iAMRES trening

AMRES

Akademska mreža Srbije

Decembar 2024.

Cilj treninga

01 Upoznavanje sa konceptima Federacije Identiteta

02 Upoznavanje sa eduGAIN interfederacijom

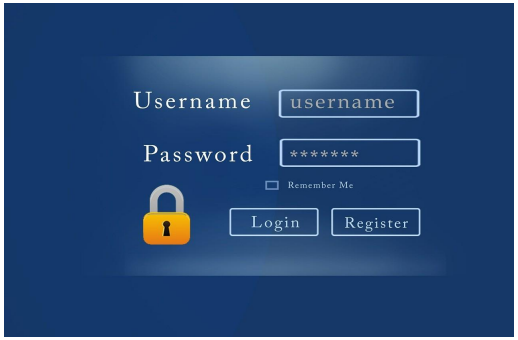
03 Sticanje znanja i veština potrebnih za implementaciju Davaoca Identiteta

04 Pridruživanje iAMRES Federaciji Identiteta

05 ...

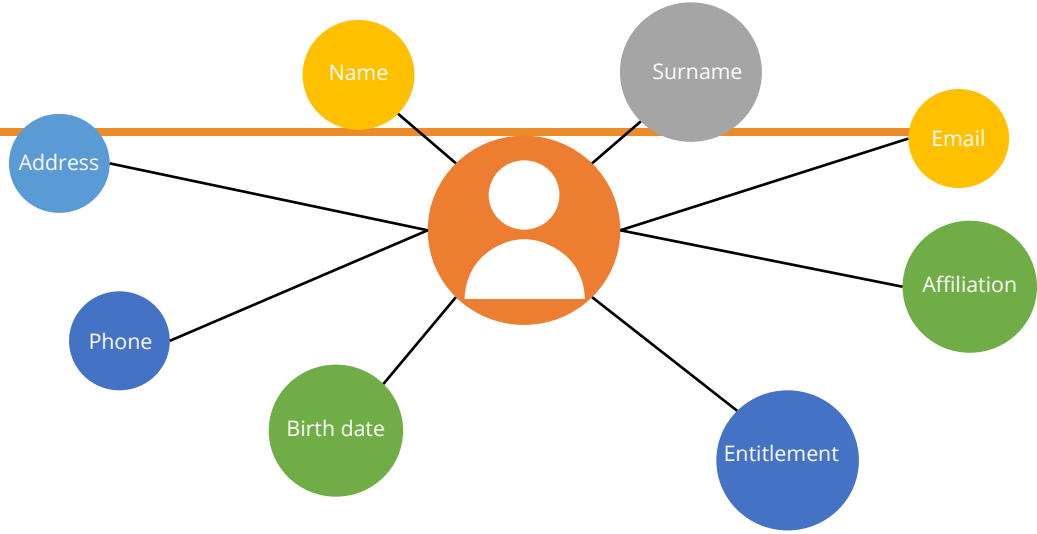
Proces upravljanja identitetima

- Identifikacija
- Autentifikacija
- Autorizacija



Digitalni Identitet

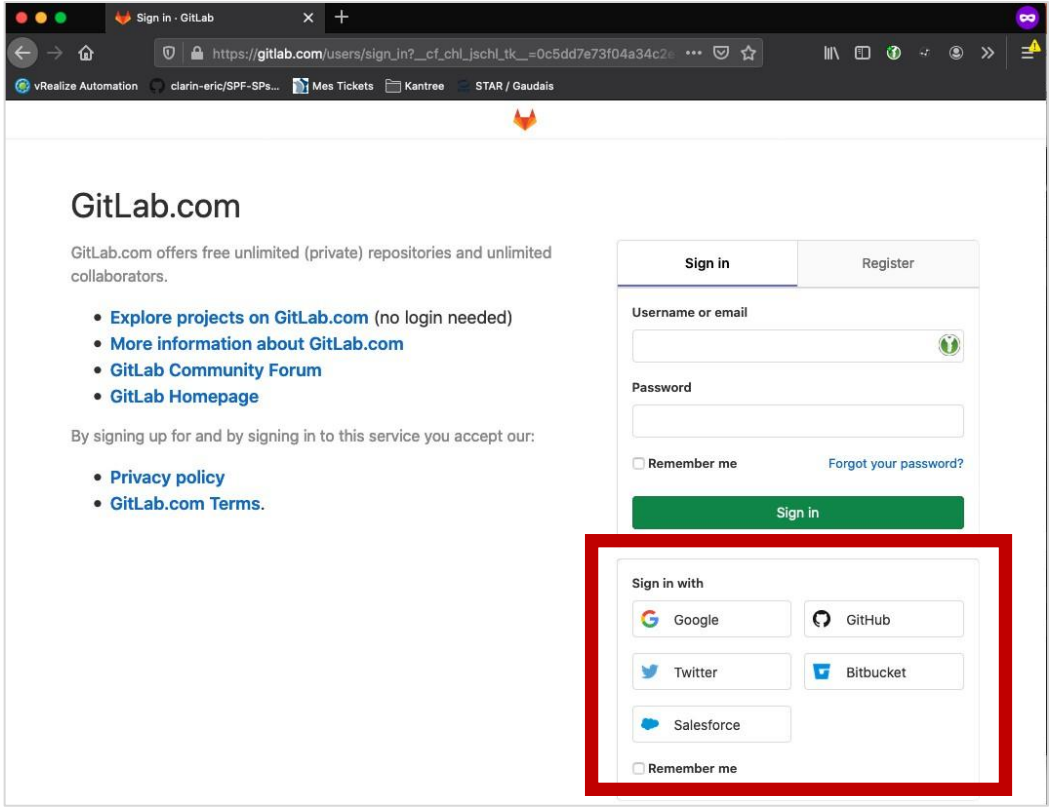
- **Skup atributa**



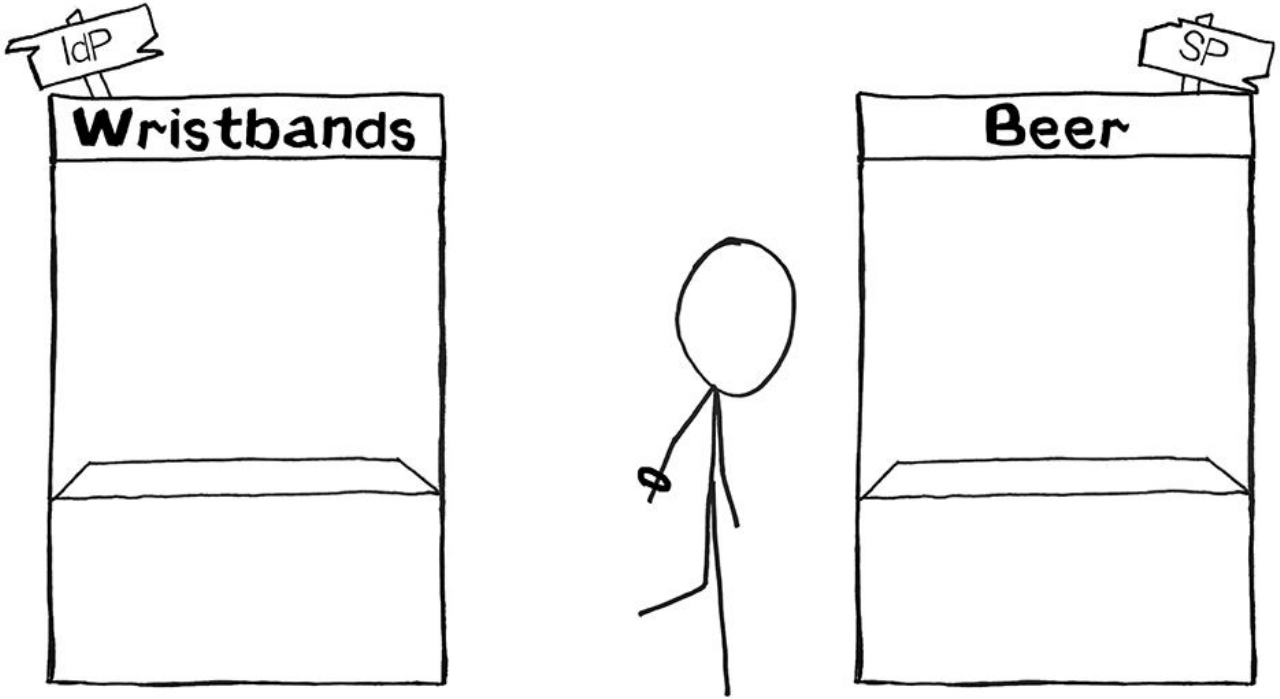
- Svrha:
  - **Identifikacija**: Predstavljanje osobe u digitalnoj formi
  - **Autentifikacija**: Dokaz da je u pitanju ista osoba koja je pristupala servisu
  - **Autorizacija**: Kontrola pristupa na osnovu vrednosti pojedinih atributa
  - **Profil**: Personalizacija, informacije o osobi kao što su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

Delegiranje procesa autentifikacije

Primer

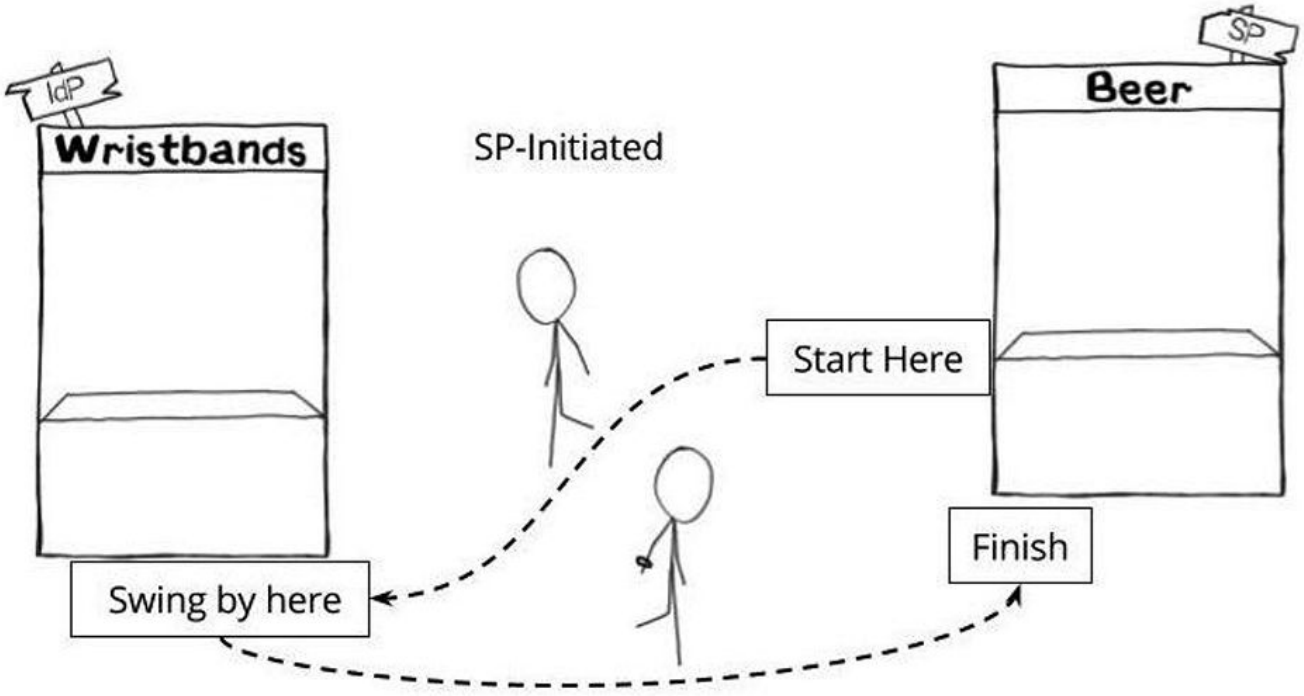

Sign in · GitLab
https://gitlab.com/users/sign_in?__cf_chl_jschl_tk__=0c5dd7e73f04a34c2
vRealize Automation
clarin-eric/SPF-SPs...
Mes Tickets
Kantree
STAR / Gaudais
GitLab.com
GitLab.com offers free unlimited (private) repositories and unlimited collaborators.
Explore projects on GitLab.com (no login 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



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

Federaciju Identiteta čine entiteti

Davalac Identiteta

Identity Provider (IdP) ~ Home organization (HO)

Davalac Servisa

Service Provider (SP) ~ Relying Party (RP)

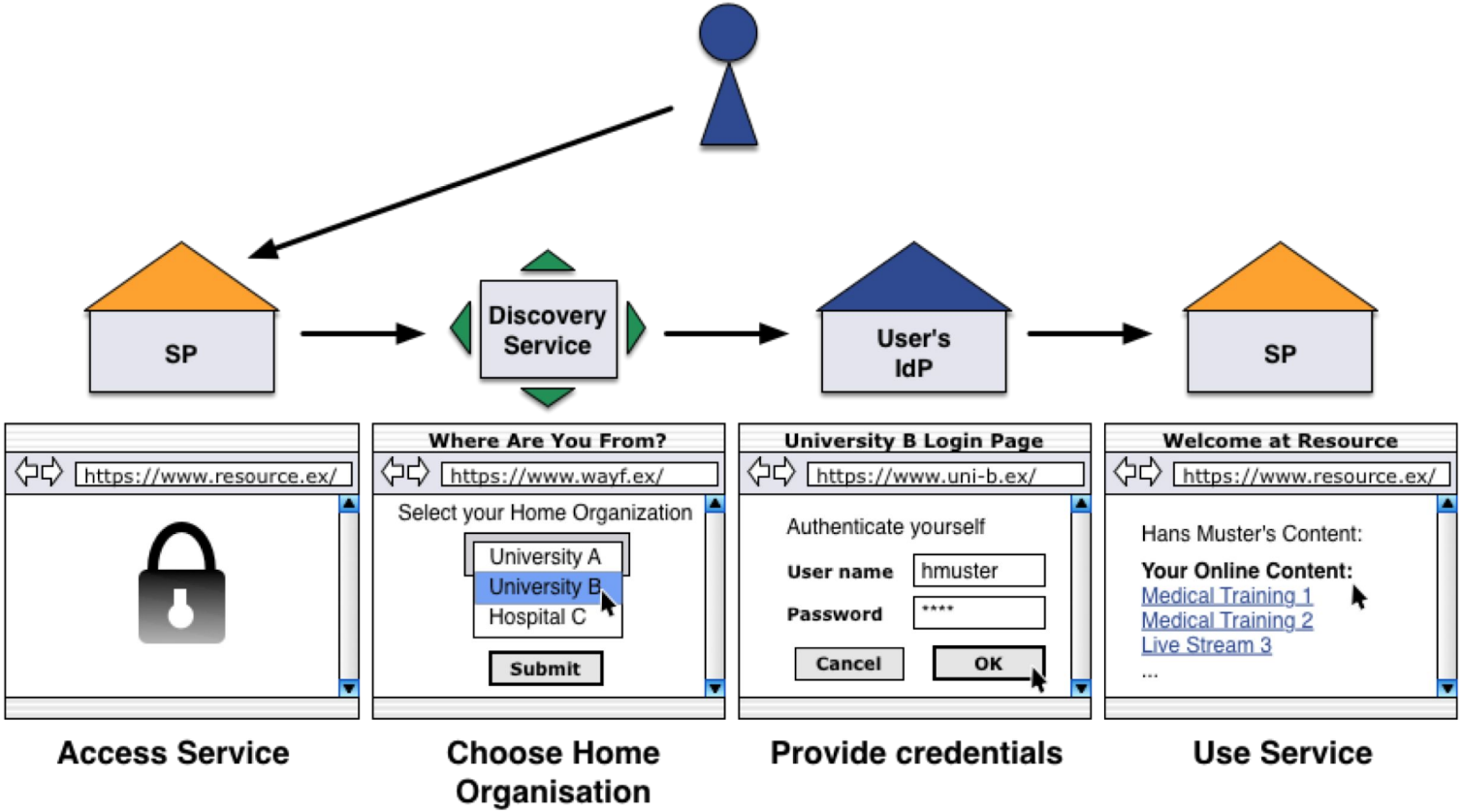
Discovery Service (DS)

Federacija Identiteta

- Protokol (SAML, OIDC, etc.)

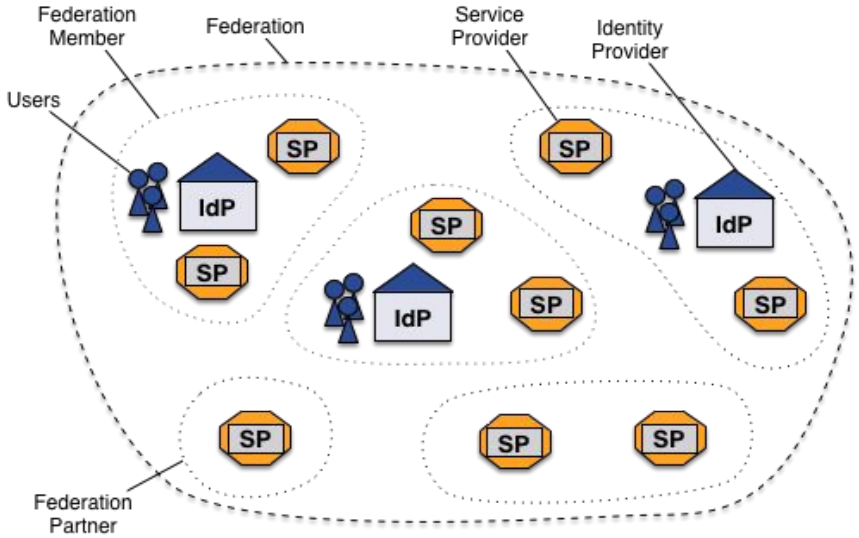
- Poverenje se uspostavlja na više načina:
  - Ugovor između SP/IdP administratora (Bilateralni sporazum)
  - Putem treće strane (Federacija)

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.



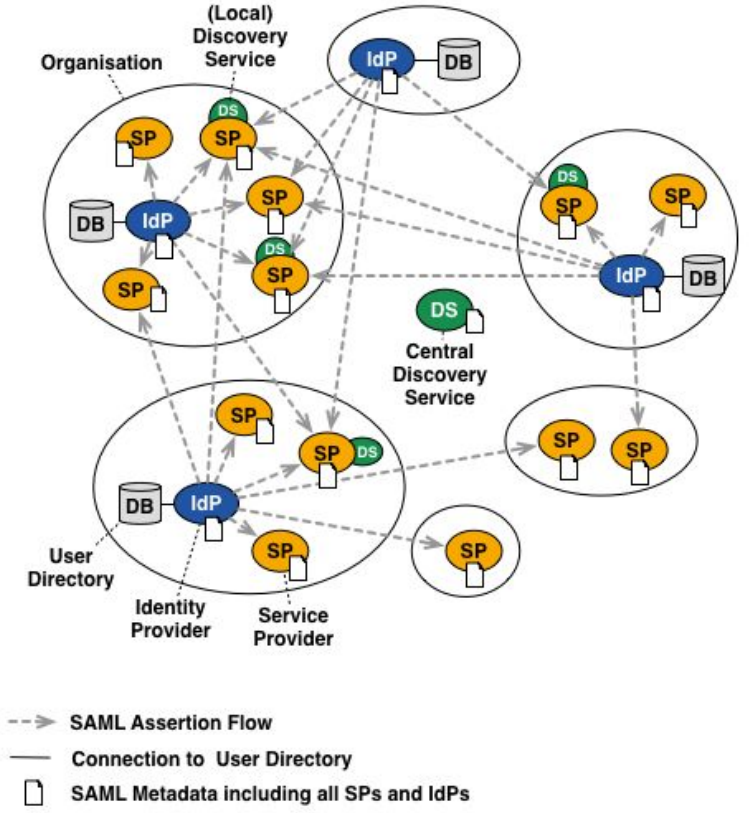
Tipovi Federacija Identiteta

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

Full Mesh Federacija Identiteta

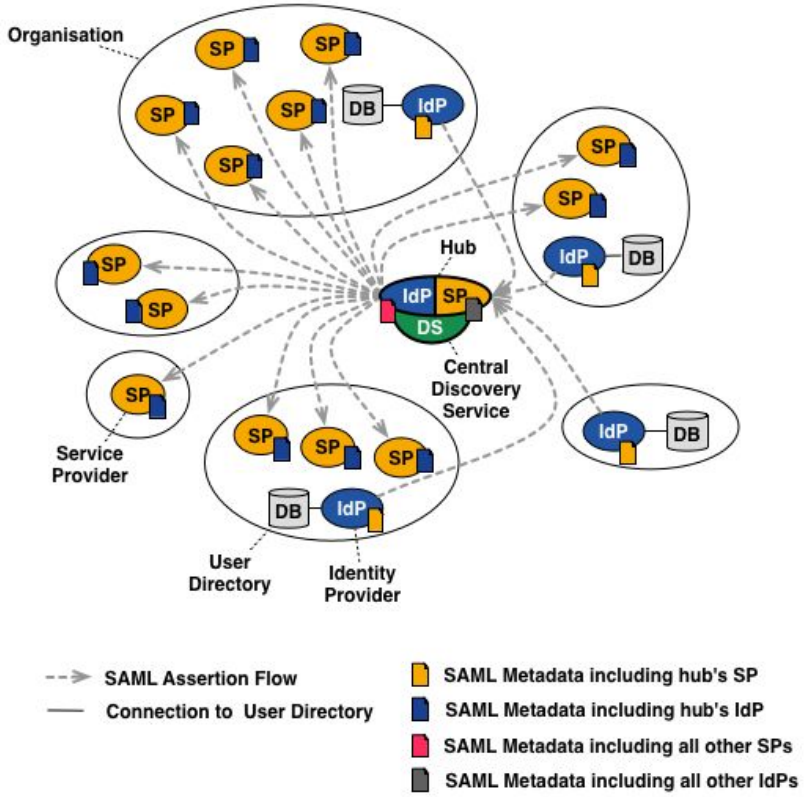
Entiteti su distribuirani

Nema centralne komponente



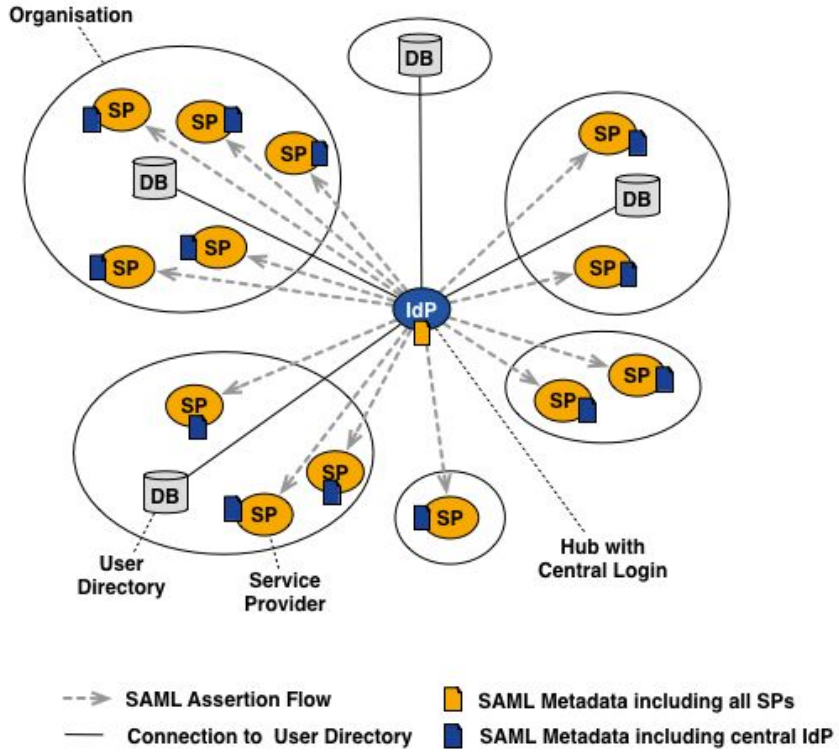
Hub & Spoke Federacija Identiteta da distribuiranim login stranicama

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



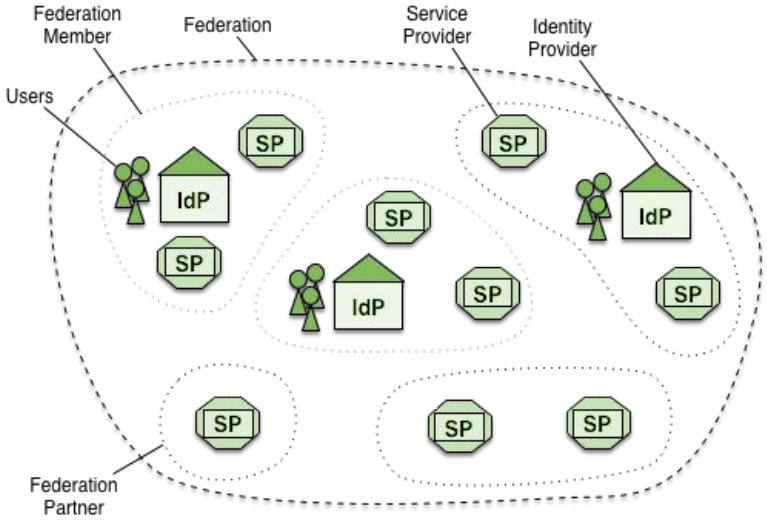
Hub & Spoke Federacija Identiteta da centralnom login stranicom

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



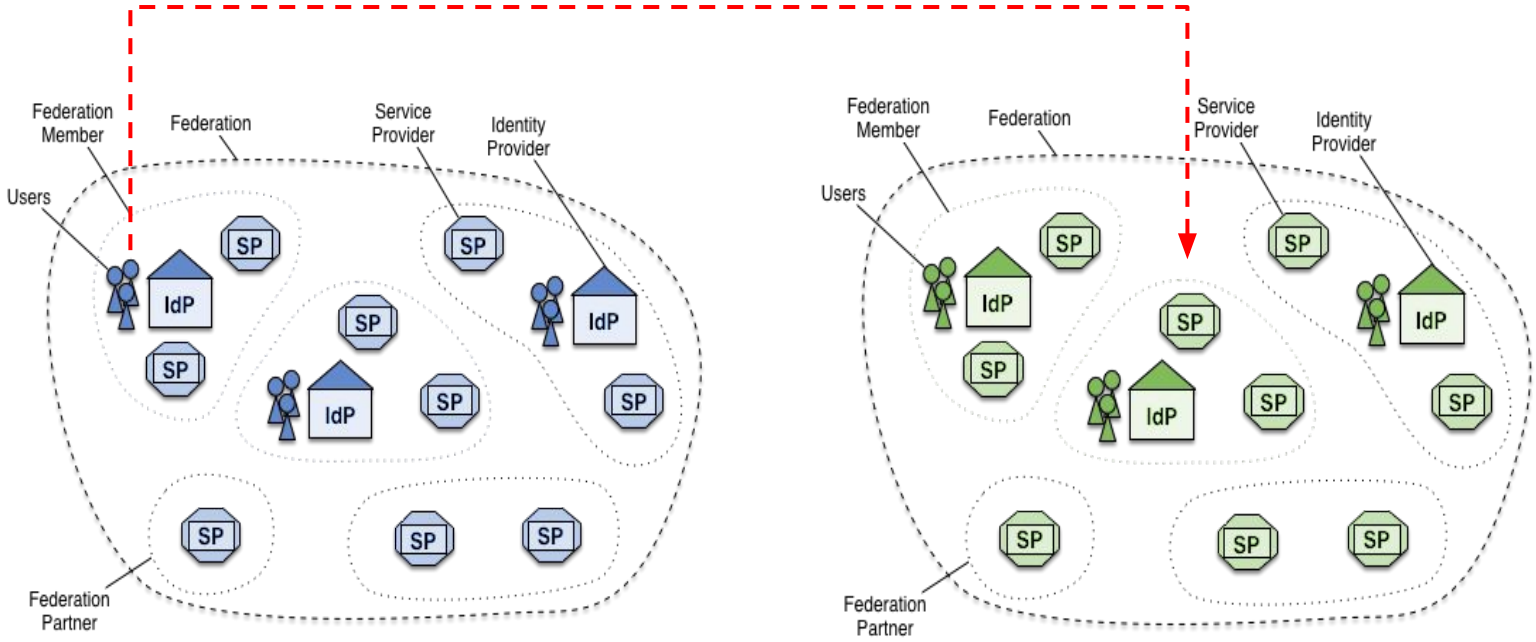
Entiteti, metapodaci i Federacija

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



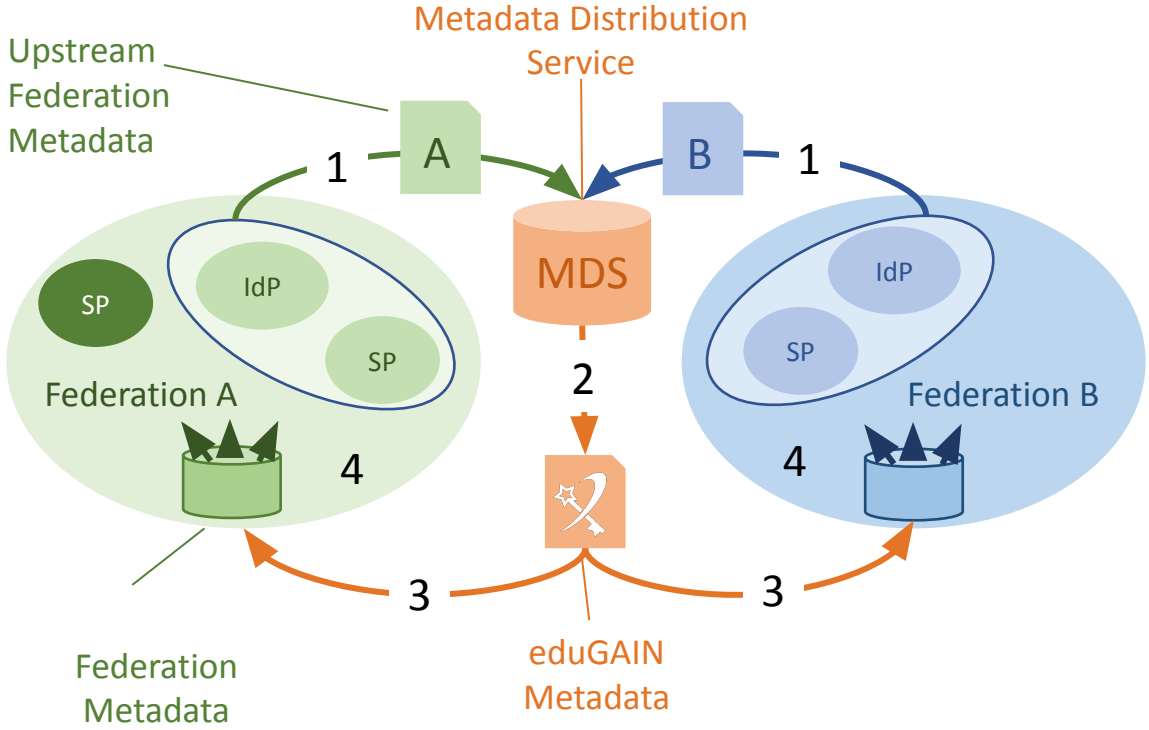
Metadata is the technical information required for integration between members of the federation.

Interfederacija

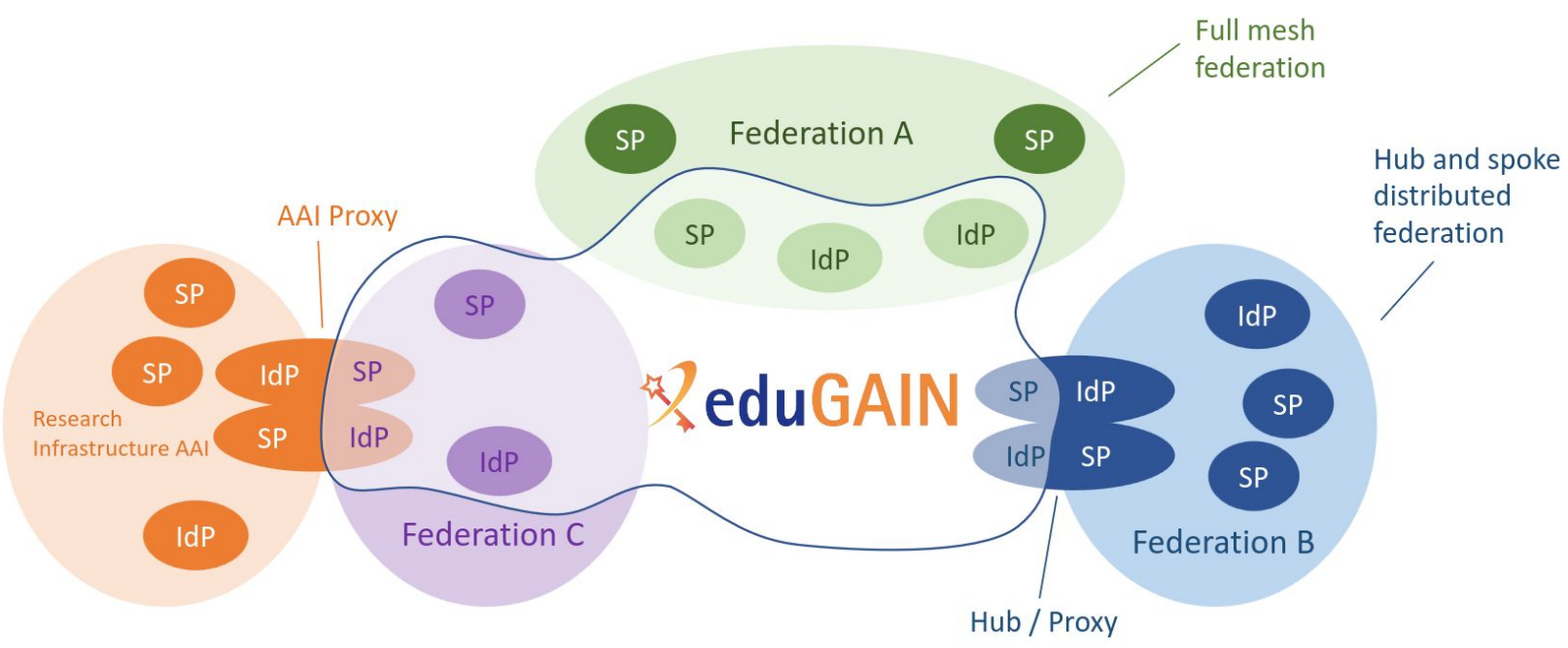


eduGAIN Metadata Distribution Service

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



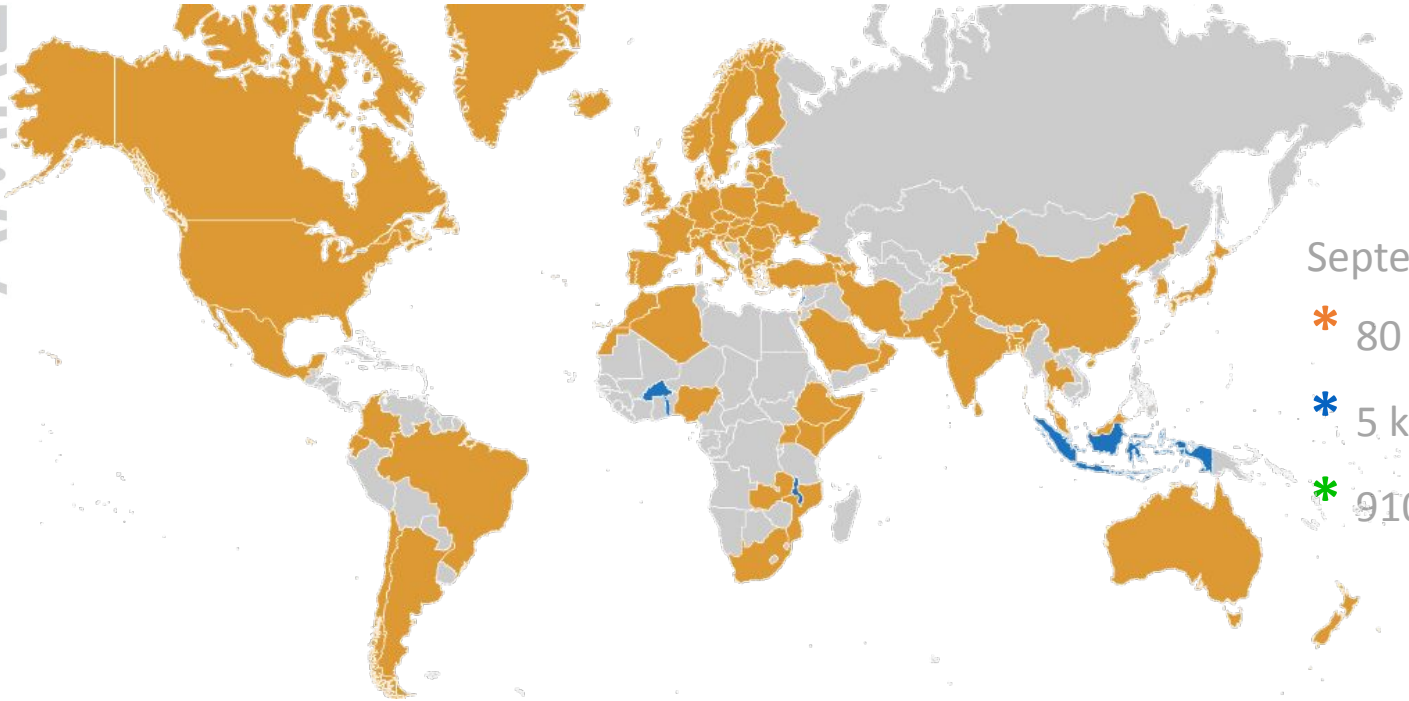
eduGAIN Interfederacija



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:

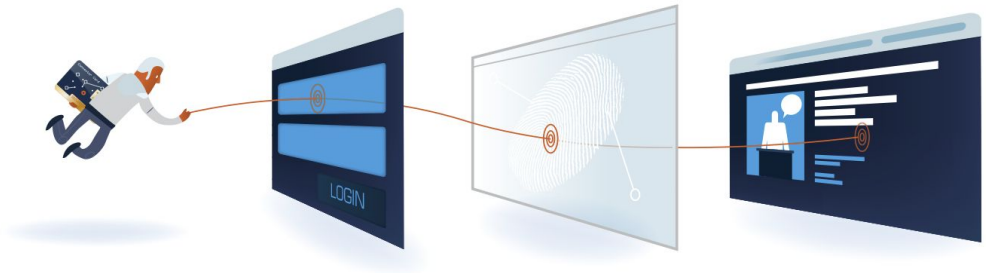
- MyAcademicID
- Erasmus Without Paper, https://esci-sd.atlassian.net/wiki/spaces/EWP/overview
- Elsevier, Scopus, SciVal
- Ostali entiteti - https://technical.edugain.org/entities .

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/

AMRES

Komponente Federacije Identiteta



01 Šta je SAML protokol?

02 Uloga SAML komponenti

03 Koncept slanja atributa

Komponente Federacije Identiteta

Security Assertion Markup Language (SAML)

- **SAML 2.0 - de facto OASIS standard za Federacije Identiteta akademske zajednice**

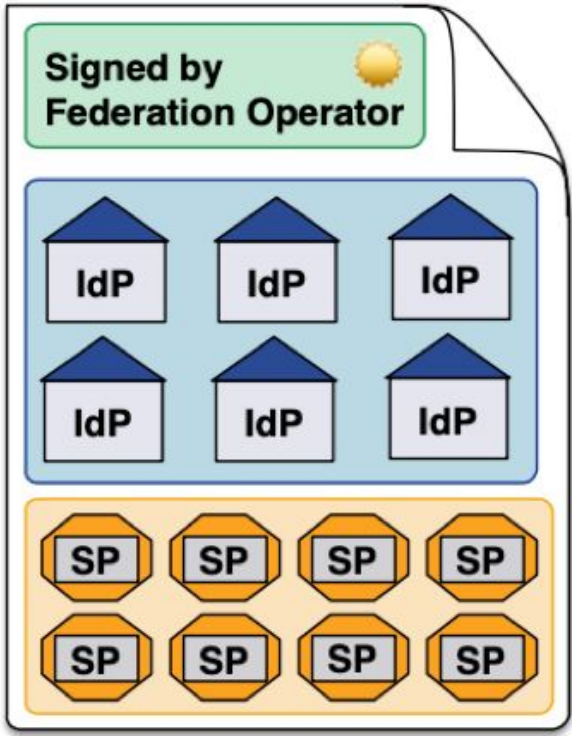
- SAML 2.0 Web Browser Single Sign On Profile
- SAML V2.0 Deployment Profile for Federation Interoperability - SAML2int

- SAML Metapodaci - XML dokument koji opisuje SAML entitete

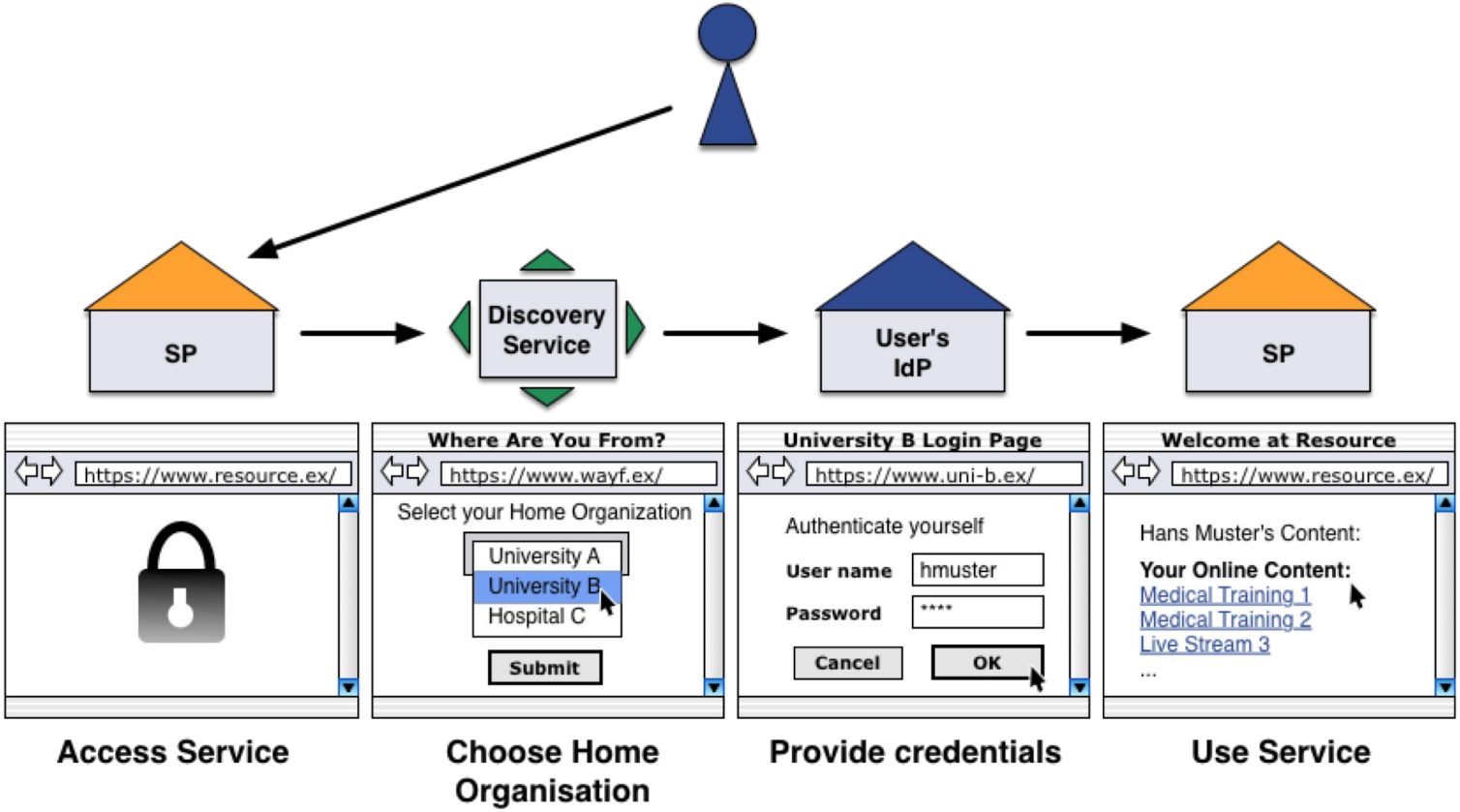
SAML Metadata Specification

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

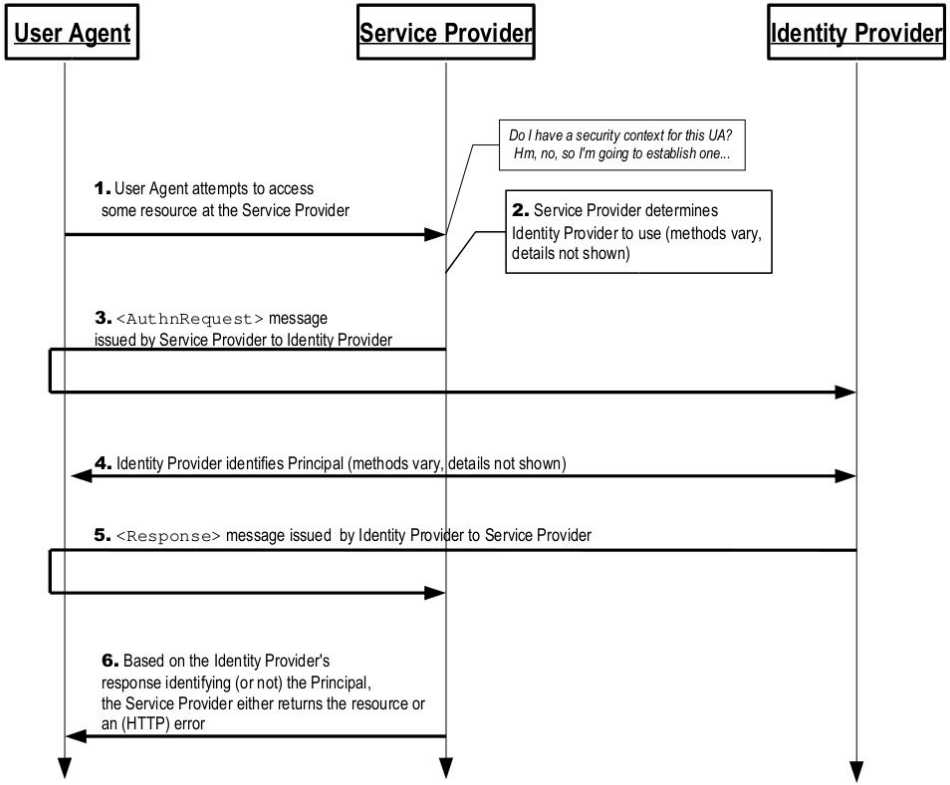
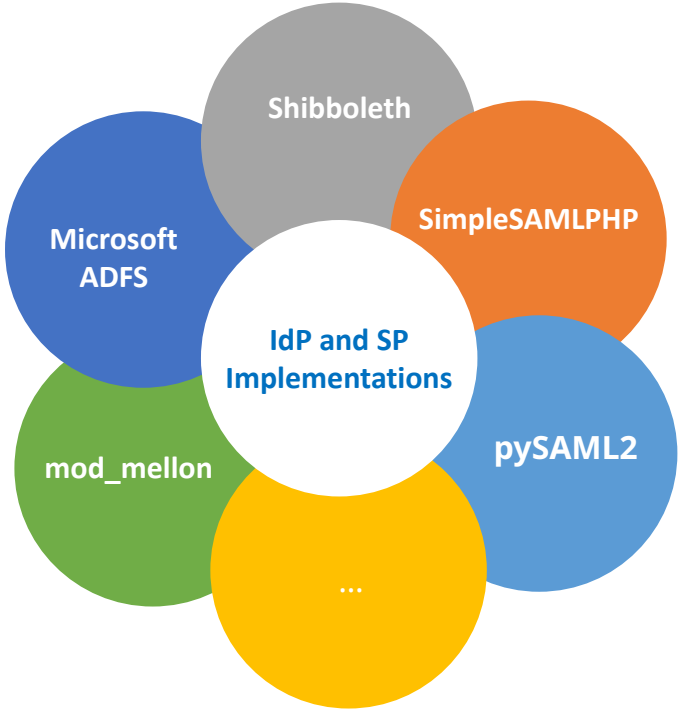


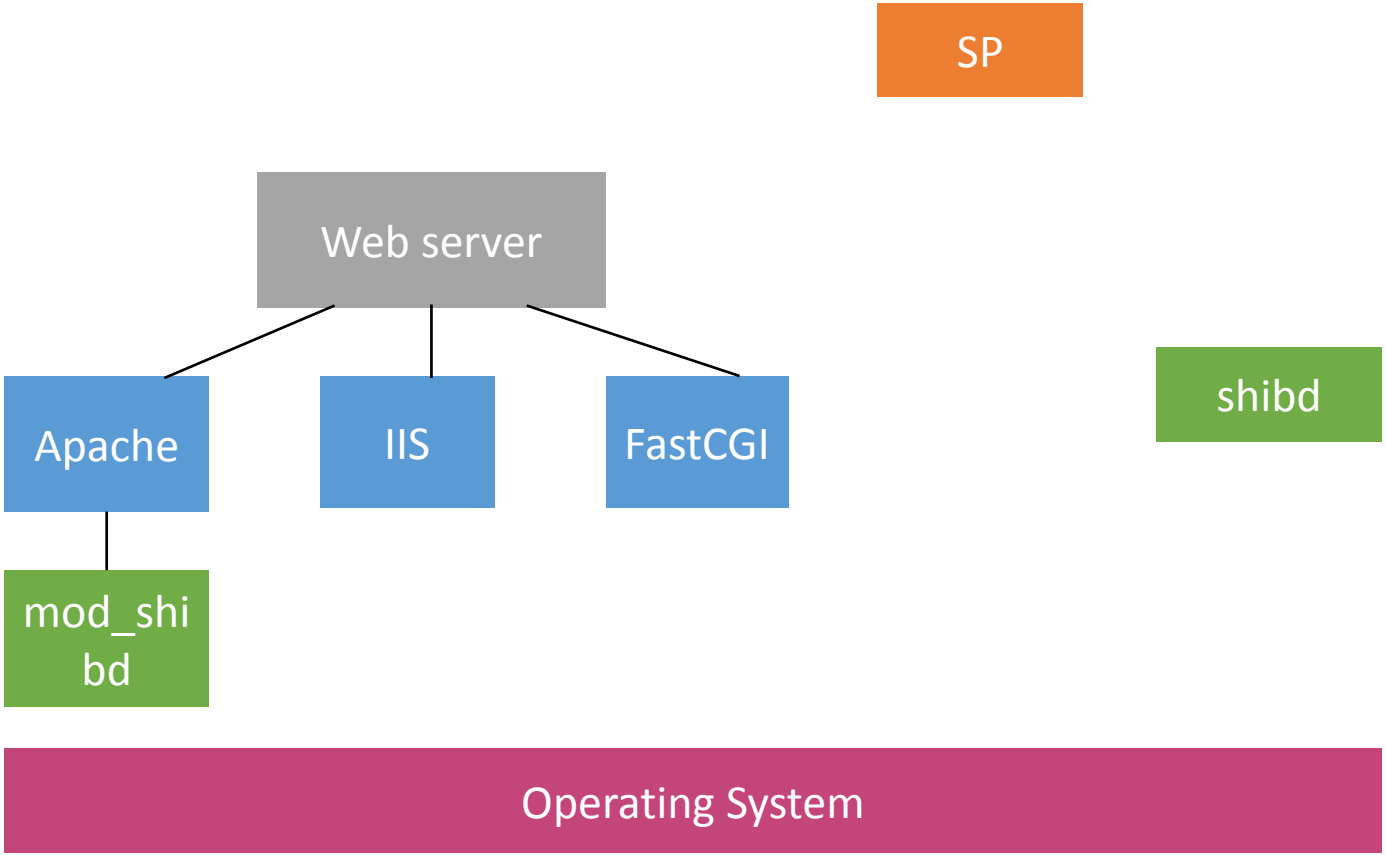
Figure 1

SAML IdP i SP implementacije

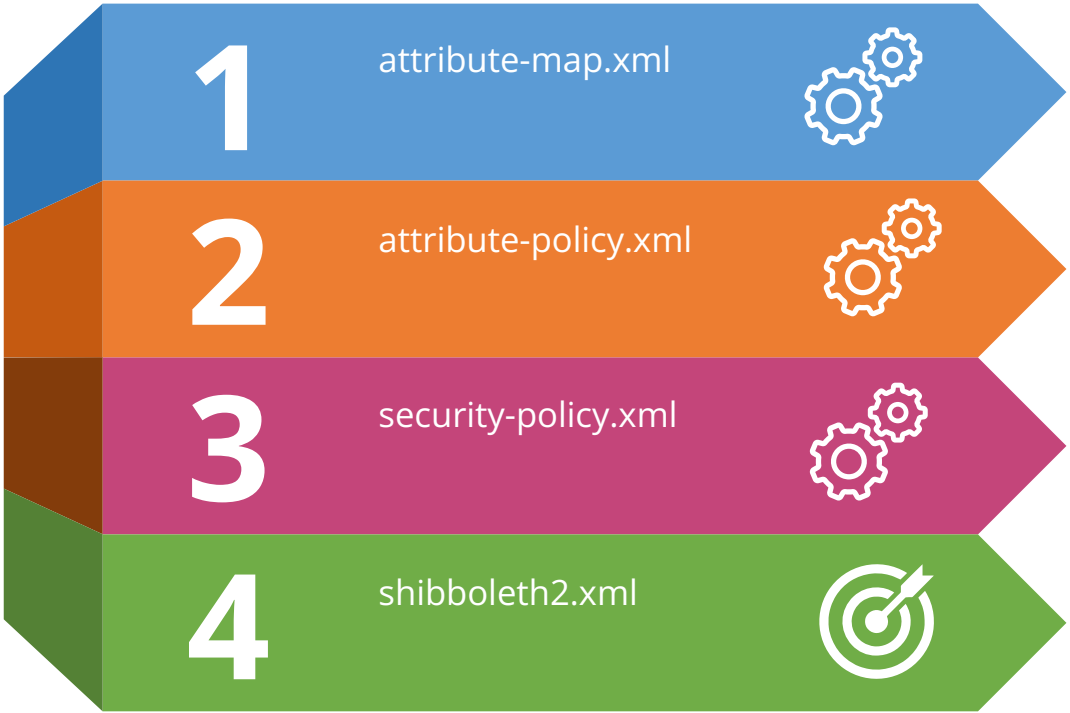


Shibboleth

Shibboleth SP

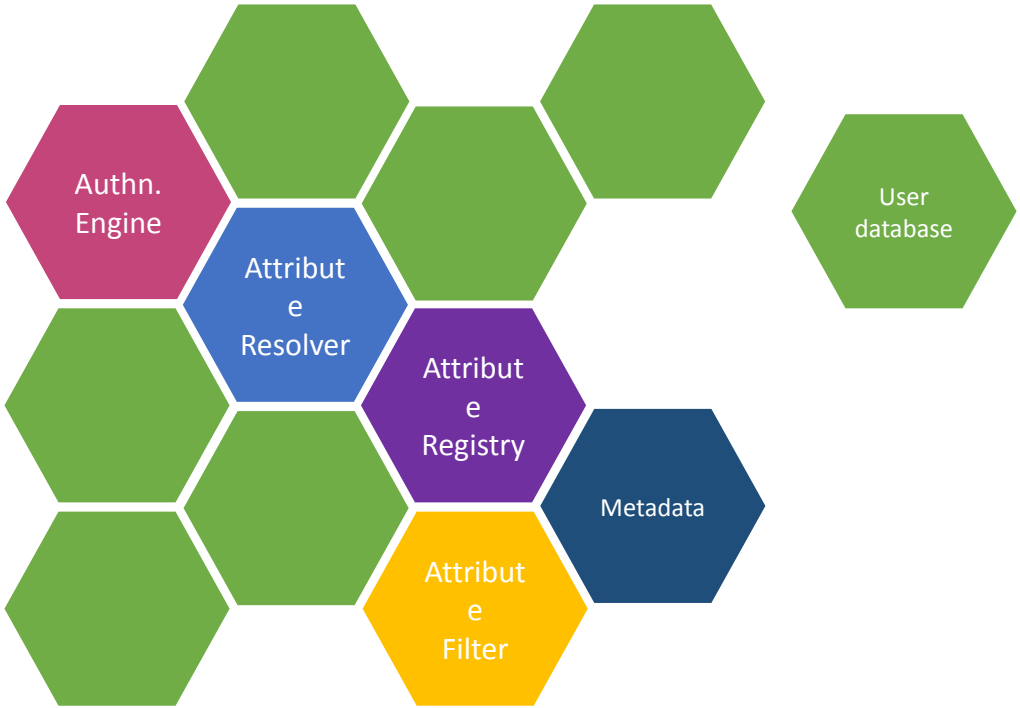


Shibboleth SP



Shibboleth IdP

- *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>
```

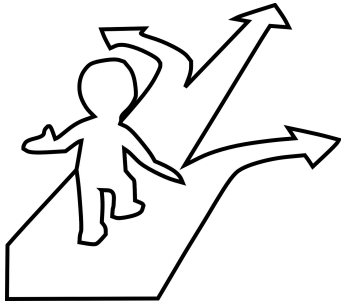
Attribute Definitions

iAMRES definicije atributa

Attribute Definition

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

Koju definiciju atributa odabrati?

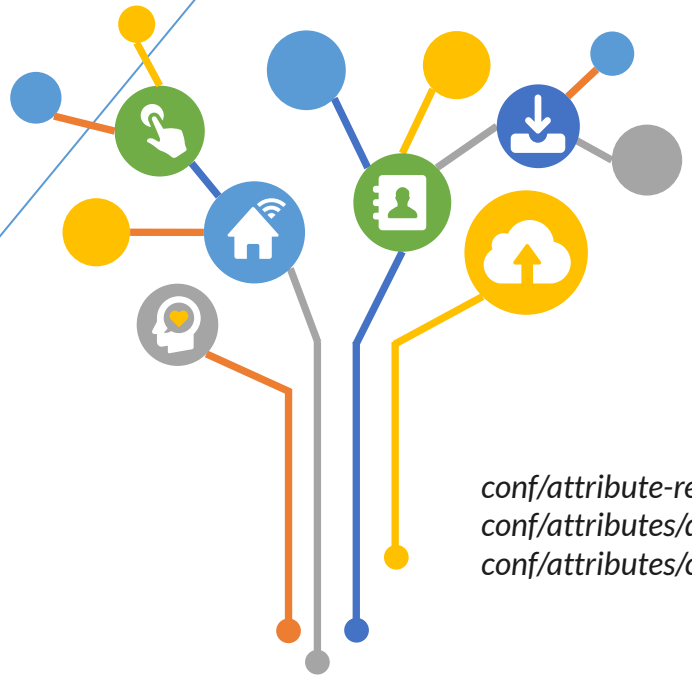


Attribute Registry

iAMRES Šema atributa

Attribute Schemas

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



conf/attribute-registry.xml,
conf/attributes/default-rules.xml,
conf/attributes/custom/

https://wiki.refeds.org/display/STAN/Schemas

Attribute Filter

iAMRES dinamički filtar

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

Attribute Resolver

Atributi koje IdP šalje:

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

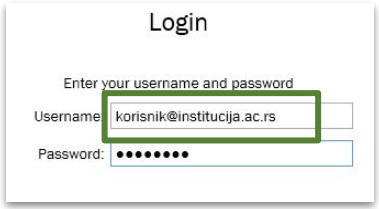
Attribute Filter

SP

https://docs.amres.ac.rs/uputstva/ldap/uvod/

https://docs.amres.ac.rs/uputstva/shibboleth/shibboleth/

iAMRES Federacija Identiteta i eduroam



RADIUS

uid
userPassword

OpenLDAP

Shibboleth / SAML

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

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 deklarišu 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)

https://refeds.org/category/research-and-scholarship

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 deklarisao kao CoCo, IdP treba da:

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

Da bi se deklarisao 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

https://refeds.org/category/code-of-conduct/v2

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

- Samostalna procena mogućnoti 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

https://refeds.org/wp-content/uploads/2022/08/Sirtfi-v2.pdf

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/*