Autentifikacijski sustavi i baze podataka

AAI / SSO / SAML / FS

Osnovni koncepti

- Elektronički identitet
- AAI
- AAA
  - AuthN
  - AuthZ

Elektronički identitet

- zapis; skup podataka o osobi
- obuhvaća i podatke (*credentials*) koji osobi služe za dokazivanje identiteta (npr. korisnička oznaka i lozinka)
- IdM (*Identity Management*) == upravljanje elektroničkim identitetima
  - ima organizacijsku, informacijsku i tehnološku dimenziju

AAA

- Autentikacija / authentication (AuthN)
- Autorizacija / authorisation (AuthZ)
- Accounting (auditing)

Autentikacija (AuthN)

- proces kojim se provjerava elektronički identitet korisnika
- autentikacija se provodi na temelju:

- onog što korisnik zna
  - korisnička oznaka/lozinka, ...

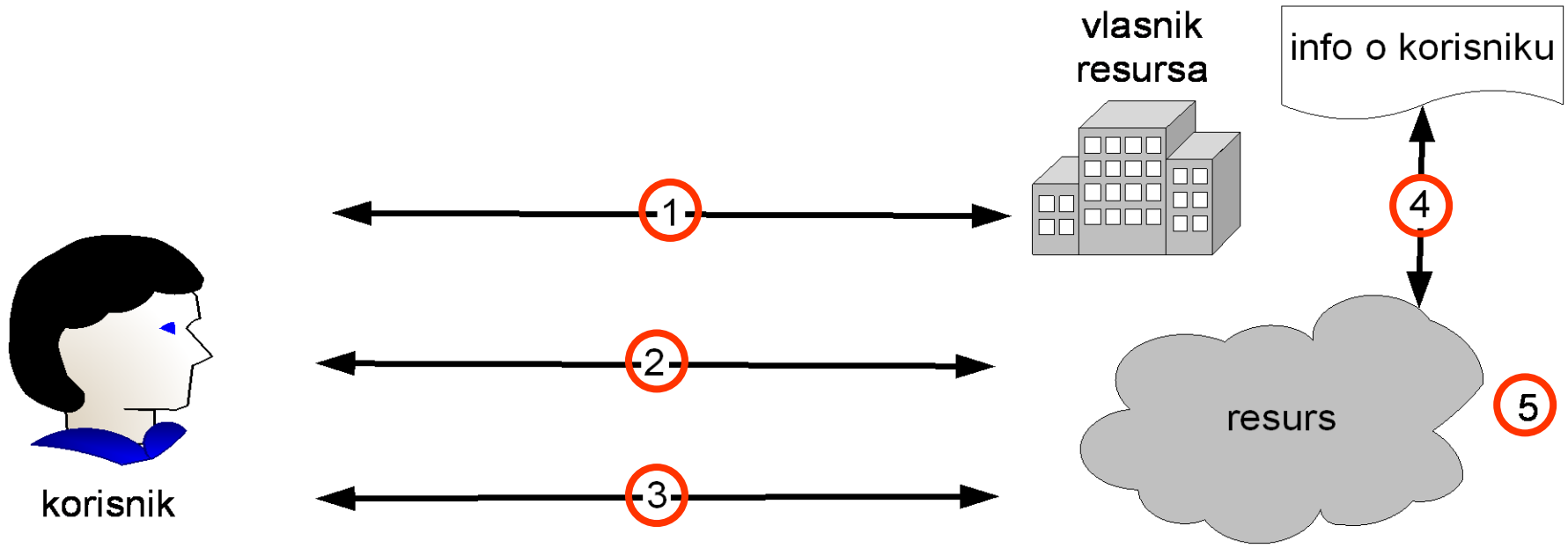
- onog što korisnik ima
  - certifikat, smart card, ...

- onog što korisnik jest
  - biometrija (npr. otisak prsta)
- metodu biramo prema (sigurnosnim) potrebama
- postupak treba biti siguran, pouzdan, efikasan

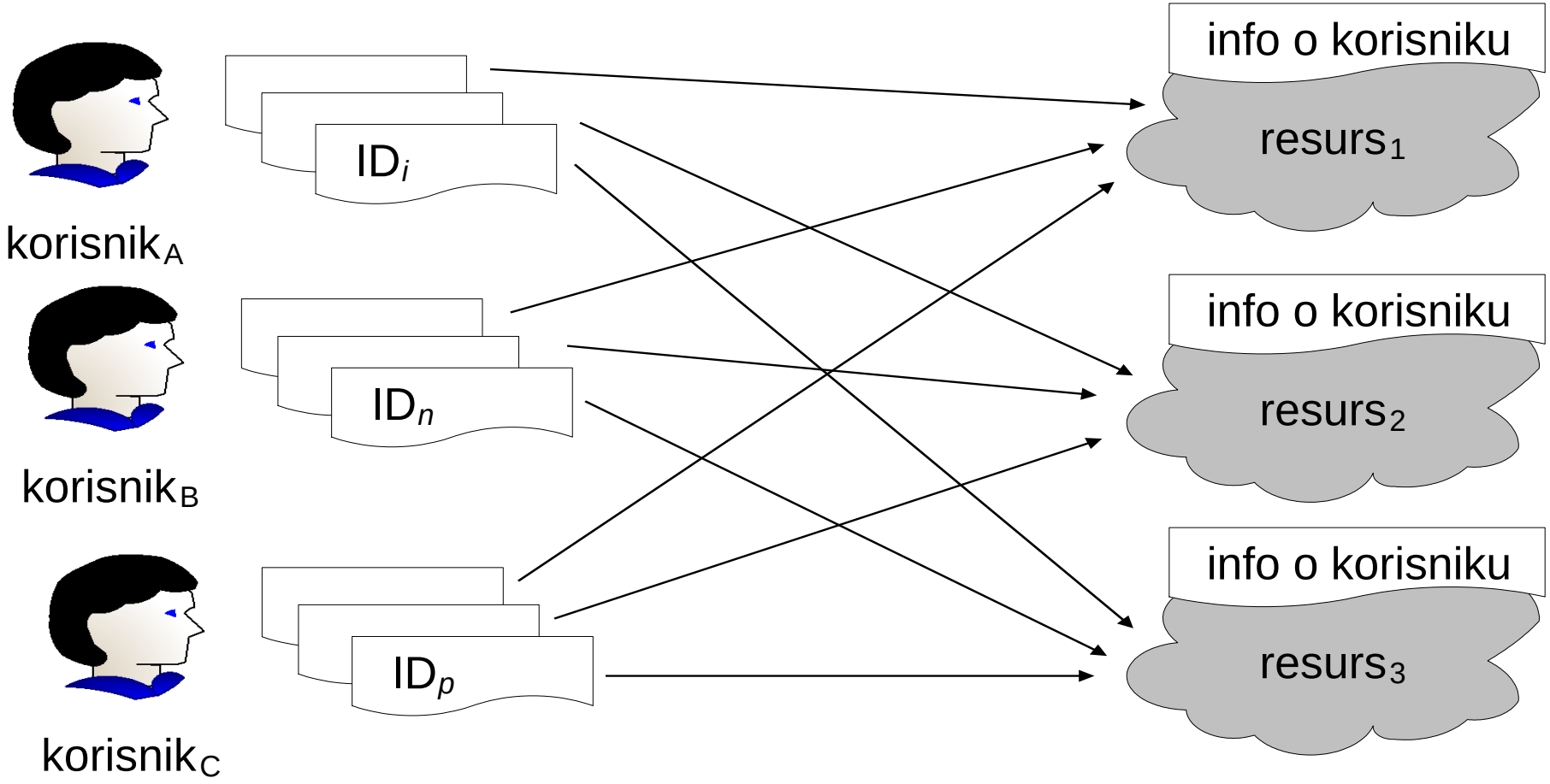
Autorizacija (AuthZ)

- proces kojim se korisniku dodjeljuje odnosno oduzima utvrđena razina prava pristupa resursu
- provodi se nakon uspješno obavljene autentikacije
- odluka se donosi na temelju raspoloživih podataka o korisniku i pravila pristupa

Koraci u procesu AA

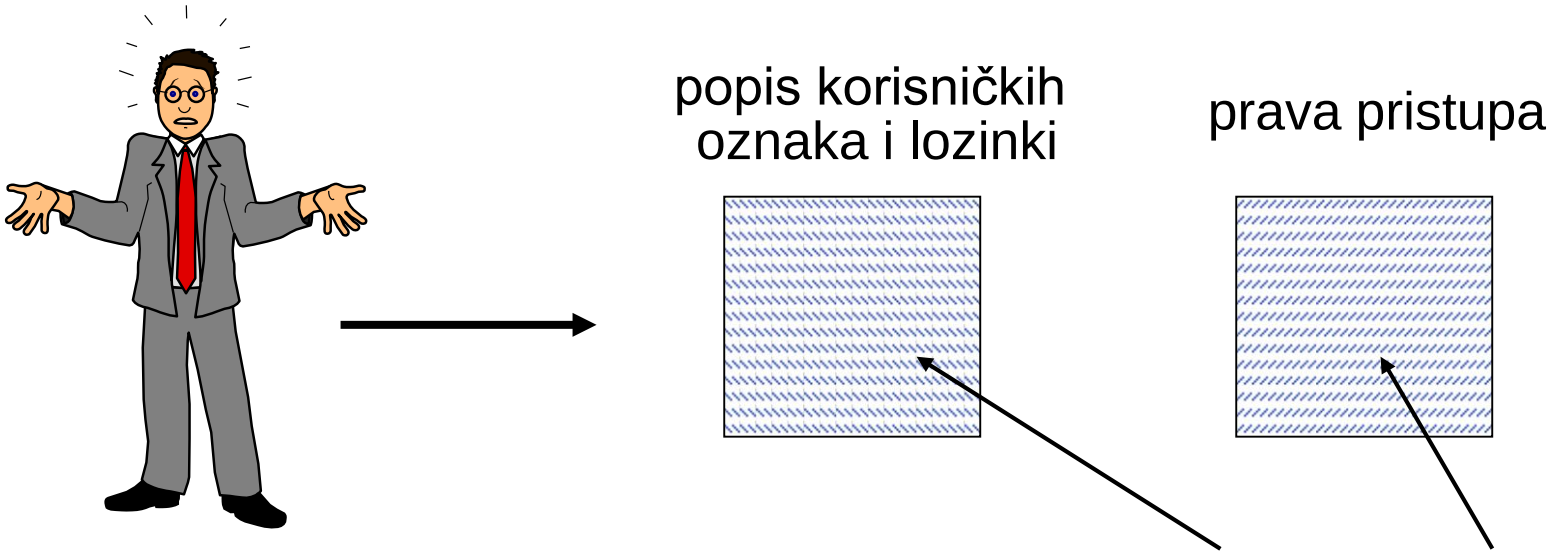


AA problem

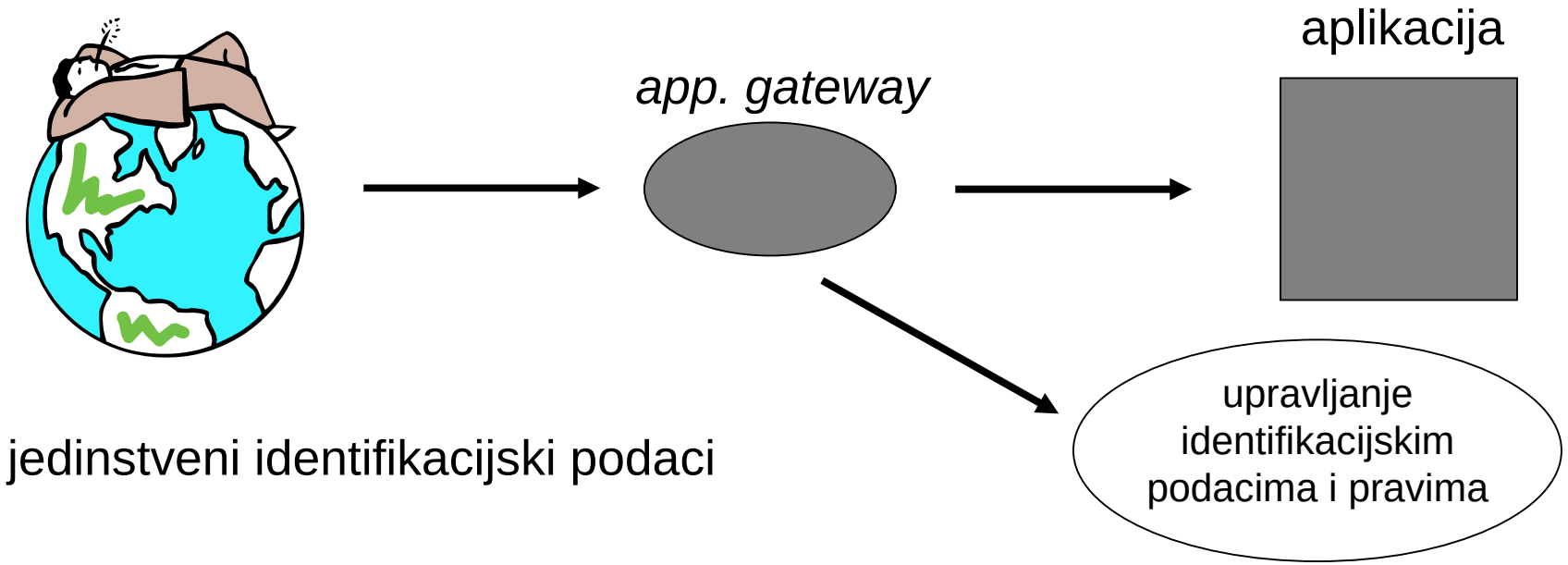

korisnik$_A$
korisnik$_B$
korisnik$_C$
ID$_i$
ID$_n$
ID$_p$
info o korisniku
resurs$_1$
info o korisniku
resurs$_2$
info o korisniku
resurs$_3$

Klasični pristup

- Interni proces aplikacije



Krajnji cilj ...

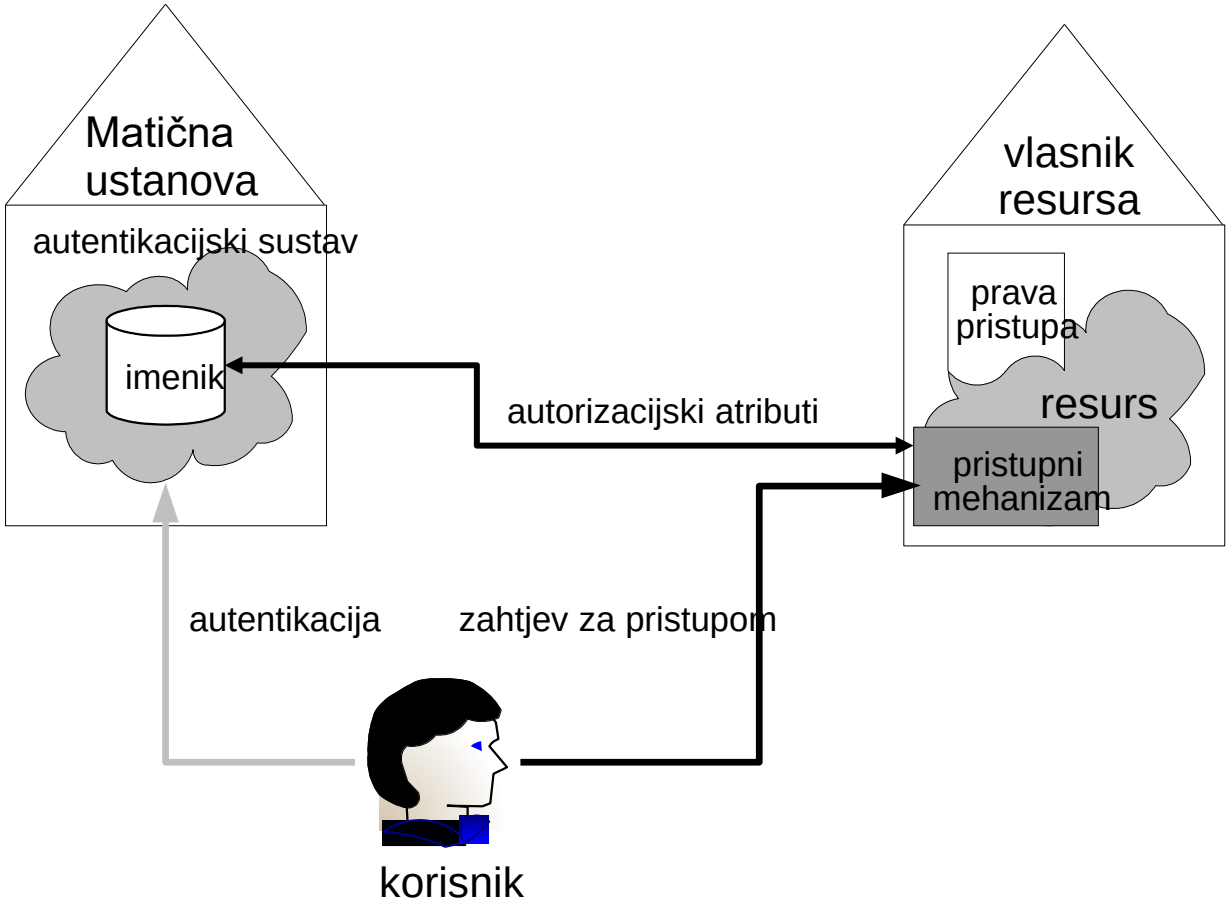


- autentikacija i autorizacija su eksterni procesi

Koje probleme rješavamo?

- interinstitucionalna AA
- mobilnost korisnika
- pristup mreži neovisno o lokaciji, načinu/tehnologiji pristupa ...
- personalizacija usluga
- minimiziran broj elektroničkih identiteta po korisniku

Model AAI


Matična ustanova
autentikacijski sustav
imenik
vlasnik resursa
prava pristupa
resurs
pristupni mehanizam
autorizacijski atributi
autentikacija
zahtjev za pristupom
korisnik

AA infrastruktura (AAI)

- rješenje problema inter-institucionalne AA
- 3 temeljna čimbenika:
  - korisnik, matična ustanova, vlasnik resursa
- 3 temeljne akcije:
  - autentikacija korisnika koju obavlja njegova matična ustanova
  - prijenos korisnikovih autorizacijskih atributa od matične ustanove do vlasnika resursa; skup atributa koji se prenose mora biti konfigurabilan kako bi se ispunili zahtjevi vlasnika resursa, ali i štitila privatnost korisnika
  - odluka o pristupu resursu koju donosi vlasnik resursa (autorizacija).

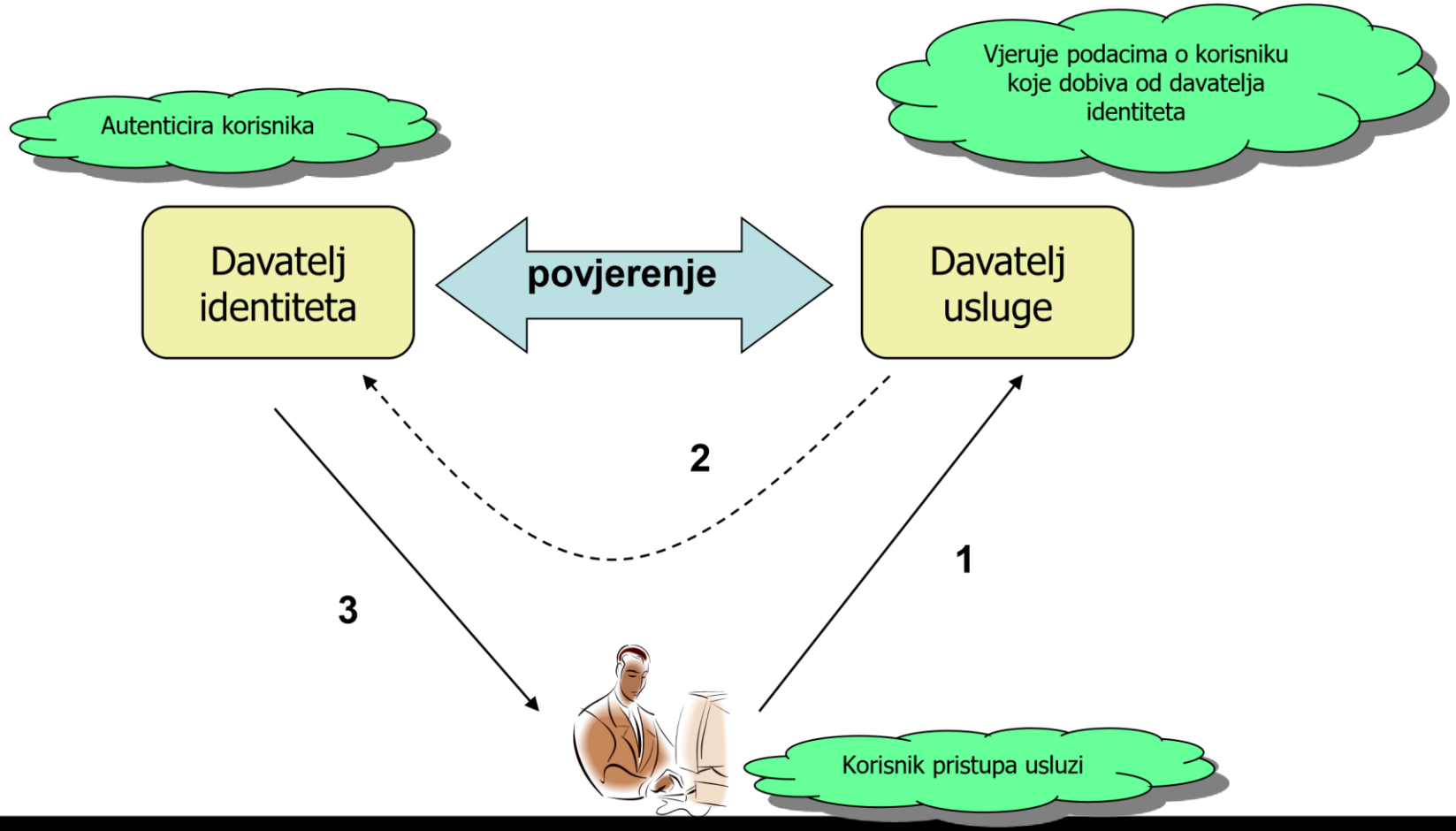
AAI: očekivanja

- AAI treba:
- biti skalabilna
- biti sigurna
- biti temeljena na standardima
- smanjiti količinu posla koju imaju administratori
- pojednostaviti i uniformirati pristup resursima za krajnje korisnike
- smanjiti na minimum potrebu za instalacijom dodatne programske podrške na korisničko računalo.

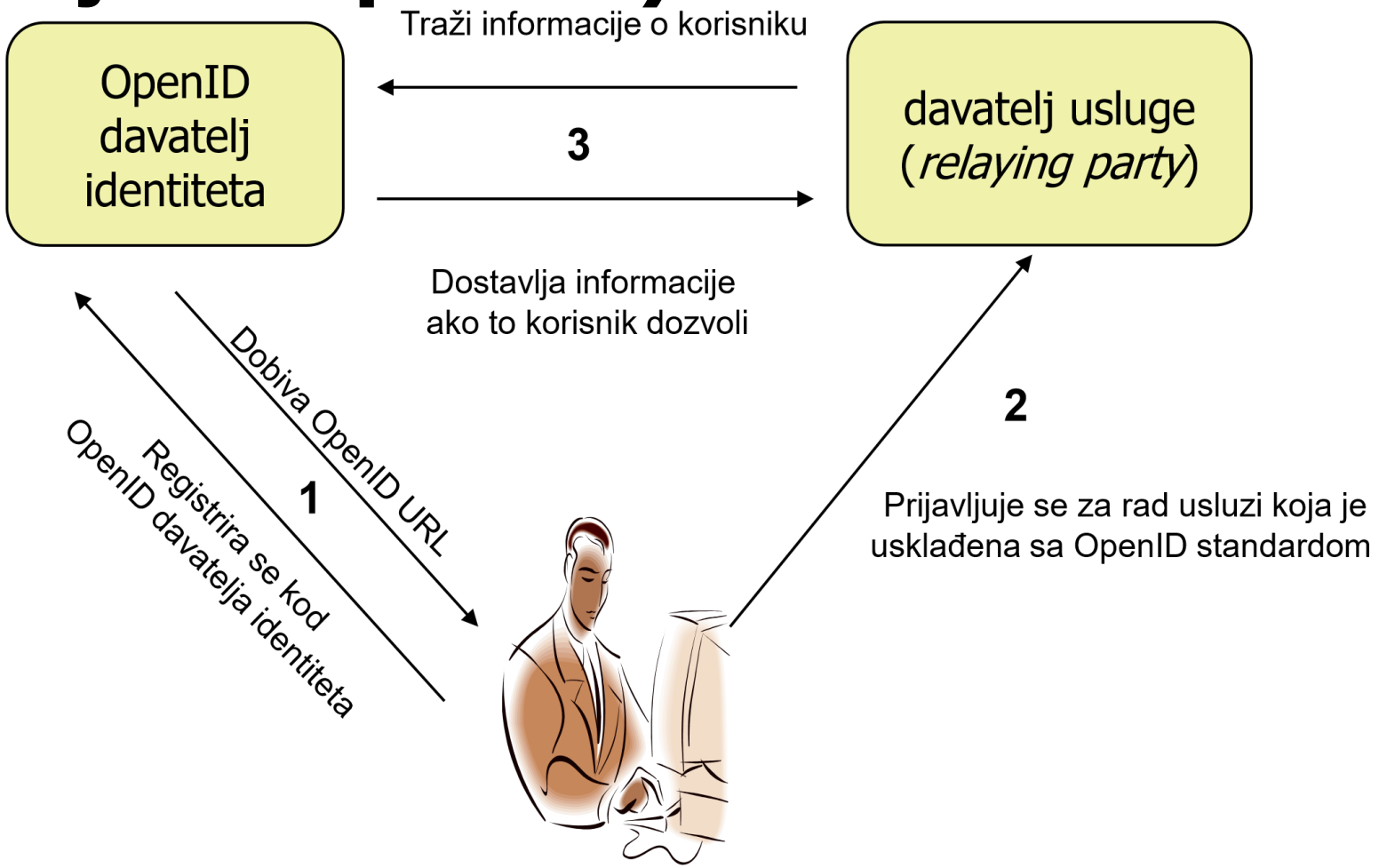
AAI: izazovi

- potrebno je precizno definirati sve organizacijske, informacijske i tehničke elemente
- izabrati odgovarajući model (ahitekturu):
  - centralizirani ↔ distribuirani ↔ hibridni
  - federacijski ↔ utemeljen na korisniku (user-centric)

Federacijski model



Model utemeljen na korisniku (primjer: OpenID)



Centralizirano ili distribuirano?

Centralizirano rješenje

- zajednički poslužitelji/servisi za sve uključene ustanove

Prednosti

- jednostavnija implementacija za ustanove
- jednostavniji model povjerenja

Mane

- skalabilnost, (ne)fleksibilnost

Distribuirano rješenje:

- dijelovi AAI nalaze se u različitim ustanovama / na različitim mjestima

Prednosti:

- skalabilnost, fleksibilnost

Mane

- složenija implementacija za ustanove
- složeniji model povjerenja

AA proces: autentikacija

- mnogo različitih rješenja:
- najčešće se koristi: korisnička oznaka/lozinka
- kombinirana rješenja: npr. višefazna autentikacija
- distribuirano ili centralizirano rješenje
- različiti protokoli: LDAP, RADIUS, SOAP/SAML, ...
- (LDAP) imenik u funkciji baze podataka u kojoj se čuvaju podaci o korisnicima (elektronički identiteti)

- **zaštita privatnosti: “Nije važno tko si nego jesi li to ti.”**

AA proces: autorizacija

- 3 temeljna scenarija:
  - AuthZ = AuthN
  - AuthZ = AuthN + dodatni atributi (iz imenika)
    - *strong privacy*: “pregovaranje” o atributima koji se razmjenjuju
  - AuthZ = AuthN + dodatni atributi (iz imenika) + informacije koje pamti resurs lokalno
    - *quota*, *black list*, ...
- moguća uporaba dediciranih AuthZ poslužitelja ❖ kod pristupa mreži cilj je implementirati pravila kontrole pristupa (*access lists*)

AA proces: kontrola sjednice

- session control
- omogućava identifikaciju klijenta
- pridonosi performantnosti AAI
- zahtjevni AuthZ proces se ne mora ponavljati
- problemi:
  - jako ovisi o konkretnim aplikacijama i protokolima
  - treba paziti na sigurnost
- Web (HTTP) tehnike:
  - Cookie
  - parametri u URL-u

SSO

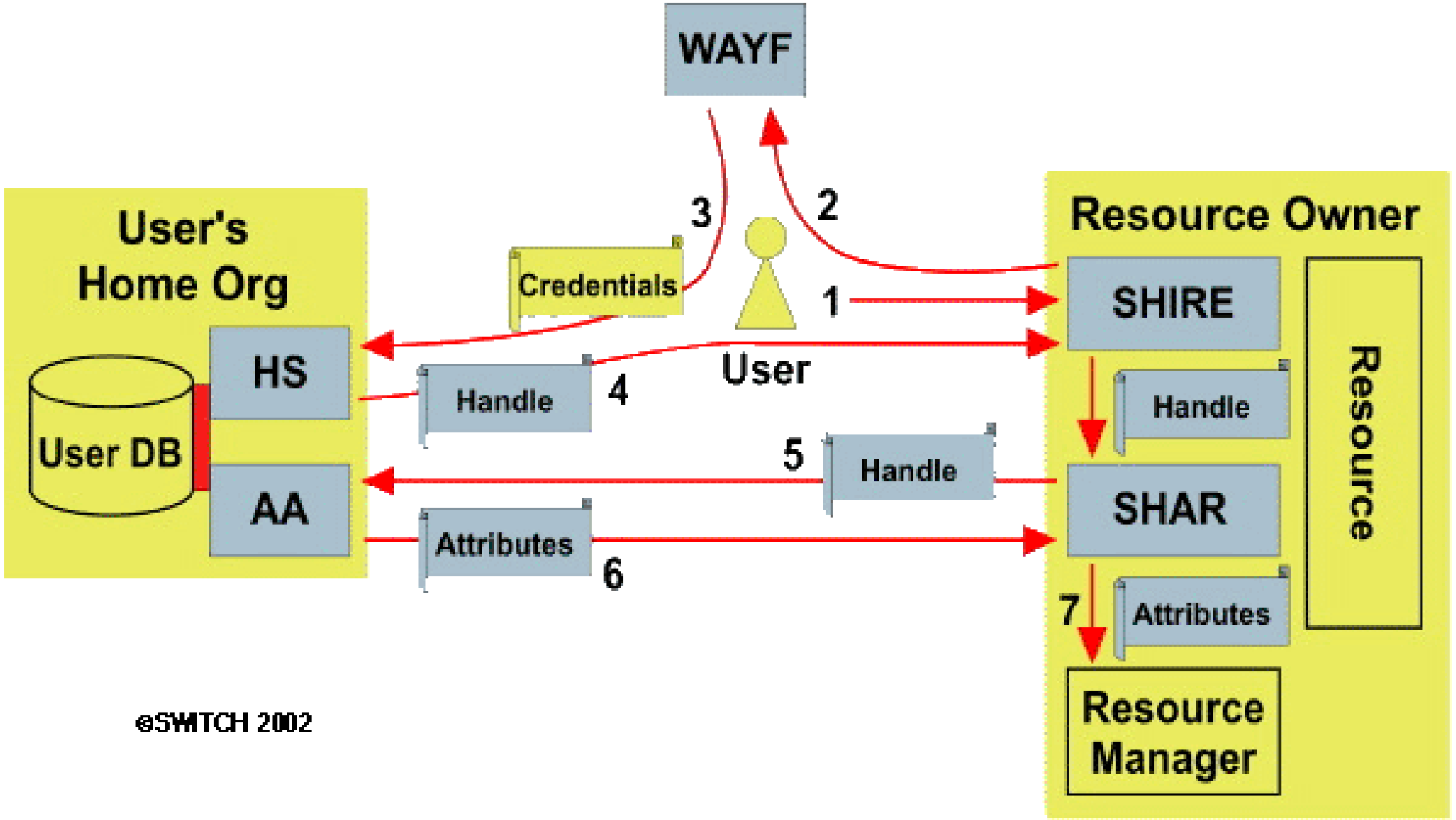
- Single Sign On
- autenticiraj se jednom, a pristupaj više puta (različitim) mrežnim resursima i/ili aplikacijama
- za SSO u kontekstu pristupa aplikacijama utemeljenim na webu postoje rješenja
- konačni cilj: univerzalni SSO
- jednostavniji zadatak: odvojeni SSO sustavi za pristup mreži i za pristup aplikacijama

Primjena

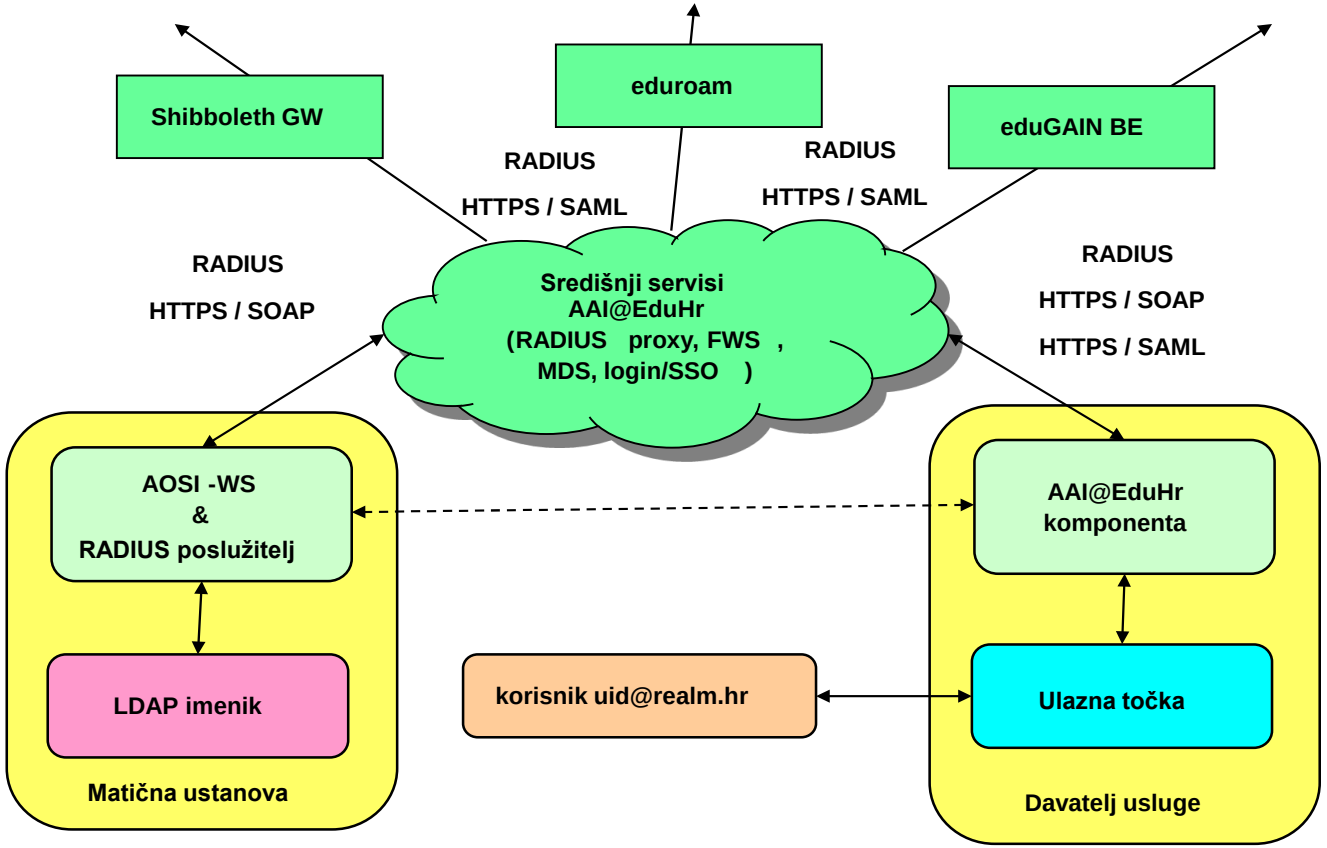
- Kada nam je bitno tko pristupa resursu:
- pristup mreži za individualne korisnike
  - (modem, wireless, wired, ...)
- pristup računalnim resursima
  - (grid, mrežni diskovi, ...)
- pristup osnovnim mrežnim uslugama
  - (ssh, e-mail, ftp, ...)
- pristup Web resursima
- pristup mrežnim aplikacijama (on-line baze, udaljeno učenje, ...)

Shibboleth (Internet2)

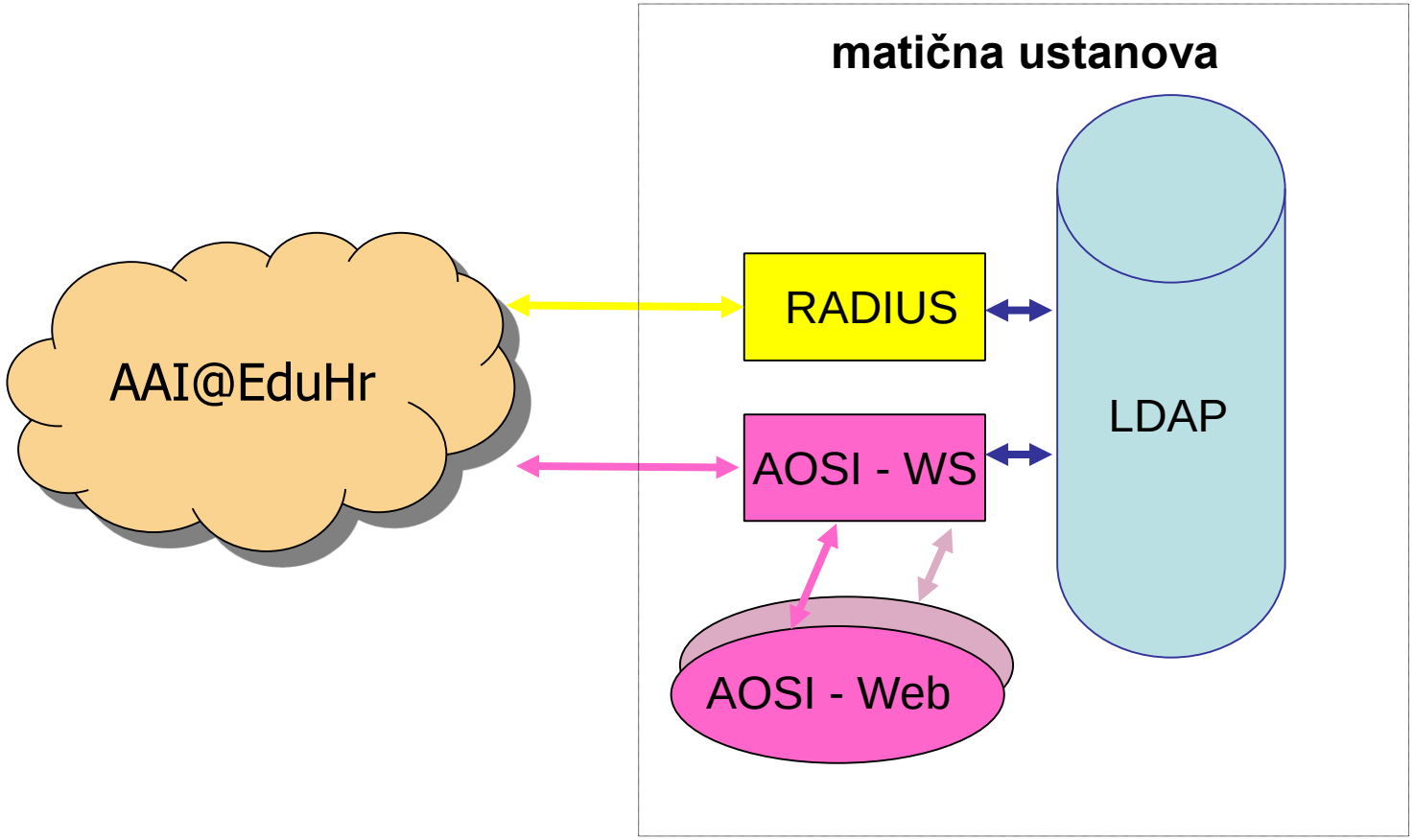
- distribuirani, federativni koncept
- sustav orjentiran na aplikacije (web)
- o autentikaciji i isporuci atributa odlučuju matične ustanove (vlasnici imenika)
- vlasnici resursa (davatelji usluge) traže podatke od matičnih ustanova i na temelju dobivenog donose odluke
- matična ustanova i korisnik mogu kontrolirati što se zbiva s podacima iz imenika (zaštita privatnosti)
- uvodi SAML (Security Assertions Markup Language) u primjenu
- https://internet2.edu/community/about-us/


WAYF
User's Home Org
HS
User DB
AA
Credentials
3
2
1
User
Handle
4
5
Handle
Attributes
6
Resource Owner
SHIRE
Handle
SHAR
Attributes
7
Resource Manager
Resource

AAI@EduHr


Shibboleth GW
eduroam
eduGAIN BE
RADIUS
HTTPS / SAML
RADIUS
HTTPS / SAML
RADIUS
HTTPS / SOAP
Središnji servisi
AAI@EduHr
(RADIUS proxy, FWS ,
MDS, login/SSO)
RADIUS
HTTPS / SOAP
HTTPS / SAML
AOSI -WS
&
RADIUS poslužitelj
LDAP imenik
Matična ustanova
korisnik uid@realm.hr
AAI@EduHr
komponenta
Ulazna točka
Davatelj usluge

Lokalno

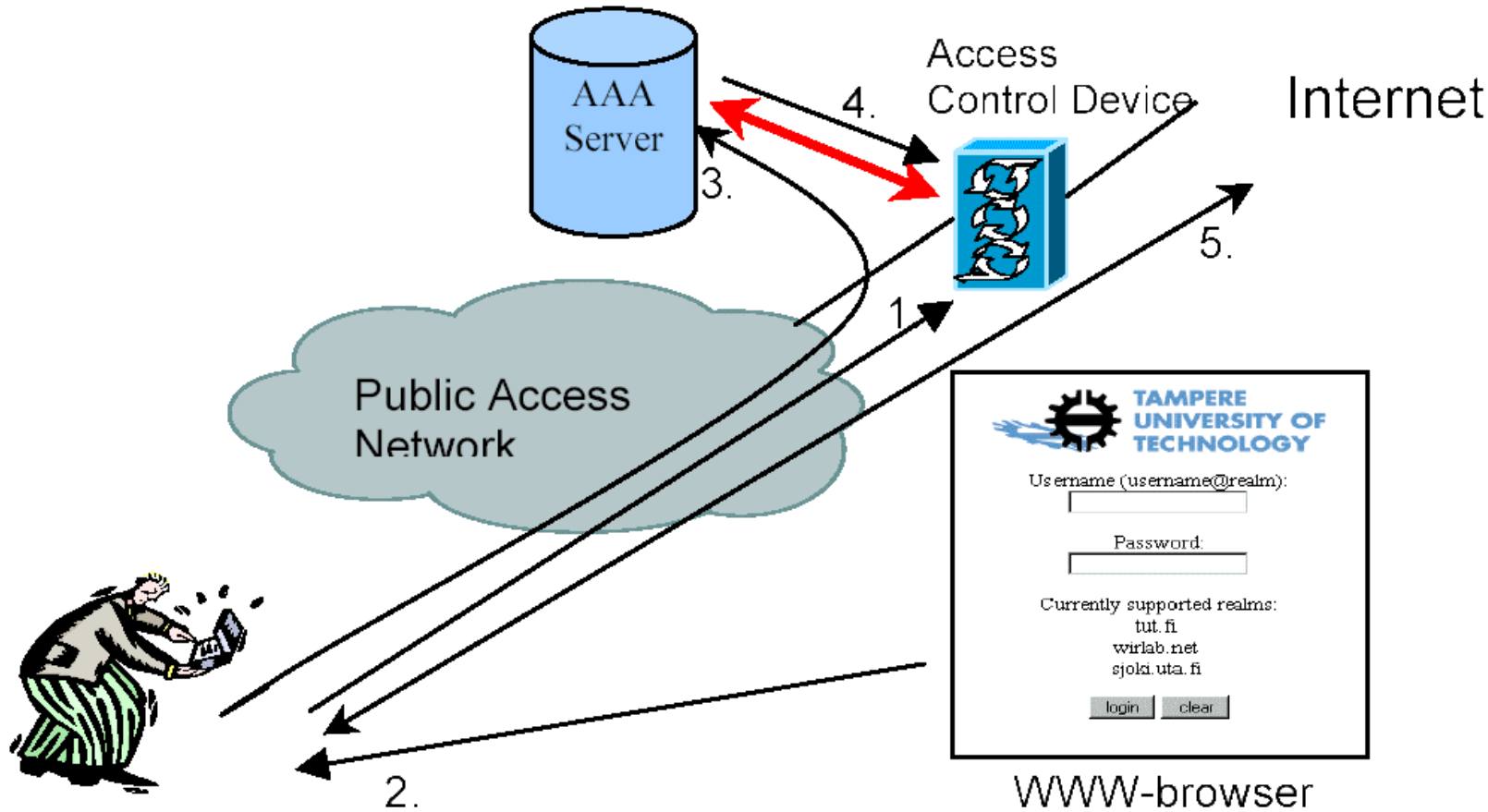


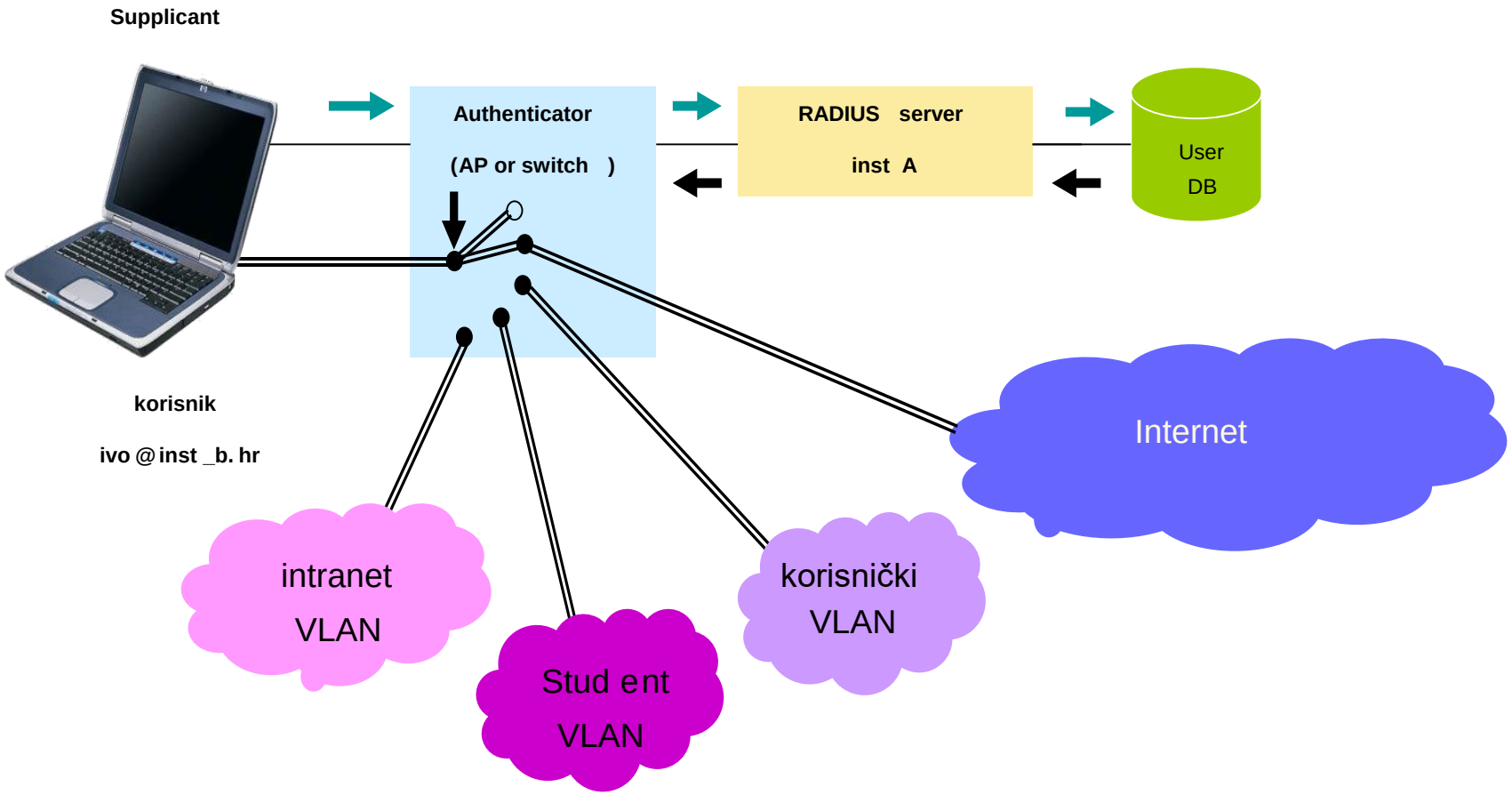
RADIUS

- Remote Authentication Dial In User Service
- protokol koji omogućuje upravljanje AAA procesom
- klijent – poslužitelj model
- definiran na aplikacijskom sloju
- koristi UDP
- RADIUS over TCP je trenutno u procesu standardizacije pri IETF-u
- široko korišten pri AA(A) za usluge pristupa mreži:
- dial-up, wired, wireless, cable, (A)DSL, VPN, ...
- puno implementacija
- serveri: FreeRADIUS, RADIATOR, Cisco, MS NPS (MS IAS), ...
- DIAMETER
- zamišljen kao nadogradnja (i buduća zamjena) protokola RADIUS
- aktualni razvojni iskoraci izjednačavaju RADIUS i DIAMETER

AA(A) i pristup mreži

- tri moguća pristupa:
- rješenje utemeljeno na Webu (Web redirect) u kombinaciji s RADIUS infrastrukturom
- rješenje utemeljeno na VPN tehnologiji
- rješenje utemeljeno na 802.1X, (IEEE standard za port-based autentikaciju) u kombinaciji s RADIUS infrastrukturom


AAA
Server
Access
Control Device
Internet
4.
3.
5.
1
Public Access
Network
TAMPERE
UNIVERSITY OF
TECHNOLOGY
Username (username@realm):
Password:
Currently supported realms:
tut.fi
wirlab.net
sjoki.uta.fi
login
clear
2.
WWW-browser

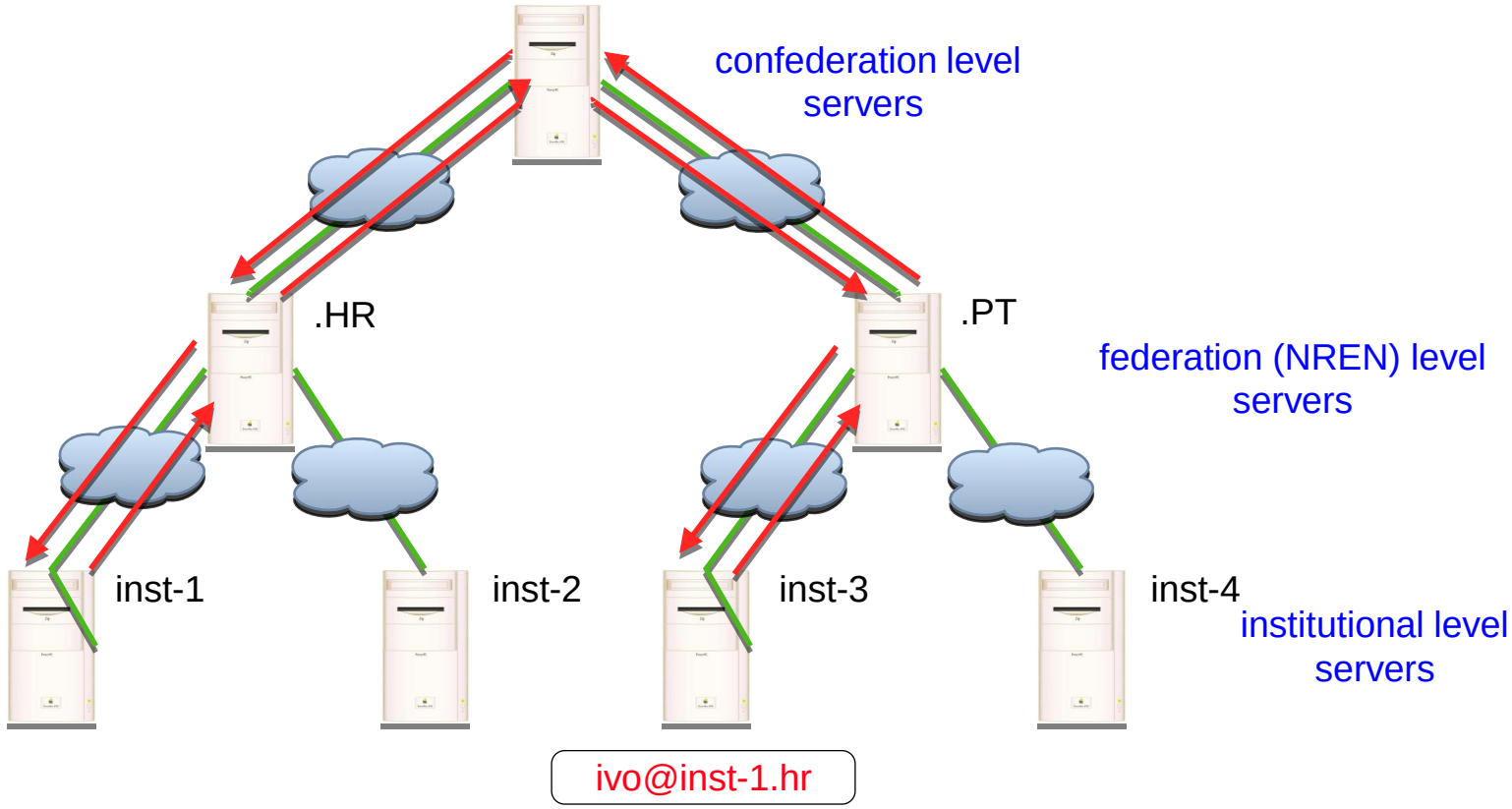

Supplicant
Authenticator
(AP or switch)
RADIUS server
inst A
User
DB
korisnik
ivo @inst _b. hr
Internet
intranet
VLAN
Stud ent
VLAN
korisnički
VLAN

- **802.1 X + EAP**

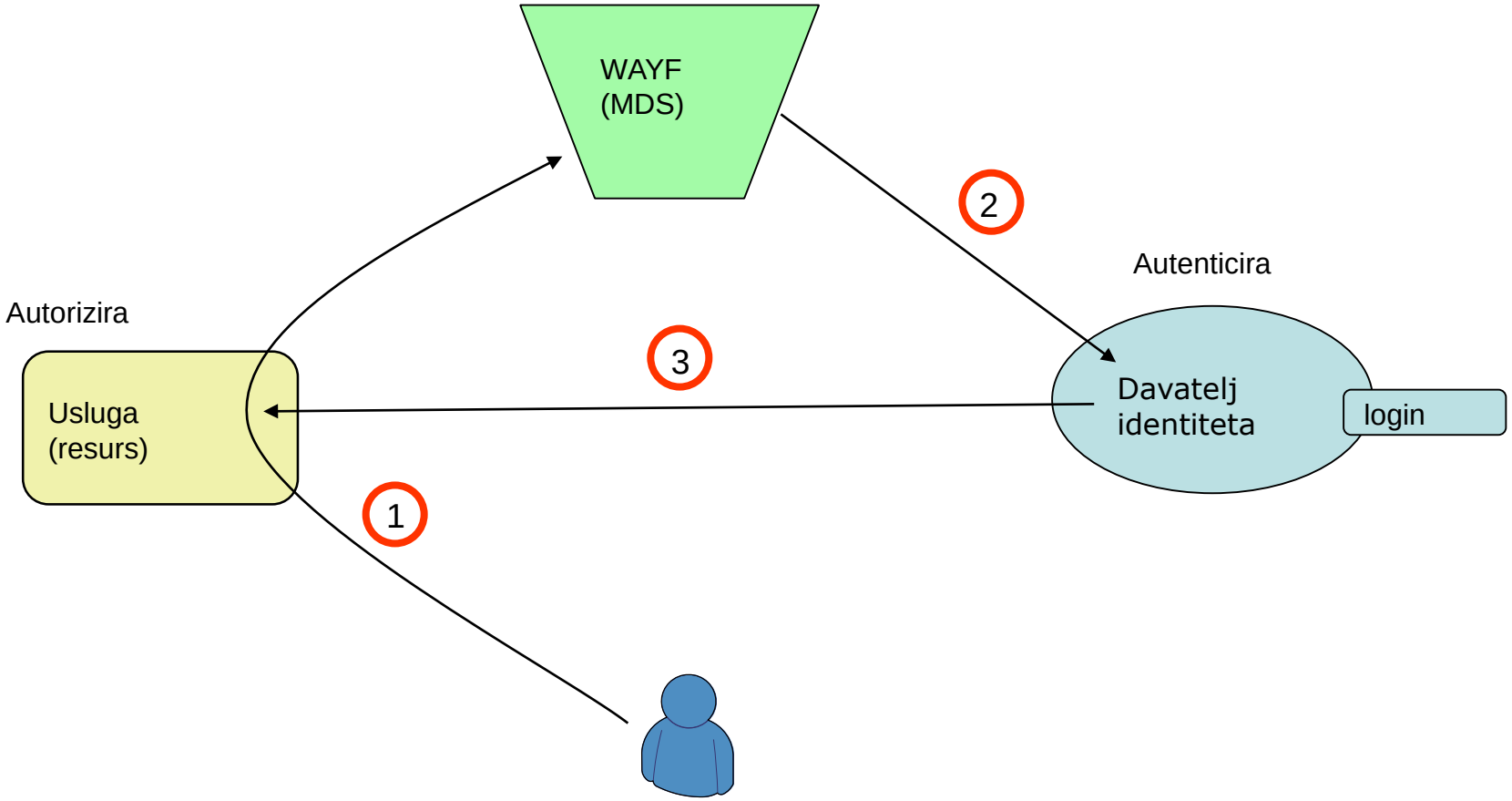
802.1x

- 802.1x – definira standard za komunikaciju pristupnog uređaja i pristupnog klijenta
- podaci se prenose putem EAP-a
- postoji više vrsta EAP metoda autentikacije
- sigurnost
- enkriptiranje svih podaka korištenjem dinamičkih ključeva
- lagana integracija sa dinamičkom dodjelom VLAN-ovima (802.1q)
- korištenje postojeće RADIUS infrastrukture
- 802.1x klijenti (supplicanti) su dostupni i jednostavni za uporabu

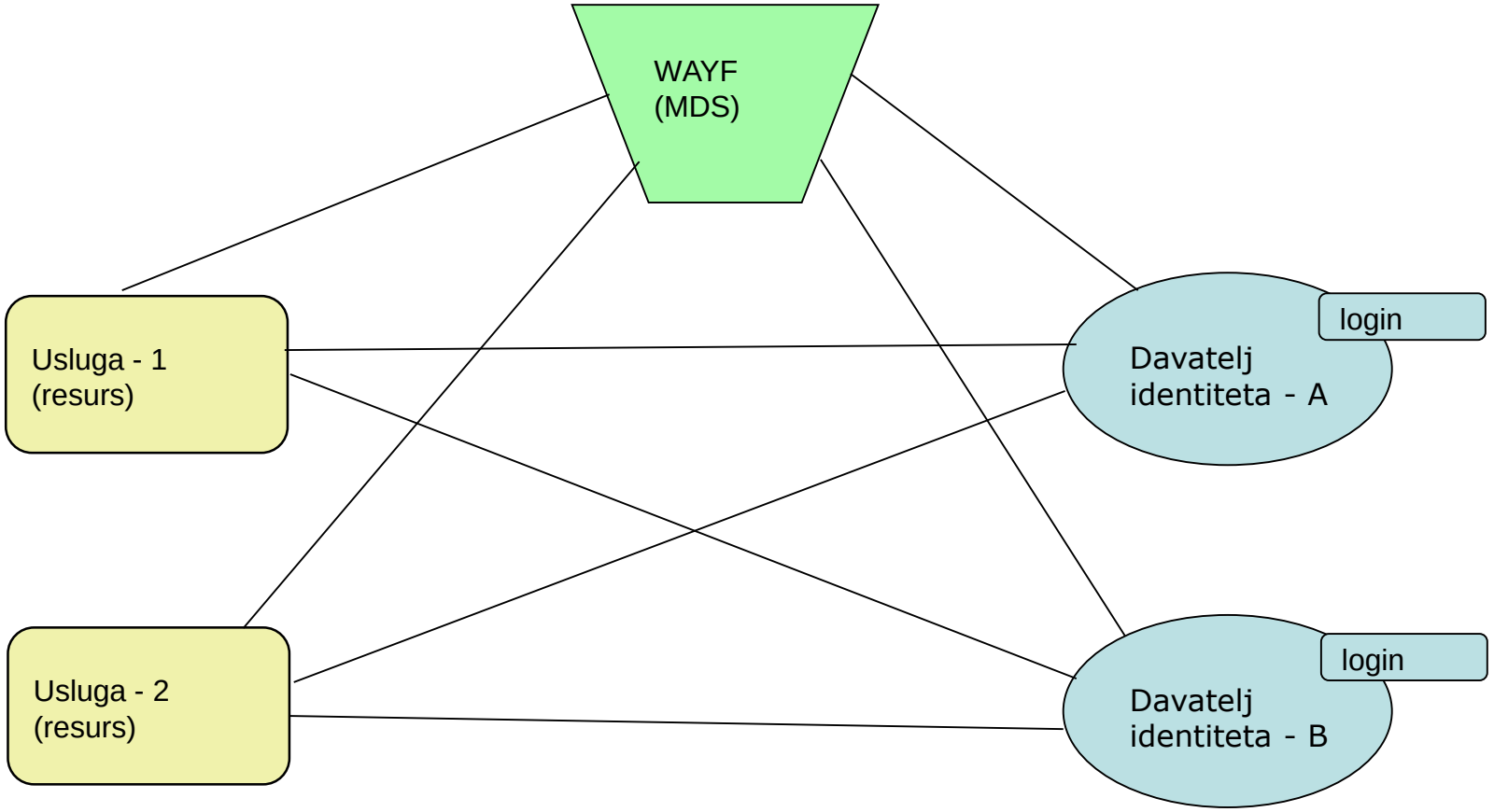
Konfederacija eduroam



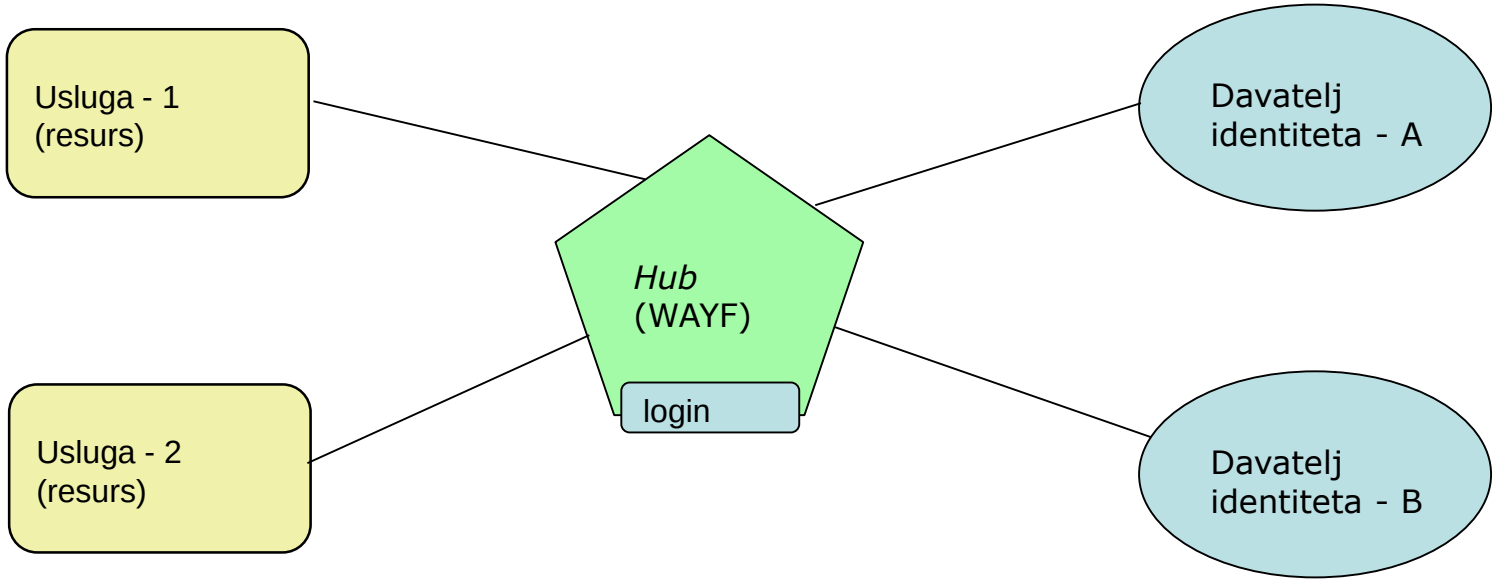
Osnovni koncept SSO



Mash federacija

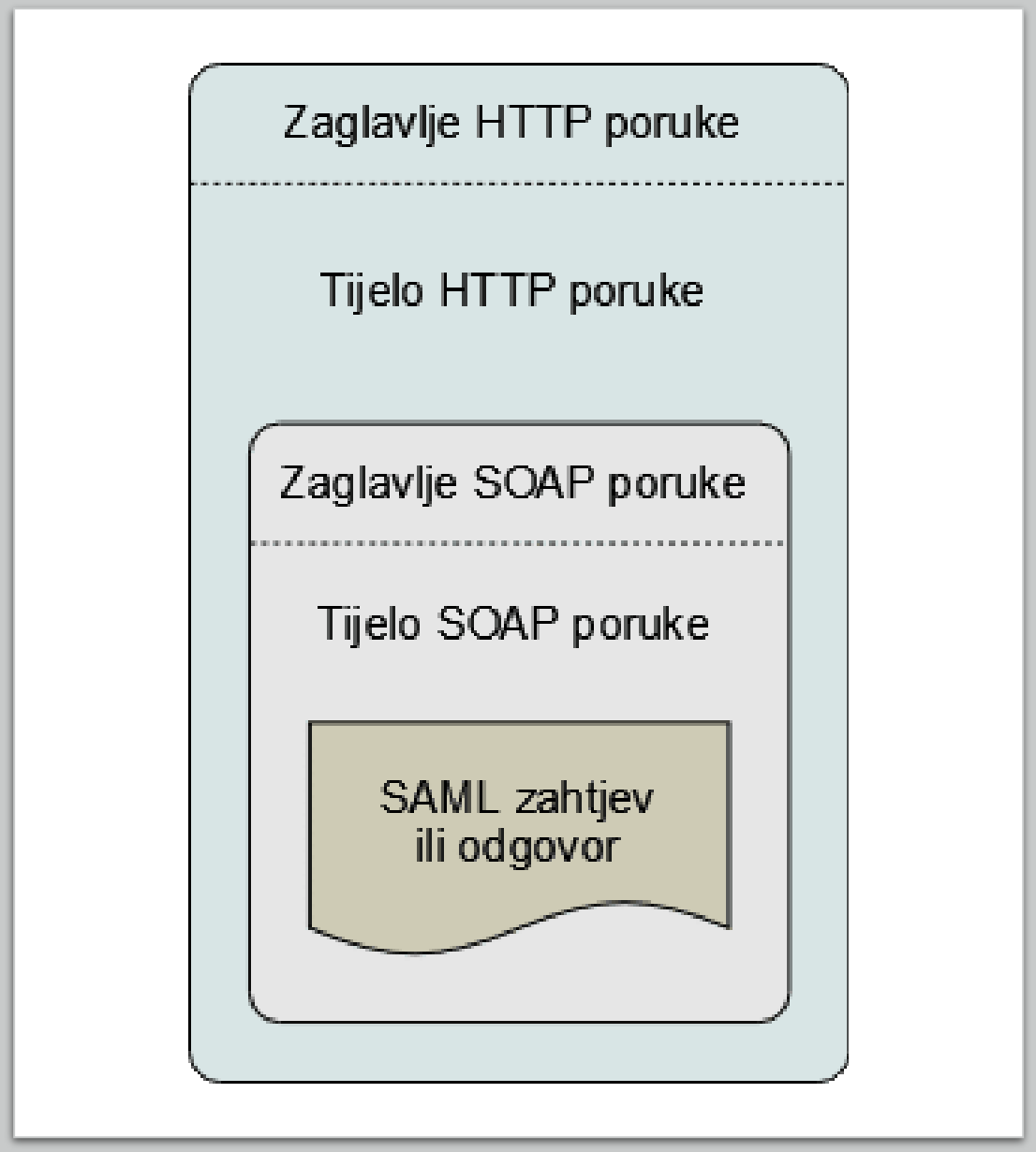


Hub-and-spoke federacija



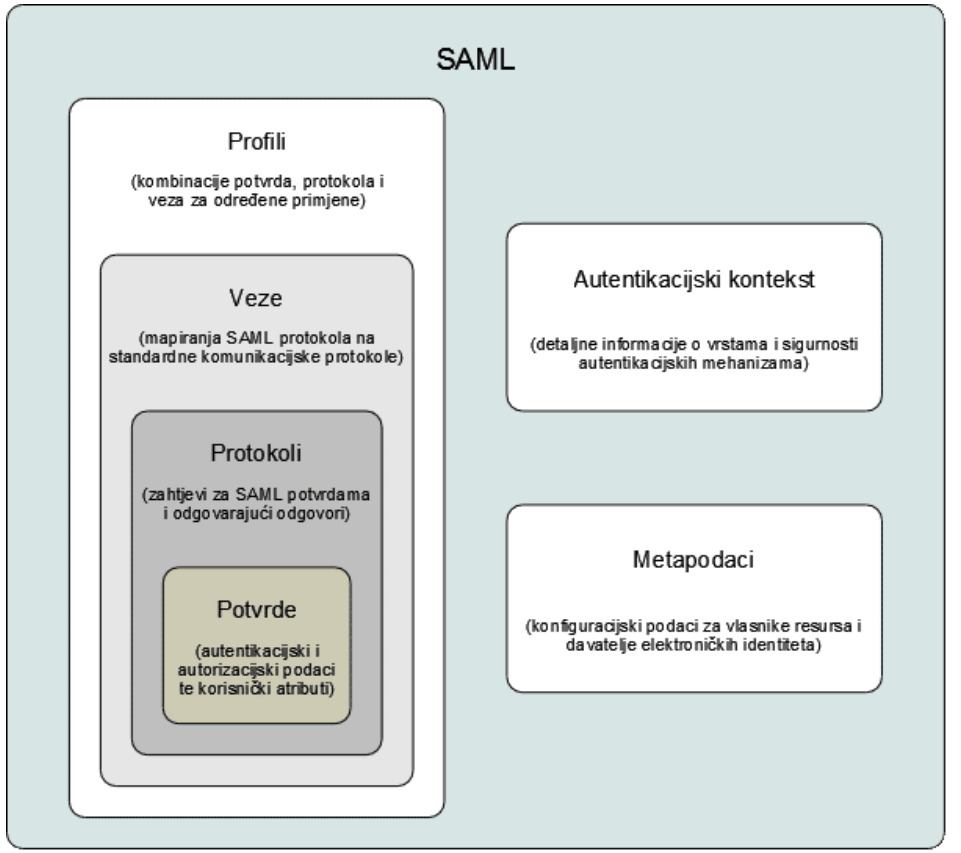
SAML

- Security Assertion Markup Language
- kreiran od strane organizacije OASIS (Organization for the Advancement of Structured Information Standards)
- aktualna inačica SAML 2.0
- cjeloviti okvir za razmjenu povjerljivih informacija
- temelji na potvrdama (SAML assertions)
- oslanja na XML, SOAP i HTTP
- SOAP (Simple Object Access Protocol) je protokol za razmijenu strukturiranih informacija u Web services arhitekturi

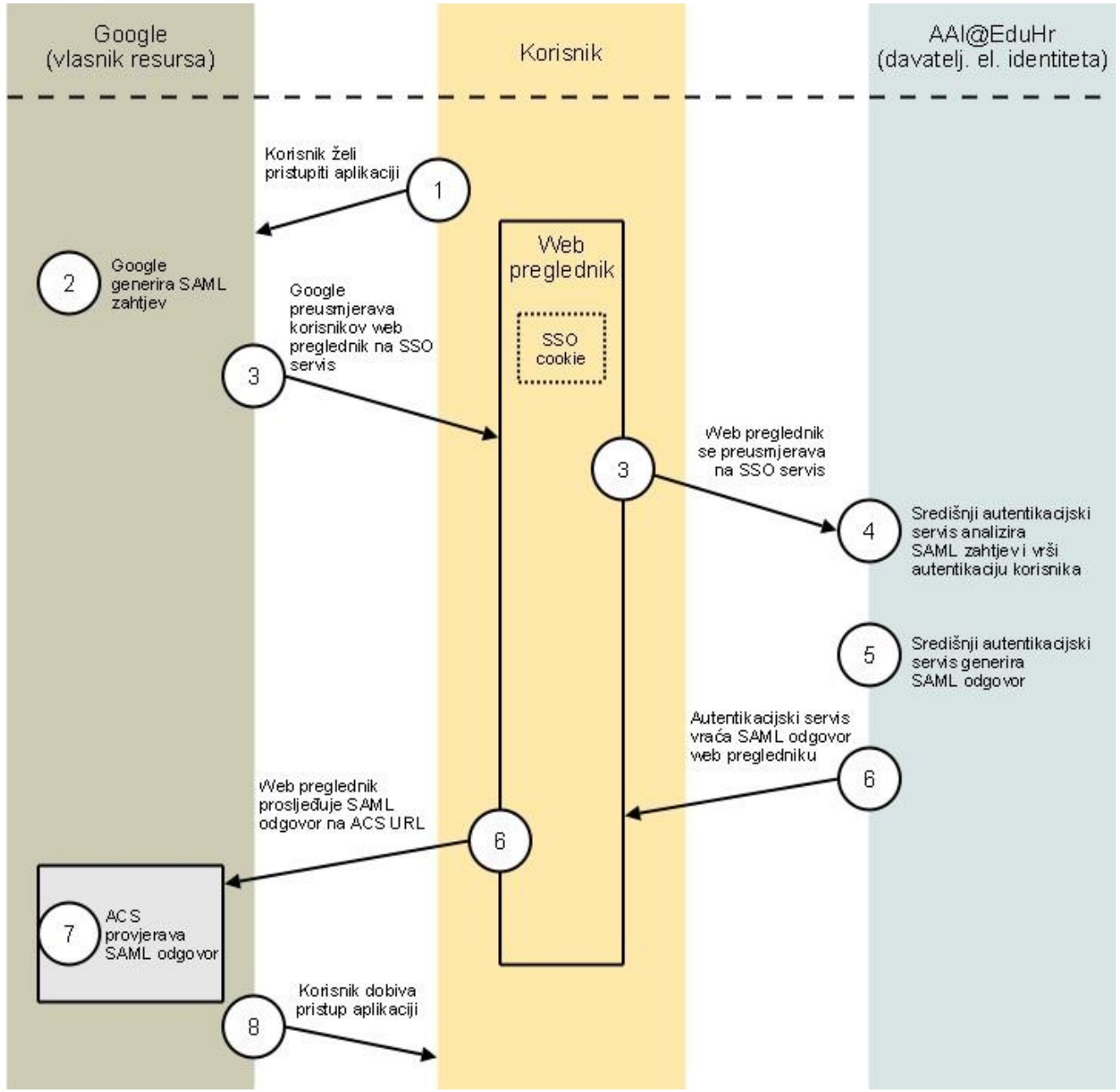


Struktura poruke

- Profil
- Veze
- Protokoli
- Potvrde
- Metapodaci



AAI@Edu


Google
(vlasnik resursa)
Korisnik
AAI@EduHr
(davatelj. el. identiteta)
Korisnik želi
pristupiti aplikaciji
1
Web
preglednik
2
Google
generira SAML
zahtjev
Google
preusmjerava
korisnikov web
preglednik na SSO
servis
3
SSO
cookie
Web preglednik
se preusmjerava
na SSO servis
3
4
Središnji autentikacijski
servis analizira
SAML zahtjev i vrši
autentikaciju korisnika
5
Središnji autentikacijski
servis generira
SAML odgovor
Autentikacijski servis
vraća SAML odgovor
web pregledniku
6
Web preglednik
prosljeđuje SAML
odgovor na ACS URL
6
7
ACS
provjerava
SAML odgovor
Korisnik dobiva
pristup aplikaciji
8

SSO / SLO

- Single LogOut
- AAI sustavi tipično nude SSO, a logout?
- logout je sigurnosni rizik, može li se prepustiti □□korisniku?
- razumije li korisnik kako radi SSO sjednica?
- prekid rada s jednom uslugom ne prekida SSO sjednicu individualnoj usluzi?
- ili je to posao kojeg treba obaviti na razini cijele federacije?
- SAML 2.0 ima Single Logout Profile
- logout informacija šalje se svim aplikacijama koje dijele aktivnu SSO sjednicu

Virtualne organizacije (VO)

- u klasičnom modelu AAI podaci o korisniku dolaze (samo) od matične ustanove
- postoji potreba (na razini usluge ili grupe usluga) da se korisnici (ad hoc) grupiraju (u virtualnu organizaciju)
- model u kojem o pripadnosti grupi i atributima vezanim uz nju odlučuje i brine matična ustanova nije dugoročno održiv, a ni skalabilan
- rješenje:
  - dodatni repozitoriji (izvori) atributa
  - koncept virtualnih organizacija (VO)

Odgovornost!

- Tko dodaje i briše korisnike
- Tko se brine o identitetu?

Pitanja

?

Hvala na pažnji!