

Srečanje članic federacije 2014

8. december 2014, Ljubljana

Lažje do eduroam certifikatov

Marko Dolničar

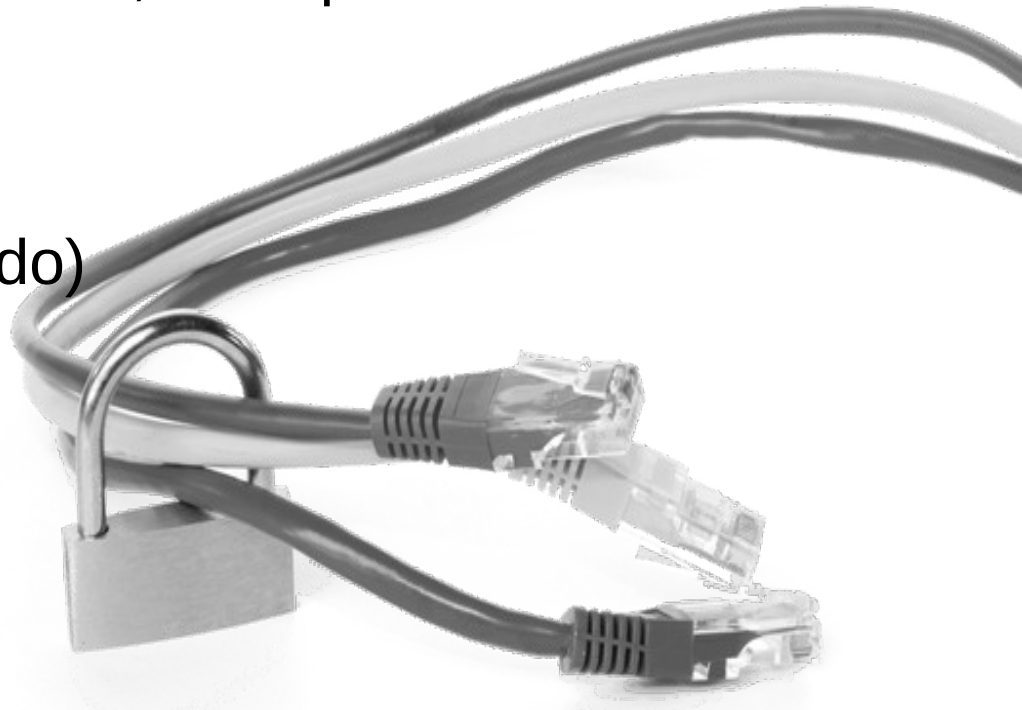
Arnes

aaa-podpora@arnes.si

<https://aai.arnes.si>

X.509 certifikati

- Digitalni dokumenti
- Vsebujejo:
 - Ime lastnika (e-mail, domena, ime spletne strani, ...)
 - Omejitve za uporabo
 - Datum veljavnosti (od – do)
 - Podpis
 - ...
- Javni / privatni ključ



Certificate:

Data:

Version: 3 (0x2)

Serial Number: 9028159383540021 (0x20131029081135)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=SI, O=ARNES, OU=AAI, CN=Arnes CA za streznike Eduroam/emailAddress=aaa-podpora@arnes.si

Validity

Not Before: Nov 5 14:38:25 2013 GMT

Not After : Nov 5 14:38:25 2015 GMT

Subject: C=SI, L=Ljubljana, O=ARNES, CN=orle.arnes.si

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (4096 bit)

Modulus:

00:dc:cb:5d:81:88:b0:e1:0a:fe:19:06:4e:72:ee:

...

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 CRL Distribution Points:

Full Name:

URI:http://www.eduroam.si/eduroam.crl

X509v3 Extended Key Usage:

TLS Web Server Authentication

X509v3 Subject Alternative Name:

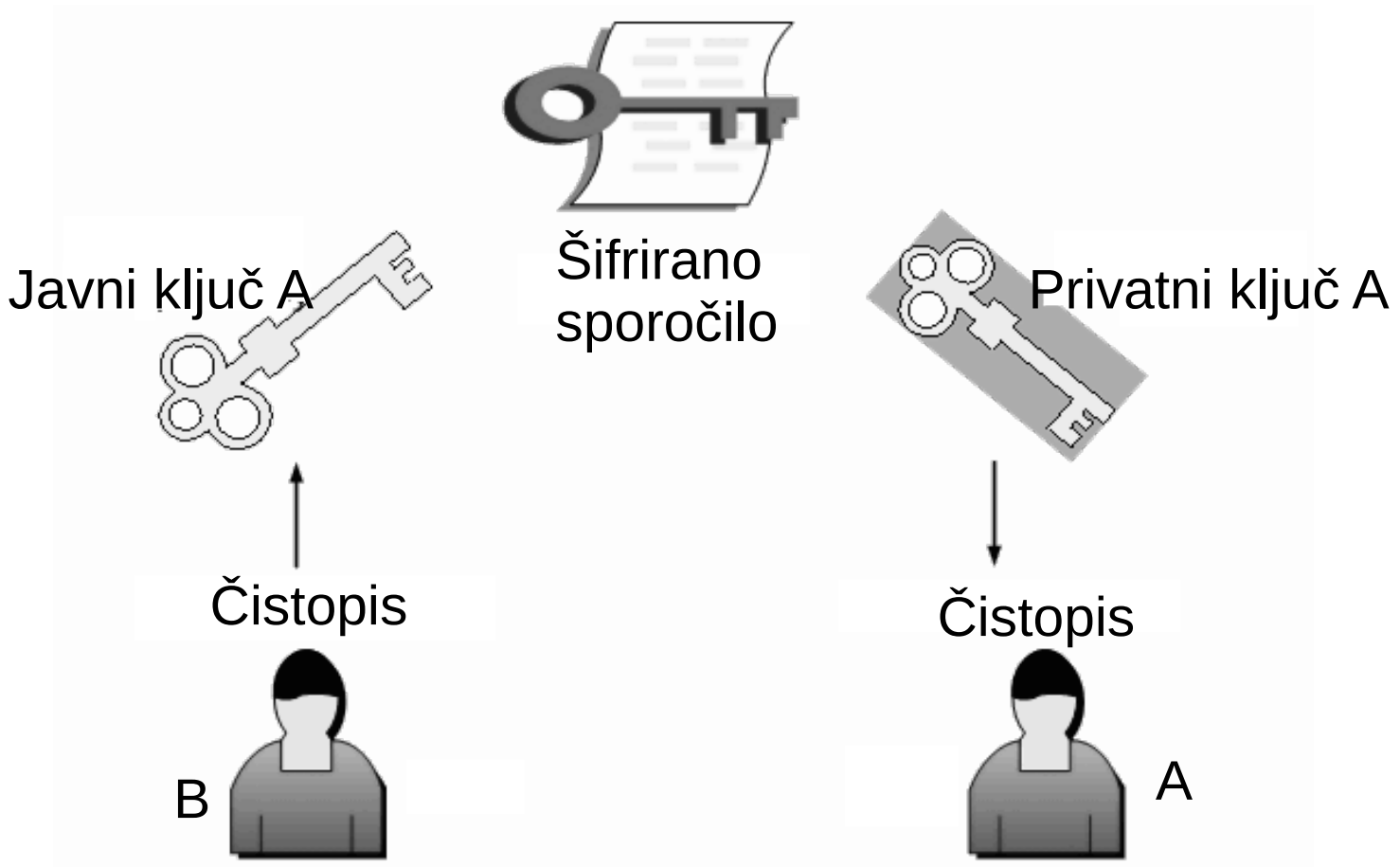
IP Address:193.2.18.130, DNS:orle.arnes.si

Signature Algorithm: sha1WithRSAEncryption

3b:91:cb:b8:bb:f8:b7:73:73:2f:c6:70:28:31:9f:da:21:36:

...

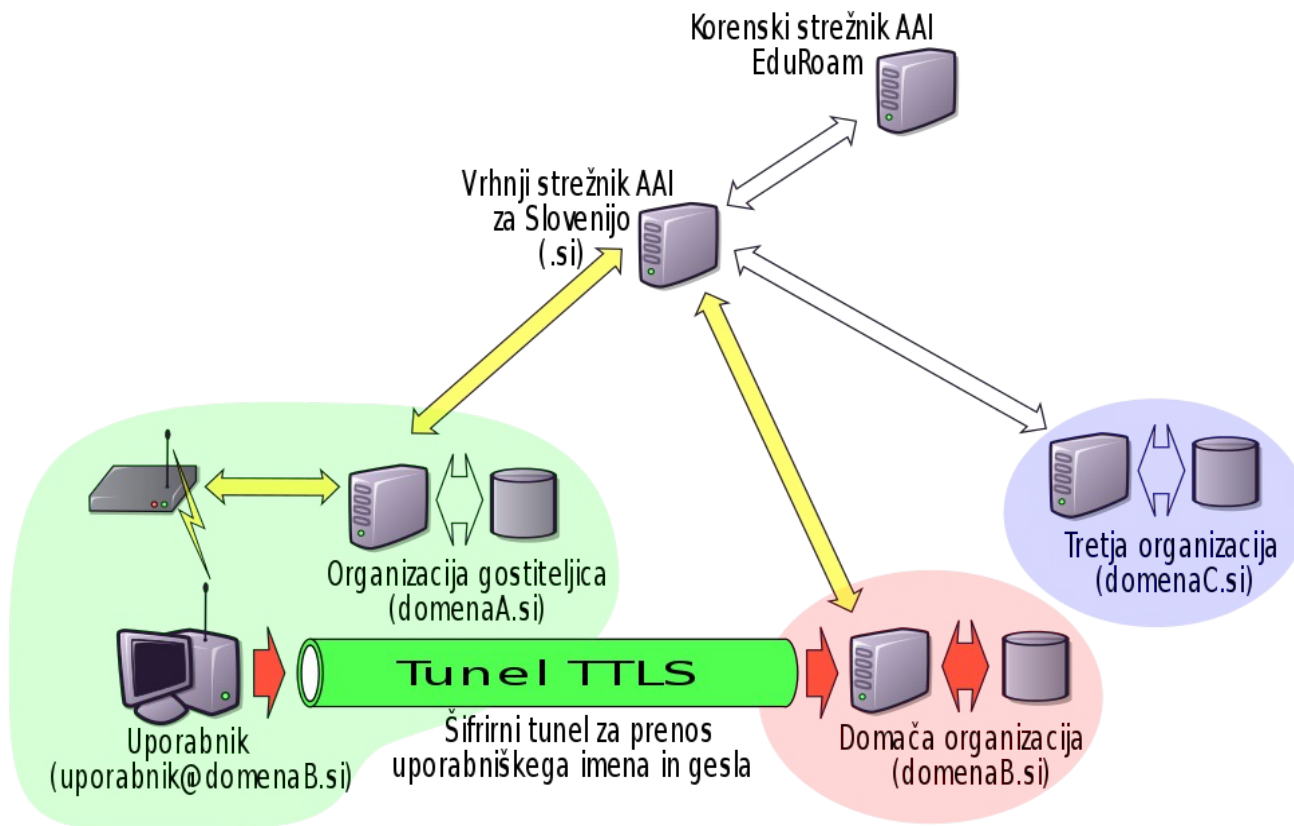
Kako se uporabljajo?



Vloga certifikatne agencije (CA)

- Preveri certifikatni zahtevek
- Podpiše certifikat
- Podpis postane del certifikata (Issuer)
- Naprava / program preveri certifikat tako, da primerja podpis certifikata z nameščenim CA certifikatom
- Zaupanje...

Uporaba certifikatov v eduroamu



Varen prenos gesla do strežnika na domači organizaciji

Upravljanje s certifikati (https://aai.arnes.si)

1. Prijava v https://aai.arnes.si

arnes AAI Organizacija ▾ Skrbnik ▾ Uporabnik ▾ Prijava

AAI prijava

Izberite domačo organizacijo

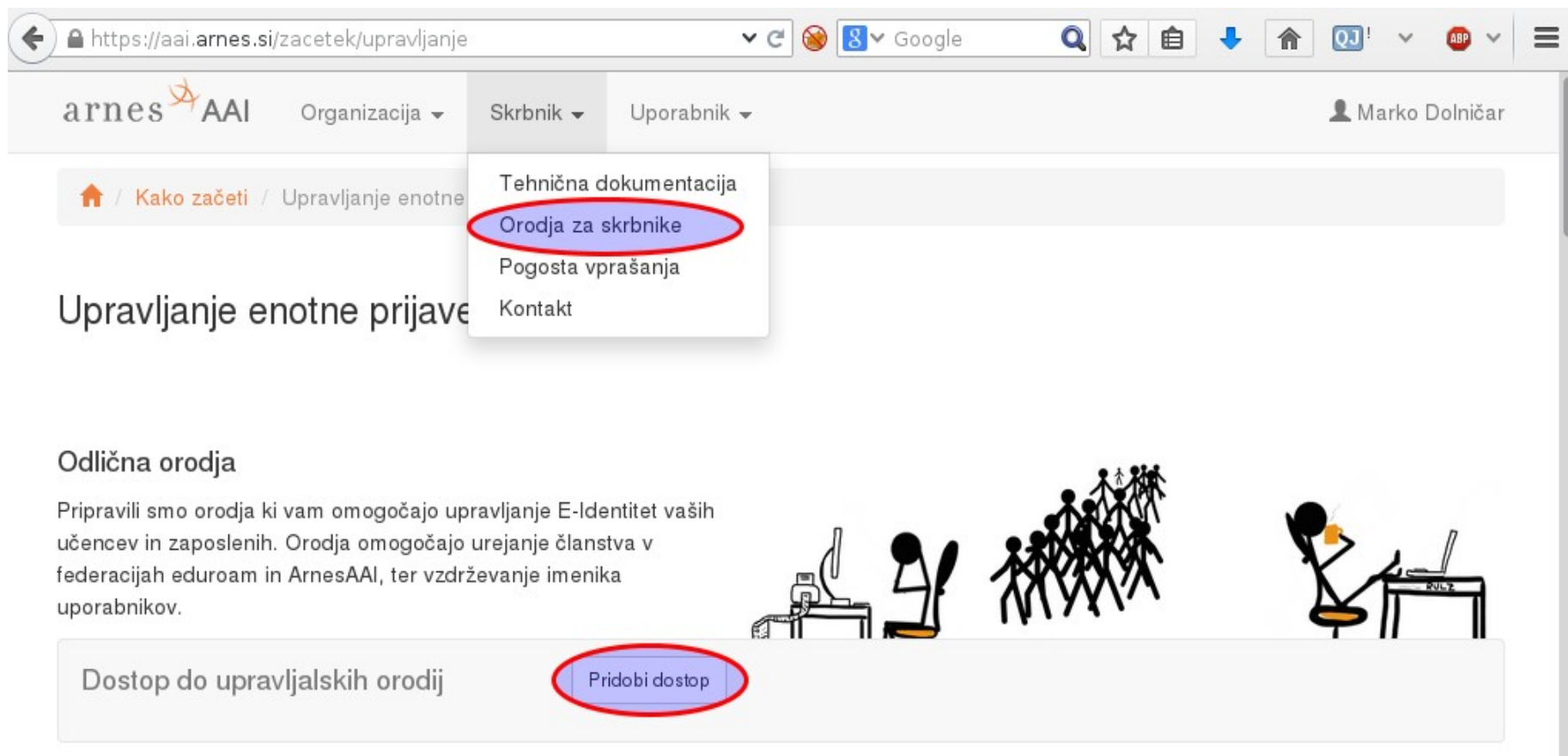
Izberi domačo organizacijo

Ne spreglejte! Srečanje člani
8. december 2014 ob 9:00

Upravljanje s certifikati

(<https://aai.arnes.si>)

2. Dostop do upravljanja



The screenshot shows a web browser window with the URL <https://aai.arnes.si/zacetek/upravljanje>. The page header includes the 'arnes AAI' logo and navigation menus for 'Organizacija', 'Skrbnik', and 'Uporabnik'. The user 'Marko Dolničar' is logged in. A dropdown menu under 'Skrbnik' is open, with 'Orodja za skrbnike' highlighted in blue. Below the header, the breadcrumb trail is 'Kako začeti / Upravljanje enotne prijave'. The main heading is 'Upravljanje enotne prijave'. The section 'Odlična orodja' contains text about E-Identit management tools and an illustration of people working. At the bottom, a button 'Pridobi dostop' is highlighted in blue.

arnes AAI Organizacija ▾ Skrbnik ▾ Uporabnik ▾ Marko Dolničar

🏠 / Kako začeti / Upravljanje enotne prijave

Tehnična dokumentacija
Orodja za skrbnike
Pogosta vprašanja
Kontakt

Upravljanje enotne prijave

Odlična orodja

Pripravili smo orodja ki vam omogočajo upravljanje E-Identitet vaših učencev in zaposlenih. Orodja omogočajo urejanje članstva v federacijah eduroam in ArnesAAI, ter vzdrževanje imenika uporabnikov.

Dostop do upravljaljskih orodij **Pridobi dostop**

Upravljanje s certifikati

(<https://aai.arnes.si>)

3. Dostop do upravljanja (nadaljevanje)

← <https://aai.arnes.si/upravljanje/zahtevek> Google

arnes AAI Organizacija ▾ Skrbnik ▾ Uporabnik ▾ Marko Dolničar

Ime organizacije

Storitev

Izberite storitev, do katere želite pridobiti dostop

Sporočilo

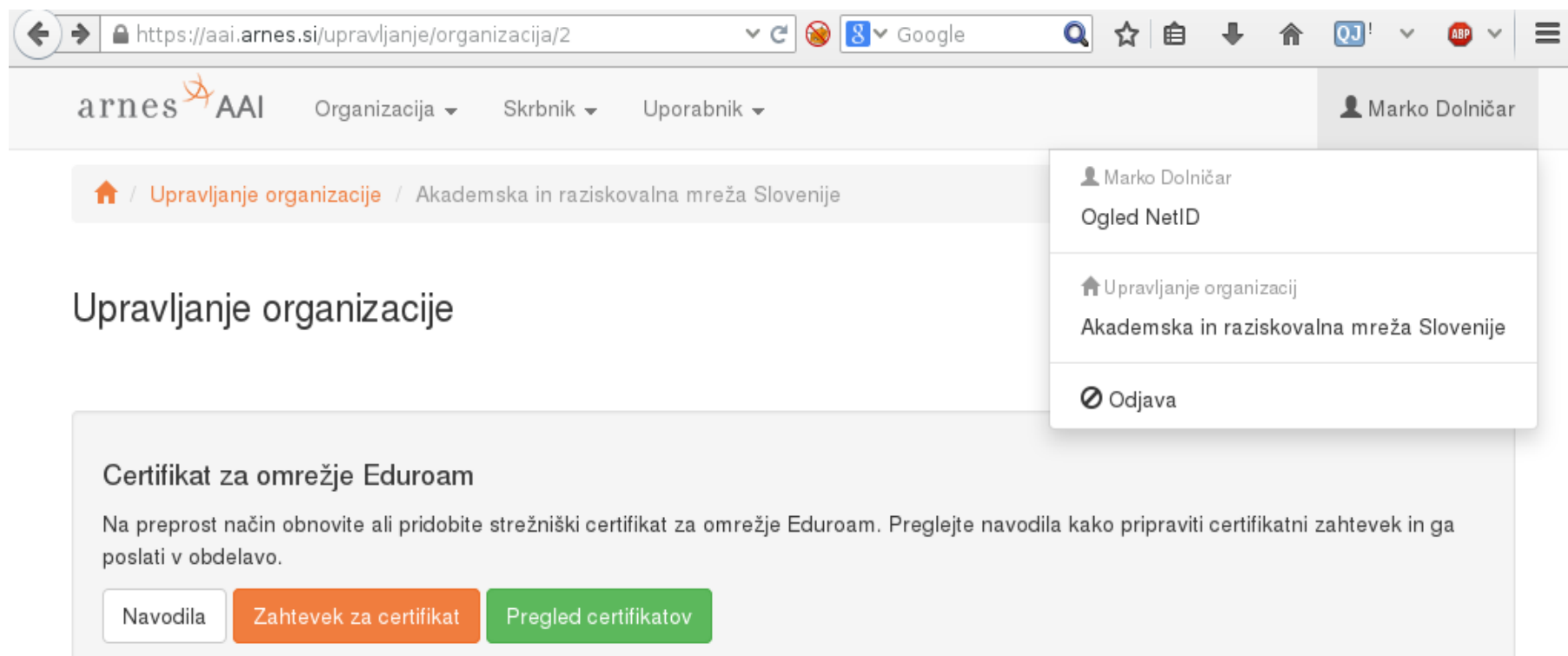
Pozdravljeni!
Prosim za dostop do upravljanja z eduroam certifikati.
Hvala, Marko!

Vnesite sporočilo, ki bo poslano Arnesovim skrbnikom storitve

Oddaj zahtevek

Upravljanje s certifikati (https://aai.arnes.si)

4. Priprava certifikatnega zahtevka



The screenshot shows a web browser window with the URL <https://aai.arnes.si/upravljanje/organizacija/2>. The page header includes the AAI logo and navigation links for 'Organizacija', 'Skrbnik', and 'Uporabnik'. The user 'Marko Dolničar' is logged in, and a dropdown menu is open, showing options: 'Marko Dolničar', 'Ogled NetID', 'Upravljanje organizacij', 'Akademsko in raziskovalna mreža Slovenije', and 'Odjava'. The main content area is titled 'Upravljanje organizacije' and features a section for 'Certifikat za omrežje Eduroam'. Below this section, there are three buttons: 'Navodila', 'Zahtevak za certifikat', and 'Pregled certifikatov'.

arnes AAI Organizacija ▾ Skrbnik ▾ Uporabnik ▾ Marko Dolničar

🏠 / Upravljanje organizacije / Akademsko in raziskovalna mreža Slovenije

Upravljanje organizacije

Certifikat za omrežje Eduroam

Na preprost način obnovite ali pridobite strežniški certifikat za omrežje Eduroam. Preglejte navodila kako pripraviti certifikatni zahtevak in ga poslati v obdelavo.

Navodila Zahtevak za certifikat Pregled certifikatov

Upravljanje s certifikati

(<https://aai.arnes.si>)

5. Priprava certifikatnega zahtevka (nadaljevanje)

```
countryName_default          = SI
localityName_default        = Ljubljana
organizationName_default    = Nasa Organizacija
commonName_default          = radius.organizacija.si

#OPCIJSKO
#organizationalUnitName_default = enota Kraljevi Pitoni Kranj

#####
### Obvezen je DNS.1, ki mora biti hkrati isti kot commonName_default(zgoraj)
### Tudi IP.1 je obvezen
### Odvečne IP / DNS zakomentirajte z "#"
#####

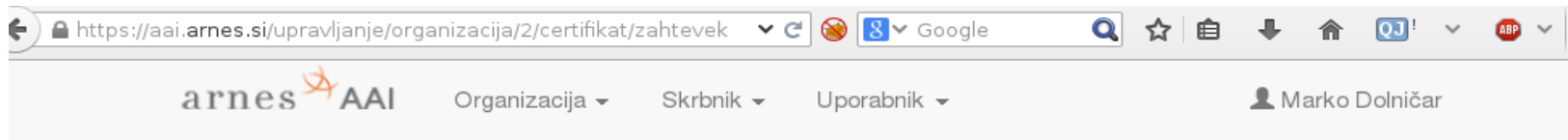
[alt_names]
DNS.1   = radius.organizacija.si
DNS.2   = eduroam.organizacija.si
#DNS.3  = streznikX.organizacija.si
IP.1    = 193.333.111.666
IP.2    = 2001:dead:beef:ZZZ::666
```

```
openssl req -batch -new -config eduroam-csr.cfg -out radius.organizacija.csr
```

Upravljanje s certifikati

(<https://aai.arnes.si>)

6. Prenos certifikatnega zahtevka



[Home](#) / [Upravljanje organizacije](#) / [Akademska in raziskovalna mreža Slovenije](#) / [Nov certifikatni zahtevk](#)

Nov certifikatni zahtevk

i Prilepite certifikatni zahtevk za eduroam strežniški certifikat. [Navodila za izdelavo zahtevka.](#)

Certifikatni zahtevk

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIFXzCCA0cCAQAwwYoxCzAJBgNVBAYTAiNMRlEwEAYDVQQHEwlManVibGphbmEx  
JjAkBgNVBAoTHVZydGVJIEJsYXphIERpdmpha2EgTGp1YmxqYW5hMSQwlgYDVQQL  
Extlbm90YSBLcmFsamV2aSBQaXRvbmkgS3Jhbm9xGTAXBgNVBAMTEHJhZGl1cy5k  
-Y7-VM-...-MA0CCG-CCIBDQEFBAQIAA41GDU-...-K-1CAOD-...-E-F-1
```

Vnesite certifikatni zahtevk za eduroam strežniški certifikat

[Dodaj](#)

Upravljanje s certifikati

(<https://aai.arnes.si>)

7. Pregled certifikatov



Certifikati in certifikatni zahtevki

ID	Organizacija	Zahteval	CN	Veljavnost	Status	Akcija
●	Akademsko in raziskovalna mreža Slovenije	██████████	Streznik Eduroam - ArnesLab - lab.arnes.si	2014-09-18 13:30:36	Potečen	
●	Akademsko in raziskovalna mreža Slovenije	██████████	Streznik Eduroam - Arnes os-prva testlab	2014-10-20 09:18:09	Potečen	
●	Akademsko in raziskovalna mreža Slovenije	██████████	██████████	2015-10-29 08:12:31	Veljaven	
●	Akademsko in raziskovalna mreža Slovenije	██████████	██████████	2015-11-05 14:38:25	Veljaven	

Zahtevki za certifikat

Srečanje članic federacije 2014

8. december 2014, Ljubljana

Hvala!

Marko Dolničar

Arnes

aaa-podpora@arnes.si

<https://aai.arnes.si>