

# Aplikacija za održavanje sadržaja imenika (AOSI)

**Denis Stančer, SRCE**

*1. AAI@EduHr seminar*

*svibanj 2005.*

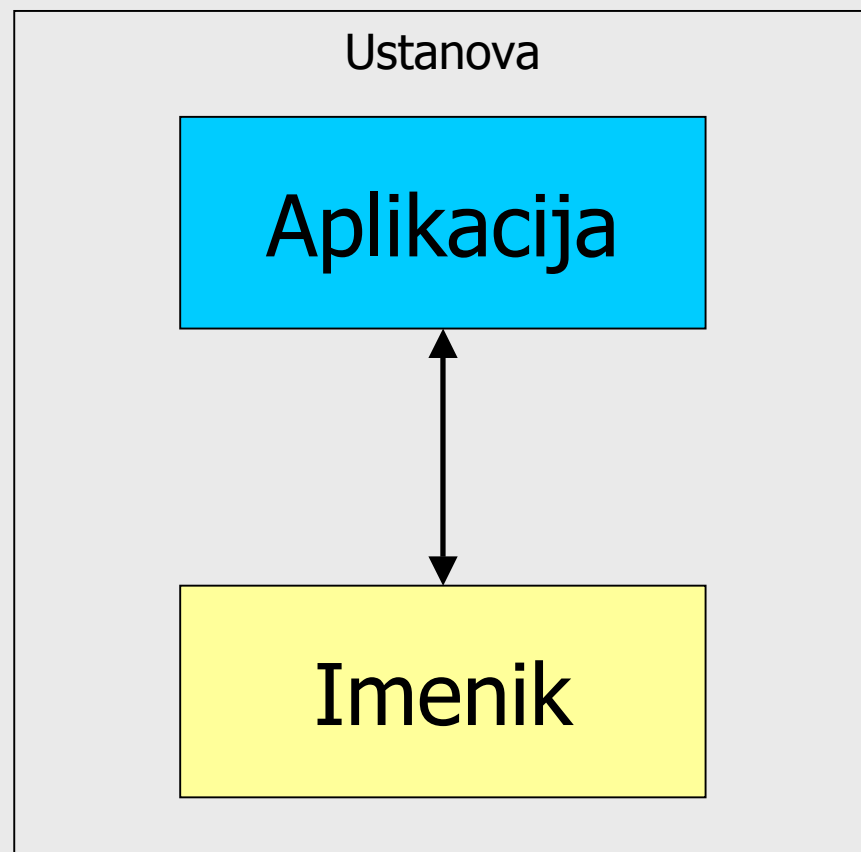
*Osijek, Rijeka, Split, Zagreb*

# Sadržaj

- ❖ Uporaba imenika
- ❖ Novi način uporabe imenika
- ❖ AOSI sustav
- ❖ Pristup sustavu
- ❖ Funkcije i format podataka
- ❖ Proširenje sustava

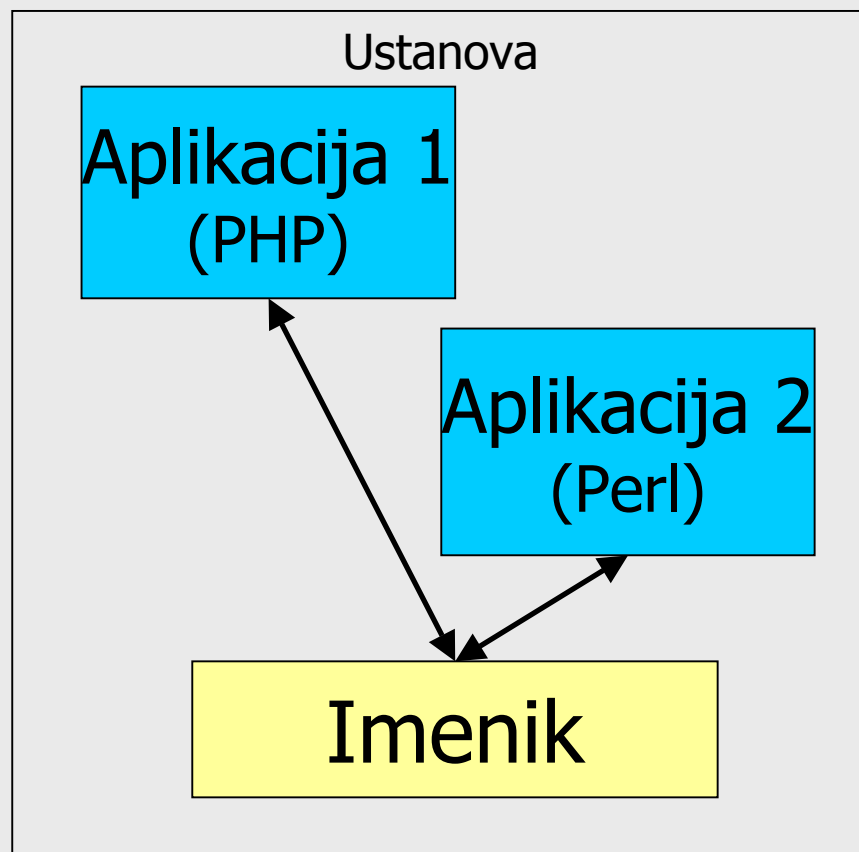
# Uporaba imenika

- ❖ Imeniku se pristupa neposredno LDAP protokolom
- ❖ Samo administrator LDAP servisa (najčešće sistemac) može mijenjati DRUGIM korisnicima attribute



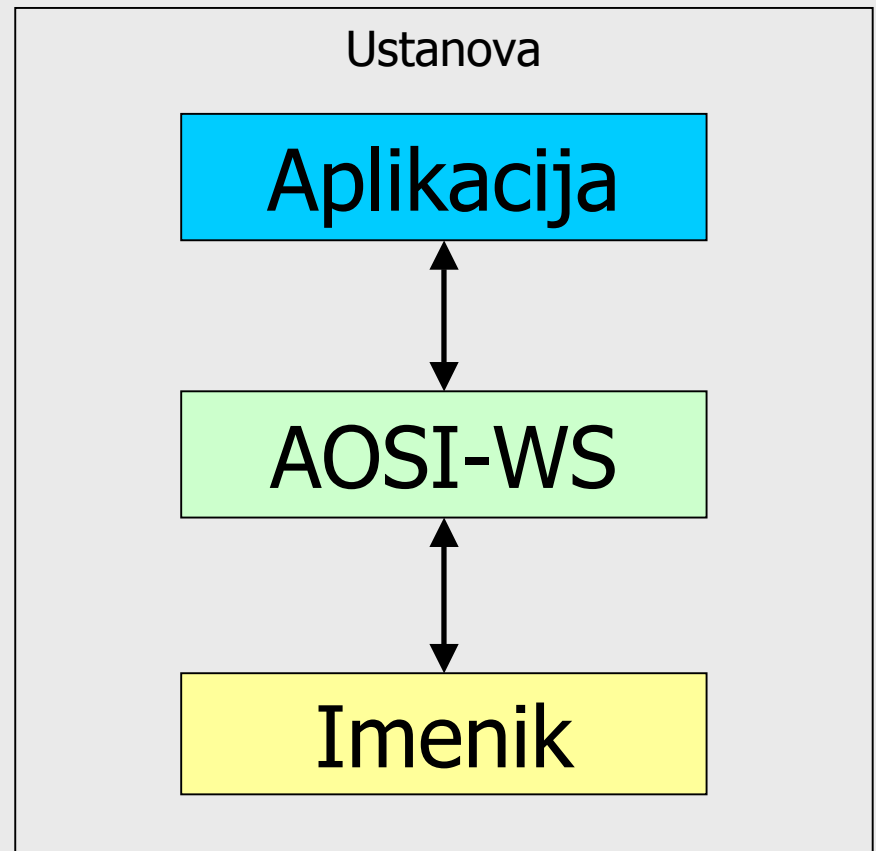
# Uporaba imenika (2)

- ❖ Za promjenu atributa drugim korisnicima svaka aplikacija treba administratorsku zaporku
- ❖ Nesigurno!!!
- ❖ Komunikacija od aplikacije do imenika nije zaštićena
- ❖ Nesigurno!!!!!!



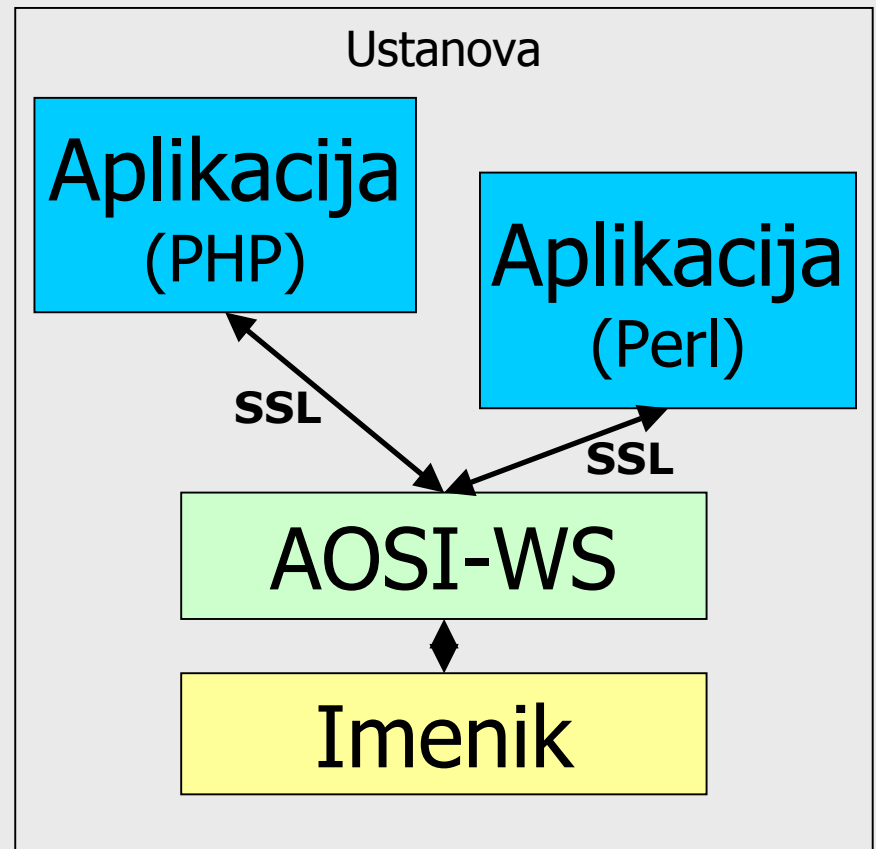
# Novi način uporabe imenika

- ❖ Imeniku se pristupa posredno preko AOSI web servisa
- ❖ Svako povezivanje je autenticirano (tj. potrebni su korisnička oznaka i zaporka)
- ❖ Administratori imenika se autenticiraju svojim korisničkim oznakama i zaporkama (tj. ne “dijeli se” administratorska zaporka)

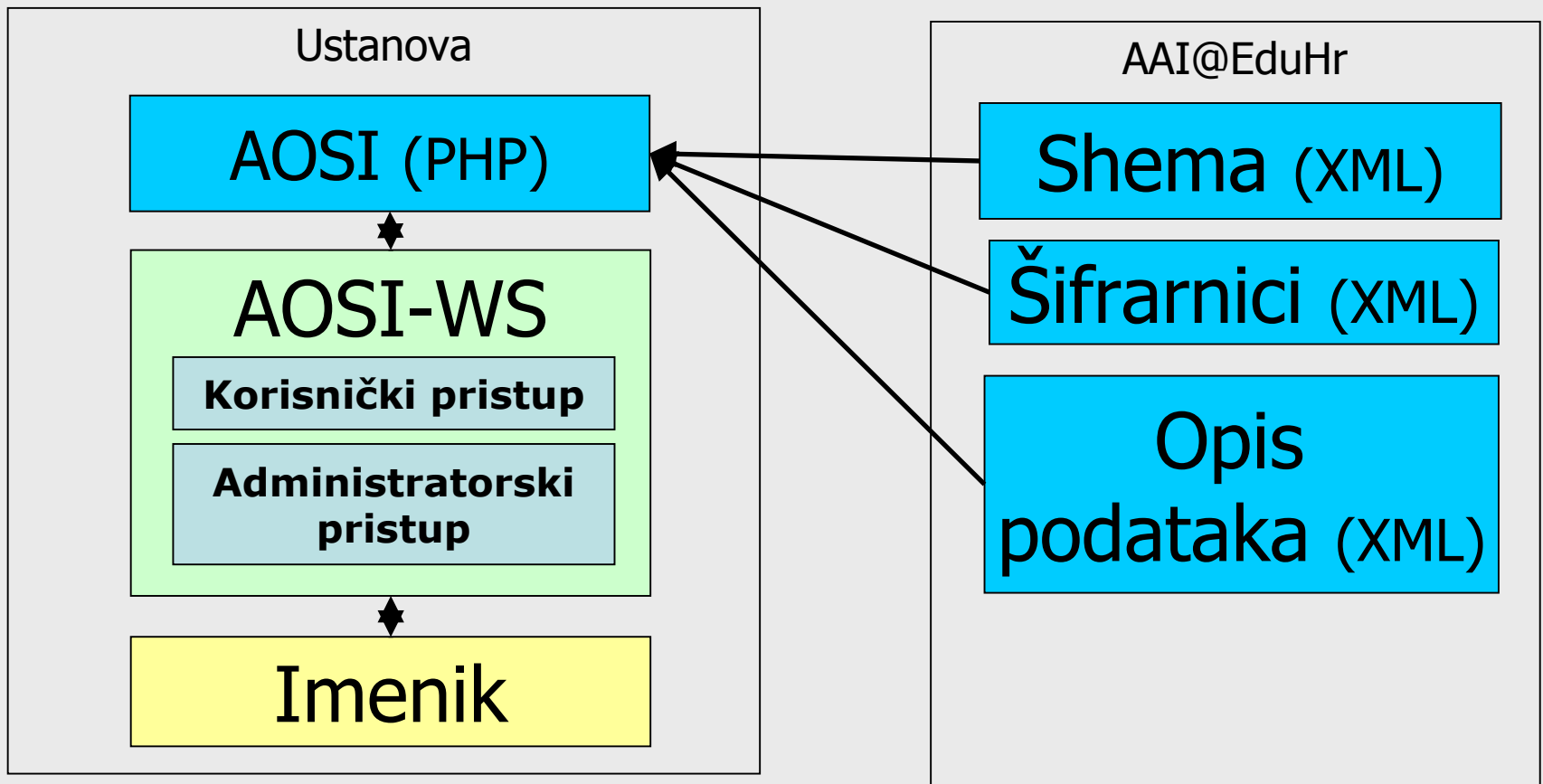


# Novi način uporabe imenika (2)

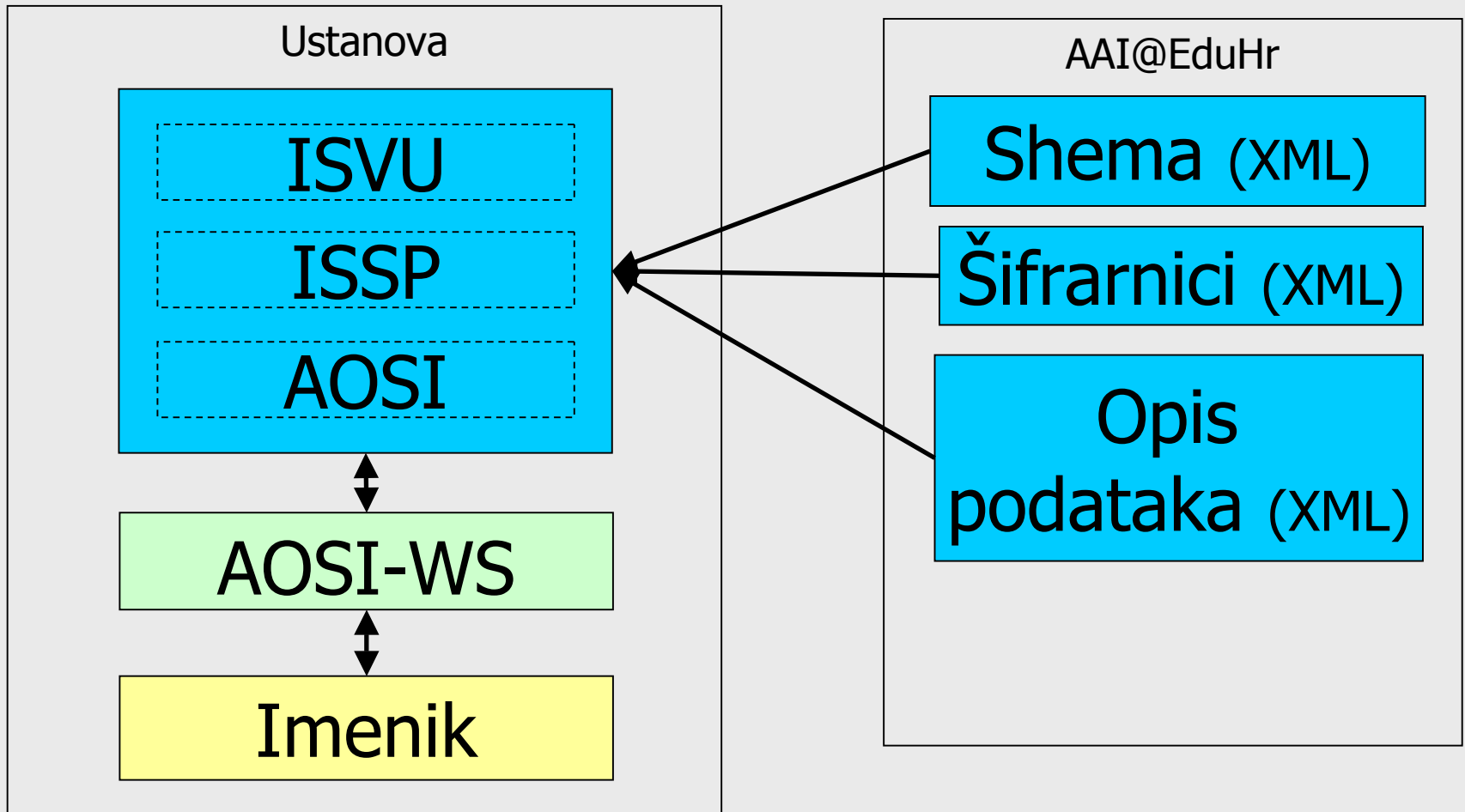
- ❖ Administrator imenika više ne mora biti administrator LDAP servisa
- ❖ Komunikacija od aplikacije do web servisa je zaštićena (SSL)



# AOSI sustav



# AOSI sustav (2)



# Administratorski pristup

- ❖ Svaka ustanova mora imenovati barem jednu osobu za održavanje sadržaja imenika
- ❖ Te osobe imaju administratorski pristup LDAP imeniku ustanove što znači da mogu:
  - ♦ dobiti popis svih korisnika u LDAP imeniku
  - ♦ dobiti sve podatke o pojedinom korisniku
  - ♦ dodati novog korisnika u LDAP imenik
  - ♦ obrisati korisnika iz LDAP imenika
  - ♦ mijenjati podatke o pojedinom korisniku u LDAP imeniku

# Korisnički pristup

- ❖ Korisnici mogu:
  - ♦ dobiti sve podatke u LDAP imeniku o sebi
  - ♦ dobiti samo javne podatke iz LDAP imenika o pojedinom korisniku
  - ♦ mijenjati podatke o sebi u LDAP imeniku

# Administratorske funkcije

- ❖ `IdapSearch(user, password, base, filter, attribute)`
- ❖ `IdapList(user, password, base, filter, attribute, from, size)`
- ❖ `IdapBinSearch(user, password, base, filter, attribute, md5)`
- ❖ `IdapBind(user, password, base)`
- ❖ `IdapUserExists(user, password, base, uid)`
- ❖ `IdapAddUser(user, password, base, xml)`
- ❖ `IdapDeleteUser(user, password, base, dn)`
- ❖ `IdapAddAttribute(user, password, base, xml)`
- ❖ `IdapDeleteAttribute(user, password, base, xml)`
- ❖ `IdapModifyAttribute(user, password, base, xml)`

# Korisničke funkcije

- ❖ `userSearch(user, password, base, filter, attribute)`
- ❖ `userBinSearch(user, password, base, filter, attribute, md5)`
- ❖ `userAddAttribute(user, password, base, xml)`
- ❖ `userDeleteAttribute(user, password, base, xml)`
- ❖ `userModifyAttribute(user, password, base, xml)`

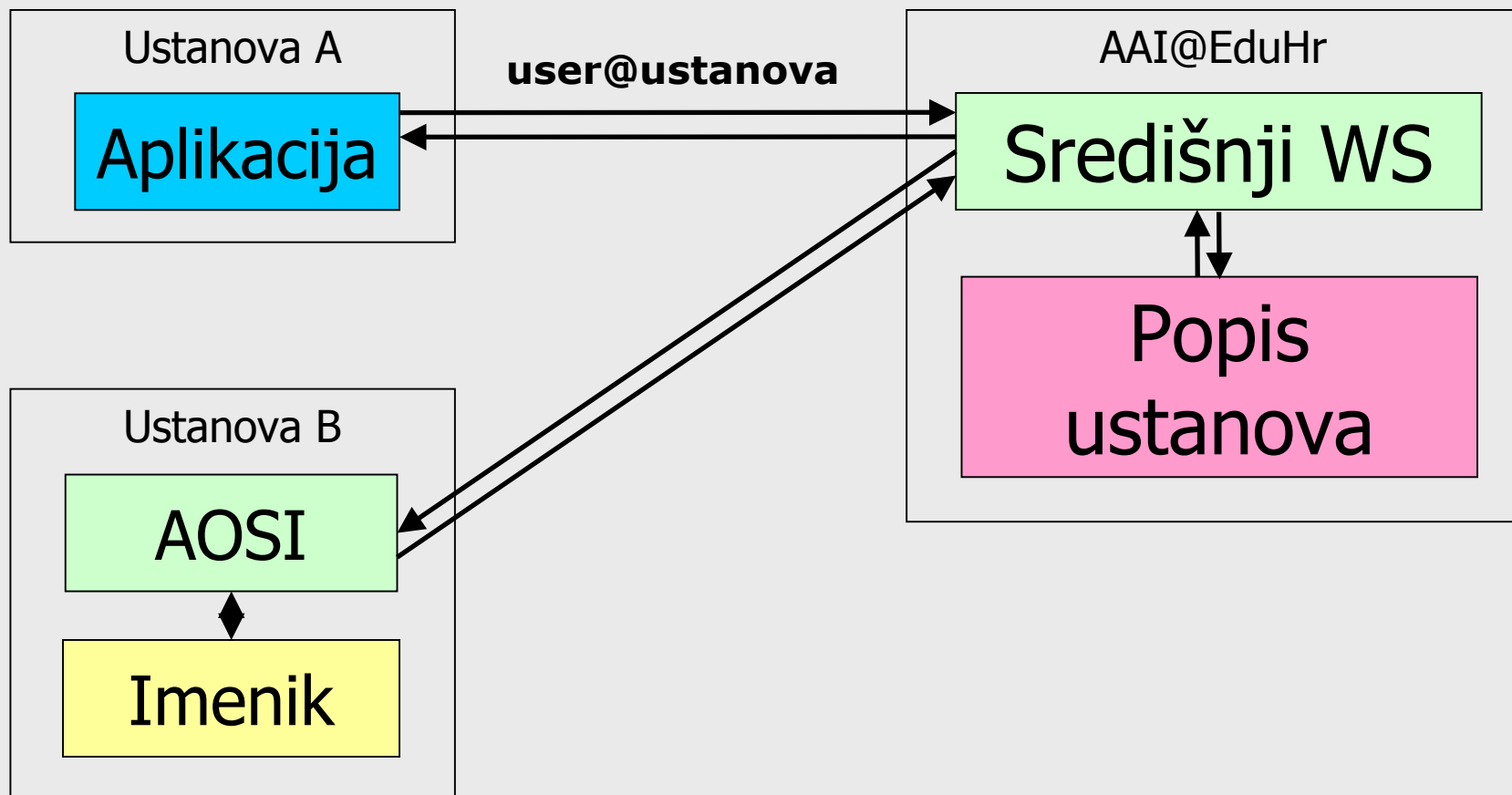
# Format podataka

```
<?xml version="1.0" encoding="UTF-8"?>
<!ELEMENT ldap (entry)*>
<!ELEMENT entry (attribute)*>
<!ATTLIST entry
  dn CDATA #REQUIRED
  num CDATA #IMPLIED
>
<!ELEMENT attribute (singlevalue|multivalue)*>
<!ATTLIST attribute
  ldapname CDATA #REQUIRED
>
<!ELEMENT singlevalue (#PCDATA)>
<!ELEMENT multivalue (value)+>
<!ELEMENT value (#PCDATA)>
```

# Format podataka (2)

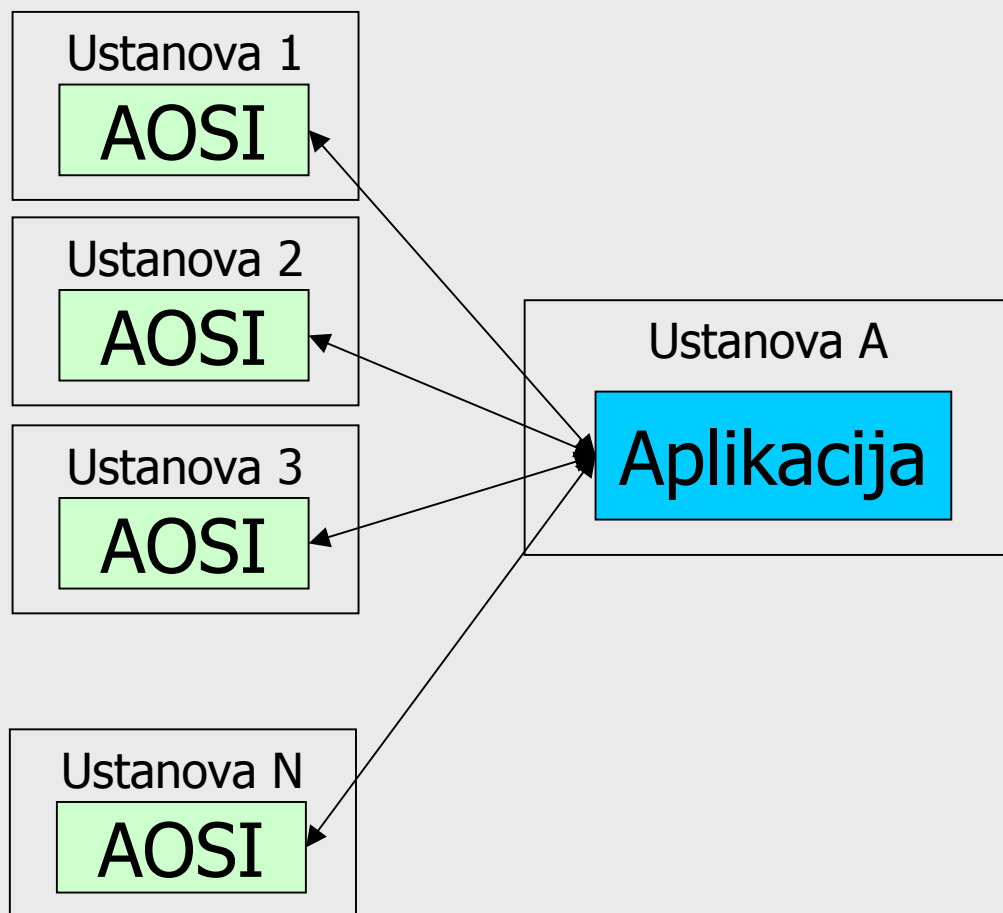
```
<ldap>
  <entry dn="uid=utest,dc=srce,dc=hr">
    <attribute ldapname="sn">
      <multivalue>
        <value>UTest</value>
        <value>UTest 2</value>
      </multivalue>
    </attribute>
    <attribute ldapname="uid">
      <singlevalue>utest</singlevalue>
    </attribute>
  </entry>
</ldap>
```

# Proširenje sustava



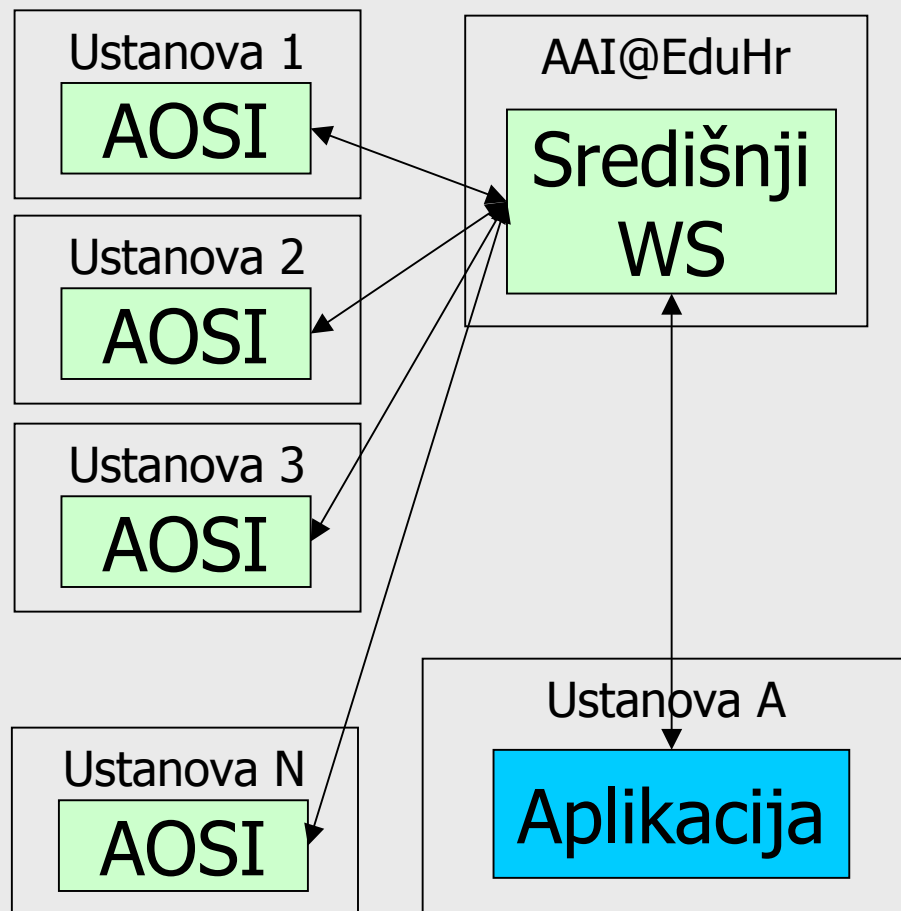
# Proširenje sustava (2)

- ❖ Aplikacija mora “poznavati” infrastrukturu
- ❖ Aplikacija mora “znati” gdje se nalazi pojedini imenik



# Proširenje sustava (3)

- ❖ Aplikacija mora “znati” samo adresu središnjeg servisa
- ❖ Središnji servis “zna” gdje se nalazi odgovarajući imenik



# Prednosti za autore aplikacija

- ❖ Aplikacije imaju središnje mjesto na kojem:
  - ♦ autenticiraju korisnike
  - ♦ dohvaćaju attribute potrebne za autorizaciju
- ❖ Autori aplikacija ne trebaju poznavati infrastrukturu (tj. gdje se nalazi imenik za određenu osobu)
- ❖ Pristup aplikacijama za sve osobe koje su u AAI sustavu (a dozvoljavaju čitanje potrebnih atributa!)

# Prednosti za ustanove

- ❖ Pristup imeniku je dozvoljen samo s određenih mjesta:
  - ♦ iz unutarnje mreže ustanove
  - ♦ iz određene točke u AAI@EduHr sustava (središnji WS)
- ❖ Ustanova vjeruje samo određenim točkama – veća sigurnost
- ❖ Korisnici u ustanovi mogu (potencijalno) koristiti sve aplikacije koje su u sustavu



AAI@EduHr

<http://www.aaiedu.hr/>

[team@aaiedu.hr](mailto:team@aaiedu.hr)