Kako deluje AAI za spletne storitve
federacija ArnesAAI

Aleks Mihičinac

Avgust Jauk

Rok Papež

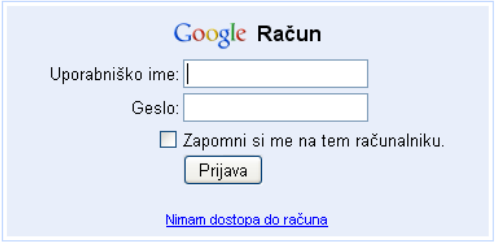
Izvedbo projekta je omogočilo sofinanciranje Evropskega socialnega sklada Evropske unije
in Ministrstva za visoko šolstvo, znanost in tehnologijo.

Kazalo

- Kje je problem?
- Demo s stališča uporabnika
- AAI v Sloveniji
  - Trenutno stanje
  - Kaj manjka
- Pogled v drobovje AAI
  - Tehnični demo
- Kako postati član federacije
- Razprava

Uporabniška imena in gesla

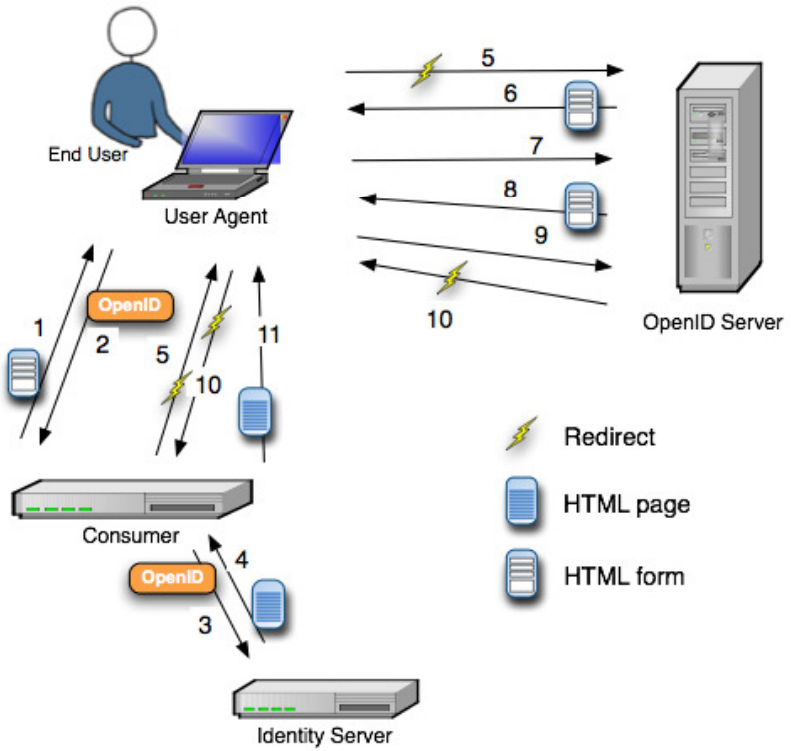
Akademska in raziskovalna mreža Slovenije



- Ena aplikacija in več uporabnikov
  - Ločevanje med uporabniki
  - Uporabniško ime in geslo
- Več aplikacij in več uporabnikov
  - N x M uporabniških imen in gesel: 10 x 50 = 500
  - Pozabljanje gesel
  - Izdajanje novih gesel (IT osebje? Administracija?)
  - Centraliziranje gesel (LDAP, Kerberos)
- Aplikacije zunaj organizacije ?!

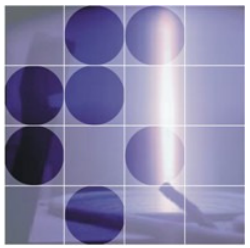
Spletne aplikacije med organizacijami

- Preverjanje identitete med organizacijami?
- Uporabniško ime in geslo?
  - LDAP?
  - Kerberos?
  - OpenID?



„Plačljive“ ali „drage“ aplikacije

- Elektronske revije (ScienceDirect)
- Dostop do baz podatkov iz CERNa
- Potrebujejo dostop do osebnih podatkov
  - Ali je uporabnik polnoleten?
  - Ali je uporabnik iz Inštituta Jožef Stefan?
  - Ime in priimek uporabnika?
  - Kam poslati račun?
  - Na kateri e-naslov poslati obvestilo?



Varnost uporabnika

- Prestrezanje uporabniškega imena in gesla
- Anonimnost uporabnika
  - Ime in priimek?
  - Drugi osebni podatki
  - Za dotično aplikacijo
  - Spremljanje uporabnika (angl. User trackin
    - Znotraj posamezne aplikacije
    - Med ponudniki različnih aplikacij

Rešitev je porazdeljeni sistem

- Ločitev aplikacije od prijave
  - Prijava „doma“, aplikacija kjerkoli
  - Enotna prijava
  - Pošlje le tiste podatke, ki jih aplikacija potrebuje
  - Podatki so „preverjeni“ (vodi jih domača organizacija)
  - Federacija
    - Tehnična kompatibilnost
    - Pravno (pridružitev v „klub“, pravila „obnašanja“)

Video in uporabniški demo!

AAI v Sloveniji

Akademska in raziskovalna mreža Slovenije

AAI v Sloveniji – dostop do omrežja

Akademska in raziskovalna mreža Slovenije

- Federacija Eduroam
  - Dostop do WLAN in LAN!
  - Operativna od 2005
    - Povezanih 62 organizacij
    - Hitra rast
  - www.eduroam.si
- Povezana v konfederacijo eduroam
  - www.eduroam.org

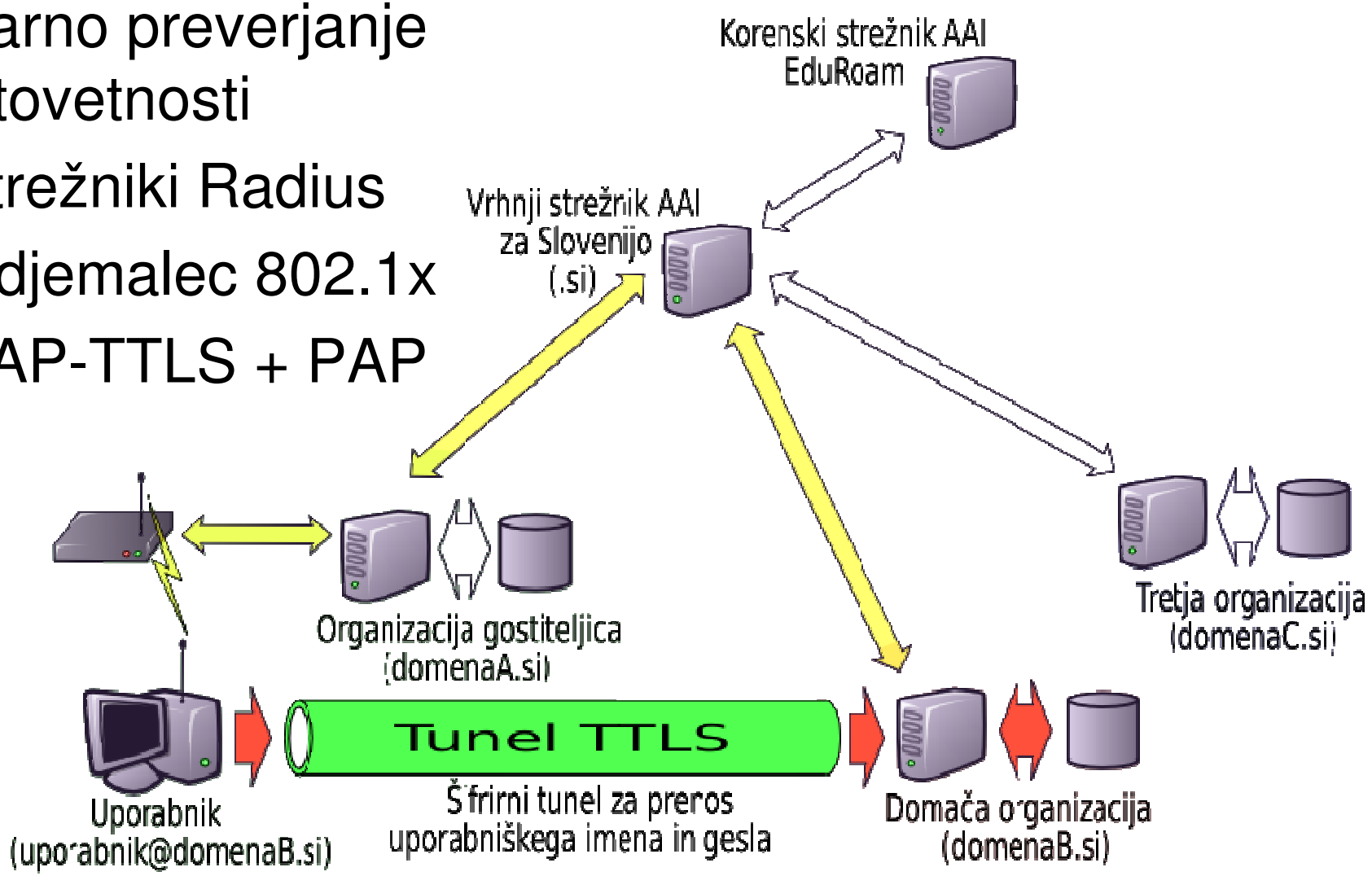
Konfederacija eduroam v Evropi

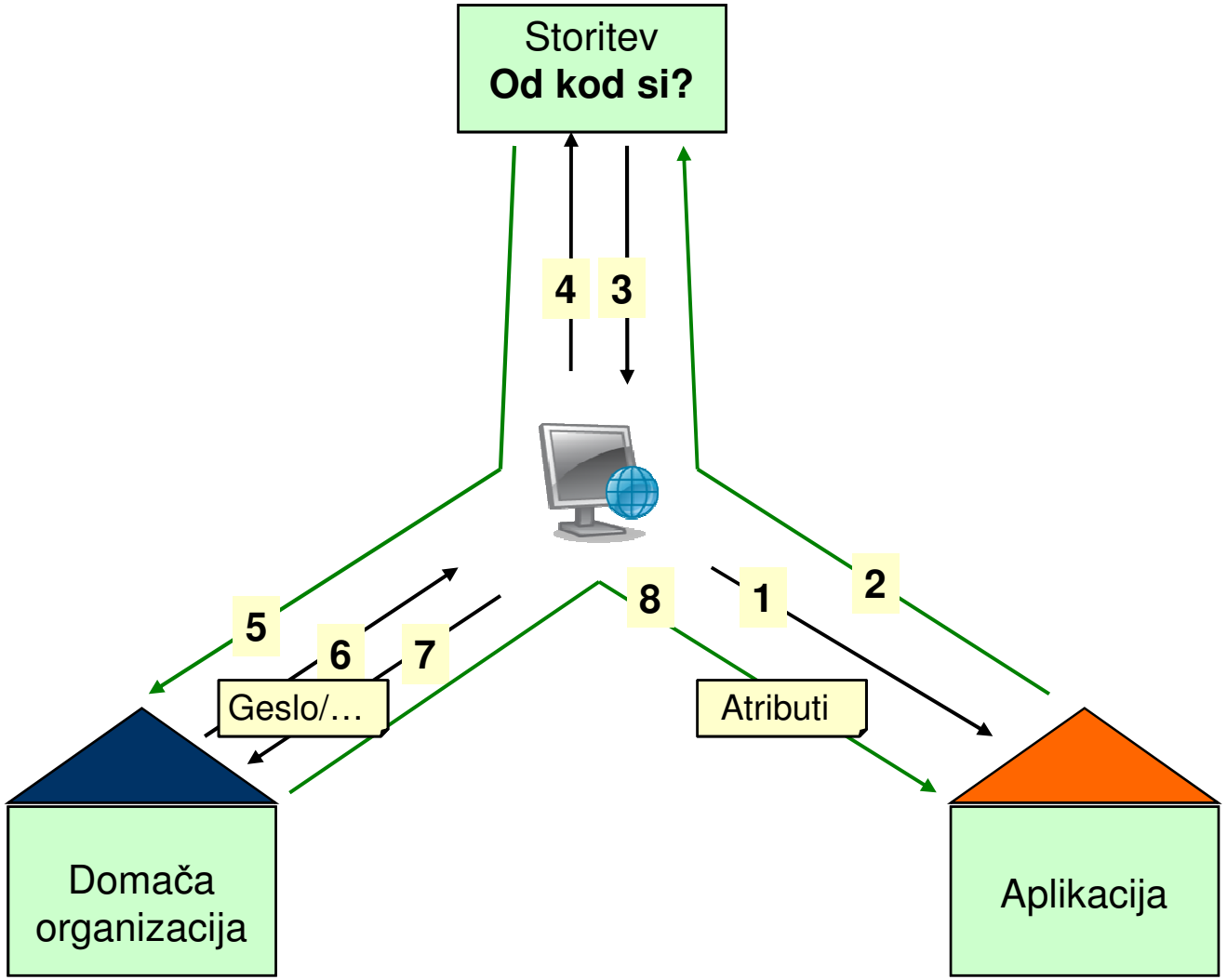
Akademska in raziskovalna mreža Slovenije

Mobilnost: WLAN

Akademska in raziskovalna mreža Slovenije

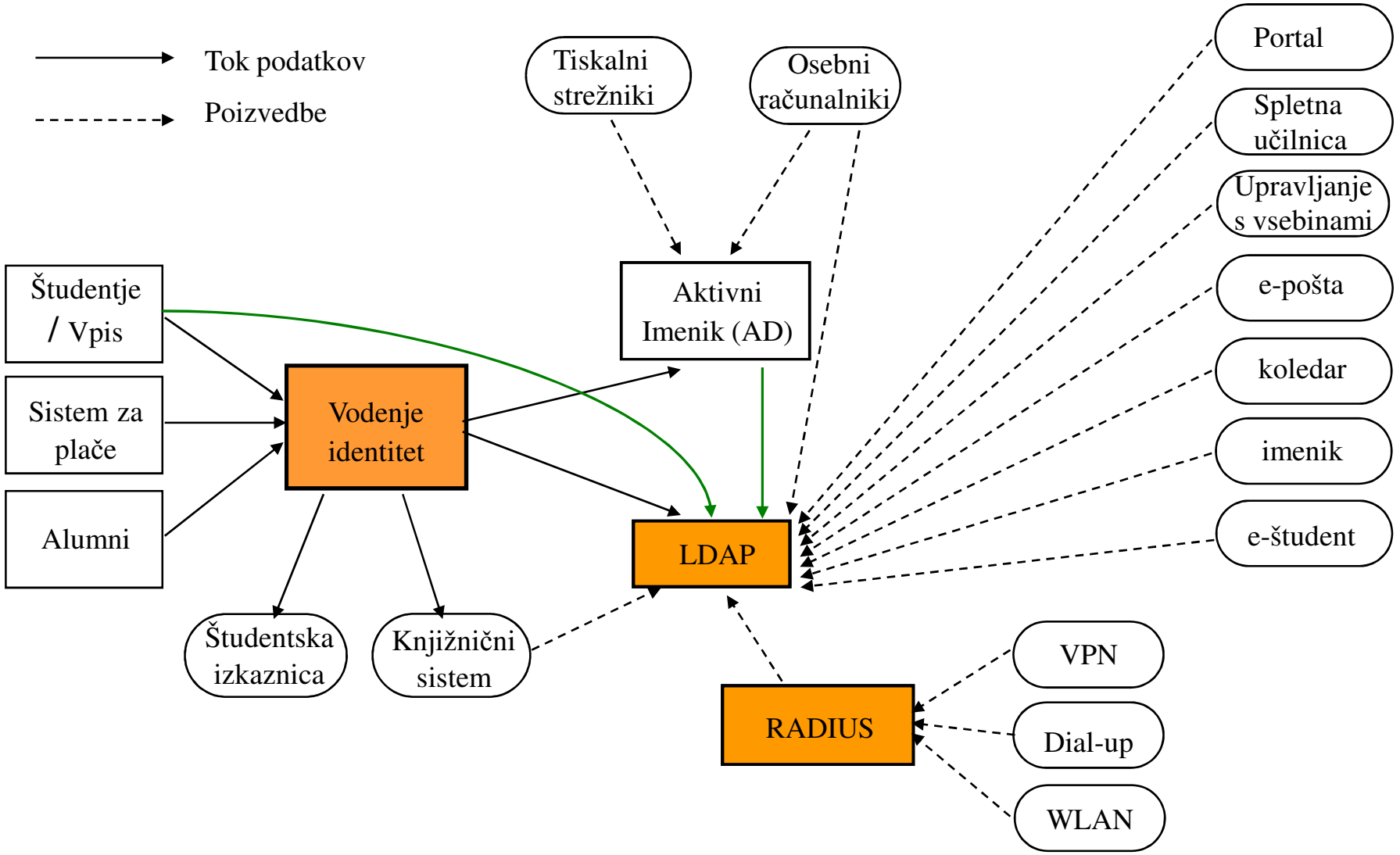
- Varno preverjanje istovetnosti
- Strežniki Radius
- Odjemalec 802.1x
- EAP-TTLS + PAP




Storitev
Od kod si?
4
3
5
6
7
8
1
2
Geslo/…
Atributi
Domača organizacija
Aplikacija

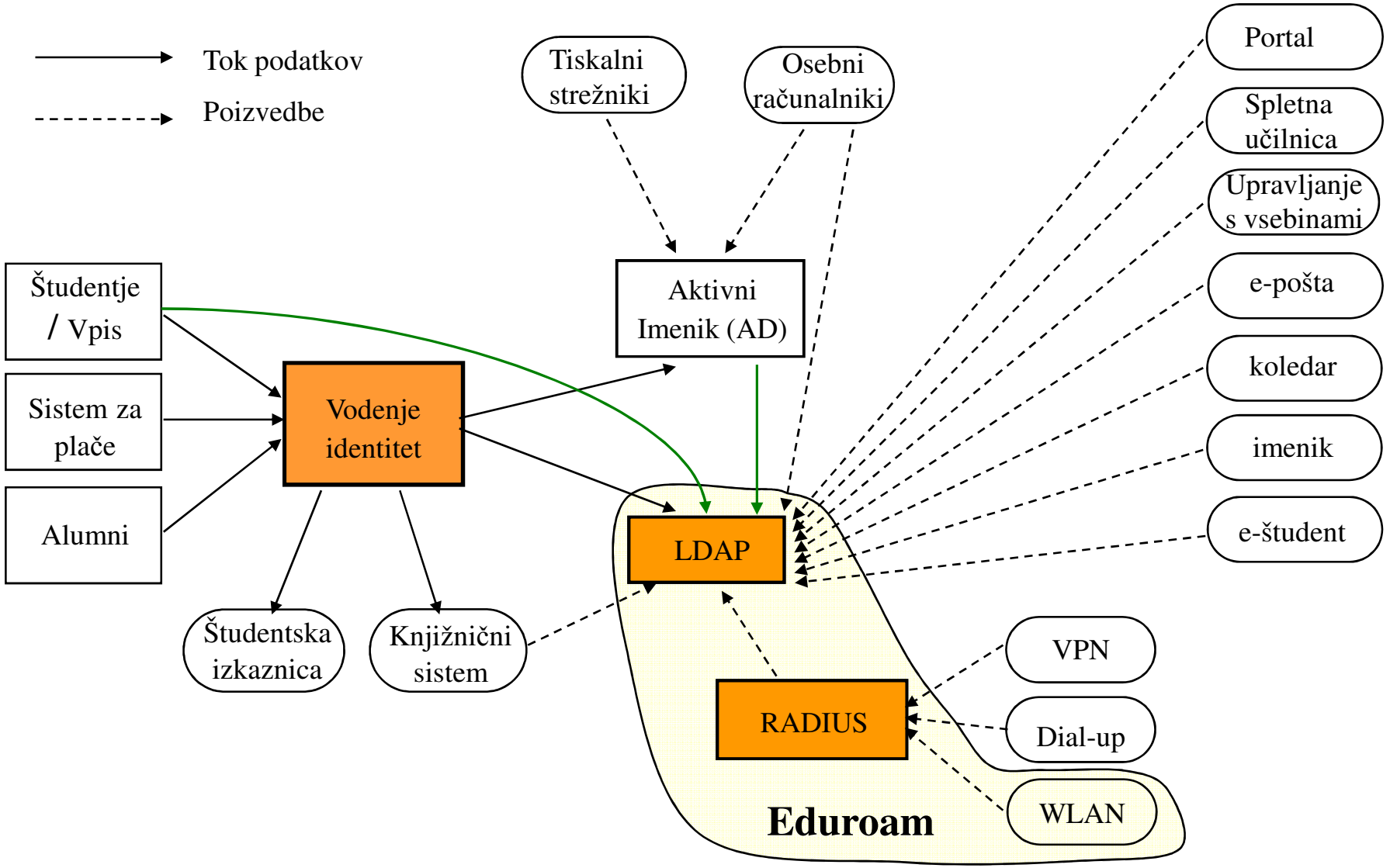
Kako iz obstoječega stanja do spletnega AAI?

Akademska in raziskovalna mreža Slovenije



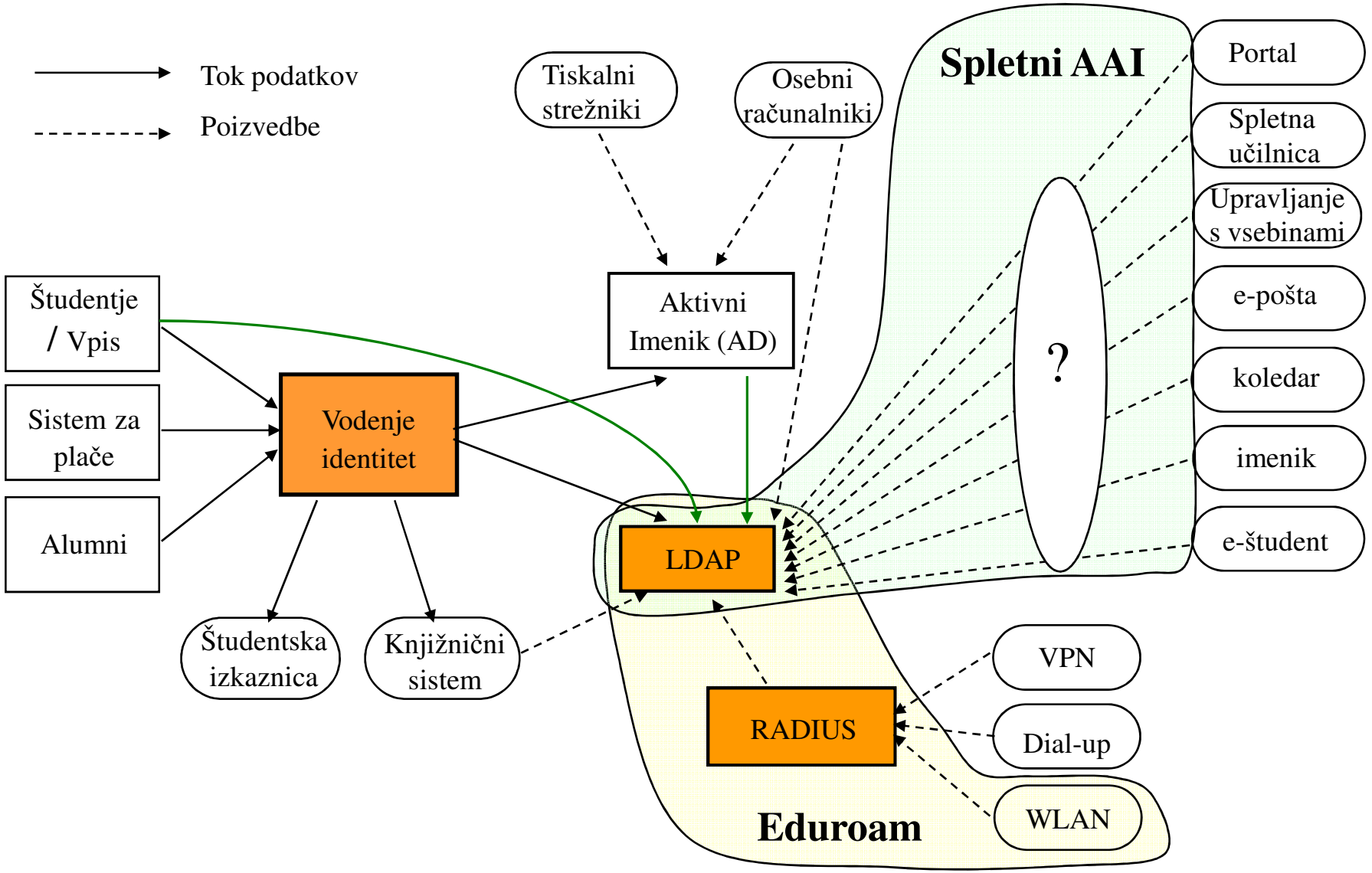
Kako iz obstoječega stanja do spletnega AAI 2?

Akademska in raziskovalna mreža Slovenije



Kako iz obstoječega stanja do spletnega AAI 3?

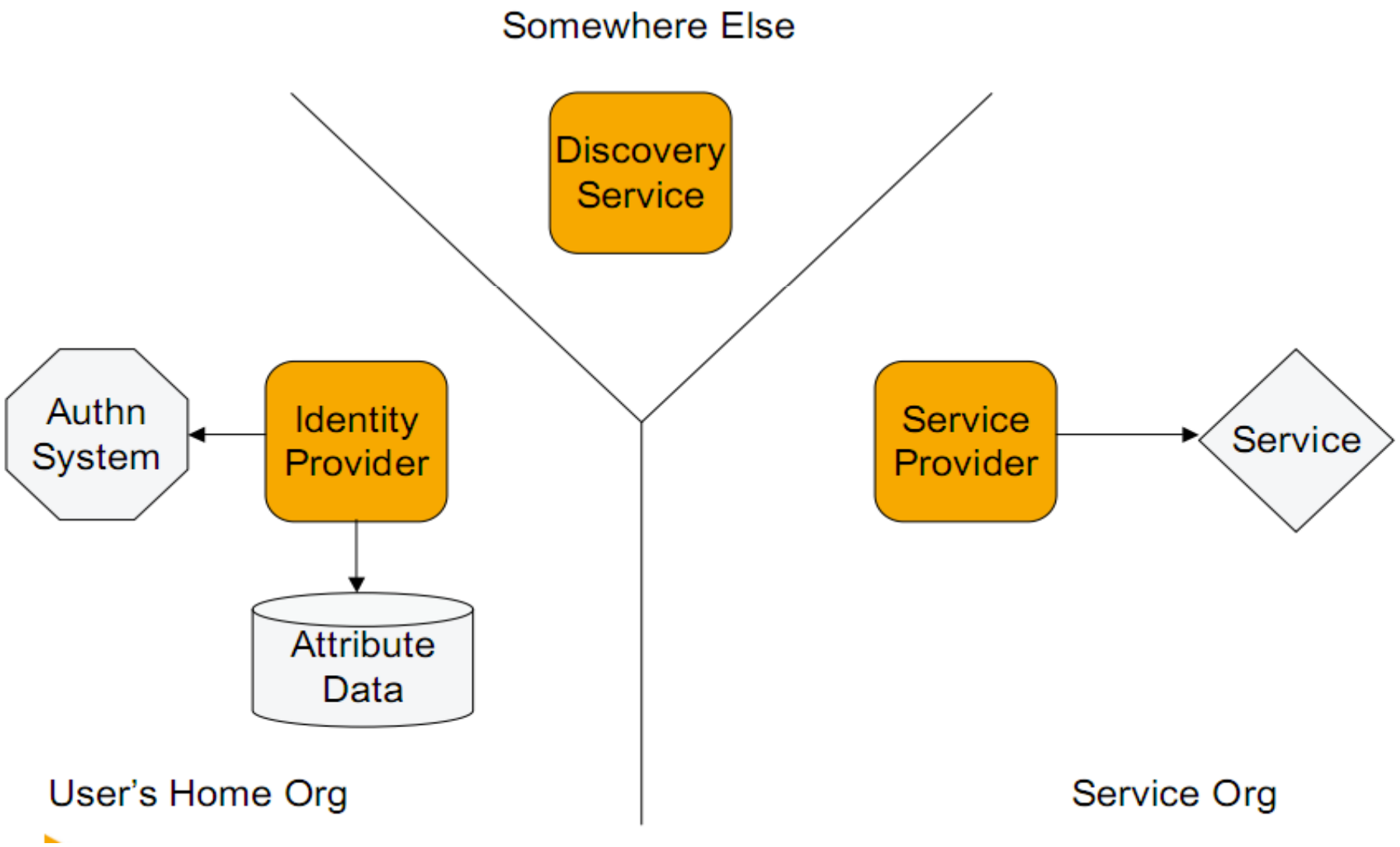
Akademska in raziskovalna mreža Slovenije



Osnovni pojmi

- Ponudnik Identitete (angl. Identity Provider – IdP)
  - Prijavni zaslon
- Ponudnik Storitev (angl. Service Provider – SP)
  - Aplikacije
- Iskalnik domače organizacija
  - angl. Discovery Service – DS (WAYF)
- Metapodatki
  - Registrirani IdP-ji in SP-ji (lokacija, certifikati SSL)

Osnovni pojmi 2



- „Klub“
  - Več organizacij
  - Vzpostavitev zaupanja
  - Tehnična povezava
  - Pravno-formalna povezava
- Metapodatki
  - Registrirani IdP-ji in SP-ji (lokacija, certifikati SSL)

Storitve pridružene ArnesAAI

Akademska in raziskovalna mreža Slovenije

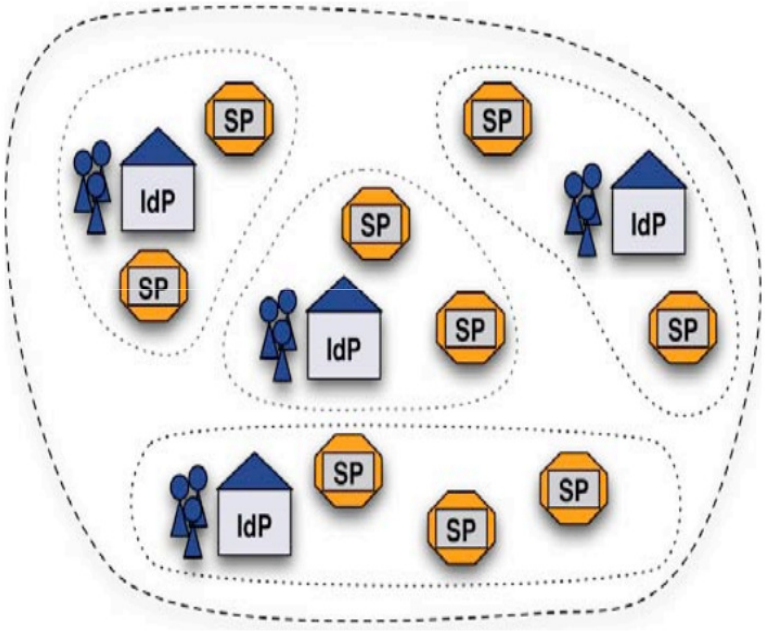
- Delujoče
  - Foodle - „pomoč pri določanju prostega termina“
  - ArnesAAI servisne strani
- V pilotni fazi
  - Adobe Connect Pro – Spletne video-konference
  - Arnes Moodle – spletne učilnice
  - Arnes Joomla – spletni sistem za urejanje vsebin
  - Arnesov novi Webmail
  - Spletni portal SIO

Federacija AAI

Akademska in raziskovalna mreža Slovenije

AAI – angl.

- Authentication
- Authorization
- Infrastructure



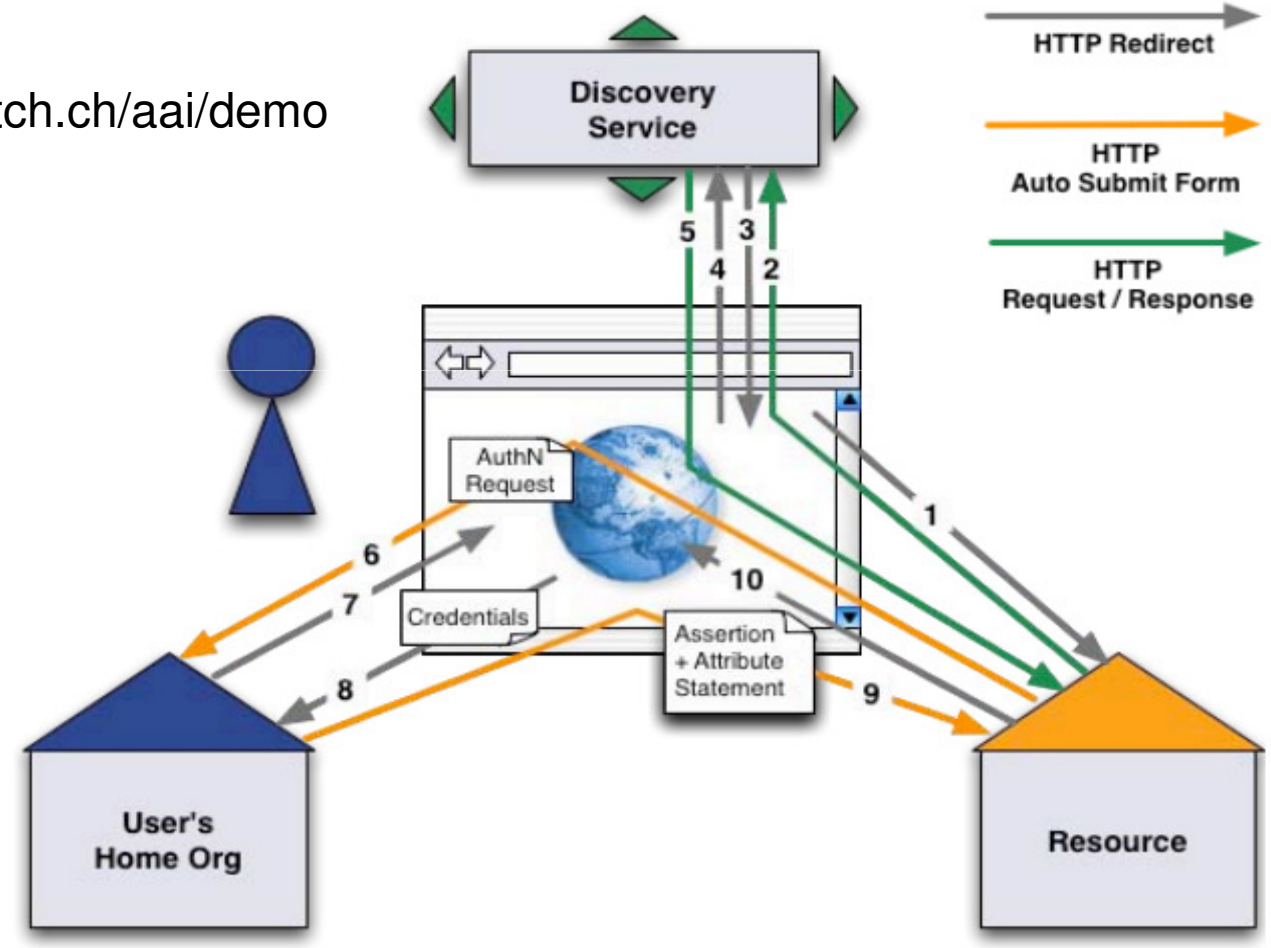
Common trust

- Legal
- Technical

Prikaz delovanja

Akademska in raziskovalna mreža Slovenije

http://www.switch.ch/aai/demo



Tehnični demo!

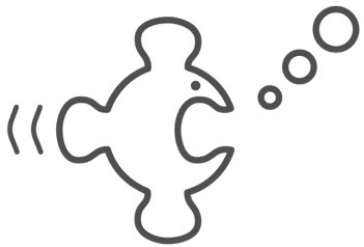
(uporaba AAI z podrobno razlago korakov)

Tehnologija SAML

- angl. Security Assertion Markup Language
  - XML
  - Šifrirane potrditve (angl. assertions)
  - Šifrirani podatki o uporabniku (angl. attributes)
  - Pošiljanje IdP -> SP
- Različica SAML 2.0
  - OASIS Standard: Marec 2005

Raznovrstna programska oprema

- Shibboleth IdP, SP
  - http://shibboleth.internet2.edu/
  - Starejši
  - Zelo nastavljiv
- SimpleSAMLphp IdP, SP
  - http://rnd.feide.no/simplesamlphp
  - Novejši
  - Zelo enostaven za uporabo



Postopek pridružitve v ArnesAAI za IdP

Akademska in raziskovalna mreža Slovenije

- Prijava namere na aaa-podpora@arnes.si
- Vzpostavitev strežnika IdP
- Pridružitev testni federaciji Arnes
- Testiranje delovanja
- Podpis pridružitvenega sporazuma
- Pridobitev testnega in servisnega uporabniškega imena
- Vpis IdP v federacijo ArnesAAI (servisne strani)

Postopek pridružitve v ArnesAAI za SP

Akademska in raziskovalna mreža Slovenije

- Prijava namere na aaa-podpora@arnes.si
- Vzpostavitev strežnika SP
- (Ni obvezno) Pridružitev testni federaciji Arnes
- (Ni obvezno) Testiranje delovanja
- Podpis pogojev uporabe za ponudnike storitev
- Pridobitev testnega in servisnega uporabniškega imena
- Vpis SP v federacijo ArnesAAI (servisne strani)

Osebni podatki

- Ločimo dva tipa podatkov
  - Uporabnik jih sam vnese
    - Aktivni e-poštni naslov
    - Naslov pošiljanja obvestil
    - Kontaktna telefonska številka
  - So vneseni na podlagi uradih podatkov
    - Davčna številka
    - Ime in priimek
    - Uradni naslov
    - Starost (datum rojstva)

Točnost podatkov o uporabnikih

- Občasno uporabljena aplikacija
  - Podatki niso točni
- Baza zaposlenih
- Baza vpisanih študentov
- Upravljanje z identitetami: IdM – Identity Management
- Največja točnost:
  - Podatke vzdržujeta skupaj organizacija in uporabnik

Upravljanje z osebnimi podatki

- Vpogled le tistih podatkov, ki se nujno potrebujejo
- Zakon o varstvu osebnih podatkov
- Vodeni osebni podatki na vpogled osebi
- Vedno potrditev uporabnika (angl. User consent) predno se katerikoli podatki posredujejo
- Standardizirano v imeniku LDAP
  - Manjši stroški
  - Združljivost

Podatki v imeniku LDAP

- Uporabljamo shemi SCHAC in eduPerson
  - Isti imenik LDAP za Eduroam.si in ArnesAAI
  - Podatki: cn, sn, userPassword, postalAddress, postalCode, registeredAddress, displayName, givenName, mail, eduPersonAffiliation, eduPersonPrimaryAffiliation, eduPersonPrincipalName, schacGender, schacDateOfBirth, schacPlaceOfBirth, schacCountryOfCitizenship, schacSn1, schacSn2, schacPersonalTitle, schacHomeOrganization, schacHomeOrganizationType, schacPersonalUniqueCode, schacPersonalUniqueID, schacUUID, schacExpiryDate.
- Razvoj: standardizacija novih atributov

Vprašanje publiki

- Kje so pri vas shranjeni osebni podatki?
  - LDAP, SQL, ActiveDirectory, Posebna aplikacija?
- Katere podatke vodite?
- Kako izdelujete in odstranjujete uporabniška imena?
- Kako vam lahko pomagamo?

AAI – kontaktni podatki

Akademska in raziskovalna mreža Slovenije

- http://aai.arnes.si
- http://www.eduroam.si
- e-mail: aaa-podpora@arnes.si
- Ekipa
  - Avgust Jauk
  - Alex Mihičinac
  - Rok Papež
  - Peter Sterle