Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF

Information Service Center WBF ISCeco

IAM WBF

Factsheet SAML 2.0 Web Browser SSO

Document name	IAM_WBF_-_Factsheet_SAML_2.0_Web_Browser_SSO_en.docx
Version	1.0.3
Status	Approved
Author(en)	Ludt Christian ISCECO (Ext.)
Publishing date	16.03.2018
Document-ID	COO.2101.105.3.119230

1 GENERAL RESTRICTIONS AND REQUIREMENTS

1.1 Supported Bindings

The following SAML 2.0 Bindings are currently supported:

- HTTP POST Binding (urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST)
- HTTP Redirect Binding (urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect) (only with signature)

1.2 Supported authentication methods

Wished or required authentication methods are specified with *AuthnContext* or *AuthnContextClassRef*, resp. (see http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf)

Authentication method	AuthnContextClassRef
Kerberos	urn.oasis.names.tc.SAML.2.0.ac.classes.Kerberos
Username and password	urn.oasis.names.tc.SAML.2.0.ac.classes.PasswordProtectedTransport
Username/password and SMS OTP	urn.oasis.names.tc.SAML.2.0.ac.classes.NomadTelephony
Software certificate	urn.oasis.names.tc.SAML.2.0.ac.classes.SoftwarePKI
Hardware certificate	urn.oasis.names.tc.SAML.2.0.ac.classes.SmartcardPKI

1.3 Supported NameID formats

- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
- urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
- urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos

Explicitly not supported is

- urn:oasis:names:tc:SAML:2.0:nameid-format:transient

1.4 RelayState support

Service providers (SP) can send some value to the Identity provider (IdP) within the RelayState URL parameter. The IdP will echo it back. The SP can use this data to maintain state (session) information.

1.5 Signing of AuthnRequests and AuthnResponses

AuthnRequests **MUST** be signed. AuthnResponses **MAY** be signed; the Assertion within the Response is signed.

1.6 Encryption

AuthnRequests **MUST NOT** be encrypted. AuthnResponses are not encrypted.

2 REQUIREMENTS ON SAML SIGNER CERTIFICATES

2.1 Key length

The key length of the asymmetric certificate key **MUST** be at least 2048 Bit.

2.2 Issuing CA of the X.509 Certificates

There is currently no restriction or requirement on the issuing certificate authority.

2.3 Requirements on the key usage (keyusage flag)

The certificate used for signing the SAML 2.0 authentication requests MUST be issued for the purpose of the creation of digital signatures (the *digitalSignature flag* **MUST** be set).

2.4 Requirements on the validity period

There is currently no restriction or requirement on the validity period of the certificate used for signing the SAML 2.0 authentication requests.

3 AUTHNREQUEST

3.1 Specifying the Assertion Consumer Service (ACS) URL

The Assertion Consumer Service URL **MUST** be specified as URL in the AuthnRequest (*AssertionConsumerServiceURL*) and not as *AssertionConsumerServiceIndex* (see example, line 4).

3.2 Destination

The destination **MUST** equal the endpoint URL of the IdP's SSO services. The URL is provide by the IdP operator or service owner (see example, line 5).

3.3 IssueInstant

IssueInstant **MUST** equal the exact point in time when the authentication request is issued (see example, line 7).

3.4 NameID policy

Any NameID policy provided at runtime will be ignored. The policy is defined at integration time (see example, line 15).

3.5 Conditions

The AuthnRequest **MAY** contain *Conditions*. However, any requested validity period will be ignored.

The validity period in the Conditions does not specify the validity period of the authentication request but the period of the assertion to be issued (see example, line 19).

3.6 AuthnContext

The AuthnContext contains information about how the user shall authenticate against an IdP or how the IdP shall authenticate the user, resp. (see 1.2). If the AuthnContext is specified, the user will only be offered those authentication methods provided in the AuthnContext.

If the AuthnContext is not specified, the IdP provides all available authentication methods to the user (this is for backwards compatibility only).

See example, line 25.

3.7 Example

```
<saml2p:AuthnRequest
    xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    AssertionConsumerServiceURL="https://www.example.com/saml/2.0/acs/"
    Destination="https://idp-kerb.iam.isceco.admin.ch/IDP/"
    ID="121ed47297400dc1426af99750f3801b97c04df8"
    IssueInstant="2017-11-16T15:03:12.130Z"
    Version="2.0">
    <saml2:Issuer>www.example.com</saml2:Issuer>
    <!-- mandatory signature -->
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ...
    </ds:Signature>
    <!-- being ignored -->
    <samlp:NameIDPolicy
        AllowCreate="true"
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
    <!-- being ignored -->
    <saml2:Conditions NotBefore="2017-11-16T15:03:12.130Z"
                      NotOnOrAfter="2017-11-16T15:08:12.130Z"
                      xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"/>
    <saml2p:RequestedAuthnContext Comparison="exact">
        <!-- Restricts the authentication to Kerberos -->
        <saml2:AuthnContextClassRef
            xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
            urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
        </saml2:AuthnContextClassRef>
    </saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>
```

4 AUTHNRESPONSE

4.1 Assertion

4.1.1 NameID (format)

The NameID format will be the format defined at integration time (see 1.3 and 3.4).

4.1.2 Conditions

The SAML assertion contains information about the assertion's validity period.

Per default, the validity period is set to 5 minutes. Extension of the period can be granted in agreement with the person responsible for information security.

4.1.3 Signature

The SAML assertion within the SAML 2.0 authentication response is signed. The signer's public certificate is provided within the assertion.

4.1.4 Audience Restriction

Per default, the assertion's audience restriction is set to the Assertion Consumer Service (ACS) URL. A different audience must be requested at integration time.

4.1.5 AuthnContext

The SAML assertion within the SAML 2.0 authentication response contains information about the actual authentication method (see 1.2 and 3.6). The SP can use this information to determine the authentication strength.

4.2 Example

```
<saml2p:Response
    xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    Destination="https://www.example.com/saml/2.0/acs/"
    ID="Response_51cdfd9396396dee87038054caff5e6f5266803a"
    InResponseTo="121ed47297400dc1426af99750f3801b97c04df8"
    IssueInstant="2017-11-16T15:03:13.570Z"
    Version="2.0">
    <saml2:Issuer>https://idp-kerb.iam.isceco.admin.ch/IDP/</saml2:Issuer>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </saml2p:Status>
    <saml2:Assertion
        ID="Assertion_08ab4f5171e2a9bfd40b2e89c0769166ecda1dd0"
        IssueInstant="2017-11-16T15:03:13.570Z"
        Version="2.0"
        xmlns:xs="http://www.w3.org/2001/XMLSchema">
        <saml2:Issuer>https://idp-kerb.iam.isceco.admin.ch/IDP/</saml2:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            ...
        </ds:Signature>
        <saml2:Subject>
            <saml2:NameID
                Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
                christian.ludt@isceco.admin.ch
            </saml2:NameID>
            <saml2:SubjectConfirmation
                Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml2:SubjectConfirmationData
                    InResponseTo="121ed47297400dc1426af99750f3801b97c04df8"
                    NotOnOrAfter="2017-11-16T15:08:13.571Z"
                    Recipient="https://wiki.isceco.admin.ch/simplesaml/module.php/
saml/sp/saml2-acs.php/wiki"/>
            </saml2:SubjectConfirmation>
        </saml2:Subject>
        <saml2:Conditions
            NotBefore="2017-11-16T15:08:13.570Z"
            NotOnOrAfter="2017-11-16T15:13:13.570Z">
            <saml2:AudienceRestriction>
                <saml2:Audience>
                    https://www.example.com/saml/2.0/acs/
                </saml2:Audience>
            </saml2:AudienceRestriction>
        </saml2:Conditions>
        <saml2:AuthnStatement
            AuthnInstant="2017-11-16T15:08:13.570Z"
            SessionIndex="Assertion_08ab4f5171e2a9bfd40b2e89c0769166ecda1dd0">
            <saml2:AuthnContext>
                <saml2:AuthnContextClassRef>
                    urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
                </saml2:AuthnContextClassRef>
            </saml2:AuthnContext>
        </saml2:AuthnStatement>
```

```
        <saml2:AttributeStatement>
            <saml2:Attribute Name="displayName">
                <saml2:AttributeValue
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                    xsi:type="xs:string">
                    Ludt Christian ISCeco
                </saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="mail">
                <saml2:AttributeValue
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                    xsi:type="xs:string">
                    christian.ludt@isceco.admin.ch
                </saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="roles">
                <saml2:AttributeValue
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                    xsi:type="xs:string">
                    ExampleApplication.Role1
                </saml2:AttributeValue>
            </saml2:Attribute>
        </saml2:AttributeStatement>
    </saml2:Assertion>
</saml2p:Response>
```

5 INTEGRATION

5.1 Information to be provided by the SP

All information is needed at integration time.

5.1.1 Issuer

Issuer as it will be used in the SAML 2.0 authentication request.

String that uniquely identifies the application and the environment (stage) (e.g. development, test, production etc.).

5.1.2 SAML signer certificate

The certificate being used to verify the SAML 2.0 authentication request's signature. Each environment (stage) **MUST** use its own SAML signer key and certificate. The certificate's subject **SHOULD** equal the Issuer from 5.1.1.

5.1.3 Required Attributes

The service provider (the business application) **MUST** define which user attributes are required. Depending on the nature of the attributes or the person responsible for the attributes, the attributes **MUST** be requested at the appropriate authority.

5.1.4 Audience Restriction (optional)

Per default, the SAML assertion's audience restriction is set to the Assertion Consumer Service (ACS) URL that is defined at integration time. If a different URI is required, it can be requested at integration time and it must adhere to RFC 3986[1].

[1] https://www.ietf.org/rfc/rfc3986.txt

5.2 Information to be provided by the IdP

The IdP provides the following information within a SAML IdP metadata file:

5.2.1 NameID format

The nameID's format according to 1.3 and 3.4.

5.2.2 Supported Bindings

- HTTP POST Binding (urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST)
- HTTP Redirect Binding (urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect)

5.2.3 Single Sign-On (SSO) Service URL

URL that MUST be used as destination within the authentication request.

5.2.4 SAML Signer certificate

Public certificate to be used to verify the SAML assertions signature.