

# 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
DTALBgNVBAoTBTE5JSUYxIDAeBgNVBAsTF0NlcnRpZmljYXRlIEF1dGhvcml0aWVz
MRUwEwYDVQQDEwxxOSU1GIFJvb3QgQ0EwHhcNMDcwMzMwMTA0OTQ5WhcNMDgwMzI5
MTA0OTQ5WjCB1zELMAkGA1UEBhMCSFUxEDA0BgNVBAoTB05JSUYgQ0EwExEDA0BgNV
BAGTB0h1bmdhcnkxETAPBgNVBACTEJ1ZGFwZXN0MUIwQAYDVQQKEz10YXRpb25h
bCBJbmZvcmlhdGlvbiBJbmZyYXN0cnVjdHVyZSBEZXZlbG9wbWVudCBJbnN0aXR1
dGUxZmFzAVBgNVBAsTDldlYnNlcnZlcjBUZWFtMRQwEgYDVQQDEwtpZHAubmlpZi5o
dTEeMBwGCSqGSIb3DQEJARYPcG9sYWtvdmlAaWlmLmh1MIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQDFu0D6yq3NlMaQoR6qyRlET1WyGT+hllH+1qXIHhwag2gL
KYByQpBXPva3uSsswn3Rjmv2G/9ifX8sUadflM/MDoCLRoq9umJkcwm0HEp1fmfa
7Gx9isEeVNY00taN9Lo15EQL6rdZMSmwAZ17DCTNs48tPdzm7ys5E0e+bHHA3wID
AQABo4IB3DCCAdgweQYJYIZIAyb4QgEBBAQDAgZAMA4GA1UdDwEB/wQEAwIE8DAa
BgNVHREEEzARgQ9wb2xha292aUBpaWYuaHUwggFZBgNVHR8EggFQMIIBTDCBvKBb
oFmkVzBVMQswCQYDVQQGEwJodTENMAsgA1UEChMETklJRjEgMB4GA1UECxMXQ2Vy
dGlmawNhdGUgQXV0aG9yaXRpZXMxFTATBgNVBAMTDE5JSUYgUm9vdCBDQYECAN6i
WaRXMFUxCzAJBgNVBAYTAmh1MQ0wCwYDVQQKEwR0SU1GMSAwHgYDVQQLEXdDZXJ0
aWZpY2F0ZSBDbXR0b3JpdGllczEVMBMGA1UEAxMMTklJRiBSb290IENBMIGKoCmg
J4YlaHR0cDovL3d3dy5jYS5uaWlmLmh1L25paWYtY2EtY3JsLmNybIECAN6iWaRX
MFUxCzAJBgNVBAYTAmh1MQ0wCwYDVQQKEwR0SU1GMSAwHgYDVQQLEXdDZXJ0aWZp
Y2F0ZSBDbXR0b3JpdGllczEVMBMGA1UEAxMMTklJRiBSb290IENBM8GA1UdIwQY
MBaAFIxiuIeJxr6Aqp7Dk/rx+o/0Po00IMBkGA1UdIAQSMBAwDgYMKwYBBAHdCgEB
```

```
DAEAMA0GCSqGSiB3DQEeBBQUAA4IBAQB262jS0aGJZr0g1Q6IVSodTnokglioJgWy
1FAojS6ML0w7T0eA1PnqX42eSfQFB2Nh71dBUmw6i++iHdQ1gyx0HIeLSdb4JF0B
PoZ+3flwySXu42QgVjJZ46fEMsq2EM0PQV8p9pgBEjlg+6ifAEgJmKbNp+WczQJ7
3rugtu+q8KKQ0oxP0bWLYGLlJ6tKLa4gJ1P/oLe6uX+GWP+P3bZfMp0q9Tu2MU+r
l/gnG2rTS0Be7AEngRmeDfKKeFiSsg1cGxorxQJoEzBZksKUa0nlA9xtd30sUQFX
0I2/Xo2ihYFcpzu551S6+mutZNHqKg0T7uID/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
DTALBgNVBAoTBEE5JSUYxIDAeBgNVBAsTF0NlcnRpZmljYXRlIEF1dGhvcml0aWVz
MRUwEwYDVQQDEwxxOSU1GIFJvb3QgQ0EwHhcNMDcwMzMwMTA00TQ5WhcNMDgwMzI5
MTA00TQ5WjCB1zELMAkGA1UEBhMCSFUxEDA0BgNVBAoTB05JSUYgQ0ExEDA0BgNV
BAGTB0h1bmdhcnkxETAPBgNVBACtCEJlZGFwZXN0MUIwQAYDVQQKEzloYXRpb25h
bCBJbmZvcmlhdGlvbiBJbmZyYXN0cnVjdHVyZSBEZXZlbG9wbWVudCBJbnN0aXR1
dGUxZzAVBgNVBAsTDldlYnNlcnZlciBUZWFtMRQwEgYDVQQDEwtpZHAubmlpZi5o
dTEeBwGCSqGSiB3DQeJARYPcG9sYWtvdmlAaWlmLmh1MIGfMA0GCSqGSiB3DQEB
AQUAA4GNADCBiQKBgQDFu0D6yq3NlMaQoR6qyRlET1WyGT+hllH+1qXIHHwag2GL
KYByQpBXPva3uSsswn3Rjmv2G/9ifX8sUadflM/MDoCLRoq9umJkcm0HEp1fmfa
7Gx9isEeVNY00taN9LoL5EQL6rdZMSmwAZ17DCTNs48tPdzm7ys5E0e+bHHA3wID
```

```

AQABo4IB3DCCAdgwEQYJYIZIAYb4QgEBBAQDAgZAMA4GA1UdDwEB/wQEAwIE8DAa
BgNVHREEEzARgQ9wb2xha292aUBpaWYuaHUwgFZBgNVHR8EggFQMIIBTDCBvKBb
oFmkVzBVMQswCQYDVQGEwJodTENMAsGA1UEChMETkLJRjEgMB4GA1UECzMXQ2Vy
dG1maWnhdGUgQXV0aG9yaXRpZXNxFtATBgNVBAMTDE5JSUYgUm9vdCBDQYECAN6i
WaRXMFUxCzAJBgNVBAYTAmh1MQ0wCwYDVQQKEwR0SULGMSAwHgYDVQQLExdDZXJ0
aWZpY2F0ZSBBDXRob3JpdGllczEVMBMGA1UEAxMMTkLJRiBSb290IENBMIGKoCmg
J4YlaHR0cDovL3d3dy5jYS5uaWlmLmh1L25paWYtY2EtY3JsLmNybieCAN6iWaRX
MFUxCzAJBgNVBAYTAmh1MQ0wCwYDVQQKEwR0SULGMSAwHgYDVQQLExdDZXJ0aWZp
Y2F0ZSBBDXRob3JpdGllczEVMBMGA1UEAxMMTkLJRiBSb290IENBMB8GA1UdIwQY
MBaAFIxiuIeJxr6Aqp7Dk/rx+o/0Po00IMBkGA1UdIAQSMBAwDgYMKwYBBAHdCgEB
DAEAMA0GCSqGSiB3DQEBBQUAA4IBAQB262jS0aGJZr0g1Q6IVSodTnokgljojgWy
1FAojS6ML0w7T0eA1PnqX42eSfQFB2Nh71dBUmw6i++iHdQ1gyx0HIeLSdb4JF0B
PoZ+3flwySXu42QgVjJZ46fEMsq2EM0PQV8p9pgBEjlg+6ifAEgJmKBnP+WczQJ7
3rugtu+q8KKQ0oxP0bWLYGllJ6tKLa4gJ1P/oLe6uX+GWP+P3bZfMp0q9Tu2MU+r
l/gnG2rTS0Be7AEngRmeDfKKeFiSsg1cGxorxQJoEzBZksKUa0nlA9xtd30sUQFX
0I2/Xo2ihYFcpzu551S6+mutZNHqKg0T7uID/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
DTALBgNVBAoTBEE5JSUYxIDAeBgNVBAsTF0NlcnRpZmljYXRlIEF1dGhvcml0aWZp
MRUwEwYDVQQDEw0SULGIFJvb3QgQ0EwHhcNMDcxMTMwMTMwNzE4WbcNMDgxMTI5

```

MTMwNzE4WjBvMQswCQYDVQGEwJIVTEQMA4GA1UEChMHTkLJRiBDQTE0MAwGA1UE  
CxMFSEJPTkUxZzAVBgNVBAsTDldlYnNlcnZlciBUZWFtMSUwIwYDVQQDEExycmQt  
bWEucGVyZnNvbWVyLnZoLmhib25lLmhm1MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB  
iQKBgQC2x6Hprj4yB6EDkXUHNMLHz250kqWBXf/UI6TziV5rvMjvS8pdFnsZcIt1  
coT03Fu4wzs6N8gtC5uW7f3JaBsG32sYZUorWbecpgVy5ttcIqTM1RnxUs0ktsM  
RuBz7qYAQ1/B9VvBH7P7DeREgIGm7Skel/Q3Qhl4oG9PtFe1wQIDAQABo4IB3DCC  
AdgwEQYJYIZIAYb4QgEBBAQDAgBAMA4GA1UdDwEB/wQEAwIE8DAaBgNVHREEezAR  
gQ9wb2xha292aUBpaWYuaHUwggFZBgNVHR8EggFQMIIBTDCBvKBboFmkVzBVMQsw  
CQYDVQGEwJodTENMA5GA1UEChMETkLJRjEgMB4GA1UECxMXQ2VydgLmaWNhdGUg  
QXV0aG9yaXRpZXNFTATBgNVBAMTDE5JSUYgUm9vdCBDQYECAN6iWaRXXMFUxCzAJ  
BgNVBAYTAmh1MQ0wCwYDVQKQEWROSUlgMSAwHgYDVQQLExdDZXJ0aWZpY2F0ZSBB  
dXR0b3JpdGllczEVMmBGA1UEAxMMTkLJRiBSb290IENBMIGKoCmgJ4YlaHR0cDov  
L3d3dy5jYS5uaWlmLmhm1L25paWYtY2EtY3JsLmNyblIECAN6iWaRXXMFUxCzAJBgNV  
BAYTAmh1MQ0wCwYDVQKQEWROSUlgMSAwHgYDVQQLExdDZXJ0aWZpY2F0ZSBBdXR0  
b3JpdGllczEVMmBGA1UEAxMMTkLJRiBSb290IENBMmB8GA1UdIwQYMBaAFIxiuIeJx  
r6Aqp7Dk/rx+o/0Po00IMBkGA1UdIAQSMBAwDgYMKwYBBAHdCgEBCQEAMA0GCSqG  
SIb3DQEBBQUAA4IBAQAUVuG4+KUXQZCYCedQmW6Ih83ggMS7inxFBFeadc4Ts1egY  
Wf6Y4CoE0rsdI7FmC7CccarDaMc6PVJg1WLDV01LMGM2+6rcoMeMs/J5pCFTDhn  
c6MPz6KedRcMvVJajY+BZvJPG9CNpyxdIUf/aDa28yRryVM0Jbm6B0FH+UrvHlVw  
w2JxlmShtk1fNmEU7gluzwo3FEZrx8nnLWkeTfmzz/iM+dudNm4sL99uGNEWGNFf  
tLi+R35McE7CfyNNf0vlskZX++dSX/Re8CERTo3wZrHmFKIo0nJzo6v48d2tEbw0  
a15Yl93MJCnLC5BUyvUMqKDLmHhTxmg0+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`-nek az összes használt metadata állományra nézve egyedinek kell lennie.

# Metadata állományok frissítése

A metadata állományok központi helyről való letöltésére a [Siterefresh](#) és a [Metadatool](#) 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>*` elemet, 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