

iAMRES trening



AMRES

Akademski mreža Srbije

Decembar 2024.



Cilj treninga

01

Upoznavanje sa konceptima Federacije Identiteta

02

Upoznavanje sa eduGAIN interfederacijom

03

Sticanje znanja i veština potrebnih za implementaciju Davaoca Identiteta

04

Pridruživanje iAMRES Federaciji Identiteta

05

...



Proces upravljanja identitetima

- Identifikacija
- Autentifikacija
- Autorizacija



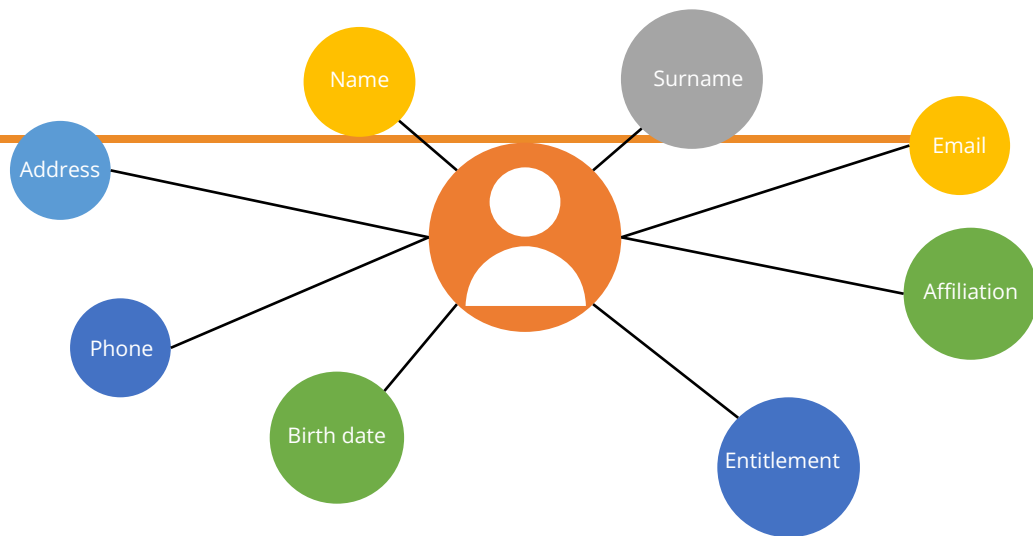
A login form on a dark blue background. It contains a 'Username' field with the text 'username', a 'Password' field with '*****', a 'Remember Me' checkbox, a yellow padlock icon, and 'Login' and 'Register' buttons.





Digitalni Identitet

- Skup atributa



- Svrha:

- **Identifikacija:** Predstavljanje osobe u digitalnoj formi
- **Autentifikacija:** Dokaz da je u pitanju ista osoba koja je pristupala servisu
- **Autorizacija:** Kontrola pristupa na osnovu vrednosti pojedinih atributa
- **Profil:** Personalizacija, informacije o osobi kao što su ime, email adresa, etc.



AMRES

Delegiranje procesa autentifikacije





Primer

Sign in · GitLab

https://gitlab.com/users/sign_in?_cf_chl_jschl_tk__=0c5dd7e73f04a34c2e...

GitLab.com

GitLab.com offers free unlimited (private) repositories and unlimited collaborators.

- [Explore projects on GitLab.com](#) (no login needed)
- [More information about GitLab.com](#)
- [GitLab Community Forum](#)
- [GitLab Homepage](#)

By signing up for and by signing in to this service you accept our:

- [Privacy policy](#)
- [GitLab.com Terms.](#)

Sign in | Register

Username or email

Password

Remember me [Forgot your password?](#)

Sign in

Sign in with

Google | GitHub

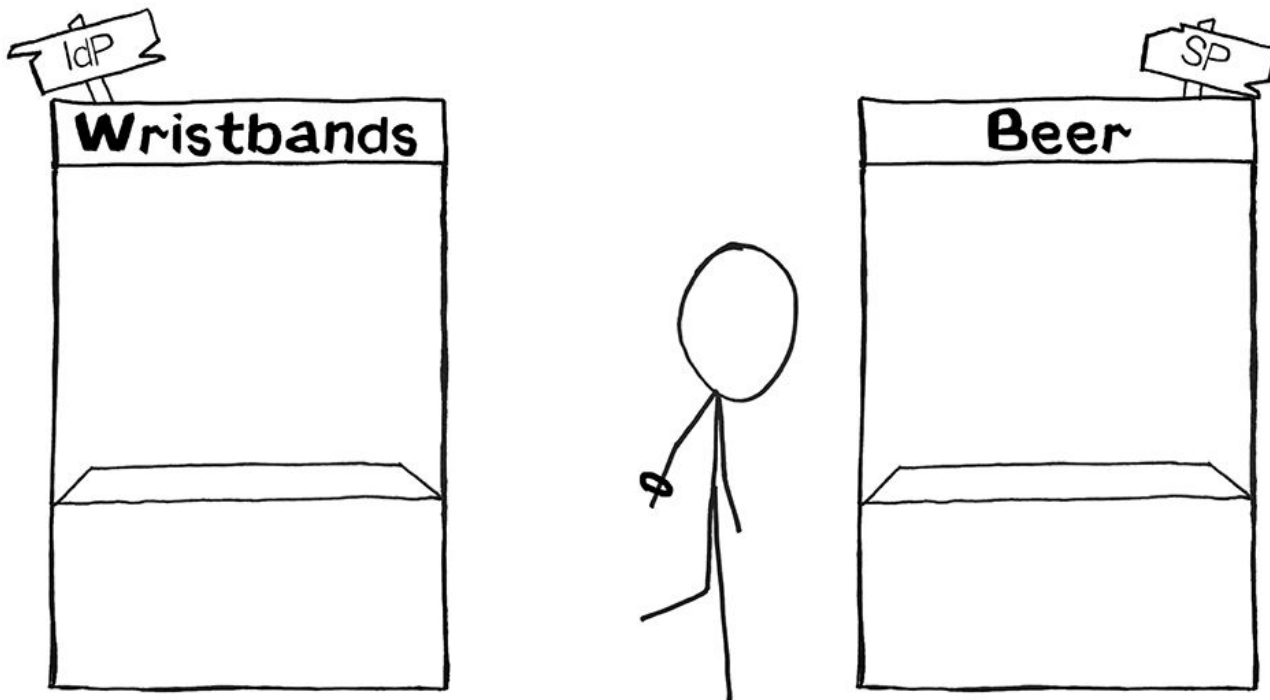
Twitter | Bitbucket

Salesforce

Remember me



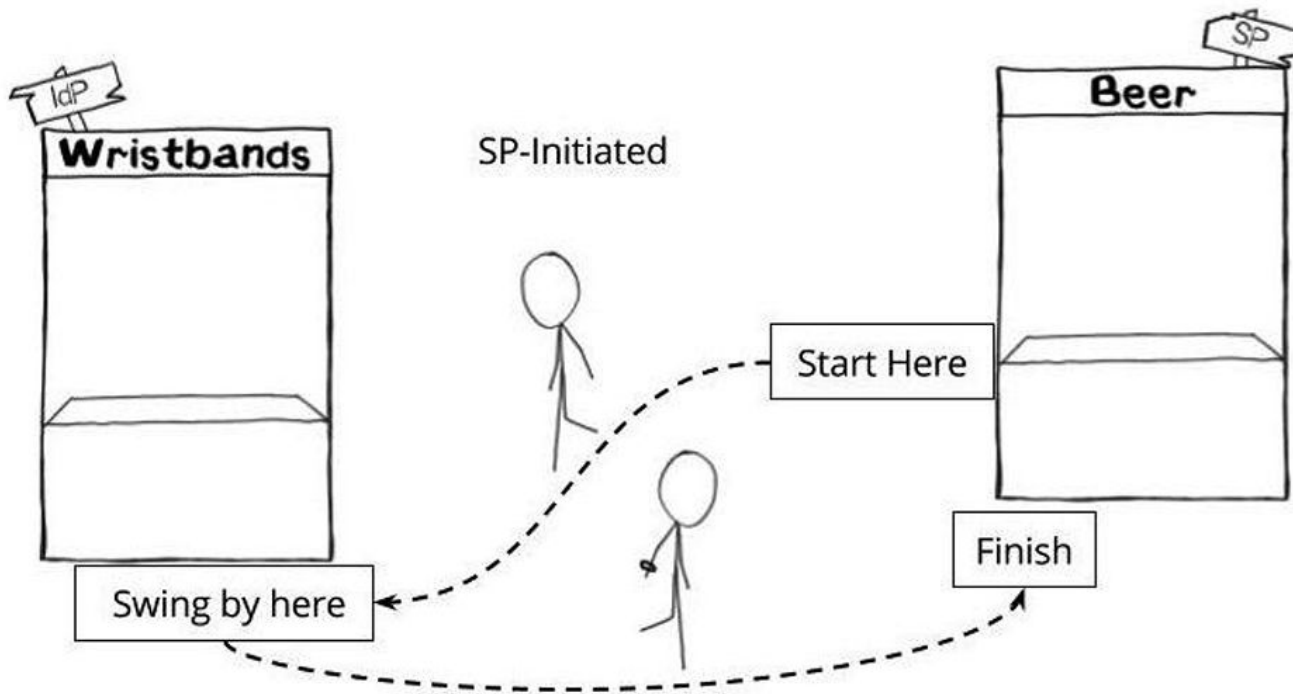
Primer



Crédit: <https://duo.com/blog/the-beer-drinkers-guide-to-saml>



Primer





AMRES

Federaciju Identiteta čine entiteti



Davalac Identiteta

Identity Provider (IdP) ~ Home organization (HO)



Davalac Servisa

Service Provider (SP) ~ Relying Party (RP)

Discovery Service (DS)





Federacija Identiteta

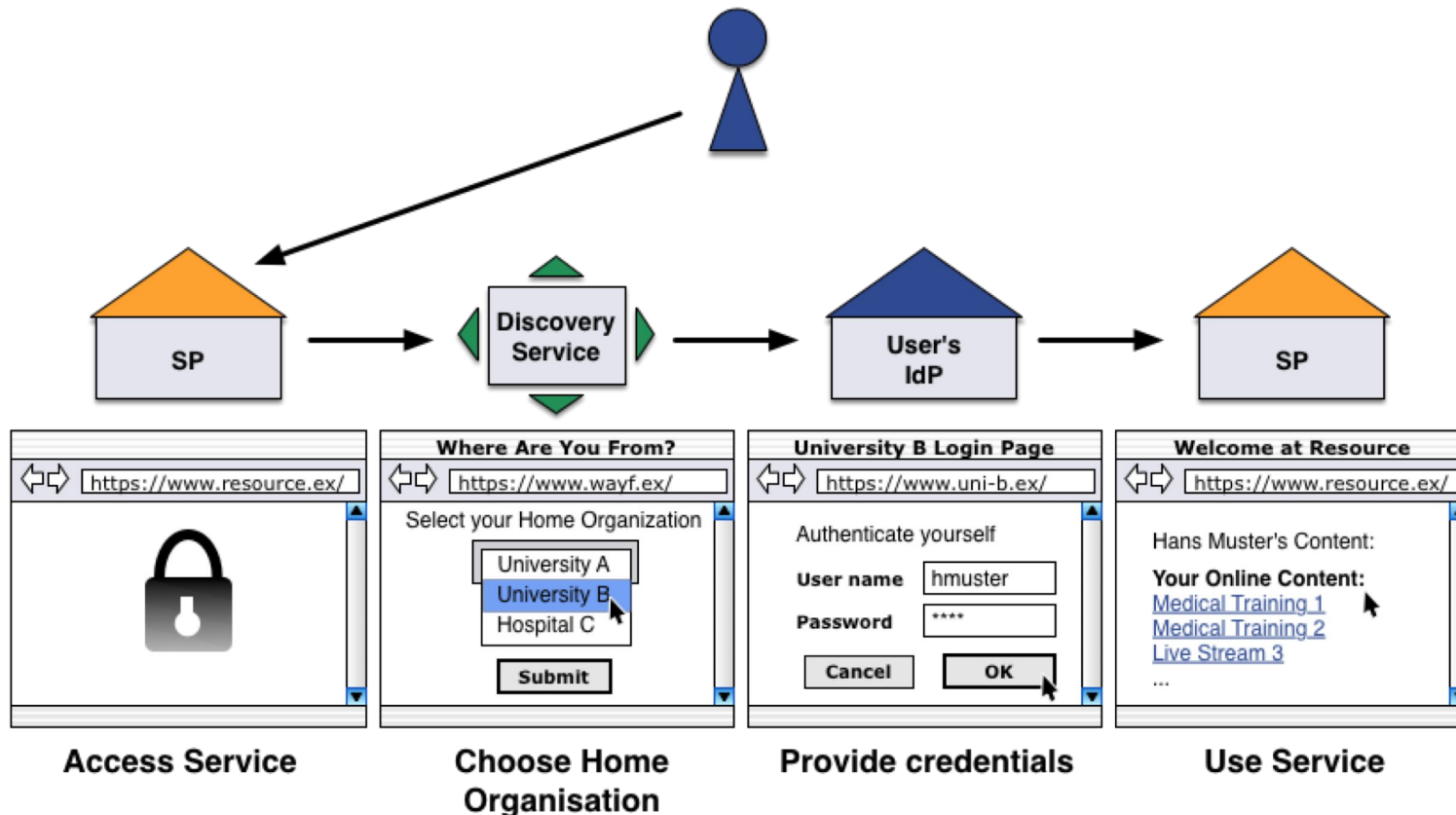


- Protokol (SAML, OIDC, etc.)
- Poverenje se uspostavlja na više načina:
 - Ugovor između SP/IdP administratora (Bilateralni sporazum)
 - Putem treće strane (Federacija)





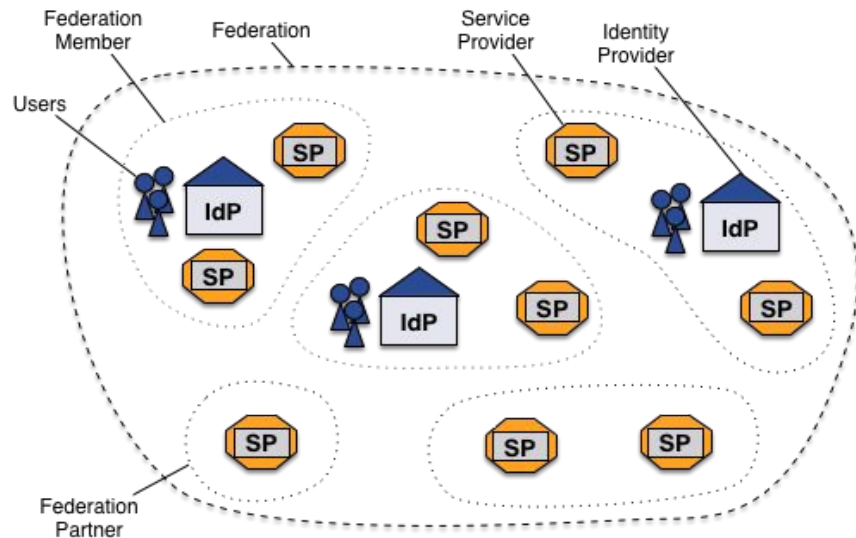
Proces autentifikacije u okviru Federacije Identiteta





Federacija Identiteta

An Identity Federation is a collection of organizations that agree to interoperate under a certain rule set.





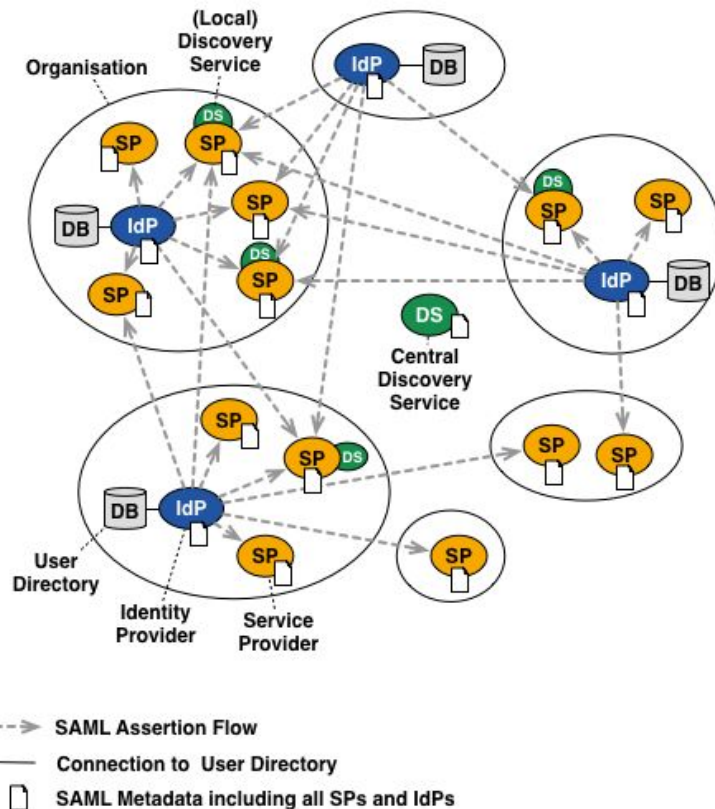
Tipovi Federacija Identiteta

- Full mesh
- Hub & Spoke sa distribuiranim login stranicama
- Hub & Spoke sa centralnom login stranicom



Full Mesh Federacija Identiteta

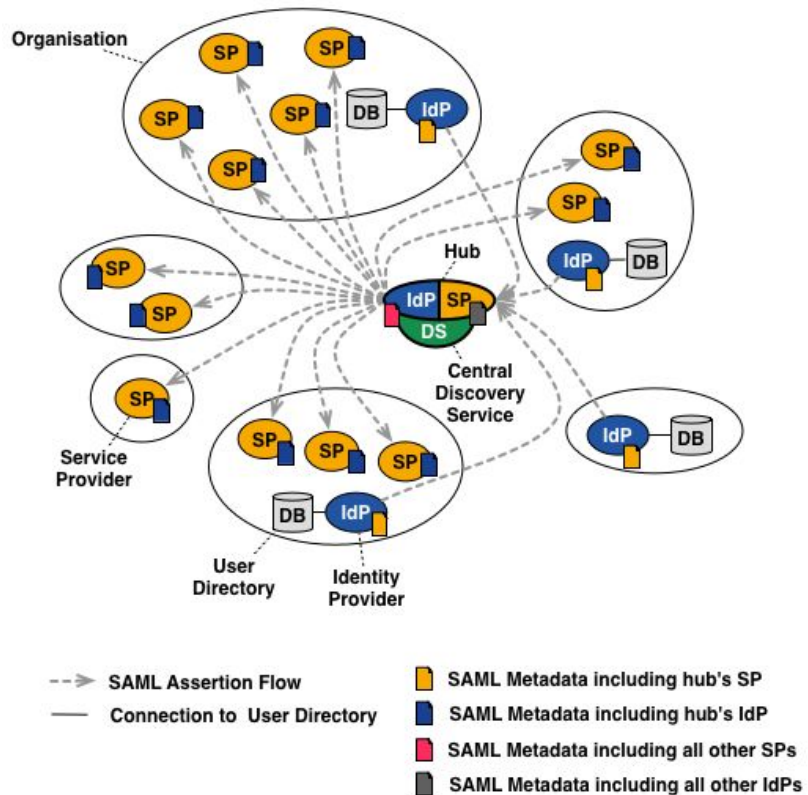
Entiteti su distribuirani
Nema centralne komponente





Hub & Spoke Federacija Identiteta da distribuiranim login stranicama

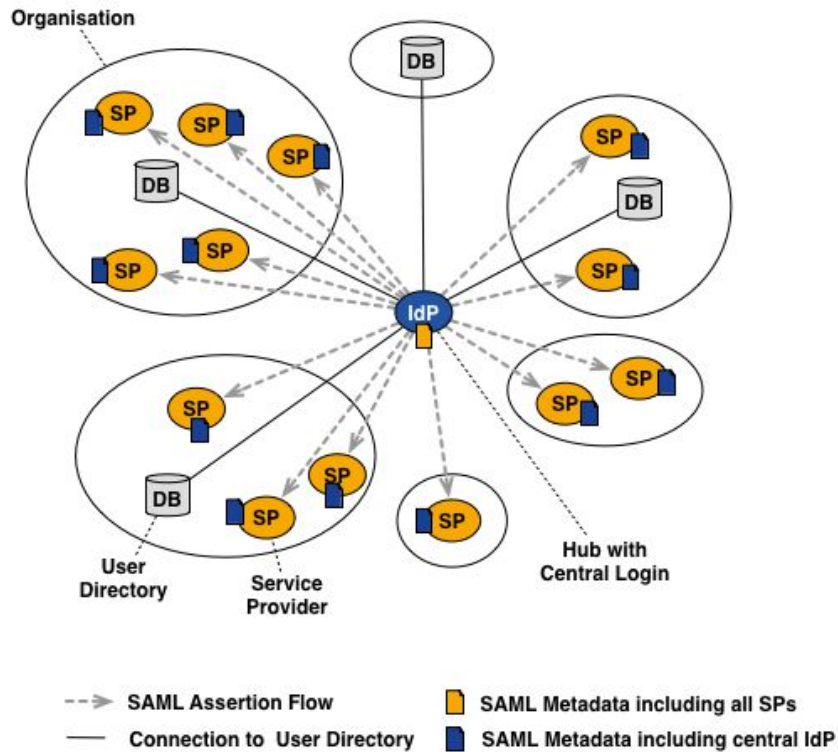
Centralni hub: SP za IdPs, IdP za SPs
Svaka organizacija ima svoj IdP
Centralni hub = Centralni *Discovery Service*





Hub & Spoke Federacija Identiteta da centralnom login stranicom

A special case in the sense as there is only one single Identity Provider in the federation



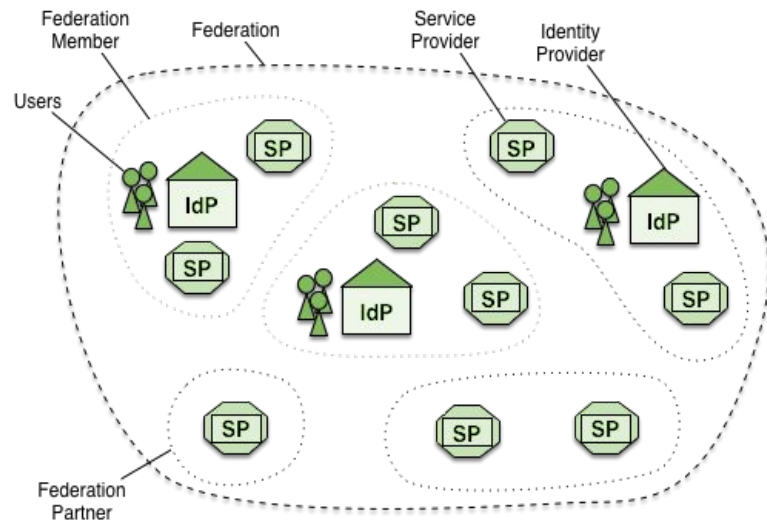


Entiteti, metapodaci i Federacija

- Entiteti registruju metapodatke
- Federacija agregira metapodatke u *metadata feed*
- Federacija potpisuje i distribuira agregirane metapodatke

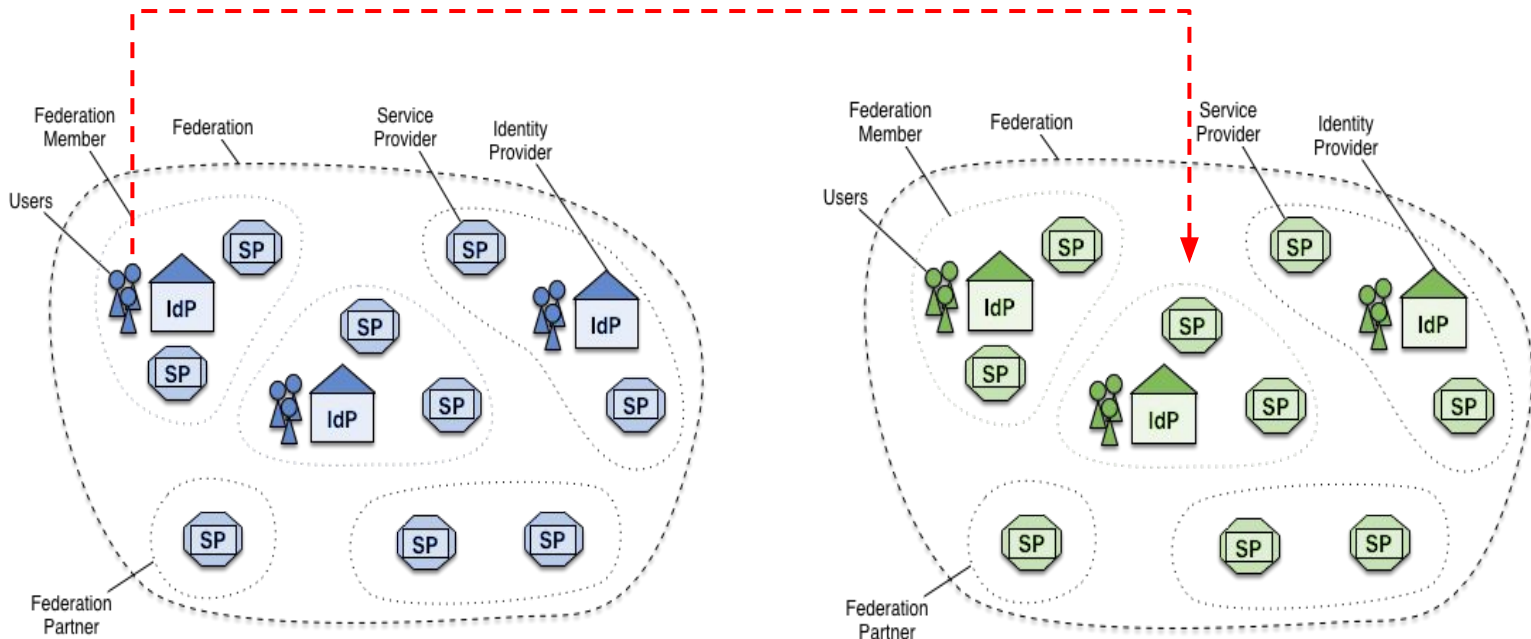


Metadata is the technical information required for integration between members of the federation.





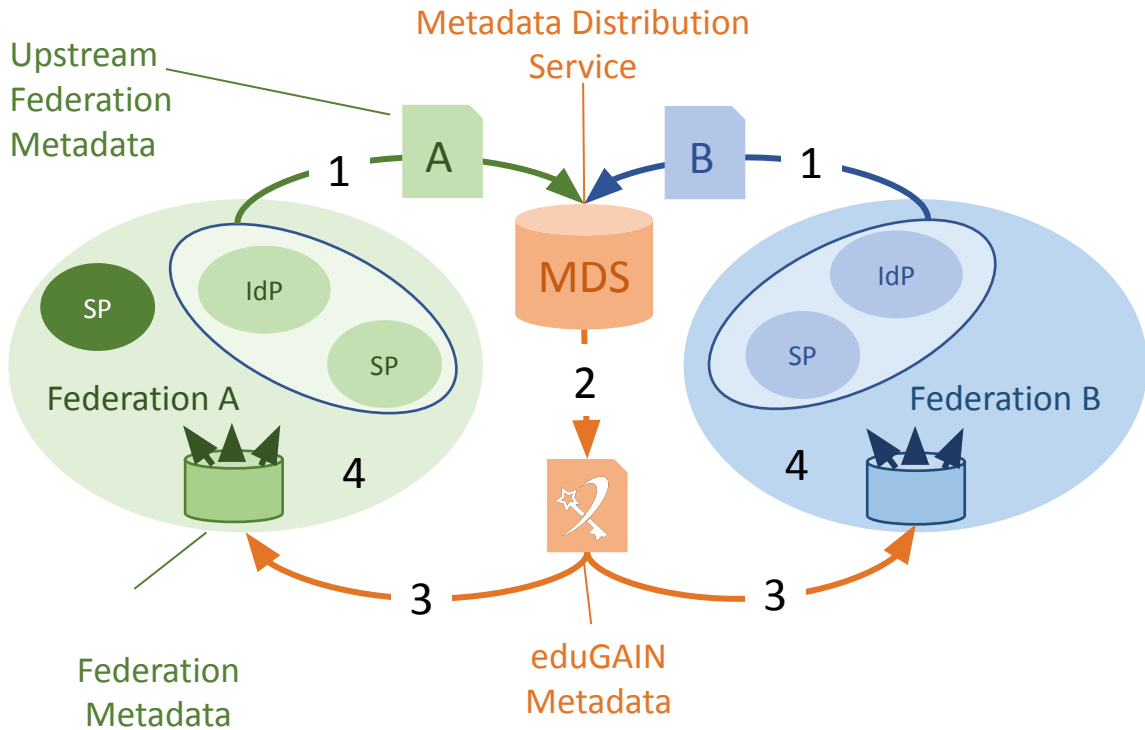
Interfederacija





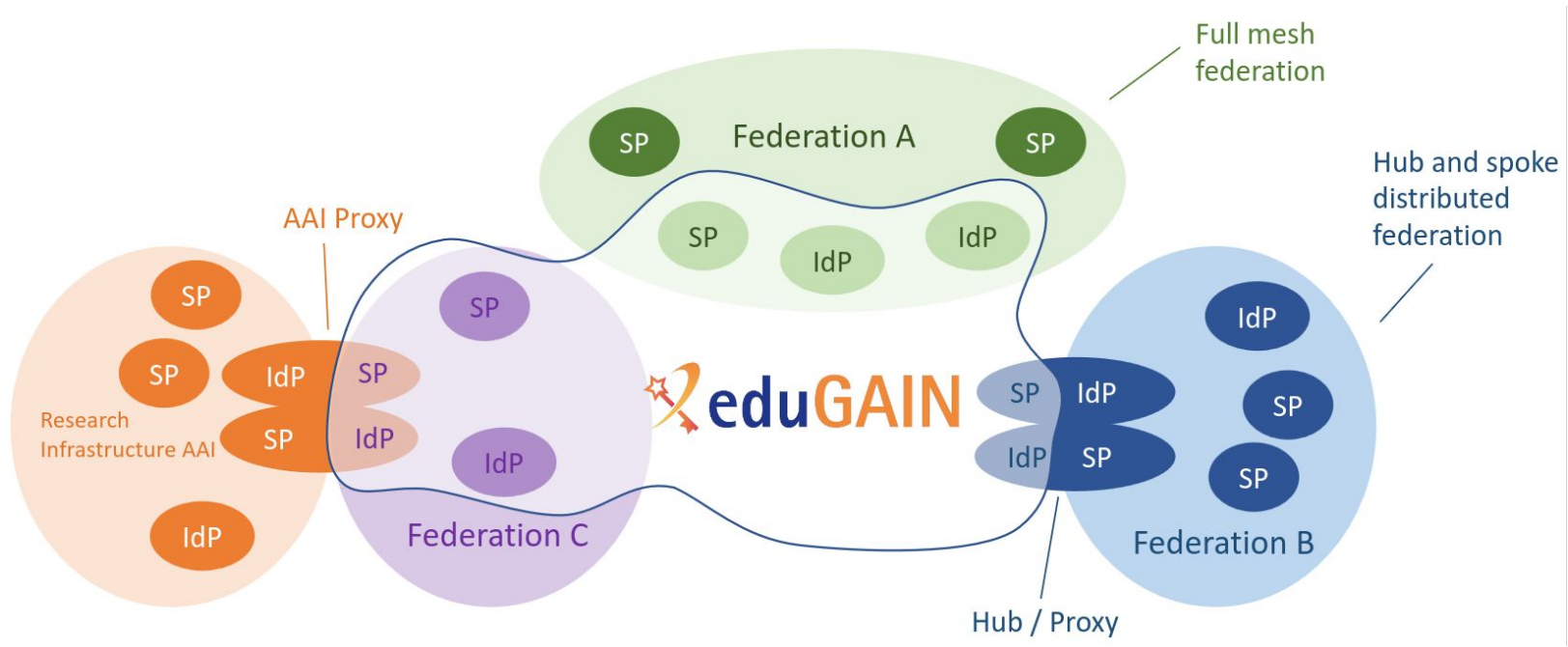
eduGAIN Metadata Distribution Service

1. Metapodaci Federacija
2. Kreiranje eduGAIN metapodataka
3. Potpisivanje i distribucija eduGAIN metapodataka
4. Federacije redistribuiraju eduGAIN metapodatke





eduGAIN Interfederacija

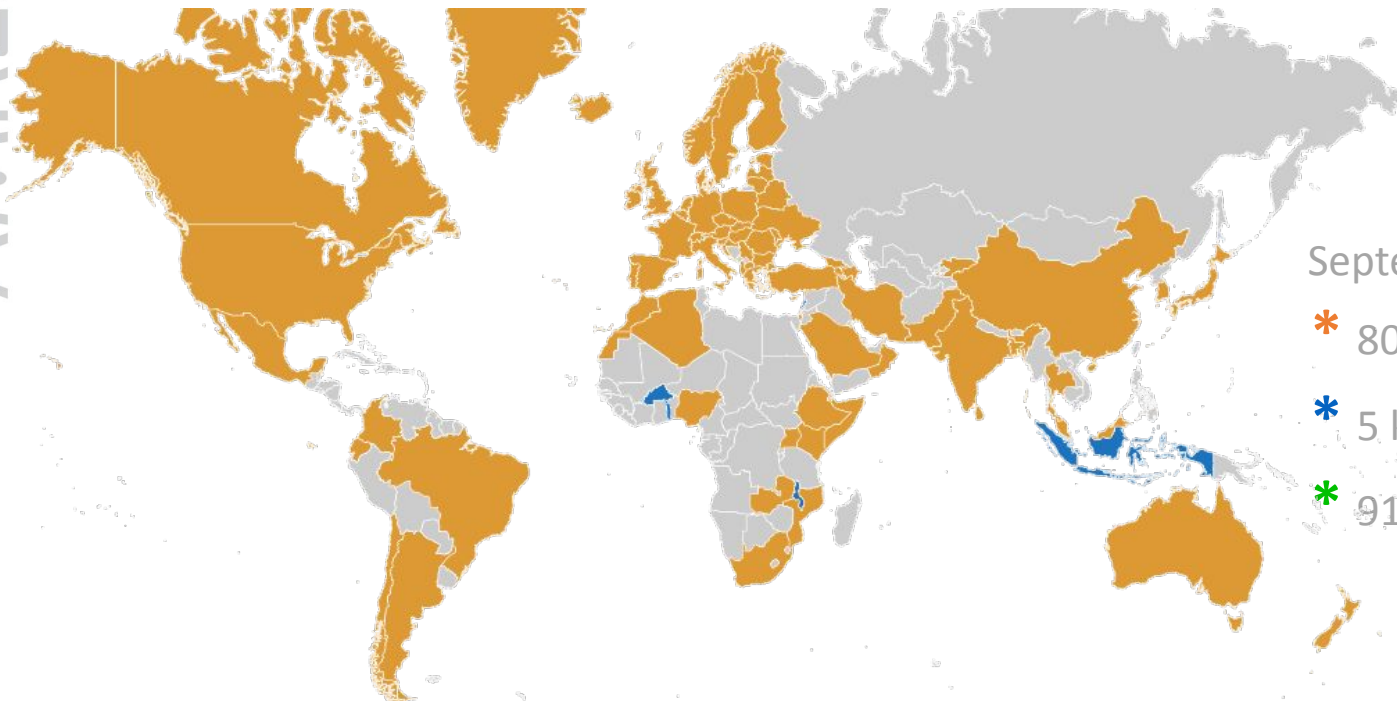




eduGAIN Interfederacija

AMRES

- Enabling access for the global research and education community



Septembar 2024:

- * 80 aktivnih Federacija
- * 5 kandidata
- * 9100+ entiteta



Dostupni Servisi

eduGAIN servisi:

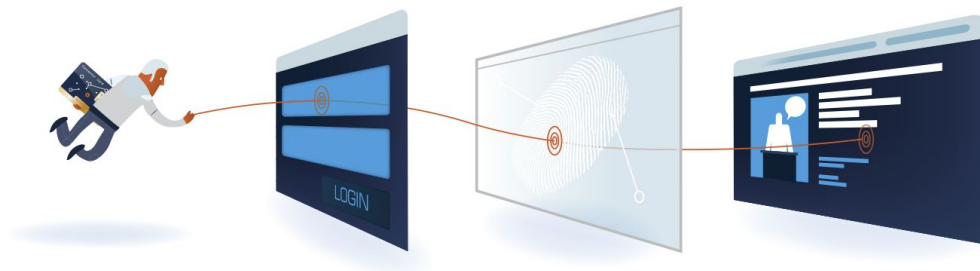
- MyAcademicID
- Erasmus Without Paper, <https://esci-sd.atlassian.net/wiki/spaces/EWP/overview>
- Elsevier, Scopus, SciVal
- Ostali entiteti - <https://technical.edugain.org/entities> .

iAMRES servisi:

- Filesender <https://filesender.amres.ac.rs>
- eduroam CAT <https://cat.eduroam.org>
- AMRES Forum <https://forum.amres.ac.rs>
- Sectigo <https://cert-manager.com/customer/AMRES>
- eduVPN, u pripremi
- eduMEET <https://edumeet.amres.ac.rs/>



Komponente Federacije Identiteta



01

Šta je SAML protokol?

02

Uloga SAML komponenti

03

Koncept slanja atributa



Komponente Federacije Identiteta

```
</ds:RSAKeyValue>
</ds:KeyValue>
<ds:X509Data>
  <ds:X509Certificate> MIIDDzCCAfcCFDRjXj5buopQY/s+nY6EZsZJFENMA0GCsGqSIb3DQEBQwUAMEQxCzAJBgNVBAYT AkLUMRYwFAYDQQKDAI1JREVNIEdBULiQUFJMR0wGwYDVQQDDBRjREVNIE1ldGFKY:
  cJAeFw0yMTEeMTkxMTEYMDFAfW0yNDEeMTkxMTEYMDFAeQwxCzAJBgNVBAYTAKLUMRYwFAYDQQK DA1JREVNIEdBULiQUFJMR0wGwYDVQQDDBRjREVNIE1ldGFKYXRhIFNpZ251c3CCASiWdQYJkoZI
  hvcNAQEBBQADgGEPADCCAQoCggEBAMay3r03AE6hgCPUVjvCyoLS0KTHs9CXDIyFAoigP+Y SdLoLSGwX6n6ks9aBbJqLzRBIEd3CpByvX7GmBuITL3EhXhMY40Cv/ULok1GbdMqMhPscU6J1f9b
  526R9Ks+bb7ZYmBRX9gmX1R867IES47vTPJfaDgH2xORL6msXjwM2DgajCOPBCct LvCWcmlUpUcpL8VHGjFAAI5EB6pwQEEPj1yqW52g2m+AHNFY6bAC9RX7Qv8MonQZwXpNNBNL+Ucn
  GLVBXtBftd4zq7XxPMN9F/ElE3YJGa0UWtYlAyaYh8f/BFEs6CwucSsCAwEAATAN BgkqhkiG9w0BAQsFAA0CAQEAn2e0JrKkQpkdyAKkIho4YNXhdKGe6XyEBP60P/Ymg062LtwPpdC
  KMFOEaiZkn2NcfvTuP0Jyex400M0PDJqeQQ13Jdd/e/hZLsm03HsvdC0u3kneA7k0tViMu9nLw0RPGHekulD9H5I6EmCuDqgHq+EN2oolB54xsAYK75LmgIw+Cb0ZCG/EPV6jMTR
  yoebeKNpAx0xIwpPF17jq4t2EB0ZnjEoE0Dip2Wj28P+sW3H0V05WVkrsLv Dzedkcm7UJ9HZYkxnmK6Yv4ohghgBwfjRhqTLU6GgpIIj0qDYN8sayaRJHcw== </ds:X509Certificate>
  </ds:X509Data>
  </ds:KeyInfo>
  </ds:Signature>
  <md:Extensions xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
    <mdrpi:PublicationInfo creationInstant="2024-05-23T12:14:44Z" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
      </md:Extensions>
    <EntityDescriptor xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:idpdisc="urn:oasis:names:tc:SAML:profiles:
    protocol" xmlns:init="urn:oasis:names:tc:SAML:profiles:S50:request-init" xmlns:profiles="urn:oasis:names:tc:SAML:profiles" xmlns:profiles="urn:oasis:names:tc:SAML:profiles"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:shibmd="urn:mace:shibboleth:1.0:metadata" xmlns:shibmd="urn:mace:shibboleth:1.0:metadata" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    entityID="https://xploreuat.ieee.org/shibboleth-sp">
      <Extensions>
        <mdrpi:RegistrationInfo registrationAuthority="http://www.idem.garr.it/" registrationInstant="2024-05-23T11:00:00Z" />
          <mdrpi:RegistrationPolicy xml:lang="en">https://www.idem.garr.it/raw/idem-mrps-1.0.md</mdrpi:RegistrationPolicy>
          </mdrpi:RegistrationInfo>
        </Extensions>
      <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" urn:oasis:names:tc:SAML:2.0:profiles:idpdisc="urn:oasis:names:tc:SAML:profiles:
      idpdisc" />
        <KeyDescriptor>
          <ds:KeyInfo>
            <ds:X509Data>
              <ds:X509Certificate> MIIcUcCCAaACCQDAKCYv5apLLTANBqgkhkiG9w0BAQsFADAeMRwGgYDVQQExNp ZWVleHBsb3JlLmllZlZwUub3JnMB4XLTU2MjUxMDYyOTkxMTEyMDY2MTUxMDY2MTUxMDE4
              OVowHjEcMBoGA1UEAxMTaWVlZXBhbG9yZS5pZWVlLn9yZzCCASiWdQYJkoZIhvCn AQEBQADgGEPADCCAQoCggEBAMx0UoovELST5WX50XZSDq/LpTRAz0hNYtkto
              WNWfH0XHN+8Wl4Z3UQUQeAU000gJ8j8js0sALUXKEbPTXDTtLV00CsuaI8hks0ft Ym90MPfgh11IaFmCGRErWx+GWPxaXkdMasIwmdcml9iutVni15rjOaz1z0wb4ZC
              H1pw0c2zYAQL9XSWerM7g3z2g4d2pVf/LS71R2urInI2UM5RxP0UN/L8M8BJatj7X SQ9eyrVIUmk7f1YskdpHLoD30xmQUXoJgn9CaPSjSx4QNmjdDB3b5tPstlwMI+
              Zu4L/jMSdq6Emwz1ABR+eJZesoWvmA/qMx0a5TiLpZrSMnECAwEAATANBgkqhkiG 9w0BAQsFAA0CAQEAyBw97Ere0Tq2UtL8iD4RBCMVN20yNG34lqmyzA4M35PlV
              sz4/Dwn2Ax4+0bd/7/Tq10f35687KNOCXnKSEi3C6xArRG7CUuI0b7y5Y3JTBZ P+hIapUpkQP+Ppxpe1ls0kqcpctqSdAm/w+MPCzm4wXgPFJselwldGvsQj++4Wn
              k0/GS1+3s/n0flrf8G60uDLgb/W6L8j4n6s6kqg/z1/E0+/Qy84otrVR9wcX25 GskE9LYnXZAYTU48Vheqjudd3g5Y04axMYxttcvG3c1qMkS44q9f90TyApRT9 py2oI9VKC04U/S7EGIDloDFP03V0UN
              </ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </KeyDescriptor>
        <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
        <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://xploreuat.ieee.org/Shibboleth/Shibboleth.sso/SAML2/POST" index="
        1" />
        <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign" Location="https://xploreuat.ieee.org/Shibboleth/Shibboleth.sso/SAML2/PO
```

What is SAML beyond a lot of XML ?



Security Assertion Markup Language (SAML)

- SAML 2.0 - de facto OASIS standard za Federacije Identiteta akademske zajednice
- SAML 2.0 Web Browser Single Sign On Profile
- SAML V2.0 Deployment Profile for Federation Interoperability - SAML2int

- SAML Metapodaci - XML dokument koji opisuje SAML entitete

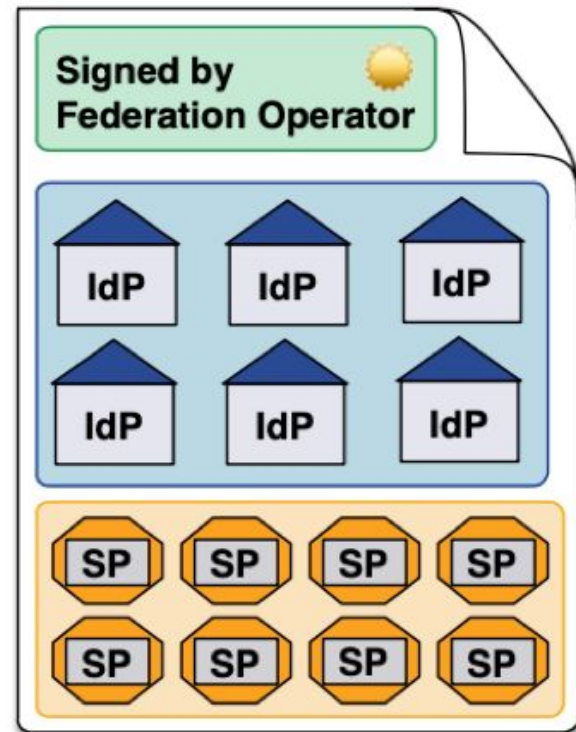
SAML Metadata Specification





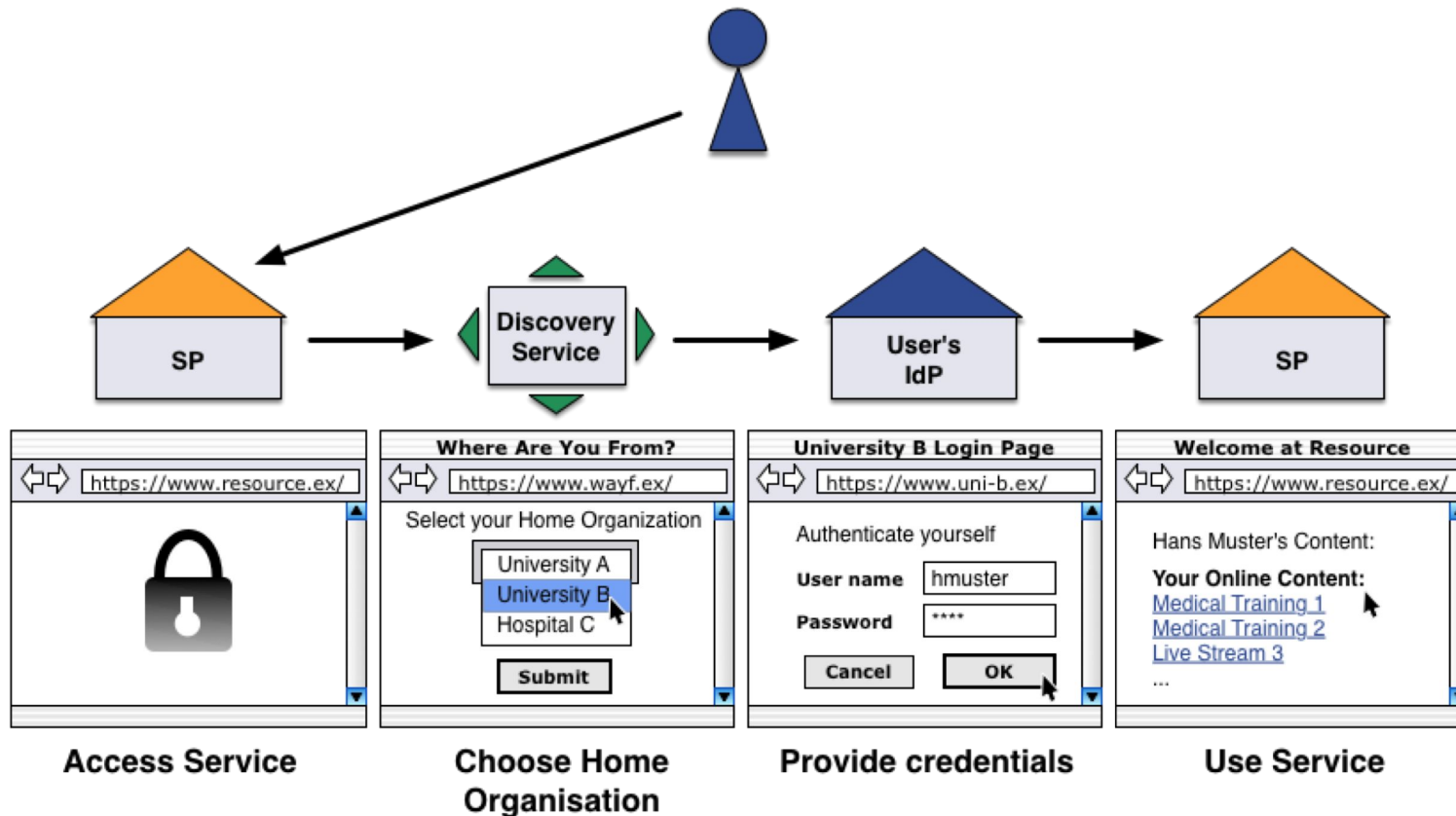
Struktura metapodataka Federacije

- Metapodaci moraju da imaju odgovarajući nivo zaštite.
- Ne postoji predefinisani redosled entiteta.
- I drugi entiteti mogu biti registrovani u okviru metapodataka, ali su ti uglavnom Davaoci Identiteta i Davaoci Servisa





Proces autentifikacije





SAML tok autentifikacije

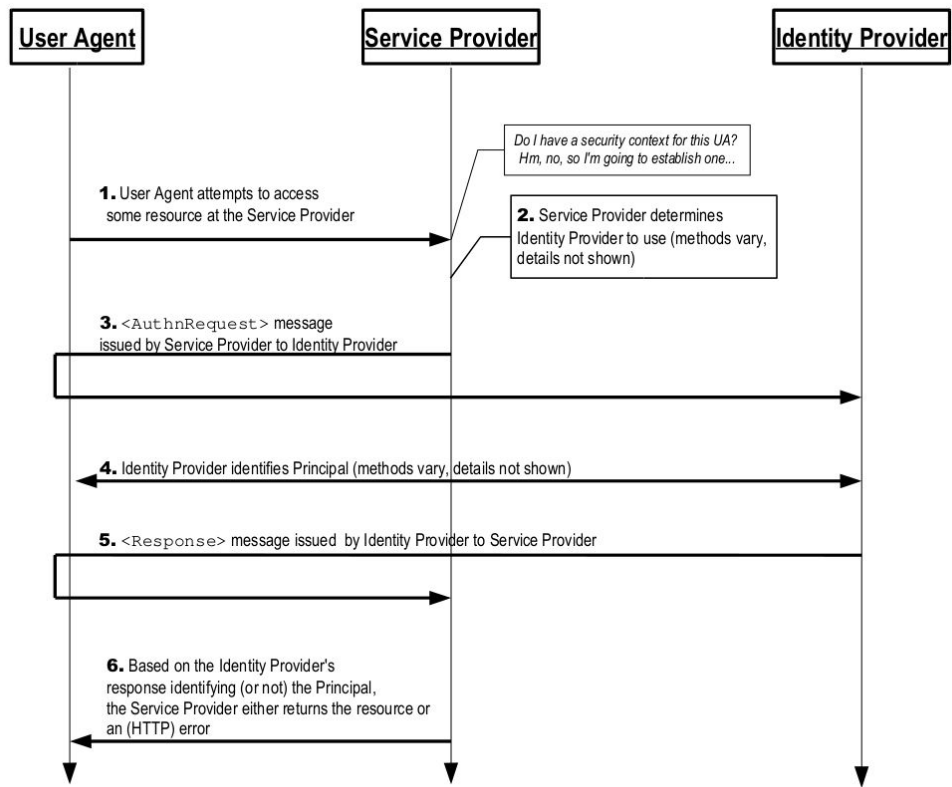
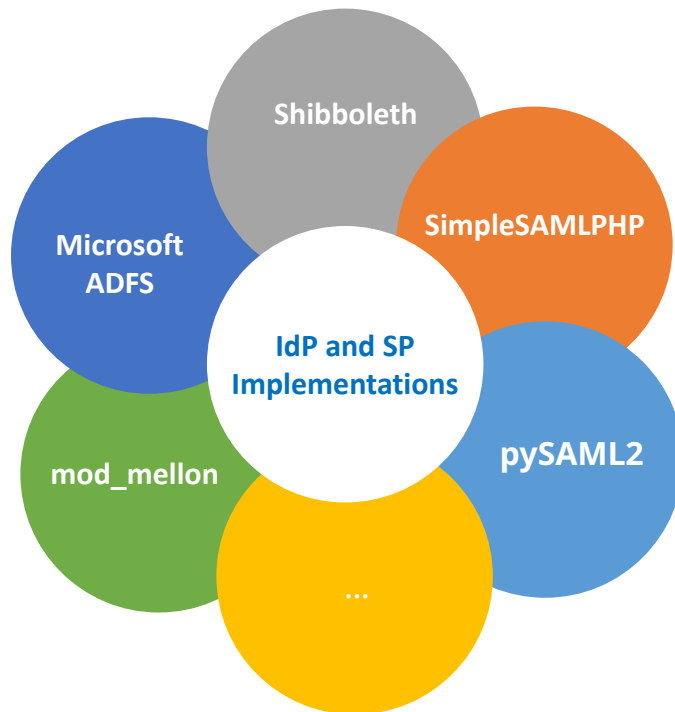


Figure 1



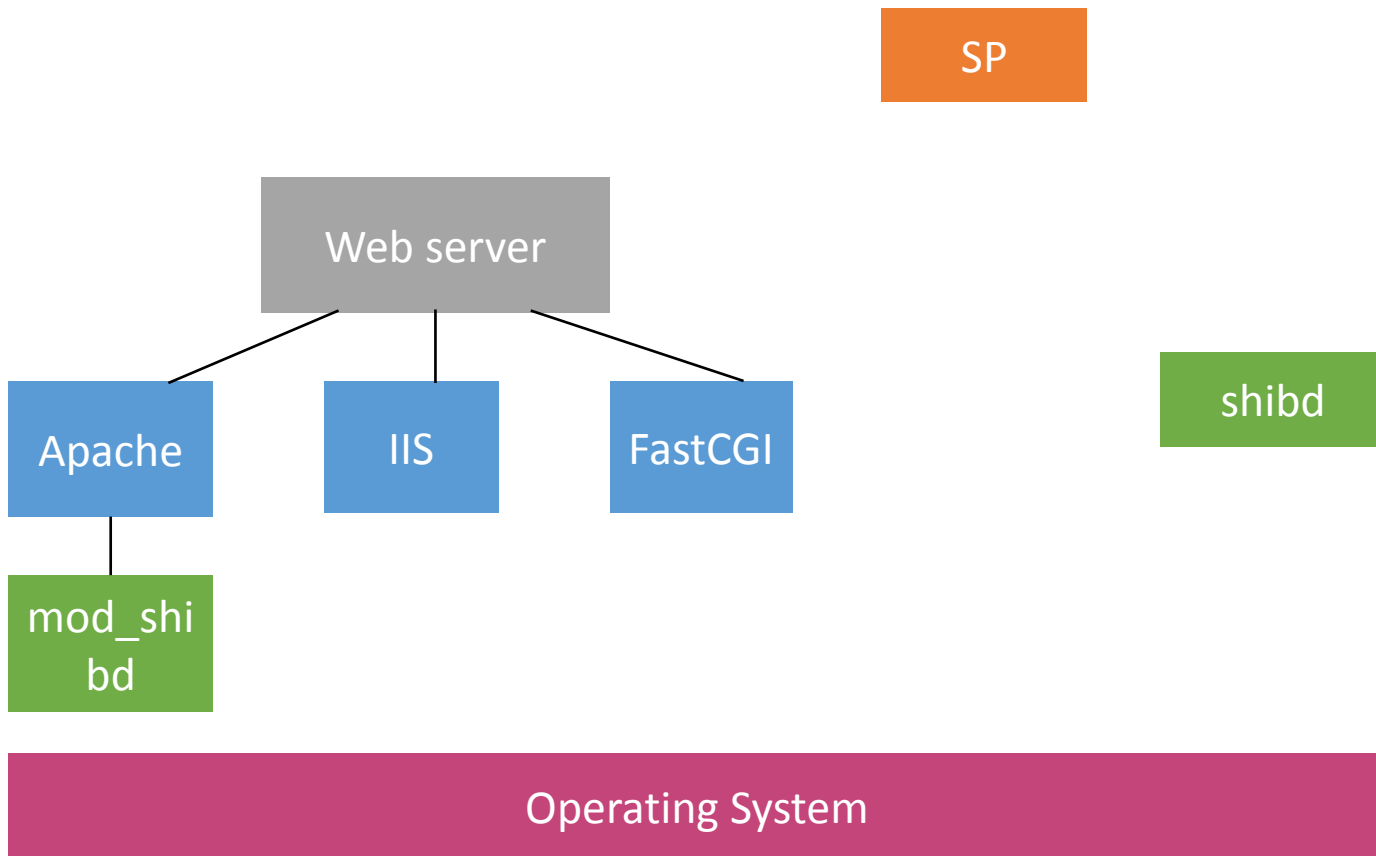
SAML IdP i SP implementacije



Shibboleth®

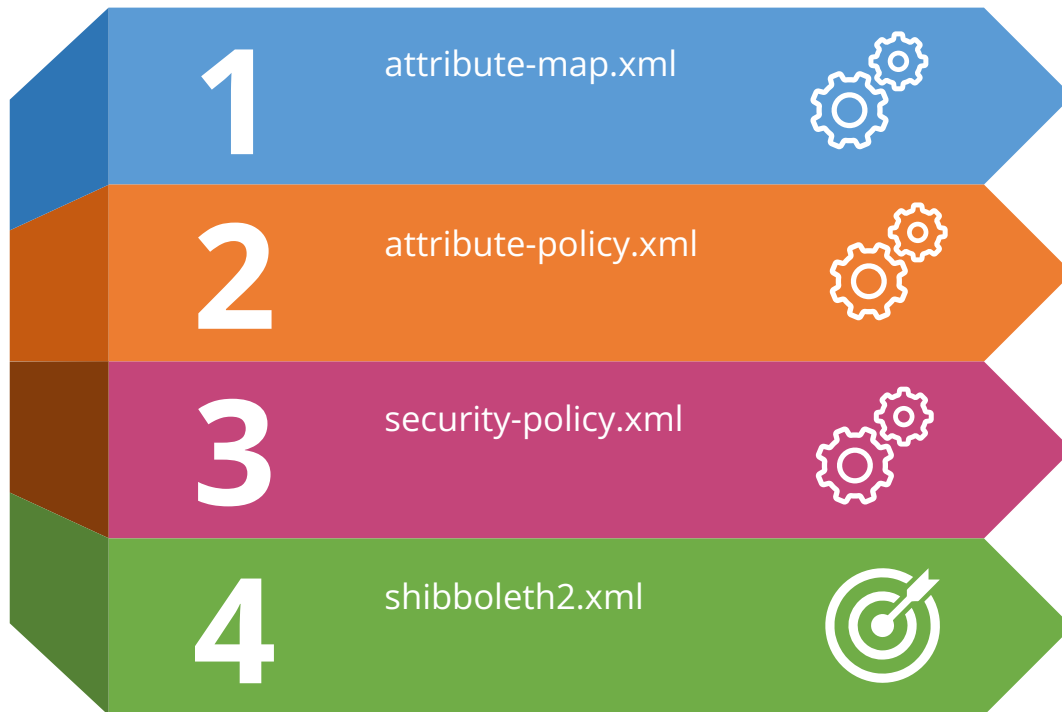


Shibboleth SP





Shibboleth SP





Shibboleth IdP

AMRES

- *Authentication Engine*
- *Attribute Resolver*
- *Attribute Registry*
- *Attribute Filter*
- *Metadata*





Authentication Engine

- Zasnovan na Spring Web Flow

- Login opcije:

- Password
- RemoteUser
- RemoteUserInternal
- X509
- X509Internal
- SPNEGO / Kerberos
- IPAddress
- External
- Multi-Factor
- Function
- SAML

Najpopularniji

Gde specificirati koji će tip autentifikacije biti korišćen ?

`/opt/shibboleth-idp/conf/authn/*`
`/opt/shibboleth-idp/conf/c14n/*`

Gde mogu da nađem dostupne tipove?

`/opt/shibboleth-idp/auth/...`



Attribute Resolver

- Inicijalni fajl i primeri su već ponuđeni
 - `/opt/shibboleth-idp/conf/attribute-resolver.xml`
- Sadrži :
 - **DataConnectors**
 - **Attribute definitions**
- *Attribute Resolver se oslanja na Attribute Registry*



DataConnectors

iAMRES konektori

DataConnector Plugin Types

- Static
- ScriptedDataConnector
- ComputedId
- StoredId
- PairwiseId
- RelationalDatabase
- LDAPDirectory
- HTTP
- Subject
- StorageService
- EntityAttributes

```
<!-- ===== -->
<!--      Data Connectors      -->
<!-- ===== -->

<!--
Example LDAP Connector

The connectivity details can be specified in ldap.properties to
share them with your authentication settings if desired.
-->
<DataConnector id="myLDAP" xsi:type="LDAPDirectory"
  ldapURL="%{idp.attribute.resolver.LDAP.ldapURL}"
  baseDN="%{idp.attribute.resolver.LDAP.baseDN}"
  principal="%{idp.attribute.resolver.LDAP.bindDN}"
  principalCredential="%{idp.attribute.resolver.LDAP.bindDNCredential}"
  useStartTLS="%{idp.attribute.resolver.LDAP.useStartTLS:true}"
  connectTimeout="%{idp.attribute.resolver.LDAP.connectTimeout}"
  trustFile="%{idp.attribute.resolver.LDAP.trustCertificates}"
  responseTimeout="%{idp.attribute.resolver.LDAP.responseTimeout}">
  <FilterTemplate>
    <![CDATA[
      %{idp.attribute.resolver.LDAP.searchFilter}
    ]]>
  </FilterTemplate>
  <ConnectionPool
    minPoolSize="%{idp.pool.LDAP.minSize:3}"
    maxPoolSize="%{idp.pool.LDAP.maxSize:10}"
    blockWaitTime="%{idp.pool.LDAP.blockWaitTime:PT3S}"
    validatePeriodically="%{idp.pool.LDAP.validatePeriodically:true}"
    validateTimerPeriod="%{idp.pool.LDAP.validatePeriod:PT5M}"
    expirationTime="%{idp.pool.LDAP.idleTime:PT10M}"
    failFastInitialize="%{idp.pool.LDAP.failFastInitialize:false}" />
</DataConnector>
```

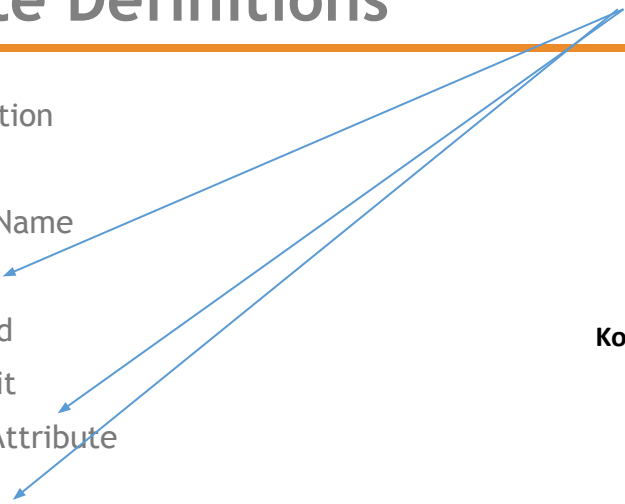


Attribute Definitions

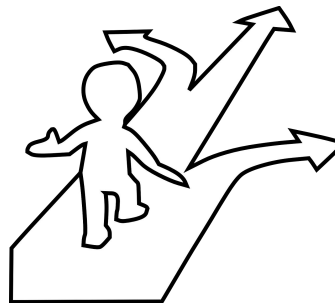
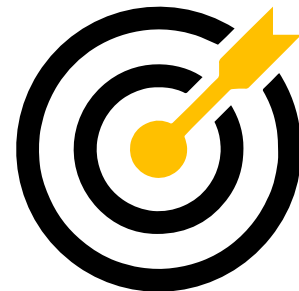
iAMRES definicije atributa

Attribute Definition

- Simple
- PrincipalName
- Scoped
- Prescoped
- RegexSplit
- ScriptedAttribute
- Mapped
- Template
- SubjectDerived
- ContextDerived
- Decrypted



Koju definiciju atributa odabrati?



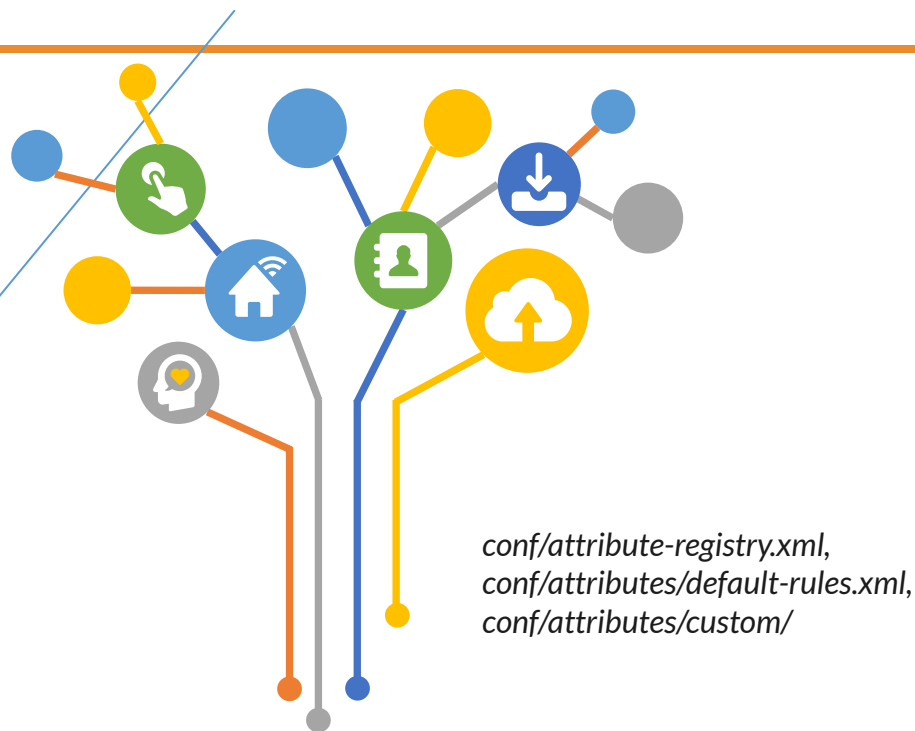


Attribute Registry

iAMRES šema atributa

Attribute Schemas

- samlSubject.xml
- eduCourse.xml
- inetOrgPerson.xml
- eduPerson.xml
- schac.xml
- Lokalne šeme - rsEdu.xml





Attribute Filter

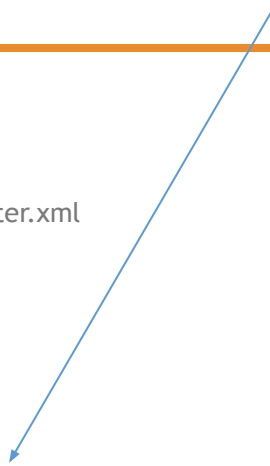
iAMRES dinamički filter

Inicijalni fajl i primeri su već ponuđeni

- /opt/shibboleth-idp/conf/attribute-filter.xml
- Definicija pravila za svaki SP
- Definicija pravila za svaki atribut

Upotreba i konfiguracija dinamičkog filtra:

- *Requested* atributi mogu biti specificirani u metapodacima (SP ili Federacija)
- IdP može biti konfigurisan da automatski salje skup atributa definisan u SP metapodacima





iAMRES Federacija Identiteta

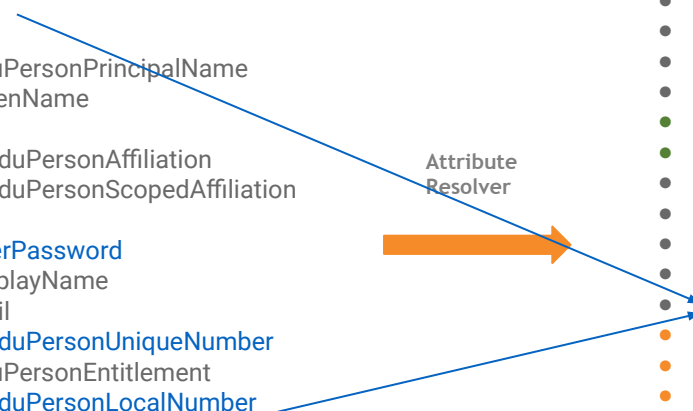
Atributi u OpenLDAP bazi:

- uid
- cn
- eduPersonPrincipalName
- givenName
- o
- rsEduPersonAffiliation
- rsEduPersonScopedAffiliation
- sn
- userPassword
- displayName
- mail
- rsEduPersonUniqueNumber
- eduPersonEntitlement
- rsEduPersonLocalNumber

Atributi koje IdP šalje:

- cn
- eduPersonPrincipalName
- givenName
- o/o
- eduPersonAffiliation
- eduPersonScopedAffiliation
- sn
- displayName
- mail
- eduPersonEntitlement
- schacPersonalUniqueCode (ESI)
- schacHomeOrganization
- schacHomeOrganizationType
- eduPersonAssurance
- persistent NameID
- eduPersonTargetedID
- samlPairwiseID

Attribute Resolver



Attribute Filter



SP



iAMRES Federacija Identiteta i eduroam

Login

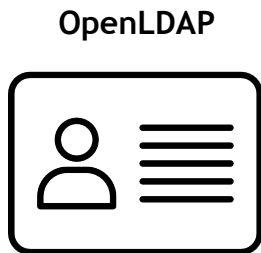
Enter your username and password

Username:

Password:



uid
userPassword



uid
cn
eduPersonPrincipalName
givenName
o
rsEduPersonAffiliation
rsEduPersonScopedAffiliation
sn
userPassword
displayName
mail
rsEduPersonUniqueNumber
eduPersonEntitlement
rsEduPersonLocalNumber

AMRES
Akademska mreža Srbije

Prijavite se na AMRES TESTSP

Korisničko ime:

Lozinka:

Ne pamti moju prijavu

Poništi raniji pristanak za prosleđivanje podataka ovom servisu.

Prijavi se



Kategorije entiteta

- Grupa entiteta koje imaju zajedničke karakteristike
- SP mora podržavati određene zahteve
- Federacija odlučuje o deklarisanju i pristupanju SP kategoriji
- Olakšavaju slanje atributa od IdP ka SP
 - Politika slanja atributa je definiše samo jednom, a ne za svaki SP
 - Ne mora ih menjati ukoliko se u okviru kategorije deklariraju i novi SP
 - IdP veruje svim servisima koji su deo kategorije

Tehnička implementacija:

SAML atribut kojim se taguju metapodaci IdP i SP entiteta - **SAML V2.0 Metadata Extension for Entity Attributes**

iAMRES kategorije entiteta:

1. Research and Scholarship (R&S)
2. CoCO (GEANT Data protection Code of Conduct) v2
3. SIRTFI (Security Incident Response Trust Framework for Federated Identity) v2

<https://wiki.refeds.org/display/ENT/Entity-Categories+Home>



Research and Scholarship (R&S)

Minimalni zahtevani skup atributa:

- eduPersonTargetedID (ePTID)
- eduPersonPrincipalName (ePPN) - **iAMRES: JEDINSTVEN I NEPONOVLJIV (unique and non-reassignable)**
- email
- displayName
- sn
- givenName
- eduPersonScopedAffiliation (ePSA)



CoCo (GEANT Data protection Code of Conduct) v2

- ❖ CoCo v1 - 2013 - zasnovan na EU zakonskom okviru iz 1995 (95/46/EG - Data Protection Directive)
- ❖ CoCo v2 - 2022 - zasnovan na EU zakonskom okviru iz 2018 (“GDPR”)

Da bi se deklarirao kao CoCo, IdP treba da:

- Šalje samo atribute koji su zahtevani u SP metapodacima kao «isRequired="true"»
- Ukoliko SP zahteva određenu vrednost multivalued atributa, IdP treba da pošalje samo tu vrednost
- Informiše korisnika o rukovanju atributima kroz **PrivacyStatementURL**

Da bi se deklarirao kao CoCo, SP treba da:

- Bude lociran EU/EEA i da podleže EU zakonima
 - Slanje podataka o korisnicima regulisano je kroz GDPR
 - Zahteva se samo minimalni set obaveznih atributa
- Zahteva neophodnih atributa kroz *RequestedAttribute statement* u obliku «isRequired="true"»
- Informiše korisnike o obradi ličnih podataka na *Privacy Policy* stranici



SIRTFI (Security Incident Response Trust Framework for Federated Identity) v2

- Samostalna procena mogućnosti reakcije na incidente
 - **Operational Security [OS]**
 - **Incident Response [IR]**
 - **Traceability [TR]**
 - **Participant Responsibilities [PR]**
- Dodati *security* kontakt u metapodacima
- Obaveza da se obaveste relevantni entiteti u slučaju incidenta



iAMRES trening

- VM hostname - `idp.institucijaN.amres.ac.rs`
- Scope LDAP aributa i shibboleth scope - **`institucijaN.amres.ac.rs`**
- Sertifikati - `/etc/ssl/private` i `/etc/ssl/certs`
- Slack - `#iamres-trening-dec-2024`
- OpenLDAP <https://docs.amres.ac.rs/uputstva/ldap/uvod/>
- Shibboleth <https://docs.amres.ac.rs/uputstva/shibboleth/shibboleth/>