SAML Compatibility Flags

Question

Which compatibility flags can be used for SAML messages?

Answer

Compatibility flags change default behaviour to support third-party systems. A list of compatibility flags for Ubisecure SSO 7.1 and SAML SP for Java 2.4.2 is (for older releases some of these might not be supported) presented below. Flags can be added for Ubisecure SSO and agents, multiple flags without comma like SigAlg ZLibHeader HttpPostResponseSign

ZLibHeader

Compatible with implementation using deflate compression with header

SigAlg

Compatible with implementation using incorrect SigAlg parameter values

HttpPostResponseSign

HTTP-Post: Response is NOT signed (IdentityProvider)

The enclosed Assertion is signed

HttpPostResponseValidate

HTTP-Post: Response signature is NOT required (ServiceProvider)(interop with ADFS)

The enclosed Assertion MUST be signed

SoapResponseSign

SOAP, SOAP/Artifact: Response is NOT signed (IdentityProvider)

SoapResponseValidate

SOAP, SOAP/Artifact: Response signature is NOT required (ServiceProvider)

The enclosed Assertion MUST be signed

SoapArtifactResponseSign

SOAP/Artifact: ArtifactResponse is NOT signed (ServiceProvider)

SoapArtifactResponseValidate

SOAP/Artifact: ArtifactResponse signature is NOT required (IdentityProvider)

SoapArtifactResolveSign

SOAP/Artifact: ArtifactResolve is NOT signed (ServiceProvider)

SoapArtifactResolveValidate

SOAP/Artifact: ArtifactResolve signature is NOT required (IdentityProvider)

AuthnRequestSign

AuthnRequest is NOT signed (ServiceProvider)

AuthnRequestValidate

AuthnRequest signature is NOT required (IdentityProvider)

WantAssertionsSignedFalse

HTTP-Post: Default value for WantAssertionsSigned is false (IdentityProvider)

MetadataCertificate

Metadata: publish public key embedded in a X.509 certificate structure

EncryptAES256

XML Encryption: use AES-256 algorithm while encrypting, default is AES-128

AssertionSignCertificate

Response/Assertion: always sign SAML Assertion and embed signer certificate with signature

SubjectConfirmationDataRecipient

SubjectConfirmationData/@Recipient: leave Recipient unassigned (interop with WIF)

AuthenticationContextDeclarationReference

AuthenticationContext/DeclarationReference: leave DeclarationReference unassigned (interop with WIF)

TokenTypeSAML11

RequestSecurityTokenResponse/RequestedSecurityToken/Assertion: use SAML 1.1 Token Type (interop with Sharepoint)

MessageDigestSHA256

Use SHA-256 digest algorithm (interop w. ADFS)

Added to Method SAML tab to enable signing of AuthnRequest messages and SAML response using RSAwithSHA256 algorithm

Required for Suomi.fi authentication service

IdpProxyDelegate

IDP-Proxy does NOT delegate AuthnRequest properties (IdentityProvider, ServiceProvider) (interop with ADFS)
For example, adding IdpProxyDelegate to the Method SAML tab will prevent sending of information about which actual application sent the original authentication request.

EncryptEmbedCertificate

XML Encryption: embed recipient encryption certificate with encrypted message

ExplicitNotBeforeCondition

Response/Assertion/Conditions/@notBefore: set conditions.notBefore to now() if not set otherwise(IdentityProvider)

NoBackChannel

Default profile, with back-channel features disabled.

Excludes: Artifact, SingleLogout/SOAP, AttributeService

Used to remove the requirement to open firewall connections for direct SP to IDP and IDP to SP conncetions.

Lite

IdP Lite or SP Lite mode

Excludes: ManageNameID, NameIDMapping, AttributeService endpoints from service

LiteNoBackChannel

IdP Lite or SP Lite, with back-channel features disabled.

Excludes: Artifact, SingleLogout/SOAP, ManageNameID, NameIDMapping, AttributeService endpoints from service.

Used to remove the requirement to open firewall connections for direct SP to IDP and IDP to SP conncetions.

Disables attribute query for ServiceProvider

SendAssertionConsumerServiceURL

Forces sending AssertionConsumerServiceURL in an outbound SAML2 Authentication Request. Some services require this optional element.

ExplicitUnspecifiedAuthnContextClassRef

Forces value *urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified* to AuthnContextClassRef in an outbound SAML2 Authentication Response. This is regardless of what might have been received in an inbound SAML2 Authentication Response. This improves compatibility with third-party applications and third-party identity providers which send different values than expected.

In all cases, negotiation between connected parties for agreed values for AuthnContextClassRef should be the first approach.

FinnishTrustNetwork (since SSO 8.3.4)

Forces sending the Finnish Trust Network SAML 2.0 Protocol Profile version 1.0 compliant SAML2 Extension `ftn`.

Currently supported extension tags:

- `lg`

DisableUsernameUserMapping (since 8.4.1)

Disables UsernameUserMapping if otherwise enabled. Can be set for server or method.

EnableUsernameUserMapping (since 8.4.1)

Enables UsernameUserMapping if otherwise disabled. Can be set for server or method.

Default in versions up to 8.4.X.

Related articles

- Use an unsolicited SSO or an IDP initiated SSO
- SAML Compatibility Flags
- How to log a user in based on an existing session
- 1. Accessing logs and adjusting logging levels of SSO and CustomerID
- Change hostname of Ubisecure SSO