Use SAML2 AuthnContextClassRef in IDP Proxy situations

A SAML request can include a RequestedAuthnContext containing one or more AuthnContextClassRef values, as a way to indicate in advance what class authentication method the application needs at run time. Similarly AuthnContextDeclRef can be used to select one specific method by reference name. This behaviour is defined in the SAML2 Core specifications.

If Ubisecure SSO is configured as an SAML2 IDP proxy, and the upstream IDP supports AuthnContextClassRef functionality, it is possible to make a choice of authentication method already at the Ubisecure SSO running in IDP Proxy configuration, or even from an SP using the Ubilogin SAML SP API.

To do this, it is necessary to configure one method (one SP) per desired AuthnContextClassRef.

eg

method1: AuthnContextClassRef is set to urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI

method2: AuthnContextClassRef is set to urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract

method3: AuthnContextClassRef is set to urn:oasis:names:tc:SAML:2.0:ac:classes:TextBasedChallengeResponse

The choice of AuthnContextClassRef can then be made by the end user at the IDP discovery page of the Ubilogin. Each type of AuthnContextClassRef will be seen as a button in the Proxy Methods login box.

An SP which trusts Ubisecure SSO as an IDP cannot make a selection using the upstream IDP's AuthnContextClassRef. Instead an SP must make selections using the AuthnContextDeclRef of the method at Ubisecure SSO.

The Authentication Context / Class Reference field of a SAML2 authentication method is sent to the upstream IDP.

The value overrides any value set at the SP initiating the request The Authentication Context / Class Reference field value can contain one or more AuthnContextClassRef values. A whitespace is used as the separator.

eg

If only two of many possible Class References are desired, set them like this:

method4: AuthnContextClassRef is set to "urn:oasis:names:tc:SAML:2.0:ac:classes:TextBasedChallengeResponse urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract"

The user must then in this case must make the selection between the two at the upstream IDP.

Related articles

Content by label

There is no content with the specified labels