Metadata

Ahhoz, hogy a föderációban résztvevő entitások biztonságosan tudjanak kommunikálni egymással, szükség van egy metaadat állományra. Ez a metaadat állomány szinte mindig humán felügyelettel jön létre, mivel a szervezetek közötti bizalmi kapcsolat technikai leképzésének ez az elsődleges eleme. (Másodlagos leképzésnek nevezhetjük az attribútum policy IdP és SP oldali megvalósítását.)

SAML 2.0 metaadatok

Pontos szabvány: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

A metadata állomány az alábbi fontosabb információkat tartalmazza

- Érvényesség, aláírás
- Identity Providerek
- Attribute authorityk
- Service Providerek
- IdP-k és SP-k tanúsítványai
- IdP-khez és SP-khez kapcsolódó szervezeti és kontakt információk

Metadata érvényesége és hitelessége

IdP

AA

SP

Tanúsítványok

Kontakt információk

Példák

Egy IdP-hez tartozó metadata

A meglehetősen komplex eseteket leszámítva általában az Identity Provider és az Attribute Authority egyetlen entitásként kezelhető.

```
<EntityDescriptor entityID="https://idp.niif.hu/shibboleth">


        <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol
urn:mace:shibboleth:1.0">
                <Extensions>
                        <shibmd:Scope>niif.hu</shibmd:Scope>
                </Extensions>
                <KeyDescriptor use="signing">
                    <ds:KeyInfo>
                        <ds:X509Data>
                                <ds:X509Certificate>
MIIFAzCCA+ugAwIBAgICAl8wDQYJKoZIhvcNAQEFBQAwVTELMAkGA1UEBhMCSFUx
DTALBgNVBAoTBE5JSUYxIDAeBgNVBAsTF0NlcnRpZmljYXRlIEF1dGhvcml0aWVz
MRUwEwYDVQQDEwxOSUlGIFJvb3QgQ0EwHhcNMDcwMzMwMTA0OTQ5WhcNMDgwMzI5
MTA0OTQ5WjCB1zELMAkGA1UEBhMCSFUxEDAOBgNVBAoTB05JSUYgQ0ExEDAOBgNV
BAgTB0h1bmdhcnkxETAPBgNVBAcTCEJ1ZGFwZXN0MUIwQAYDVQQKEzlOYXRpb25h
bCBJbmZvcm1hdGlvbiBJbmZyYXN0cnVjdHVyZSBEZXZlbG9wbWVudCBJbnN0aXR1
dGUxFzAVBgNVBAsTDldlYnNlcnZlciBUZWFtMRQwEgYDVQQDEwtpZHAubmlpZi5o
dTEeMBwGCSqGSIb3DQEJARYPcG9sYWtvdmlAaWlmLmh1MIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQDFuOD6yq3NlMaQoR6qyRlET1WyGT+hllH+1qXIHHwag2gL
KYByQpBXPva3uSsswn3Rjmv2G/9ifX8sUadflM/MDoCLRoq9umJkcwmOHEp1fMfa
7Gx9isEeVNYO0taN9Lol5EQL6rdZMSmwAZ17DCTNs48tPdzm7ys5EOe+bHHA3wID
AQABo4IB3DCCAdgwEQYJYIZIAYb4QgEBBAQDAgZAMA4GA1UdDwEB/wQEAwIE8DAa
BgNVHREEEzARgQ9wb2xha292aUBpaWYuaHUwggFZBgNVHR8EggFQMIIBTDCBvKBb
oFmkVzBVMQswCQYDVQQGEwJodTENMAsGA1UEChMETklJRjEgMB4GA1UECxMXQ2Vy
dGlmaWNhdGUgQXV0aG9yaXRpZXMxFTATBgNVBAMTDE5JSUYgUm9vdCBDQYECAN6i
WaRXMFUxCzAJBgNVBAYTAmh1MQ0wCwYDVQQKEwROSUlGMSAwHgYDVQQLExdDZXJ0
aWZpY2F0ZSBBdXRob3JpdGllczEVMBMGA1UEAxMMTklJRiBSb290IENBMIGKoCmg
J4YlaHR0cDovL3d3dy5jYS5uaWlmLmh1L25paWYtY2EtY3JsLmNybIECAN6iWaRX
```

```
MFUxCzAJBgNVBAYTAmh1MQ0wCwYDVQQKEwROSUlGMSAwHgYDVQQLExdDZXJ0aWZp
Y2F0ZSBBdXRob3JpdGllczEVMBMGA1UEAxMMTklJRiBSb290IENBMB8GA1UdIwQY
MBaAFIxuIeJxr6Aqp7Dk/rx+o/0PoOOIMBkGA1UdIAQSMBAwDgYMKwYBBAHdCgEB
DAEAMA0GCSqGSIb3DQEBBQUAA4IBAQB262jS0aGJZrOg1Q6IVSodTnokgliojgWy
1FAojS6ML0w7T0eA1PnqX42eSfQFB2Nh71dBUmw6i++iHdQ1gyxOHIelSDb4JFOB
PoZ+3flwySXu42QgVjJZ46fEMsq2EM0PQV8p9pgBEjlG+6ifAEgJmKBnP+WCzQJ7
3rugtu+q8KKQ0oxP0bWLYGllJ6tKLa4gJ1P/oLe6uX+GWP+P3bZfMpOq9Tu2MU+r
l/gnG2rTSOBe7AEngRmeDfKKeFiSsg1cGxorxQJoEzBZksKUa0nlA9xtd30sUQFX
OI2/Xo2ihYFcpzu551S6+mutZNHqKgOT7uID/TCHr5R0Q1h7CPCS
                              </ds:X509Certificate>
                         </ds:X509Data>
                    </ds:KeyInfo>
                </KeyDescriptor>
                <ArtifactResolutionService index="1"
                        Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
                        Location="https://idp.niif.hu:8443/shibboleth-idp/Artifact"/>
                <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
                <SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"
                                     Location="https://idp.niif.hu/shibboleth-idp/SSO"/>
        </IDPSSODescriptor>

        <AttributeAuthorityDescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">
                <Extensions>
                        <!-- This is a Shibboleth extension to express attribute scope rules.
-->
                        <shibmd:Scope>niif.hu</shibmd:Scope>
                </Extensions>
                <KeyDescriptor use="signing">
                    <ds:KeyInfo>
                        <ds:X509Data>
                                <ds:X509Certificate>
MIIFAzCCA+ugAwIBAgICAl8wDQYJKoZIhvcNAQEFBQAwVTELMAkGA1UEBhMCSFUx
DTALBgNVBAoTBE5JSUYxIDAeBgNVBAsTF0NlcnRpZmljYXRlIEF1dGhvcml0aWVz
MRUwEwYDVQQDEwxOSUlGIFJvb3QgQ0EwHhcNMDcwMzMwMTA0OTQ5WhcNMDgwMzI5
MTA0OTQ5WjCB1zELMAkGA1UEBhMCSFUxEDAOBgNVBAoTB05JSUYgQ0ExEDAOBgNV
BAgTB0h1bmdhcnkxETAPBgNVBAcTCEJ1ZGFwZXN0MUIwQAYDVQQKEzlOYXRpb25h
bCBJbmZvcm1hdGlvbiBJbmZyYXN0cnVjdHVyZSBEZXZlbG9wbWVudCBJbnN0aXR1
dGUxFzAVBgNVBAsTDldlYnNlcnZlciBUZWFtMRQwEgYDVQQDEwtpZHAubmlpZi5o
dTEeMBwGCSqGSIb3DQEJARYPcG9sYWtvdmlAaWlmLmh1MIGfMA0GCSqGSIb3DQEB
```

```
AQUAA4GNADCBiQKBgQDFuOD6yq3NlMaQoR6qyRlET1WyGT+hllH+1qXIHHwag2gL
KYByQpBXPva3uSsswn3Rjmv2G/9ifX8sUadflM/MDoCLRoq9umJkcwmOHEp1fMfa
7Gx9isEeVNYO0taN9Lol5EQL6rdZMSmwAZ17DCTNs48tPdzm7ys5EOe+bHHA3wID
AQABo4IB3DCCAdgwEQYJYIZIAYb4QgEBBAQDAgZAMA4GA1UdDwEB/wQEAwIE8DAa
BgNVHREEEzARgQ9wb2xha292aUBpaWYuaHUwggFZBgNVHR8EggFQMIIBTDCBvKBb
oFmkVzBVMQswCQYDVQQGEwJodTENMAsGA1UEChMETklJRjEgMB4GA1UECxMXQ2Vy
dGlmaWNhdGUgQXV0aG9yaXRpZXMxFTATBgNVBAMTDE5JSUYgUm9vdCBDQYECAN6i
WaRXMFUxCzAJBgNVBAYTAmh1MQ0wCwYDVQQKEwROSUlGMSAwHgYDVQQLExdDZXJ0
aWZpY2F0ZSBBdXRob3JpdGllczEVMBMGA1UEAxMMTklJRiBSb290IENBMIGKoCmg
J4YlaHR0cDovL3d3dy5jYS5uaWlmLmh1L25paWYtY2EtY3JsLmNybIECAN6iWaRX
MFUxCzAJBgNVBAYTAmh1MQ0wCwYDVQQKEwROSUlGMSAwHgYDVQQLExdDZXJ0aWZp
Y2F0ZSBBdXRob3JpdGllczEVMBMGA1UEAxMMTklJRiBSb290IENBMB8GA1UdIwQY
MBaAFIxuIeJxr6Aqp7Dk/rx+o/0PoOOIMBkGA1UdIAQSMBAwDgYMKwYBBAHdCgEB
DAEAMA0GCSqGSIb3DQEBBQUAA4IBAQB262jS0aGJZrOg1Q6IVSodTnokgliojgWy
1FAojS6ML0w7T0eA1PnqX42eSfQFB2Nh71dBUmw6i++iHdQ1gyxOHIelSDb4JFOB
PoZ+3flwySXu42QgVjJZ46fEMsq2EM0PQV8p9pgBEjlG+6ifAEgJmKBnP+WCzQJ7
3rugtu+q8KKQ0oxP0bWLYGllJ6tKLa4gJ1P/oLe6uX+GWP+P3bZfMpOq9Tu2MU+r
l/gnG2rTSOBe7AEngRmeDfKKeFiSsg1cGxorxQJoEzBZksKUa0nlA9xtd30sUQFX
OI2/Xo2ihYFcpzu551S6+mutZNHqKgOT7uID/TCHr5R0Q1h7CPCS
                                </ds:X509Certificate>
                            </ds:X509Data>
                        </ds:KeyInfo>
                </KeyDescriptor>
                <AttributeService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
                                  Location="https://idp.niif.hu:8443/shibboleth-idp/AA"/>

                <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
        </AttributeAuthorityDescriptor>

</EntityDescriptor>
```

Egy SP-hez tartozó metadata

```
<EntityDescriptor entityID="https://rrd-ma.perfsonar.vh.hbone.hu/shibboleth">
        <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">
                <KeyDescriptor use="signing">
                    <ds:KeyInfo>
                        <ds:X509Data>
                                <ds:X509Certificate>
```

```
MIIEmjCCA4KgAwIBAgICArwwDQYJKoZIhvcNAQEFBQAwVTELMAkGA1UEBhMCSFUx
DTALBgNVBAoTBE5JSUYxIDAeBgNVBAsTF0NlcnRpZmljYXRlIEF1dGhvcml0aWVz
MRUwEwYDVQQDEwxOSUlGIFJvb3QgQ0EwHhcNMDcxMTMwMTMwNzE4WhcNMDgxMTI5
MTMwNzE4WjBvMQswCQYDVQQGEwJIVTEQMA4GA1UEChMHTklJRiBDQTEOMAwGA1UE
CxMFSEJPTkUxFzAVBgNVBAsTDldlYnNlcnZlciBUZWFtMSUwIwYDVQQDExxycmQt
bWEucGVyZnNvbmFyLnZoLmhib25lLmh1MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQC2x6Hpjr4yB6EDkXUHNMlHz250kqWBXf/UI6TziV5rvMjvS8pdFnsZcIt1
coT03Fu4wzs6N8gtC5uW7f3JaBsG32sYZUorWcbecpgVy5ttcIqTM1RnxUsOktsM
RuBz7qYAQ1/B9VvBH7P7DeREgIGm7Skel/Q3Qhl4oG9PtFe1wQIDAQABo4IB3DCC
AdgwEQYJYIZIAYb4QgEBBAQDAgbAMA4GA1UdDwEB/wQEAwIE8DAaBgNVHREEEzAR
gQ9wb2xha292aUBpaWYuaHUwggFZBgNVHR8EggFQMIIBTDCBvKBboFmkVzBVMQsw
CQYDVQQGEwJodTENMAsGA1UEChMETklJRjEgMB4GA1UECxMXQ2VydGlmaWNhdGUg
QXV0aG9yaXRpZXMxFTATBgNVBAMTDE5JSUYgUm9vdCBDQYECAN6iWaRXMFUxCzAJ
BgNVBAYTAmh1MQ0wCwYDVQQKEwROSUlGMSAwHgYDVQQLExdDZXJ0aWZpY2F0ZSBB
dXRob3JpdGllczEVMBMGA1UEAxMMTklJRiBSb290IENBMIGKoCmgJ4YlaHR0cDov
L3d3dy5jYS5uaWlmLmh1L25paWYtY2EtY3JsLmNybIECAN6iWaRXMFUxCzAJBgNV
BAYTAmh1MQ0wCwYDVQQKEwROSUlGMSAwHgYDVQQLExdDZXJ0aWZpY2F0ZSBBdXRo
b3JpdGllczEVMBMGA1UEAxMMTklJRiBSb290IENBMB8GA1UdIwQYMBaAFIxuIeJx
r6Aqp7Dk/rx+o/0PoOOIMBkGA1UdIAQSMBAwDgYMKwYBBAHdCgEBCQEAMA0GCSqG
SIb3DQEBBQUAA4IBAQAVuG4+KUxQZcYCedQmW6Ih83gqMS7inxfBFeadc4Ts1egY
Wf6Y4CoEOrsdI7FmC7CCccarDaMC6PVJg1WlDV01LMGM2+6rcoMeMs/J5pCFTDhn
c6MPz6KedRcMvVJajY+BZvJPG9CNpyxdiUf/aDa28yRryVM0Jbm6BOFH+UrVHlVw
w2JxlmsHtk1fNmEU7gluzwo3FEZrx8nnLWkeTfMzz/iM+dudNm4sL99uGNEWGNFf
tLi+R35McE7CfyNNfOvlskZX++dSX/Re8CERTo3wZrHmFKIoOnJzo6v48d2tEbw0
a15Yl93MJCNlC5BUyvUMqKDLmHhTxmgO+HIaV7Kf
                                </ds:X509Certificate>
                            </ds:X509Data>
                        </ds:KeyInfo>
                    </KeyDescriptor>

                    <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>

                    <AssertionConsumerService index="1" isDefault="true"
                            Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"
                            Location="https://rrd-
ma.perfsonar.vh.hbone.hu/Shibboleth.sso/SAML/Artifact"/>
                    <AssertionConsumerService index="2"
                            Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"
                            Location="https://rrd-
```

```
ma.perfsonar.vh.hbone.hu/Shibboleth.sso/SAML/POST"/>
        </SPSSODescriptor>
</EntityDescriptor>
```

Shibboleth 1.3

A Shibboleth (mind az SP, mind az IdP) a metaadatokat kizárólag a másik féllel kapcsolatban használja, tehát a saját konfigurációjával kapcsolatban figyelmen kívül hagyja.

Az 1.3-as verzió kizárólag lokális állományokkal dolgozik (ez változni fog a 2.0-ban).

Scope

A Shibboleth 1.3 kiterjesztette a SAML2 metadata struktúrát egy saját, `Scope` mezővel. Ez a "scope" igazából egy *postfix* tagot definiál, melynek segítségével bizonyos attribútumok értelmezési helye jól meghatározható.

Erre jó példa az `eduPersonPrincipalName` attribútum, mely a felhasználó egyedi azonosítóját adja meg. Ez az azonosító két részből áll:

- egy intézményen belüli egyedi azonosítóból (pl. `bajnokk`)
- az intézmény azonosítójából, a scope-ból (pl. `niif.hu`)

Ha a metadatában használjuk a `Scope` mezőt, akkor az SP ellenőrizni tudja, hogy az IdP jogosult-e ilyen scope-pal rendelkező attribútumot kiadni.

Szintén gyakran használt scope-os attribútum az `eduPersonScopedAffiliation`.

Metadata eszközök

- Metadatatool
- Siterefresh

Több metadata állomány használata

Mind az IdP, mind az SP képes arra, hogy több metadata állományt használjon. Így például különvehetjük az SP-ket az IdP-ktől, ill. több föderációban lehet benne a provider.

A metadata állományok tartalma összeadódik.

Figyelem

Ugyanaz az `entityId` (más néven [[providerId]]) nem szerepelhet többször! Az `entityId`-knek az összes használt metadata állományra nézve egyedinek kell lennie.

Metadata állományok frissítése

A metadata állományok központi helyről való letöltésére a Siterefresh és a Metadatatool eszközök valók.

Az átszerkesztett/új metadata állományt mind az IdP, mind az SP automatikusan beolvassa, újraindítás nem szükséges.

Nem SAML 2.0 metaadatokat használó alkalmazások

simpleSAMLphp

Az újabb verziók már támogatják az XML formátumú metaadatokat, de az SSP moduljai szeretik még mindig a flatfile formátumot használni. Van egy *metarefresh* nevű modul, ami képes webről leszedni a metaadatokat, ellenőrizni az aláírást, és flatfile formátumú metaadatokat generálni. Fontos momentum, hogy figyelembe veszi a `*<RequestedAttribute>*` elementet, ezáltal megoldható az IdP-k attribútum kiadási szabályzatának automatikus frissítése is.

A szócikk vagy fejezet még megírásra vár

Switch WAYF

A szócikk vagy fejezet még megírásra vár

Változat #3
cziernorbert hozta létre 2026-04-14 13:22:03 CEST
cziernorbert frissítette 2026-04-17 13:00:16 CEST