Alapok és fogalmak

- Föderáció
- Föderációs modellek
- Metadata
- Pont-pont bizalmi kapcsolati modell
- WAYF
- SAML
- OpenID
- MetadataTrust

Föderáció

Az **Identitás Föderáció** olyan intézmények halmaza, amelyek között lehetséges az identitás-információk átadása. Az intézmények - szabályozott keretek között - *megbíznak* a másik intézmény által kiállított identitás-információkban.

A Föderáció a pont-pont bizalmi kapcsolati modell általánosítása. Ekkor nem szükséges egy intézménynek minden egyes társintézménnyel külön megállapodást kötnie, hanem a szövetséghez csatlakozással automatikusan létrejön közöttük a lehetőség az identitás-információk átadására. Általában lehetőség van arra, hogy egy intézmény több Föderációhoz is kapcsolódjon, ill. külön bilaterális megállapodásai legyenek.

Célja

A föderációk célja, hogy az identitás információk egyébként autonóm rendszerek között átjárhatók legyenek. Ez a következő előnyökkel járhat:

- **redundáns felhasználó-adminisztráció elkerülése**: az identitáshoz kapcsolódó adatoknak elegendő egy helyen rendelkezésre állni; nem kell "idegen", "külsős" felhasználókat felvenni az intézményi adatbázisba
- **Single Sign-on**: a felhasználónak elég egyszer megadni az azonosító adatait, a többi rendszer automatikusan megszerzi az identitáshoz kötődő információkat. Ez egyrészt kényelmesebb a felhasználónak, másrészt megkönnyíti a több faktoros (pl. smartcard) azonosítási módszerek bevezetését.

Szerepek

A legtöbb föderációs modell lehetővé teszi azt, hogy egy intézmény egyszerre több szereppel is részt vegyen egy föderációban.

Identitás szolgáltatók (Identity Provider, IdP)

A felhasználók adatait az identitás szolgáltató tárolja. Az identitás szolgáltató funkciói: **Azonosítás**

- Felhasználó azonosítása
- Felhasználó azonosítással kapcsolatos információk átadása a tartalomszolgálatóknak (SP)
- Tartalomszolgáltatóktól érkező azonosítási kérések (AuthRequest) feldolgozása

Attribútumok kiadása

- Felhasználóhoz köthető attribútumok meghatározása
- A tartalomszolgáltató számára hozzáférhető felhasználói adatok átadása a tartalomszolgáltatónak (közvetlenül ill. a felhasználón keresztül)

Felhasználó menedzsment

- Felvétel / törlés
- Attribútumok, role-ok kezelése
- Jelszó ill. adatmódosítás

Tartalom / erőforrás szolgáltatók (Service Provider, SP)

A tartalomszolgáltatók védett tartalmakat szolgáltatnak a felhasználók számára. Általában nincsenek közvetlenül a felhasználókhoz kapcsolatos adataik, ezért nem szükséges a felhasználókat adminisztrálniuk sem.

A tartalomszolgáltató funkciói (a funkciók föderációs modelltől függően ezektől eltérhetnek):

- azonosított kapcsolat létrehozása az identitás szolgáltató segítségével (általában HTTP átirányítás használatával)
- az identitás szolgáltatótól kapott adatok értelmezése
- az identitás szolgáltatótól kapott adatok alapján meghatározni, hogy a felhasználó jogosult-e a művelet végrehajtására (**autorizáció**)

Metadata adminisztráció

A szolgálatókhoz kötődő háttérinformációkat (pl. tanúsítvány, név, scope, stb.) sok esetben a föderációs szoftver számára is elérhetővé kell tenni, ez esetben Metadata használatáról beszélünk. Adminisztrációja általában központilag történik, és *push* vagy *pull* módszerrel jut el a föderációba bevont számítógépekhez.

Speciális szolgáltatás a "Where Are You From?" (WAYF) szolgáltatás, amely a felhasználó számára lehetőséget ad, hogy az identitás szolgáltatóját kiválassza. Ez a szolgáltatás a föderációs metadata állomány(ok)ra épül.

Föderációs alapelvek

1. A föderáció célja, hogy a felhasználók úgy vehessenek igénybe szolgáltatásokat - amennyiben erre jogosultak -, hogy a saját intézményük azonosítja őket.
2. Az IdP és az SP egyértelműen azonosítja magát, amikor üzenetet váltanak egymással.
3. Az IdP csak valós személyeket azonosít (teszt felhasználókat csak meghatározott módon, korlátozásokkal szabad azonosítani)
4. Az IdP csak abban az esetben azonosít egy felhasználót, ha az illető valamilyen - ismert - viszonyban van (volt) az intézménnyel.
5. Az IdP és az SP nem ad meg magáról hamis, félrevezető információt.
6. Az IdP minden tőle telhetőt megtesz annak érdekében, hogy a kiadott információ a lehető legpontosabb legyen. Az SP tisztában van vele, hogy bizonyos információkat a felhasználók maguk is szerkeszthetnek.
7. Az IdP gondoskodik róla, hogy a felhasználót azonosító információk (pl. jelszó) védett módon legyenek tárolva, ill. a felhasználók ezt biztonságosan adhassák meg.
8. Az SP csak a működéséhez minimálisan szükséges adatmennyiséget igényli a felhasználóról.
9. Az SP nem kérheti a felhasználót, hogy adja meg az IdP-nél érvényes jelszavát. Jelszó az SP-nek nem adható ki (kivéve speciális esetben egyszer használatos vagy rövid lejáratú jelszavak).
10. Az SP az IdP-től származott információt harmadik félnek nem adja tovább.
11. Felhasználói visszaélések esetén az IdP és az SP együttműködik egymással.
12. Az IdP és az SP az informatikai rendszereit az elvárható gondossággal üzemelteti.

Technológiák

- Föderációs modellek

Szabályozás

A lazán csatolt modellek (pl. az OpenID) nem igényelnek központi szabályozást, de a magasabb biztonság-igényű, nagy bizalmat igénylő modellek esetén szükséges az, hogy a föderációban résztvevő intézmények kidolgozzák (esetleg szerződésbe is foglalják) az együttműködés feltételeit.

A megállapodás pl. az alábbi területeket érintheti

- Felhasználó-kezelés (pl. lejárt azonosítók inaktívvá tétele, password policy)
- Felhasználói adatok védelme (privacy követelmények)
- Felhasználó-azonosítási technológiák, ezek elnevezése
- Scope-ok kiosztása

- Felhasználói attribútumok használatának a feltételei (pl. milyen feltételekkel mondhatja egy intézmény XY-ról, hogy ő egy *oktató*?)
- Metadata információk karbantartása
- Új intézmény csatlakozásának feltételei (IdP, ill. SP szerepben)
- Audit, nemmegfelelőségi szankciók
- Költségviselés szabályai
- stb.

Föderációs modellek

- SAML
- Liberty Alliance
- WS-Federation
- OpenID
- Ügyfélkapu
- .NET Passport
- Moira
- PAPI
- EduGAIN
- EduROAM

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

Pont-pont bizalmi kapcsolati modell

Két intézmény egymással közvetlenül köt megállapodást az identitás-információk átadásáról. Ez lehet egy föderáción belüli megállapodás kiterjesztése, ill. teljesen új megállapodás. Mindkét intézmény működhet identitás szolgáltatóként és tartalomszolgáltatóként is.

A pont-pont modell hátránya az adminisztrációs többletteher, mivel az együttműködő intézménnyel közvetlenül kell megállapodni. Leggyakrabban akkor használják, ha egy projektben szükség van 1-2 partnerrel külön megállapodást kötni (ekkor a partnereknek nem kell a föderációban részt venniük).

- Kutatói föderációkban piaci szereplők általában nem vehetnek részt mint azonosítási szolgáltatók. Előfordulhat, hogy egy projektben - ahol megosztott közös erőforrásokat kell használni több intézmény munkatársainak - piaci és kutató intézmény dolgozik együtt, ilyenkor jó megoldás lehet a közvetlen megállapodás

WAYF

A **WAYF** szó a *Where Are You From?* mondat rövidítése. Olyan szolgáltatást jelent, amely kideríti, hogy a felhasználót melyik IdP képes azonosítani. A SAML2 szabvány ezt a szolgáltatást **Discovery Service**-nek nevezi.

Legegyszerűbb esetben a WAYF kilistázza az elérhető IdP-ket, amelyek közül a felhasználó választhat. A választást bizonyos ideig (a böngésző bezárásáig, néhány napig, stb) megjegyeztethetjük, ekkor a WAYF szerver a választásunkat cookie-ban tárolja.

A WAYF lehet az IdP-nek és az SP-nek is része, ill. különálló elem, a működést ez nem befolyásolja.

** Szoftverek:**

- SWITCHaai WAYF (http://www.switch.ch/aai/support/tools/wayf.html)
- A Shibboleth 1.3 IdP tartalmaz WAYF alkalmazást

SAML

SAML 1.1

SAML 2.0

Bindingok

- TODO

Profilok

- SAMLBrowserPOST
- SAMLBrowserArtifact
- TODO

OpenID

Mi az OpenID?

Az OpenID egy nyílt, decentralizált, ingyenes keretrendszer felhasználóközpontú digitális identitásmenedzsmenthez. Az OpenID elképzelés abból indul ki, hogy az interneten bárki azonosíthatja önmagát egy URI (avagy URL, web cím) segítségével, pontosan úgy, ahogy a weboldalak is teszik. Mivel az URIk a web felépítésének alapvető elemei, biztos alapjául szolgálhatnak a felhasználóközpontú identitásmenedzselésnek is.

Az OpenID keretrendszer egyik fő eleme az autentikáció, vagyis hogy miképp bizonyítod, te birtokolsz egy adott URI-t. Manapság a weboldalak felhasználóneveket és jelszavakat kérnek a belépéshez, ami azt jelenti, hogy sokan ugyanazt a jelszót használják minden weboldalon. Az OpenID autentikáció esetében a felhasználóneved a saját URI-d, jelszavad (vagy további adatod) pedig biztonságosan el lesz tárolva az OpenID szolgáltatódnál (amelyet te magad is működtethetsz, vagy használhatsz egyéb identitás szolgáltatót).

Egy OpenID-re nyitott weboldalra történő belépéshez (még ha sosem jártál rajta ezelőtt) csak add meg az OpenID URI-dat. A weboldal ezután át fog irányítani az OpenID szolgáltatódhoz, ahol meg kell adnod a szükséges adatokat. Amint megtörténik az autentikáció, OpenID szolgáltatód visszairányít a weboldalra a belépéshez szükséges adatokkal együtt. Ha erős autentikációra van szükség, az OpenID keretrendszer számos tranzakció típushoz is használható - az egyszerű Single-Sign-On eljárás vagy a megosztott adatok érzékenységének rugalmas kiterjesztésére.

Az autentikáció mellett az OpenID keretrendszer eszközöket is biztosít a felhasználóknak ahhoz, hogy megosszák digitális identitásuk egyéb összetevőit. A folyamatosan bővülő OpenID Attribute Exchange specifikáció alapján a felhasználók képesek pontosan meghatározni az Identitás szolgáltatójuk által megosztható információk körét.

MetadataTrust

Ez a szócikk a Metadata bizalmi kérdéseivel foglalkozik. A föderációk üzemeltetéhez hozzátartozik a föderációs metadata állomány karbantartása is. A föderációban való bizalom technikai értelemben megegyezik a metadatába vetett bizalommal, így ezen bizalom fenntartása rendkívül fontos.

További információkkal szolgál a Trust Management oldal a Shibboleth wikin.

Központi metadata bizalmi modellek

Alapvetően kétféle módon lehet biztosítani a metadata hitelességét:

- aláírás + lejárati idő
- hiteles helyről letöltés (SSL/TLS) + gyorstárazási idő

Előbbi módszer esetén a szállítási protokoll biztonsága nem szükséges (tehát a metadata nem hiteles helyről is beszerezhető - pl. http, email, ...), a digitális aláírás ellenőrzésével a hitelesség megállapítható.

A lejárati idő - `validUntil` ebben az esetben kulcsfontosságú, hiszen egy lejárati idő nélküli metadatát nem lehetséges visszavonni (egy rosszindulatú támadó egy régi metadata példányt később bármikor felhasználhat), így az esetleg kompromittált entitások az egész föderáció biztonságát veszélyeztethetik.

Utóbbi módszer használata esetén a föderációs entitások kötelesek a metadatát egy központi helyről, biztonságos csatornán (pl. https megfelelő tanúsítvány-ellenőrzéssel) adott időközönként letölteni. Ezt a frissítési időközt határozza meg a gyorstárazási idő, a `cacheDuration`.

Metadata bizalom a HREF Föderációban

A HREF Föderációban a metadata biztonságát digitális aláírás és 72 órás lejárati idő együttes alkalmazása biztosítja. A metadata óránként generálódik a Resource_Registry-ben, és aláírásra kerül a metadata aláíró kulccsal.

Aláírás ellenőrzése az aláíró kulcs tanúsítványának segítségével

Az aláírás ellenőrizhető a metadata aláíró kulcs tanúsítványának segítségével, mely elérhető a https://metadata.eduid.hu/href-metadata-signer-2011.crt címről.

Shibboleth IdP illetve SP használata esetén a metadata állomány ellenőrzésére az ún. MetadataFilter használatos, mely az aláírást ellenőrzi a tanúsítvány segítségével.

Shibboleth 2 IdP esetén

Metadata provider beállítása:

```
<MetadataProvider id="href" xsi:type="FileBackedHTTPMetadataProvider"
 xmlns="urn:mace:shibboleth:2.0:metadata"
 metadataURL="http://rr.aai.niif.hu/metadata/href-metadata.xml"
 backingFile="/path/to/metadata/href-metadata.xml" >
 <MetadataFilter xsi:type="ChainingFilter">
  <MetadataFilter xsi:type="RequiredValidUntil"
    maxValidityInterval="604800" />
  <MetadataFilter xsi:type="SignatureValidation"
    trustEngineRef="shibboleth.MetadataTrustEngine"
    requireSignedMetadata="true" />
 </MetadataFilter>
</MetadataProvider>
```

Illetve a hozzá tartozó `TrustEngine` konfiguráció:

```
<!-- Trust engine used to evaluate the signature on loaded metadata. -->
<security:TrustEngine id="shibboleth.MetadataTrustEngine"
  xsi:type="security:StaticExplicitKeySignature">
  <security:Credential id="MyFederation1Credentials" xsi:type="security:X509Filesystem">
    <security:Certificate>/path/to/href-metadata-signer-2011.crt</security:Certificate>
```

```
    </security:Credential>
  </security:TrustEngine>
```

Shibboleth 2 SP esetén

```
  <MetadataProvider type="XML"
    url="http://metadata.eduid.hu/current/href.xmll"
    backingFilePath="href.xml">
   <MetadataFilter type="RequireValidUntil" maxValidityInterval="604800"/>
   <MetadataFilter type="Signature" certificate="href-metadata-signer-2011.crt"/>
</MetadataProvider>
```

SimpleSAMLphp esetén

SimpleSAMLphp használata esetén a metarefresh modul használható a metadata időzített letöltésére és ellenőrzésére. Ezzel kapcsolatban további információkat tartalmaz a SimpleSAMLphp HREF integráció fejezet.

Az aláíró kulcs visszavonása

A fent leírt modell egyetlen problémája az aláíró kulcs kezelésében rejlik. Az aláíró kulcs visszavonása ugyanis csak a rendszeren kívül történhet, egy új kulcs bevezetéséhez az összes partner rendszerében meg kell változtatni az ellenőrzést. Sőt, az átmeneti időben mindkét kulcs használata szükséges lehet (két különböző metadatán).

Amennyiben az aláíró kulcs kompromittálódik, az azonnali visszavonása és egy új kulcs használata esetén azok a rendszerek, melyek még a régi tanúsítványt használták, a metadata lejárati idő letelte után működésképtelenné válnak.

CA használata

Ezen problémák kiküszöbölhetőek egy CA használatával. Ekkor ugyanis az aláíró kulcs tanúsítványát a CA aláírhatja, a partnerek pedig magát a CA tanúsítványt jelölhetik megbízhatónak.

A metadata aláírásakor ebben az esetben nem elég csak az aláíró tanúsítványt beágyazni (`Signature/KeyInfo/X509Certificate` elembe), hanem a CA tanúsítványát is el kell helyezni az aláírt metadatába.

Tanúsítvány visszavonása

CA használata esetén a tanúsítvány visszavonási listák (CRL) illetve on-line ellenőrzés (OCSP) is alkalmazható az aláíró tanúsítvány érvényességének megállapítására. Ezen kívül - mivel magát a tanúsítványt nem kell külön csatornán eljuttatni a partnerekhez -, alkalmazhatóak rövidebb lejáratú (pár hónap, maximum egy év) tanúsítványok is.

Hitelesség ellenőrzése

A metadata aláírásának ellenőrzése ebben az esetben a beágyazott tanúsítvánnyal történik, az aláírás hitelesítése után pedig megtörténik a megfelelő, megbízhatónak jelölt CA-ra történő PKI ellenőrzés.

Shibboleth IdP esetén

A fenti IdP konfigurációs példában a `TrustEngine` konfigurációt kell megváltoztatni, hogy PKIX validációt végezzen. Fontos, hogy a CRL fájl folyamatosan frissítésre kerüljön, ugyanis a Shibboleth nem ad lehetőséget ezen fájl távoli elérésére.

```
<security:TrustEngine xsi:type="security:StaticPKIXSignature"
  id="shibboleth.MetadataTrustEngine">
 <ValidationInfo xsi:type="PKIXFilesystem" xmlns="urn:mace:shibboleth:2.0:security"
   id="HREFCA" VerifyDepth="1" >
  <Certificate>/path/to/trusted/ca-cert.pem</Certificate>
  <CRL>/path/to/trusted/ca-crl.pem</CRL>
 </ValidationInfo>
</security:TrustEngine>
```

> **Figyelem**
>
> A fenti konfigurációs kódrészlet nem alkalmazható a CRL rendszeres, időzített letöltése és előzetes tesztelés nélkül!

Shibboleth SP esetén

A fenti Shibboleth SP példában a `SignatureMetadataFilter`-t kell módosítani az alábbiak szerint

```
<SignatureMetadataFilter verifyName="false">
 <TrustEngine type="StaticPKIX">
  <CredentialResolver type="File">
   <Certificate>
    <Path>ca-cert.pem</Path>
   </Certificate>
   <CRL>
    <Path>ca-crl.pem</Path>
   </CRL>
  </CredentialResolver>
 </TrustEngine>
</SignatureMetadataFilter>
```

Az újabb Shibboleth SP verziókban lehetőség van a CRL URL-ről történő letöltésére is, ezzel kapcsolatban további információk.

> **Figyelem**
>
> A fenti konfigurációs kódrészlet nem alkalmazható előzetes tesztelés nélkül!

SimpleSAMLphp esetén

> **A szócikk vagy fejezet még megírásra vár**

Külön eszközzel

Az NIIF által fejlesztett metadata aláíró/ellenőrző eszköz támogatja a CA tanúsítványok használatát és a PKI validációt (MDSigner forrás).