1. srečanje članic federacij
ArnesAAI in eduroam

Avgust Jauk
Arnes, p.p. 7, SI - 1001 Ljubljana
jauk@arnes.si

8. 12. 2014

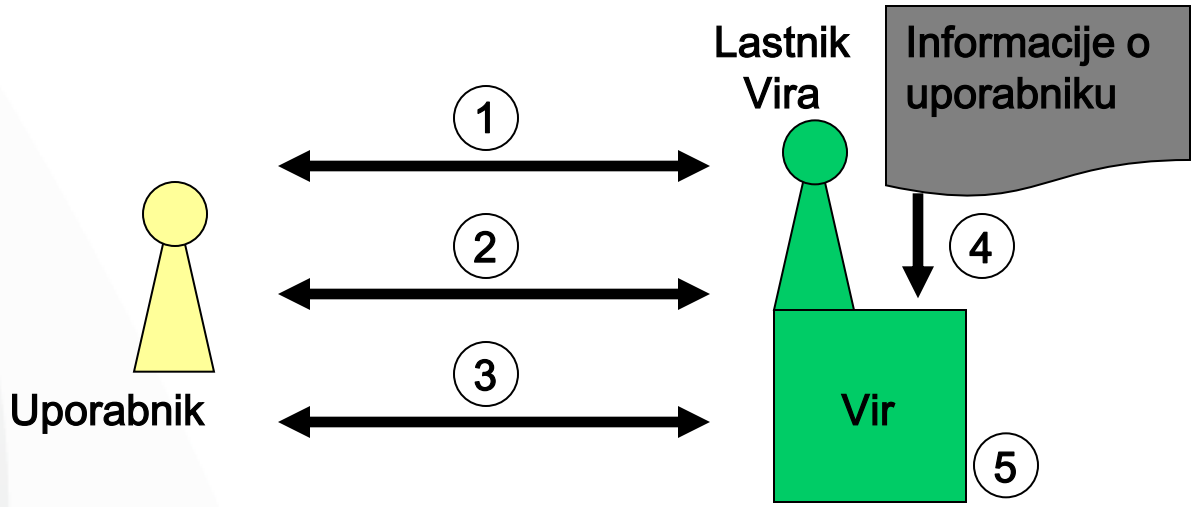
Namen srečanja

- AAI in eduroam dozorevata
  - 10 let eduroam v SI (BIO v 2004)
  - 5 let ArnesAAI
- Leta izkušenj -> (problemi) -> novosti
  - Tehnologija
  - Storitve Arnesa
- Kreiranje skupnosti
  - Mailing lista
  - …?

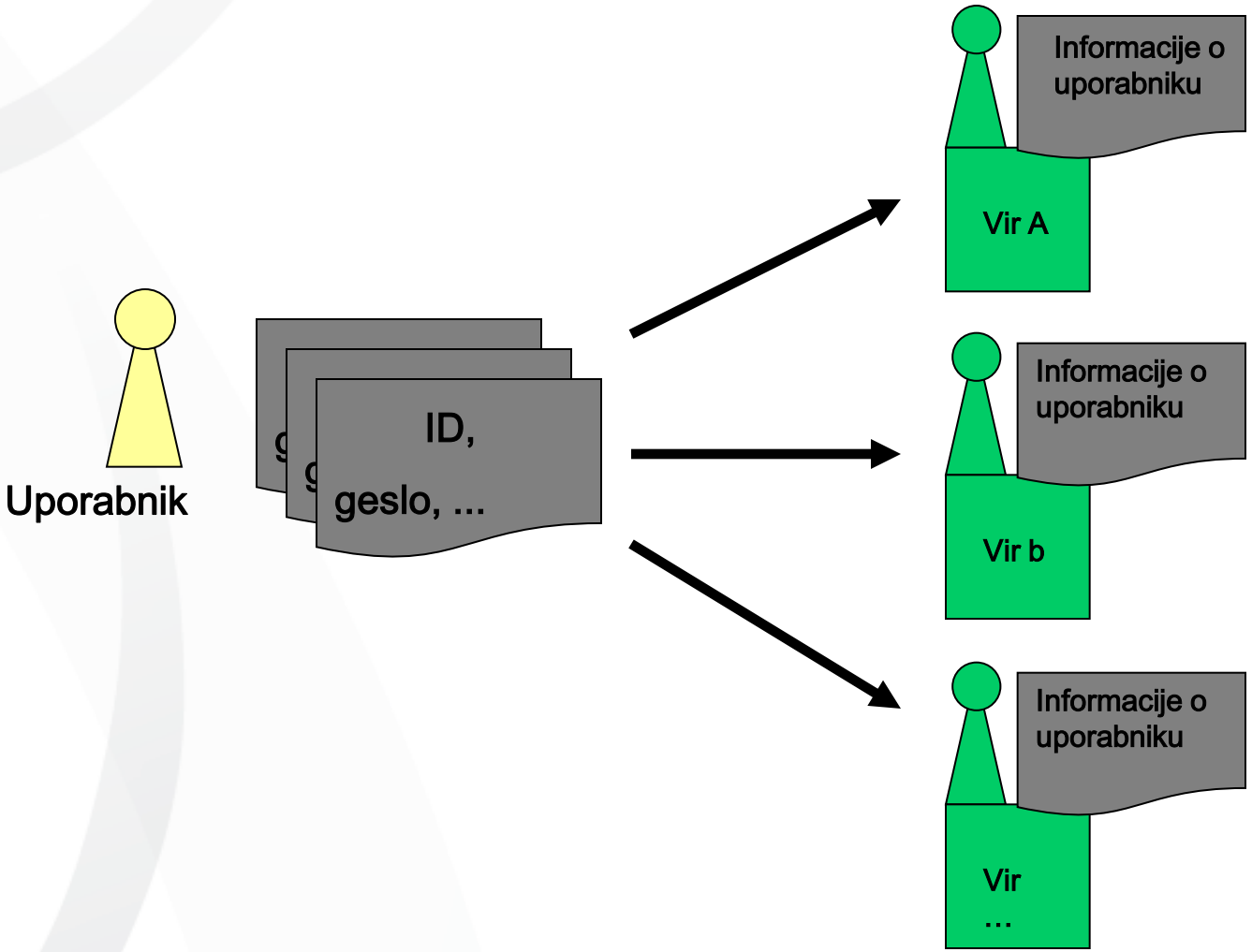
Federacije: zakaj že?

- Množica storitev, povsod prijava
  - Aplikacije
  - Računalniki
  - Omrežje
  - Mobilnost -> potreba po gostovanju
- Množica uporabniških imen
  - Težko jih je pridobiti
  - Gesla pozabljamo
    - Obremenitev helpdeska
    - Nejevolja uporabnikov

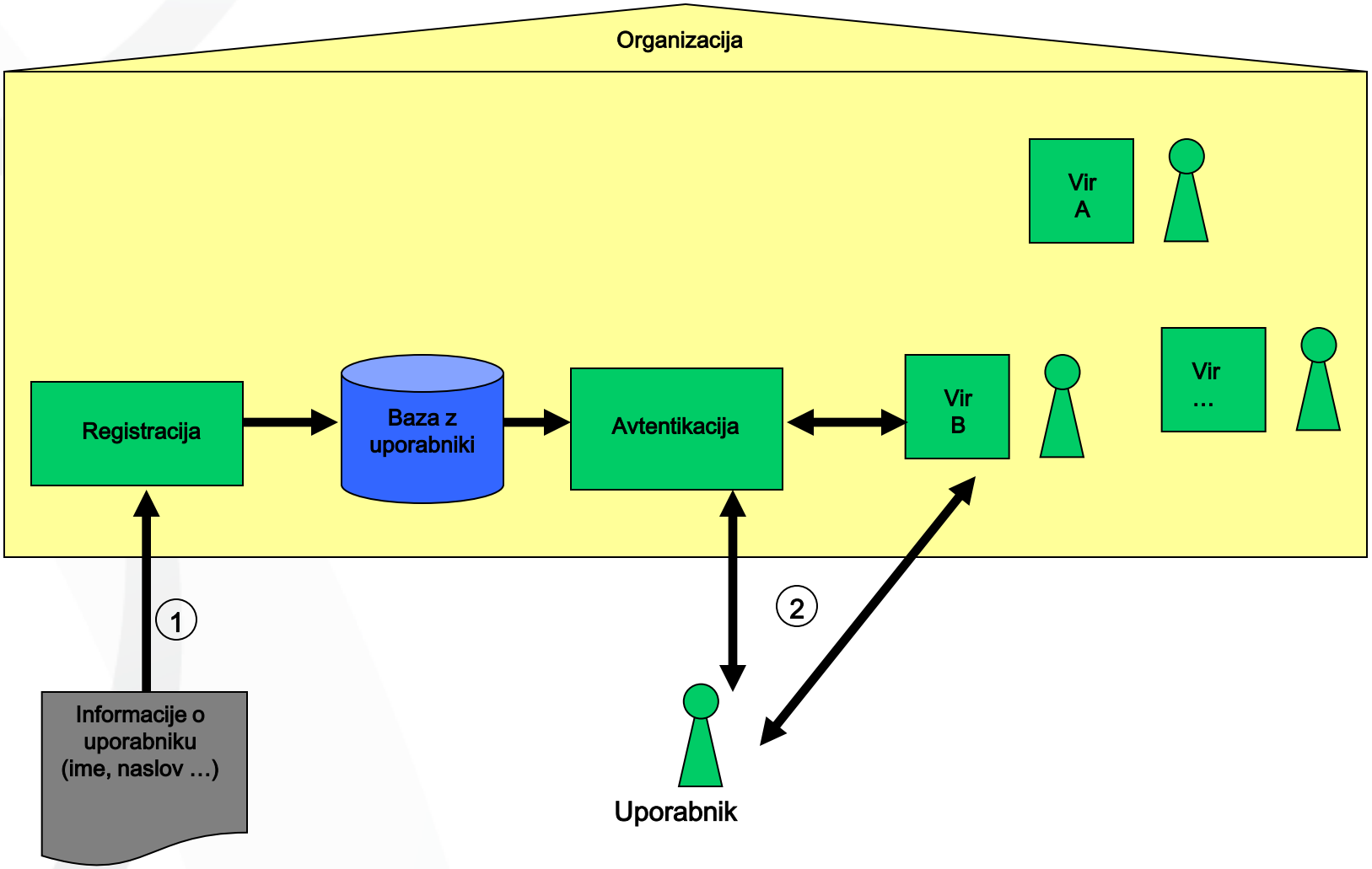
Prijava – običajen način



Prijava – običajen način (2)



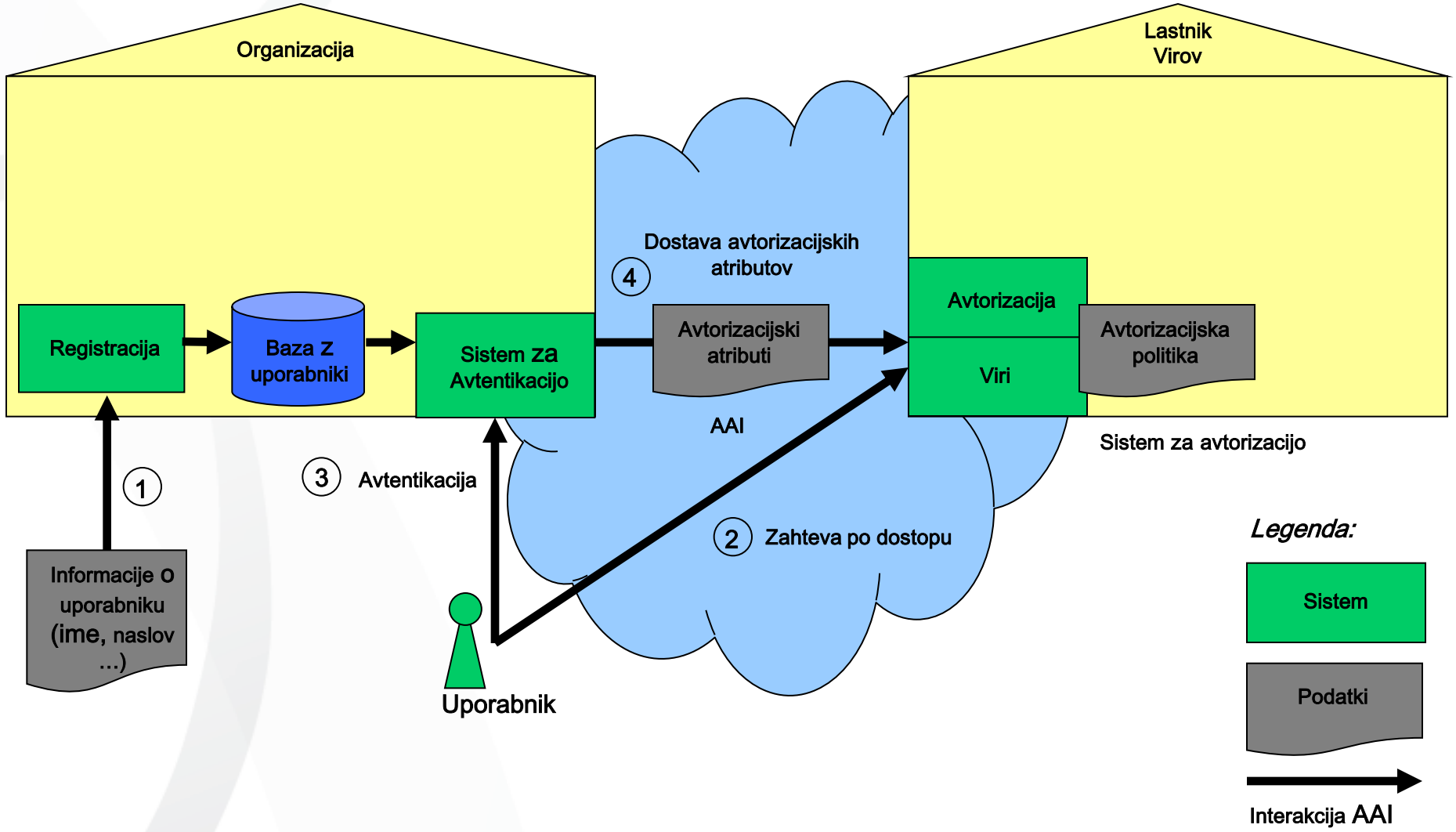
Enotna prijava: v eni organizaciji



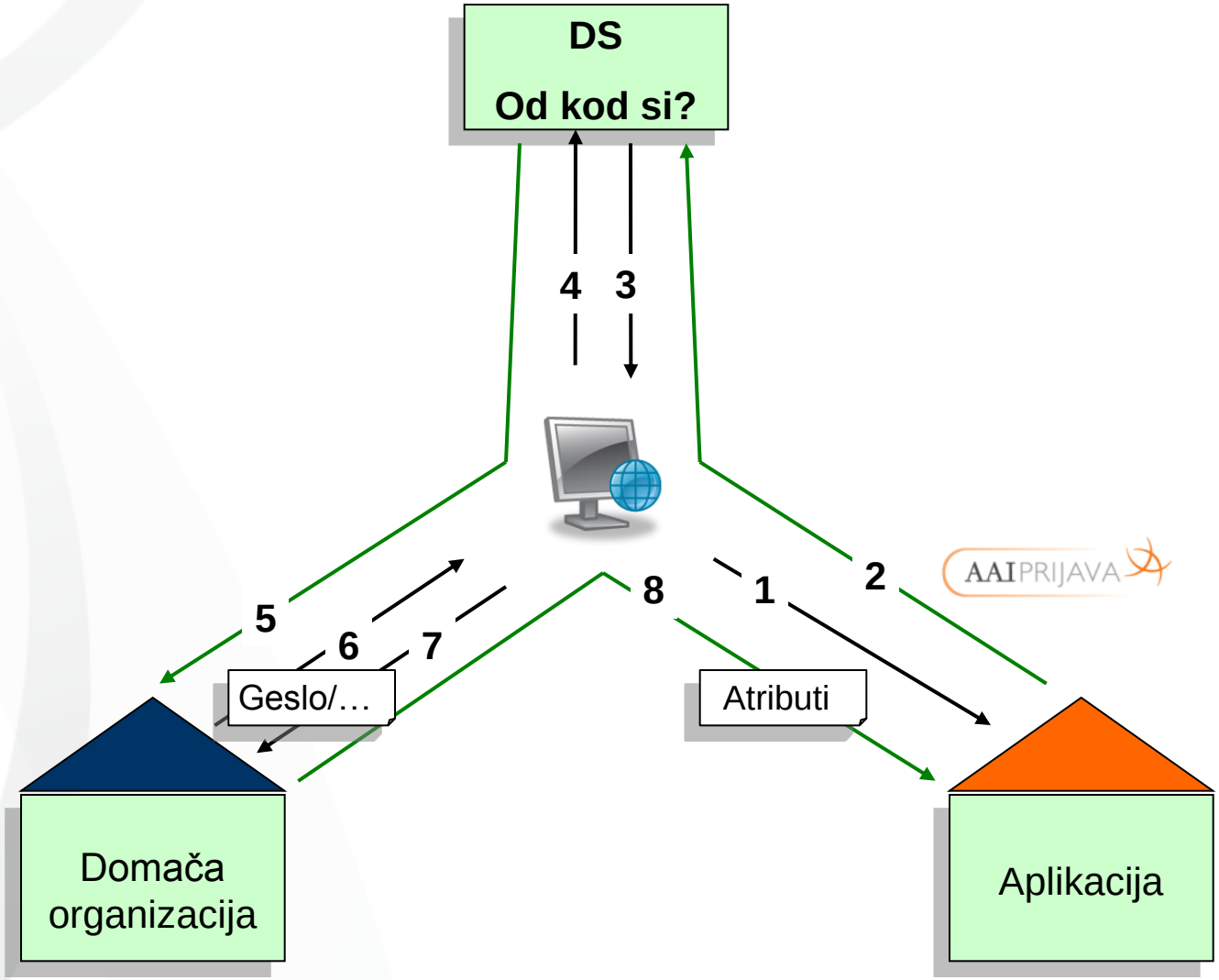
Željena rešitev?

- Enotno uporabniško ime
  - **NetID, AAI uporabniško ime/račun**
  - Uporabno za storitve doma in po svetu
  - Tudi za priklop v omrežje
- Dodeli ga „domača“ organizacija
  - Ponudnik identitete
- Implementacija: federacije
  - Ponudniki identitet (**LDAP, IdP**)
  - Ponudniki storitev (**SP**)
  - Pravila, standardi, zaupanje (tehnično, pravno)

Enotna prijava – v federaciji



AAI za spletne storitve



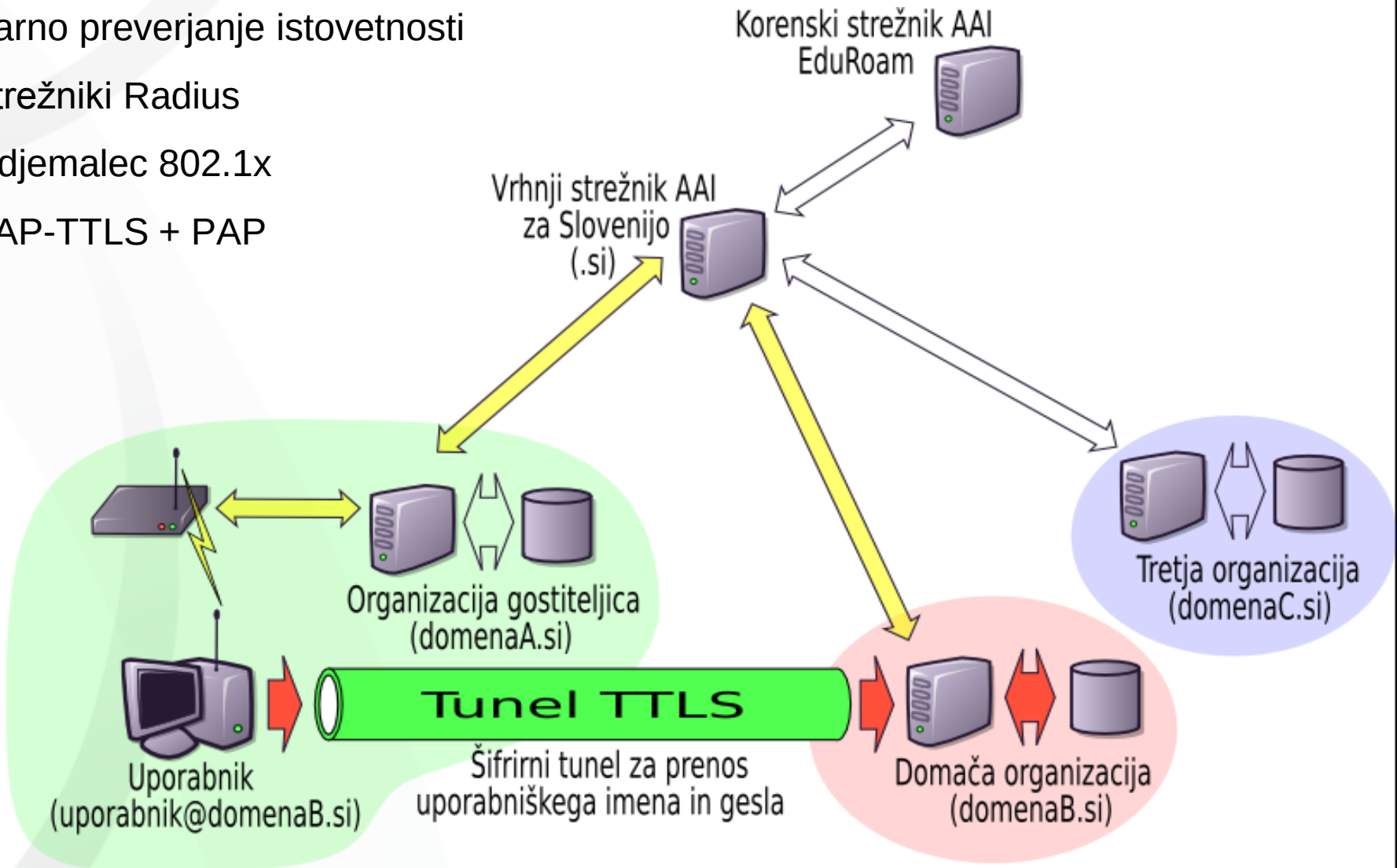
Mobilnost: WLAN

Varno preverjanje istovetnosti

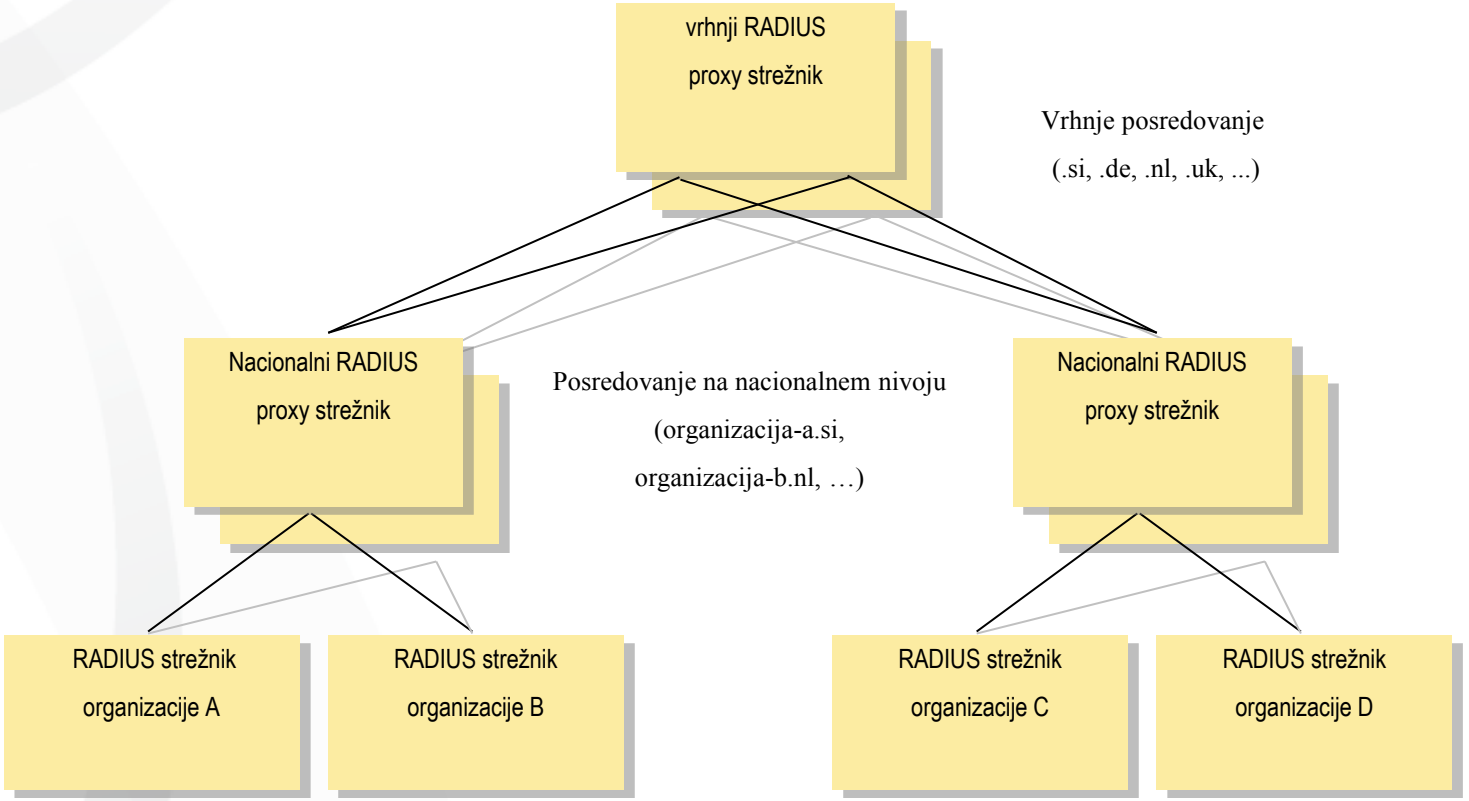
Strežniki Radius

Odjemalec 802.1x

EAP-TTLS + PAP



Mednarodna hierarhija strežnikov RADIUS za eduroam



Odločitev za eduroam

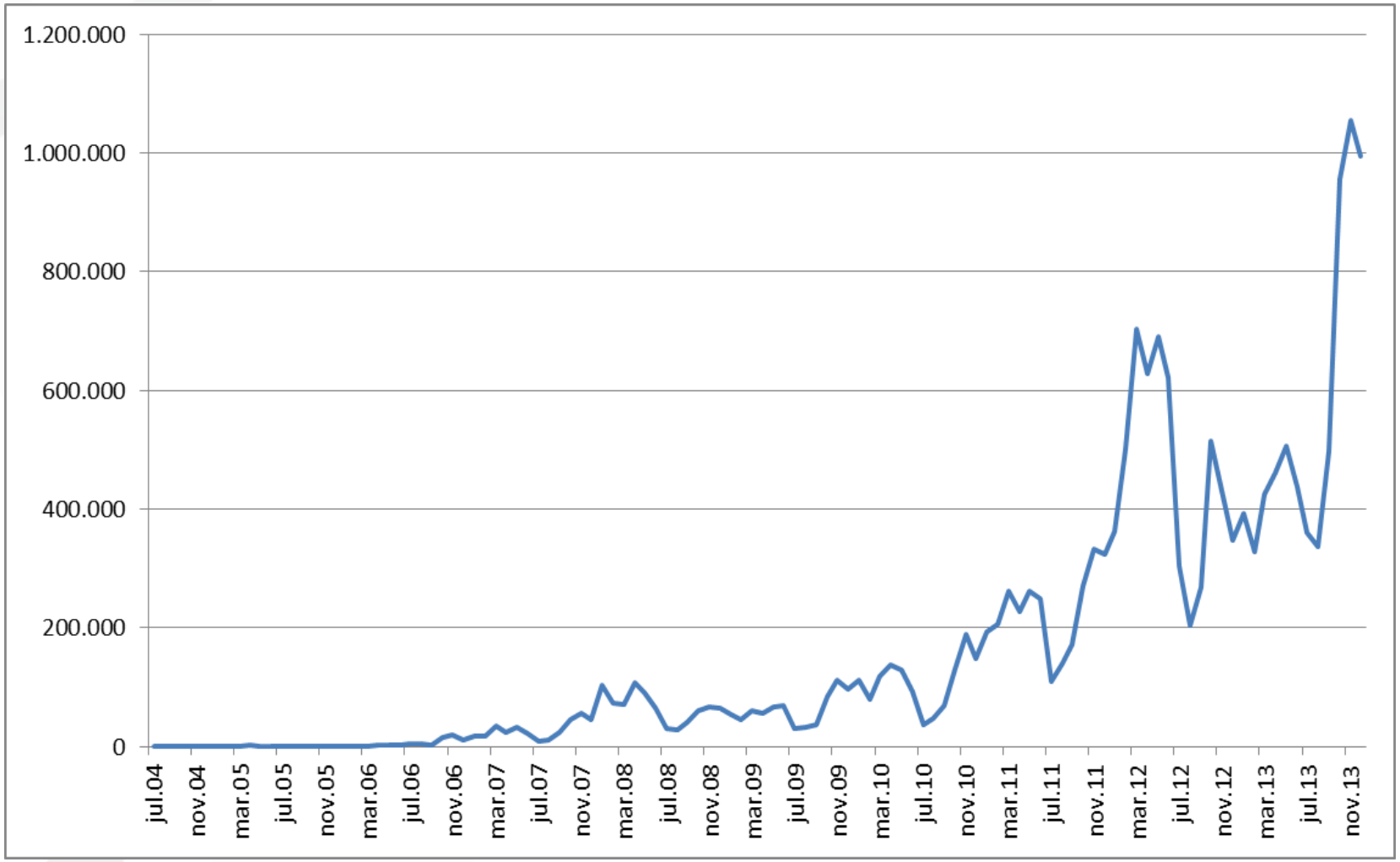
Primerjava posameznih rešitev

Akademska in raziskovalna mreža Slovenije

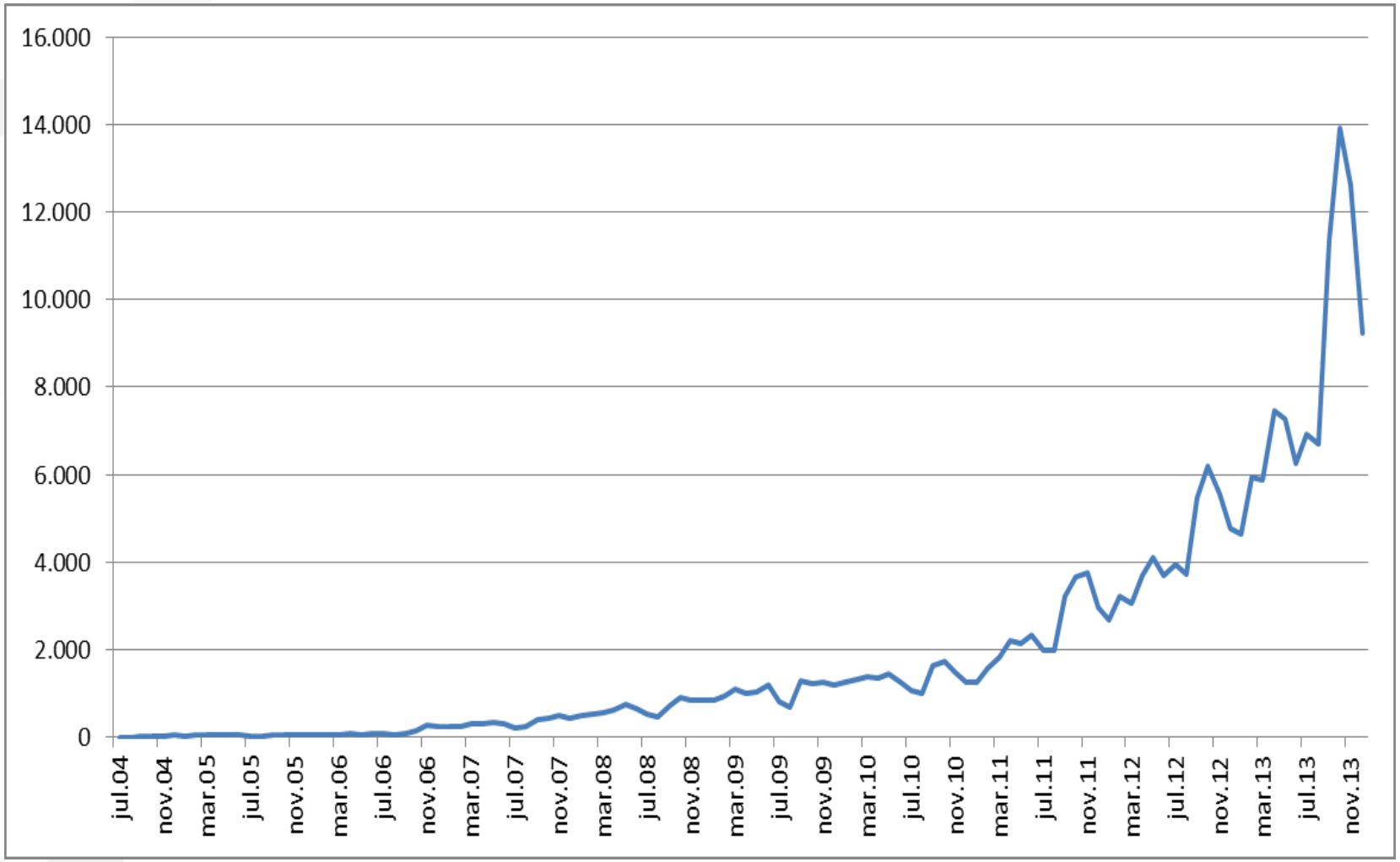
	WEB	VPN	802.1x
Enostavna uporaba s strani uporabnika	+	-potrebna posebna programska oprema	- potrebna posebna programska oprema
Razširljivost	+	-potreben seznam VPN koncentrator	+
Standardna	-	-	+
Varnost	-	+	+
Vpliv na dolžino podatkovne prenosne poti	+	-	+
Potrebna dodatna oprema	- Unix strežnik	- VPN kocentrator	+

Vir: 18. Strokovni svet Arnesa, 15.12.2003

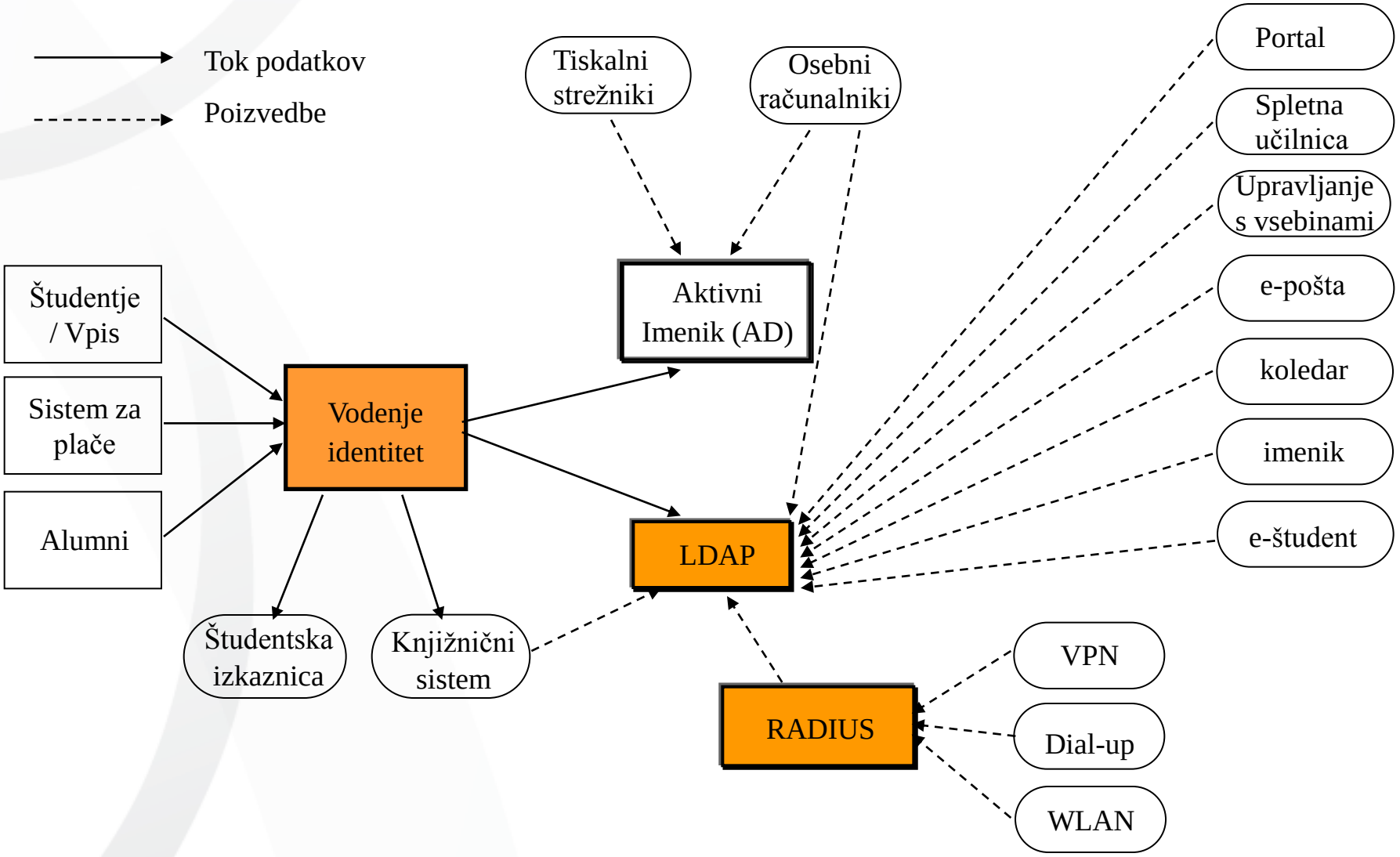
Eduroam – prijave pri gostovanju



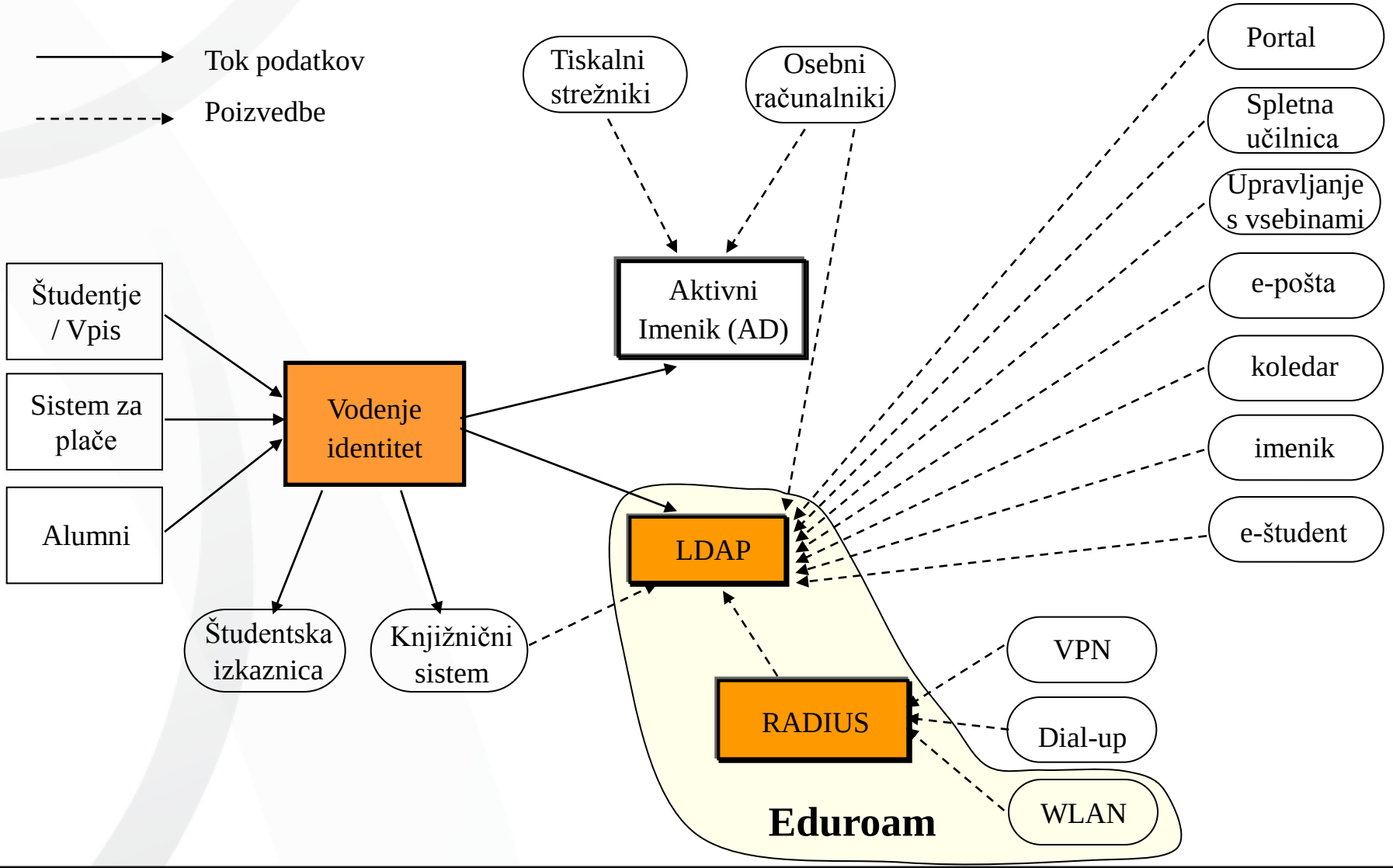
Eduroam – št. AP pri gostovanju



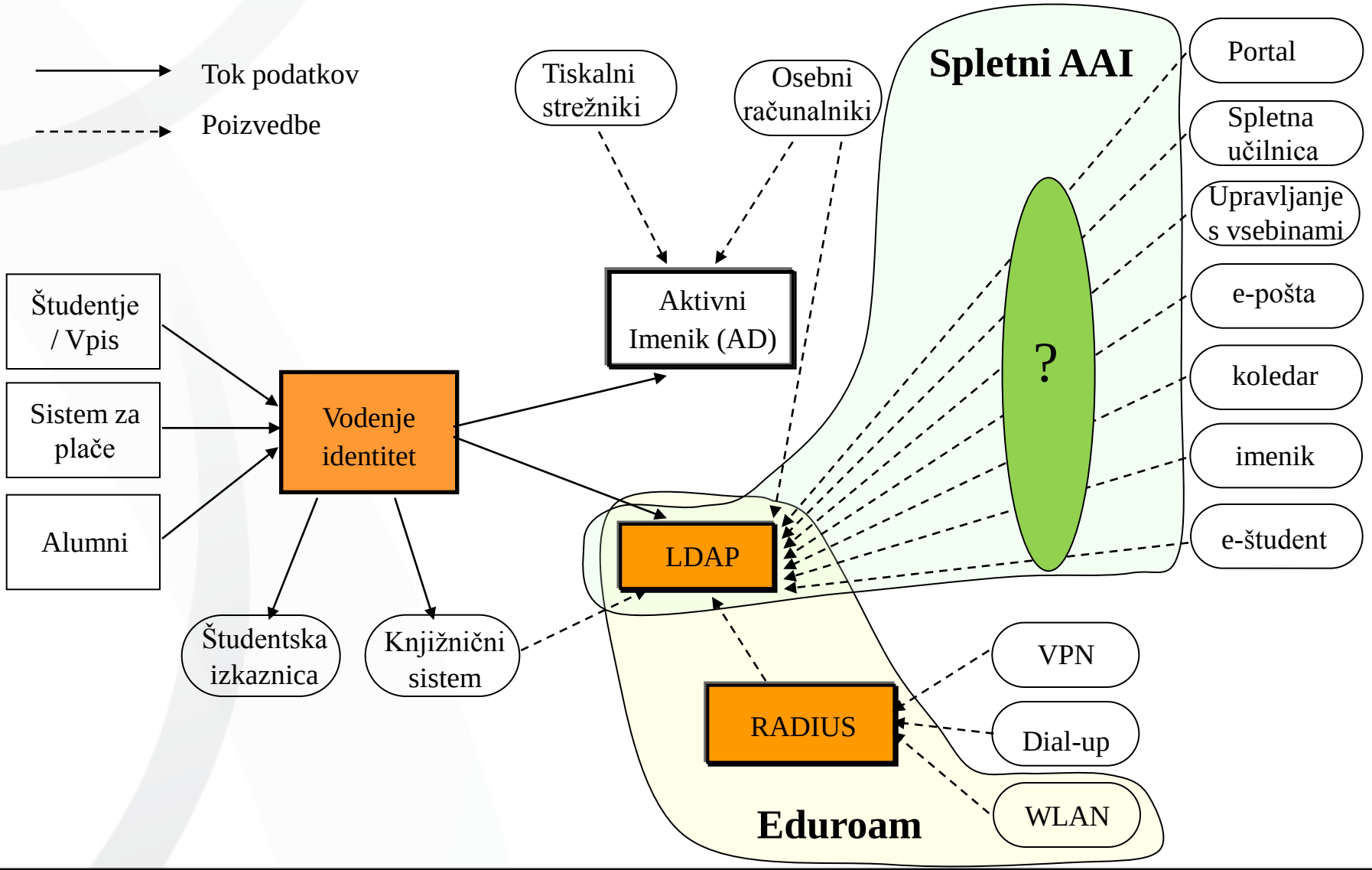
Kako v federacijo?



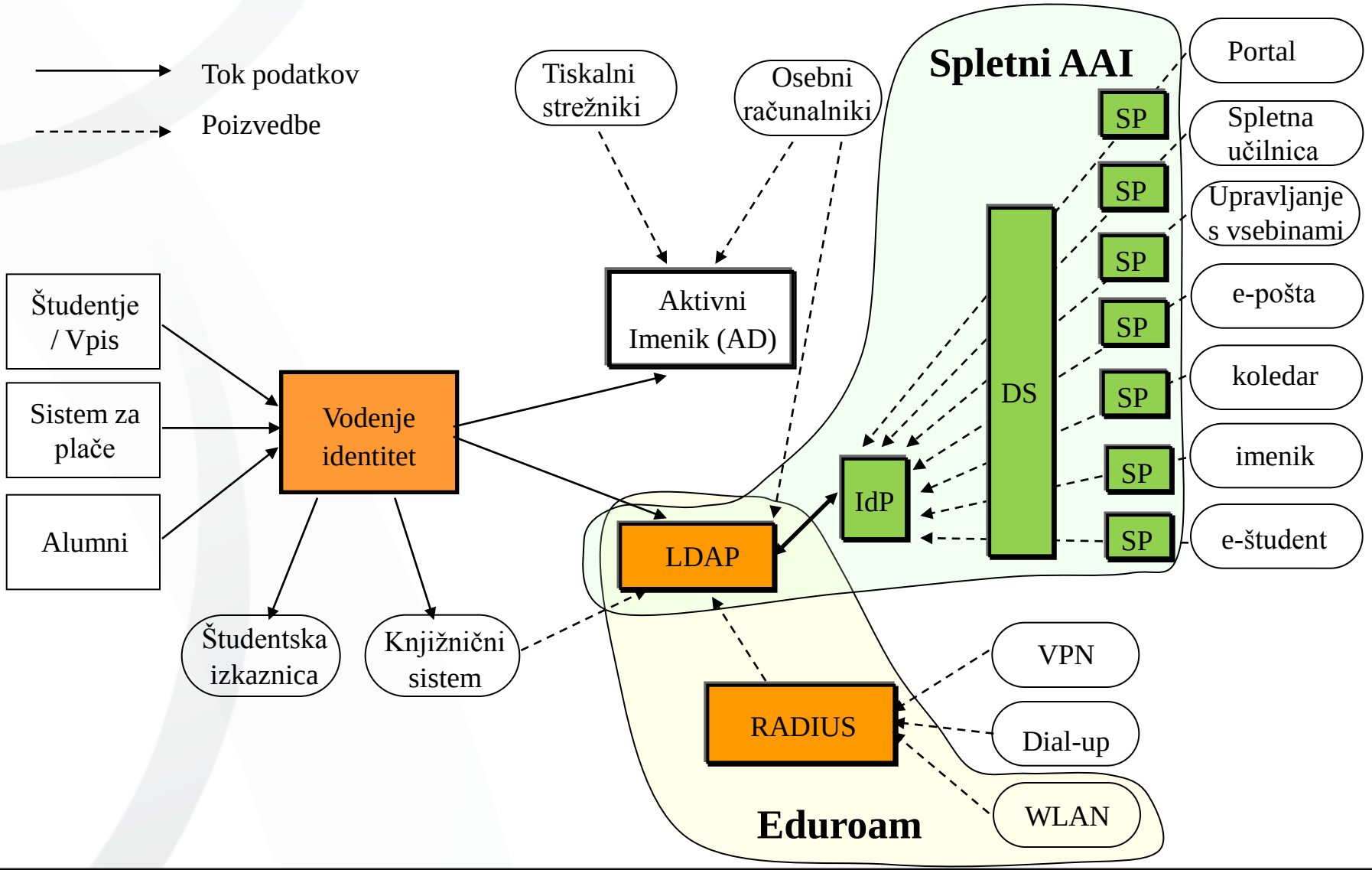
Kako v federacijo 2?



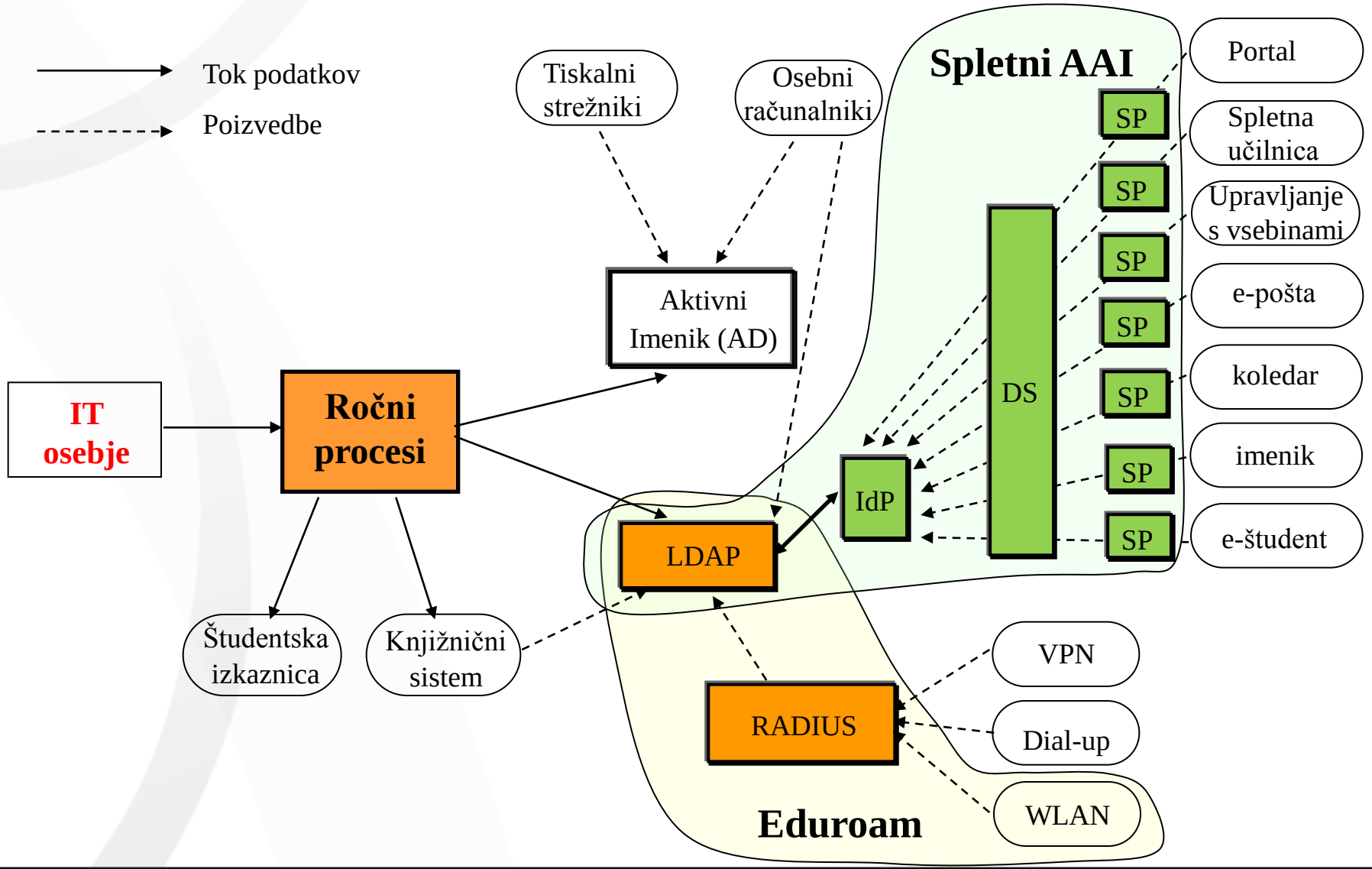
Kako v federacijo 3?



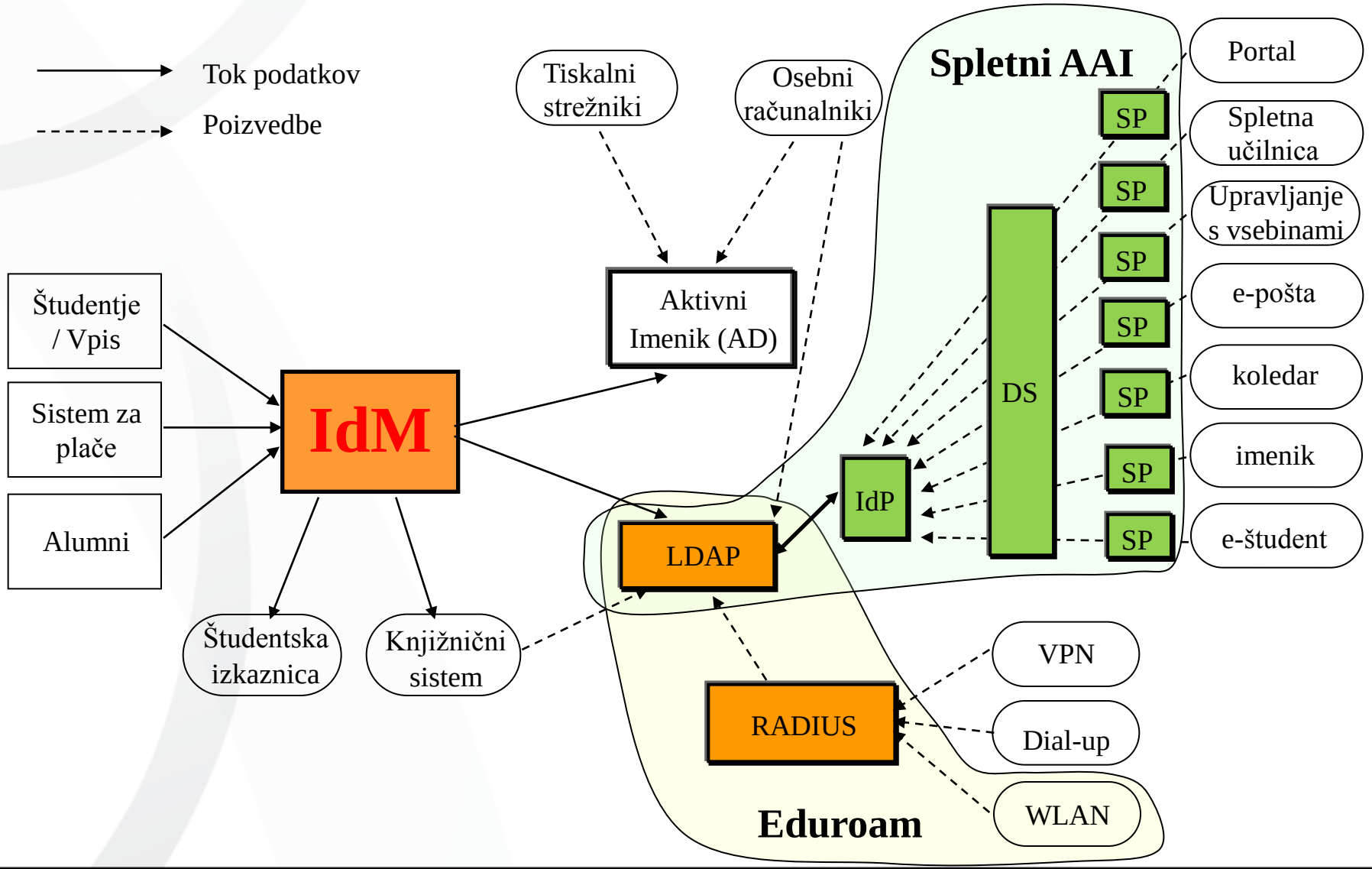
Kako v federacijo 4?



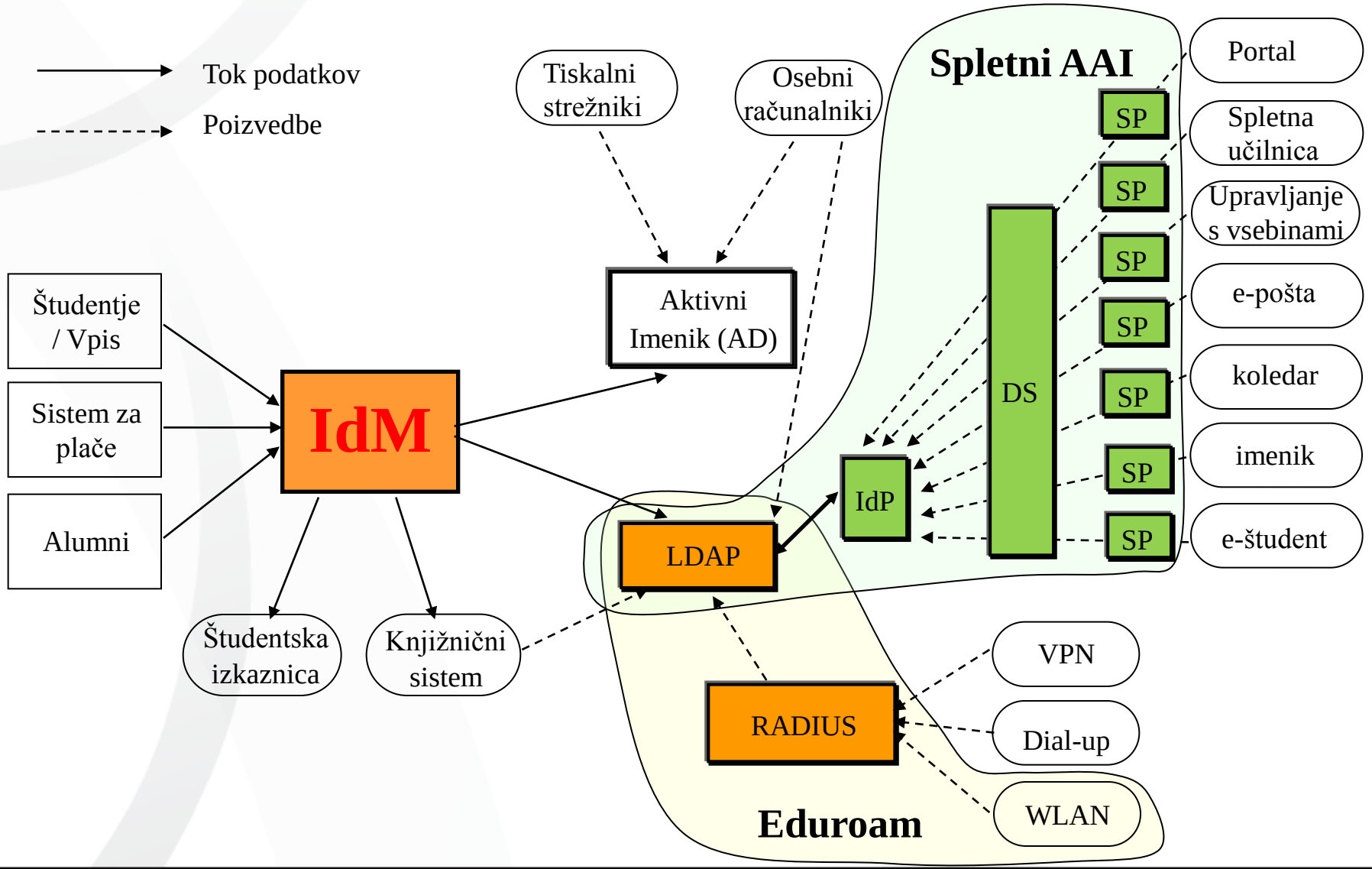
Vodenje identitet - primitivno



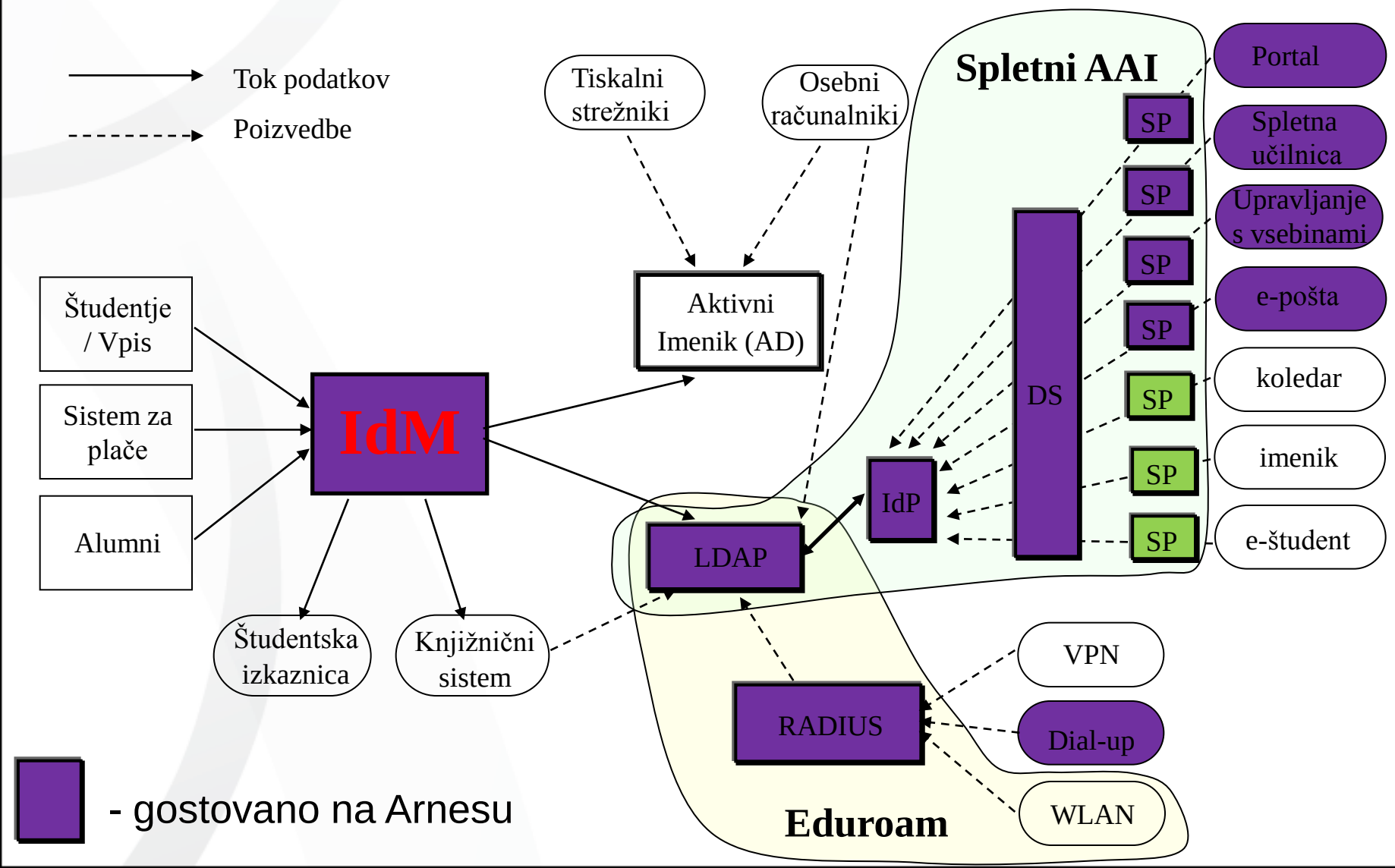
Vodenje identitet - napredno



Preveč kompleksno?



Preveč kompleksno (2)?



Kaj torej dobite na Arnesu

- Gostovanje gradnikov federacij
  - Eduroam: LDAP, RADIUS
  - ArnesAAI: IdP, DS, (SP+aplikacije)
  - IdM
- Portal članic, modul AAI
  - Pridružitev federaciji
  - Naročanje in upravljanje gostovanja IdP, LDAP, IdM
- Orodja
  - Preverjanje IdP, gesel, …
  - Pridobivanje certifikatov
  - Konfiguriranje odjemalcev za eduroam
  - …
- Navodila za administratorje in uporabnike
- Pomoč

Nadaljevanje programa

- AAI
  - AAI za uporabnike velika novost
  - Veliko dela na uporabniški izkušnji
    - Pohitritev postopka prijave (> 10 x)
    - Lažja izbira domače organizacije
    - Branding prijavne strani
  - Pridružitev eduGAIN
  - Orodje za preverjanje IdP
  - Nove verzije IdP, SP, navodila
  - „Portal članic“: upravljanje članstva

Nadaljevanje programa

- Kako polniti imenik
  - LDAP kot mačka
  - Kar nekaj orodij
    - WebIdM, LDAP Admin, Jxplorer
    - Pomanjkljiva funkcionalnost
    - Kompleksnost, nevarnost
- IdM (SIO MdM) – rešitev problemov
  - Enostavnost, potrebna funkcionalnost
    - Tudi tiskanje obvestil o dodelitvi uporabniških imen
  - Prenos podatkov v OpenLDAP in AD

Nadaljevanje programa

- Eduroam (za uporabnike)
  - Problemi uporabnikov
    - konfiguriranje odjemalcev
    - Pomanjkljiva diagnostika
  - Rešitve
    - CAT: orodje za konfiguriranje odjemalcev
    - ArnesLink: Windows odjemalec, diagnostika!
    - Orodje za test pravilnosti gesla

Nadaljevanje programa

- Eduroam (za organizacije)
  - Konfiguracije
    - WLAN za goste brez eduroam računa
    - Redundantna postavitev eduroam
    - …
  - Nove verzije FreeRADIUS, LDAP
  - Orodje za delo s certifikati
    - Pridobivanje, preverjanje, …

AAI/Eduroam ekipa

- Rok Papež
- Blaž Divjak
- Marko Dolničar
- Gregor Cimerman