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

Dokumentname	IAM_WBF_-_Factsheet_SAML_2.0_Web_Browser_SSO_de_v1.0.3.docx
Version	1.0.3
Status	Genehmigt zur Nutzung
Author(en)	Ludt Christian ISCECO (Ext.)
Ausgabedatum	16.03.2018
Dokument-ID	COO.2101.105.3.119236

1 ALLGEMEINE RESTRIKTIONEN UND ANFORDERUNGEN

1.1 Unterstützte Bindings

Es werden aktuell folgende SAML 2.0 Bindings akzeptiert:

- 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) (nur mit Signatur)

1.2 Unterstützte Authentifizierungsverfahren

Authentifizierungsverfahren werden über *AuthnContext* bzw. *AuthnContextClassRef* spezifiziert (siehe http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf)

Verfahren	AuthnContextClassRef
Kerberos	urn.oasis.names.tc.SAML.2.0.ac.classes.Kerberos
Benutzername und Passwort	urn.oasis.names.tc.SAML.2.0.ac.classes.PasswordProtectedTransport
Benutzername/Passwort und SMS-OTP	urn.oasis.names.tc.SAML.2.0.ac.classes.NomadTelephony
Soft-Zertifikat	urn.oasis.names.tc.SAML.2.0.ac.classes.SoftwarePKI
Zertifikat auf Hardtokens	urn.oasis.names.tc.SAML.2.0.ac.classes.SmartcardPKI

1.3 Unterstütze NameID-Formate

- 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

Explizit nicht unterstützt wird

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

1.4 Unterstützung des RelayStates

Service Provider (SP) **KÖNNEN** unter dem URL-Parameter *RelayState* ein Token mitgeben, das eine Referenz auf eine Session-Information ist, die vom Service Provider verwaltet wird.

1.5 Signieren der AuthnRequests und AuthnResponses

AuthnRequests **MÜSSEN** signiert sein. AuthnResponses **KÖNNEN** signiert sein, Assertions in der Response **sind** signiert.

1.6 Verschlüsselung

AuthnRequests **DÜRFEN NICHT** verschlüsselt sein. AuthnResponses sind nicht verschlüsselt.

2 ANFORDERUNGEN AN SAML-SIGNER-ZERTIFIKATE

2.1 Anforderung an die Schlüssellänge

Die Schlüssellänge der asymmetrischen Zertifikatsschlüssel **MUSS** mindestens 2048 Bit betragen.

2.2 Anforderung an die ausgebende CA des X.509-Zertifikats

Aktuell gibt es keine Anforderungen an die ausgebende CA.

2.3 Anforderung an den Verwendungszweck (keyusage)

Das für die Signatur des SAML 2.0-AuthnRequests verwendete Zertifikat **MUSS** für den Verwendungszweck des Erstellens digitaler Signaturen von der Zertifizierungsstelle ausgestellt sein (das *digitalSignature*-Flag **MUSS** gesetzt sein).

2.4 Anforderungen an die Gültigkeitsdauer

Aktuell gibt es keine Anforderungen an die Gültigkeitsdauer des für das Signieren des SAML 2.0-AuthnRequests verwendeten Zertifikats.

3 AUTHNREQUEST

3.1 Spezifikation der Assertion Consumer Service (ACS) URL

Die Assertion Consumer Service URL **MUSS** als URL im AuthnRequest spezifiziert werden (*AssertionConsumerServiceURL*) und nicht über *AssertionConsumerServiceIndex* (siehe Beispiel Zeile 4).

3.2 Destination

Die Destination **MUSS** den Wert des SSO-Services (URL) des IdPs haben. Die URL wird vom IDP-Betreiber geliefert (siehe Beispiel Zeile 5).

3.3 IssueInstant

Der *IssueInstant* **MUSS** auf den exakten Zeitpunkt, an dem der AuthnRequest ausgestellt wird, gesetzt sein (siehe Beispiel Zeile 7).

3.4 NameID-Policy

Angaben in der NameID-Policy zur Laufzeit werden ignoriert. Das Format der NameID wird bei der Integration festgelegt (siehe Beispiel Zeile 15).

3.5 Conditions

Der AuthnRequest **KANN** das Element *Conditions* enthalten. Die darin angeforderte Gültigkeitsdauer der Assertion wird jedoch nicht berücksichtigt für die Ausstellung der Assertion.

Die Gültigkeitsdauer spezifiziert nicht die Gültigkeitsdauer des AuthnRequests sondern der auszustellenden Assertion (siehe Beispiel Zeile 19).

3.6 AuthnContext

Der AuthnContext enthält Informationen darüber, wie die Authentifizierung des Benutzers auf dem Identity Provider (IdP) durchzuführen ist (siehe 1.2). Wird der AuthnContext spezifiziert,

werden dem Benutzer nur die durch den AuthnContext spezifizierten Login-Möglichkeiten angeboten.

Wird der AuthnContext nicht spezifiziert, werden alle vom IdP angebotenen Authentisierungen zugelassen.

Siehe Beispiel Zeile 25.

3.7 Beispiel

```
<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>
    <!-- Zwingend notwendige Signatur -->
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ...
    </ds:Signature>
    <!-- wird ignoriert -->
    <samlp:NameIDPolicy
        AllowCreate="true"
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
    <!-- wird ignoriert -->
    <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">
        <!-- Besagt, dass nur Kerberos als Authentisierungs-Möglichkeit zugelassen
ist -->
        <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)

Das NameID-Format ist das bei der Integration festgelegte Format (siehe 1.3 und 3.4) (siehe Beispiel Zeile 24).

4.1.2 Conditions

Die in der SAML 2.0-AuthnResponse enthaltene SAML-Assertion enthält Informationen zur Gültigkeitsdauer der Assertion (siehe Beispiel Zeile 37 und 38).

Die Gültigkeitsdauer der Assertion ist standardmässig auf 5 Minute gesetzt. Eine längere Gültigkeitsdauer kann in Absprache mit den Verantwortlichen der Informationssicherheit gewährt werden.

4.1.3 Signatur

Die in der SAML 2.0-AuthnResponse enthaltene SAML-Assertion (das SAML-Token) ist signiert. Das öffentliche Zertifikat wird in den jeweiligen XML-Strukturen mitgeliefert.

4.1.4 Audience Restriction

Die Audience Restriction der Assertion wird default-mässig auf die Assertion Consumer Service (ACS)-URL gesetzt. Wird eine andere URI gewünscht, ist dies explizit zu beantragen (siehe Beispiel Zeile 41).

4.1.5 AuthnContext

Die in der SAML 2.0-AuthnResponse enthaltene SAML-Assertion (das SAML-Token) enthält im AuthnContext das verwendete Authentifizierungsverfahren (siehe 1.2 und 3.6). Anhand des AuthnContextes kann der SP erkennen, wie stark sich ein Benutzer authentisiert hat bzw. wie stark er authentifiziert wurde (siehe Beispiel Zeile 50).

4.2 Beispiel

```
1  <saml2p:Response
2      xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
3      xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
4      Destination="https://www.example.com/saml/2.0/acs/"
5      ID="Response_51cdfd9396396dee87038054caff5e6f5266803a"
6      InResponseTo="121ed47297400dc1426af99750f3801b97c04df8"
7      IssueInstant="2017-11-16T15:03:13.570Z"
8      Version="2.0">
9      <saml2:Issuer>https://idp-kerb.iam.isceco.admin.ch/IDP/</saml2:Issuer>
10     <saml2p:Status>
11         <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
12     </saml2p:Status>
13     <saml2:Assertion
14         ID="Assertion_08ab4f5171e2a9bfd40b2e89c0769166ecda1dd0"
15         IssueInstant="2017-11-16T15:03:13.570Z"
16         Version="2.0"
17         xmlns:xs="http://www.w3.org/2001/XMLSchema">
18         <saml2:Issuer>https://idp-kerb.iam.isceco.admin.ch/IDP/</saml2:Issuer>
19         <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
20             ...
21         </ds:Signature>
22         <saml2:Subject>
23             <saml2:NameID
24                 Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
25                 christian.ludt@isceco.admin.ch
26             </saml2:NameID>
27             <saml2:SubjectConfirmation
28                 Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
29                 <saml2:SubjectConfirmationData
30                     InResponseTo="121ed47297400dc1426af99750f3801b97c04df8"
31                     NotOnOrAfter="2017-11-16T15:08:13.571Z"
32                     Recipient="https://wiki.isceco.admin.ch/simplesaml/module.php/
33 saml/sp/saml2-acs.php/wiki"/>
34             </saml2:SubjectConfirmation>
35         </saml2:Subject>
36         <saml2:Conditions
37             NotBefore="2017-11-16T15:08:13.570Z"
38             NotOnOrAfter="2017-11-16T15:13:13.570Z">
39             <saml2:AudienceRestriction>
40                 <saml2:Audience>
41                     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 Vom SP zu liefernde Angaben

5.1.1 Issuer

Issuer, wie er im SAML 2.0-AuthnRequest verwendet wird.

String, der die Applikation und die Umgebung (bspw. Entwicklung, Test, Produktion) eindeutig definiert.

5.1.2 SAML-Signer-Zertifikat

Das öffentliche Zertifikat, das zum Signieren des SAML 2.0-AuthnRequests verwendet wird. Es **MUSS** für jede Umgebung ein eigenes SAML-Signer-Zertifikat verwendet werden. Der Antragsteller (Subject) des Zertifikats **SOLL** mit dem Issuer aus 5.1.1 übereinstimmen.

5.1.3 Zurückzuliefernde Attribute

Der anzubindende Service Provider (die anzubindende Applikation) **MUSS** angeben, welche Attribute eines Benutzers er benötigt. Gegebenenfalls sind die Attribute bei einer zu bewilligenden Stelle zu beantragen.

5.1.4 Audience Restriction (optional)

Die Audience Restriction der SAML-Assertion wird default-mässig auf die Assertion Consumer Service (ACS)-URL gesetzt. Wird eine andere URI gewünscht, ist dies explizit zu beantragen. Die URI muss konform mit RFC 3986[1] sein.

5.2 Vom IDP zu liefernde Angaben

Der IDP stellt die folgenden Angaben in Form einer SAML-IDP-Metadaten-Datei bereit:

5.2.1 NameID-Format

Das Format, in dem die nameID geliefert wird. Siehe 1.3 und 3.4.

5.2.2 Unterstützte 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) (nur mit Signatur)

5.2.3 Single Sign-On (SSO) Service-URL

URL, die im AuthnRequest als Destination anzugeben ist.

5.2.4 SAML-Signer-Zertifikat

Öffentliches Zertifikat, mit dem die SAML-Assertion signiert ist.

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