above specifications, what is considered optional.  Values in the list: Consent, Destination, Issuer, Extensions, AssertionConsumerServiceUrl, AssertionConsumerServiceIndex, AttributeConsumingServiceIndex, ProtocolBinding, IsPassive, ForceAuthn, ProviderName, Scoping, RequestedAuthenticationcontext, Conditions, NameIDPolicy, and Subject. |
| LogoutRequest | | False | | Specify for the logout request message a comma-separated list of optional attribute/element of the SAML message since some implementations don’t support all the optional attribute/element as per protocol and above specifications, what is considered optional.  Values in the list: Consent, Destination, Issuer, Extensions, NotOnOrAfter, Reason, and SessionIndex. |

**Note** This is very unusual to suppress them.

The *InputClaimsTransformations* XML element is absent.

The *InputClaims* XML element is empty or absent.

The *PersistedClaims* XML element is absent.

The *OutputClaims* XML element contains the claims bag as the output with possible mapping information between a *ClaimType* already defined in the *ClaimsSchema* section in the policy XML file and that partner claim type. **This also enables to take the subject name of the SAML assertion instead of as an attribute**:

<OutputClaim ClaimTypeReferenceId="UserId" PartnerClaimType="assertionSubjectName" />

The *OutputClaimsTransformations* XML element may contain a collection of *OutputClaimsTransformation* to be used to check or modify the output claims, or generate new ones.

The following XML snippet illustrates a technical profile for a SAML 2.0 claims provider:

<TechnicalProfile Id="IdP-SAML2-Outbound">

<DisplayName>Foo IdP</DisplayName>

<Description>Some suitable description for foo IdP</Description>

<Protocol Name="SAML2" />

<Metadata>

<Item Key="WantsSignedAssertions">false</Item>

<Item Key="TreatUnsolicitedResponseAsRequest">true</Item>

<Item Key="ResponsesSigned">false</Item>

<Item Key="IssuerUri">https://te.cpim.windows.net/csdii.onmicrosoft.com/B2C\_1A\_casinitiated</Item>

<Item Key="PartnerEntity">

<![CDATA[

<md:EntityDescriptor entityID="https://web.dev1.foo.com/saml20"

xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">

<md:IDPSSODescriptor WantAuthnRequestsSigned="true"

protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

<md:KeyDescriptor use="signing">

<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">

<X509Data>

<X509Certificate>MIIF1DCCA7ygAwIBAgIHC4Dr2wGTODMA…15lH8uDLHNp/ctEQ=</X509Certificate>

</X509Data>

</KeyInfo>

</md:KeyDescriptor>

<md:KeyDescriptor use="encryption">

<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">

<X509Data>

<X509Certificate>MIIF0jCCA7qgAwIBAgIHC4D4+…P4V2neBrOzAQWFo</X509Certificate>

</X509Data>

</KeyInfo>

<md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1\_5"/>

</md:KeyDescriptor>

<md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"

Location="https://web.dev1.foo.com/saml20/soap"

index="0"

isDefault="true"/>

<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"

Location="https://web.dev1.foo.com/saml20/slo"/>

<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"

Location="https://web.dev1.foo.com/saml20/slo"/>

<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"

Location="https://web.dev1.foo.com/saml20/soap"/>

<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>

<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>

<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>

<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:encrypted</md:NameIDFormat>

<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>

<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"

Location="https://web.dev1.foo.com/saml20/login"/>

<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"

Location="https://web.dev1.foo.com/saml20/login"/>

</md:IDPSSODescriptor>

<md:Organization>

<md:OrganizationName xml:lang="en">Foo Inc.</md:OrganizationName>

<md:OrganizationDisplayName xml:lang="en">Foo Inc.</md:OrganizationDisplayName>

<md:OrganizationURL xml:lang="en"/>

</md:Organization>

<md:ContactPerson contactType="technical">

<md:Company>Foo Inc.</md:Company>

<md:GivenName>John</md:GivenName>

<md:SurName>Doe</md:SurName>

<md:EmailAddress>john.doe@foo.com</md:EmailAddress>

<md:TelephoneNumber>4254166431</md:TelephoneNumber>

</md:ContactPerson>

</md:EntityDescriptor>

]]>

</Item>

</Metadata>

<InputClaims />

<OutputClaims>

<OutputClaim ClaimTypeReferenceId="AccessLevel" PartnerClaimType="accessLevel" />

<OutputClaim ClaimTypeReferenceId="AddressCity" PartnerClaimType="city" />

<OutputClaim ClaimTypeReferenceId="GivenName" PartnerClaimType="cn" />

<OutputClaim ClaimTypeReferenceId="Email" PartnerClaimType="email" />

<OutputClaim ClaimTypeReferenceId="Gender" PartnerClaimType="gender" />

<OutputClaim ClaimTypeReferenceId="MiddleName" PartnerClaimType="middleName" />

<OutputClaim ClaimTypeReferenceId="AddressZip" PartnerClaimType="postalCode" />

<OutputClaim ClaimTypeReferenceId="SurName" PartnerClaimType="sn" />

<OutputClaim ClaimTypeReferenceId="AddressState" PartnerClaimType="stateCode" />

<OutputClaim ClaimTypeReferenceId="AddressLine2" PartnerClaimType="streetAddressLine2" />

<OutputClaim ClaimTypeReferenceId="AddressLine1" PartnerClaimType="streetAddressLine1" />

<OutputClaim ClaimTypeReferenceId="UserId" PartnerClaimType="assertionSubjectName" />

</OutputClaims>

</TechnicalProfile>

1. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf [↑](#footnote-ref-1)
2. Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf [↑](#footnote-ref-2)
3. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf [↑](#footnote-ref-3)
4. Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf [↑](#footnote-ref-4)