Srečanje članic federacije 2014

8. december 2014, Ljubljana

Lažje do eduroam certifikatov

Marko Dolničar

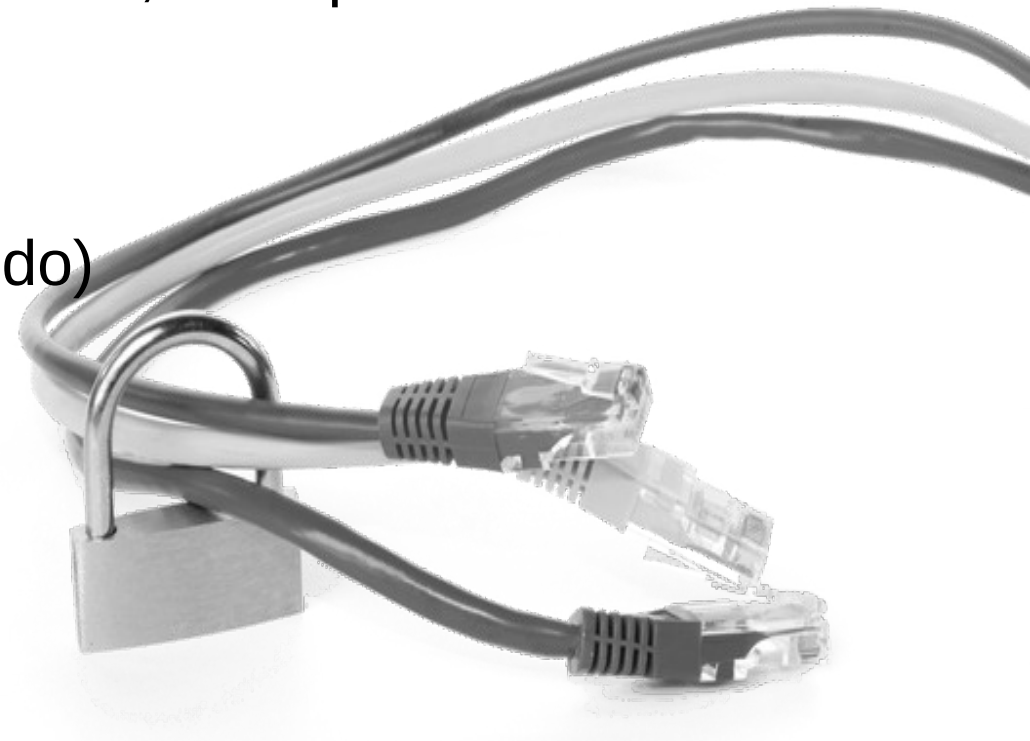
Arnes

aaa-podpora@arnes.si

https://aai.arnes.si

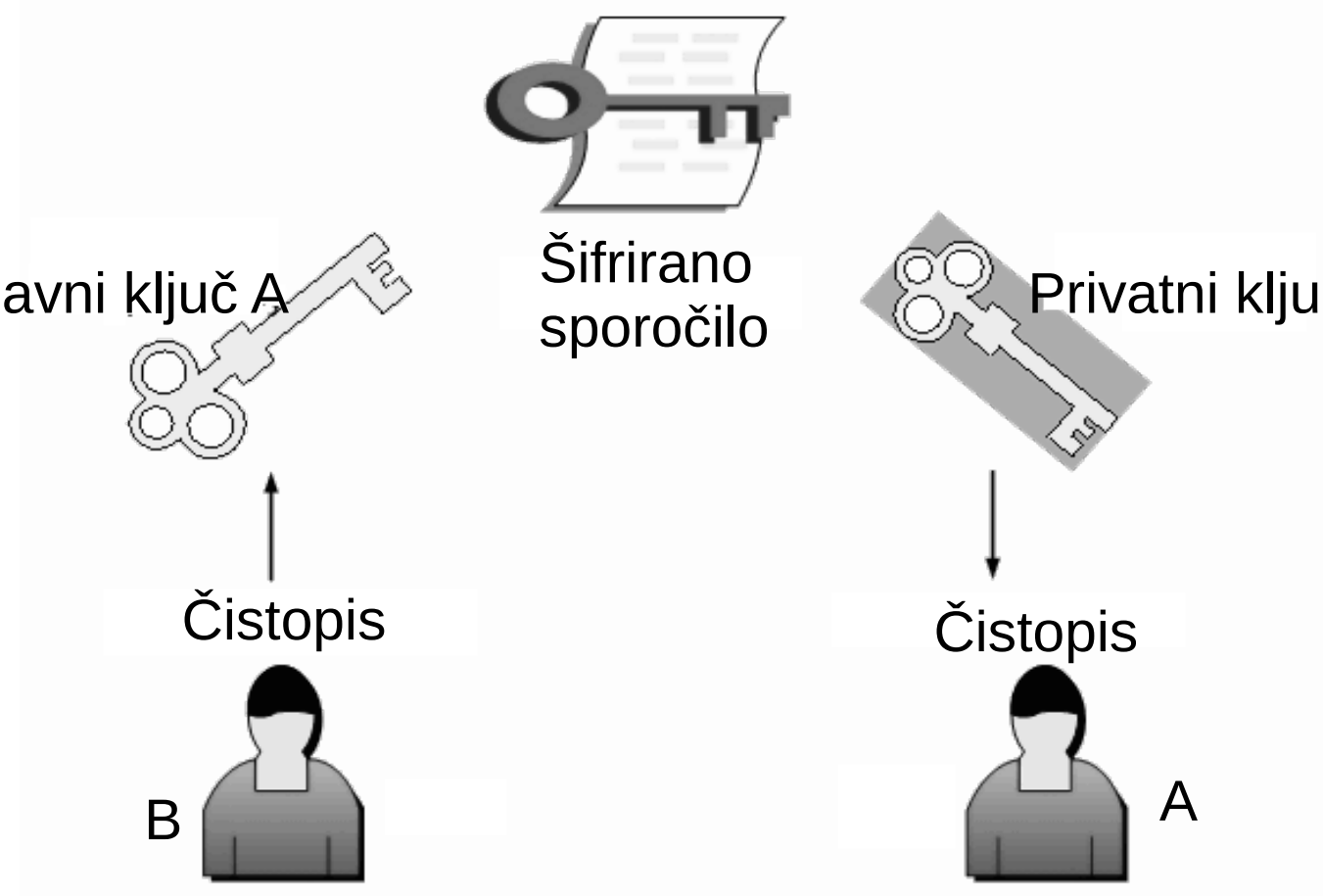
X.509 certifikati

- 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:
                ...
```

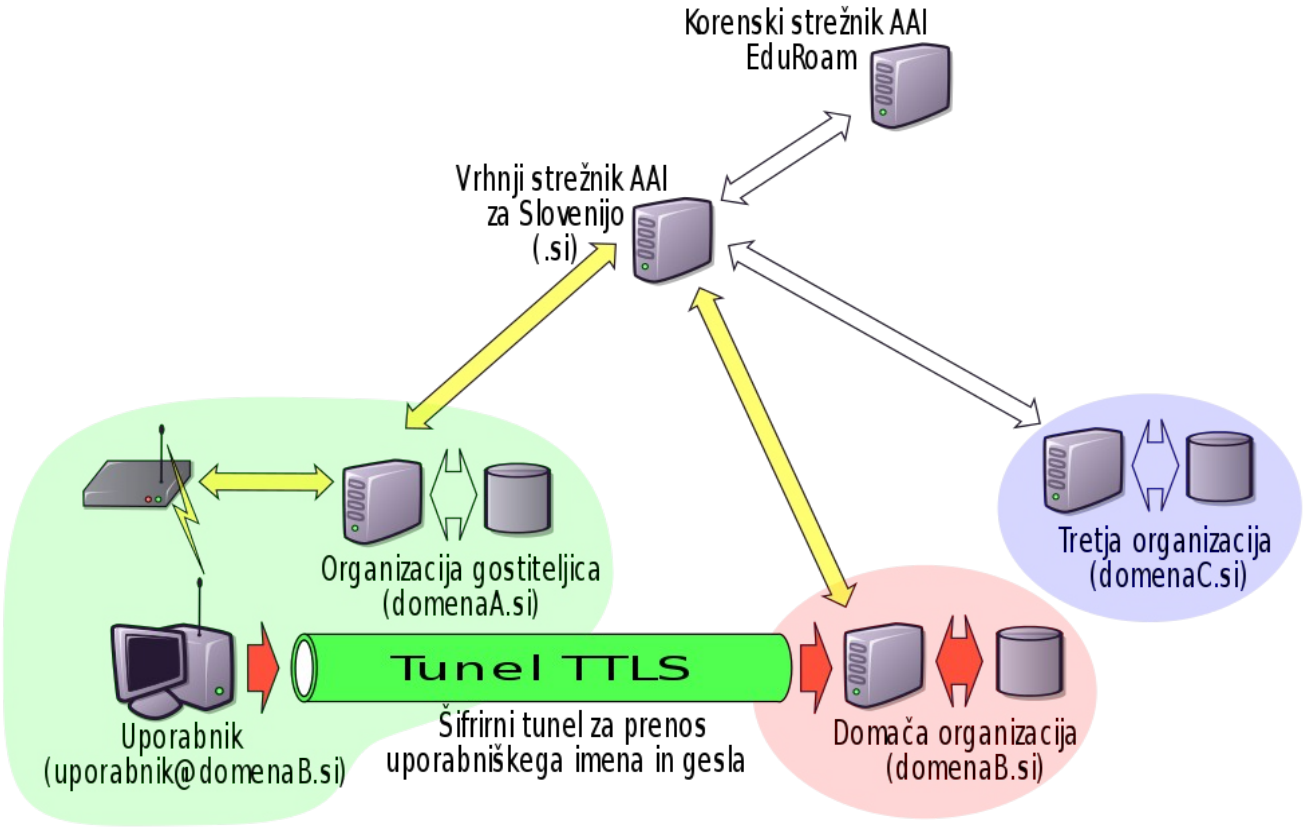
Kako se uporabljajo?



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...

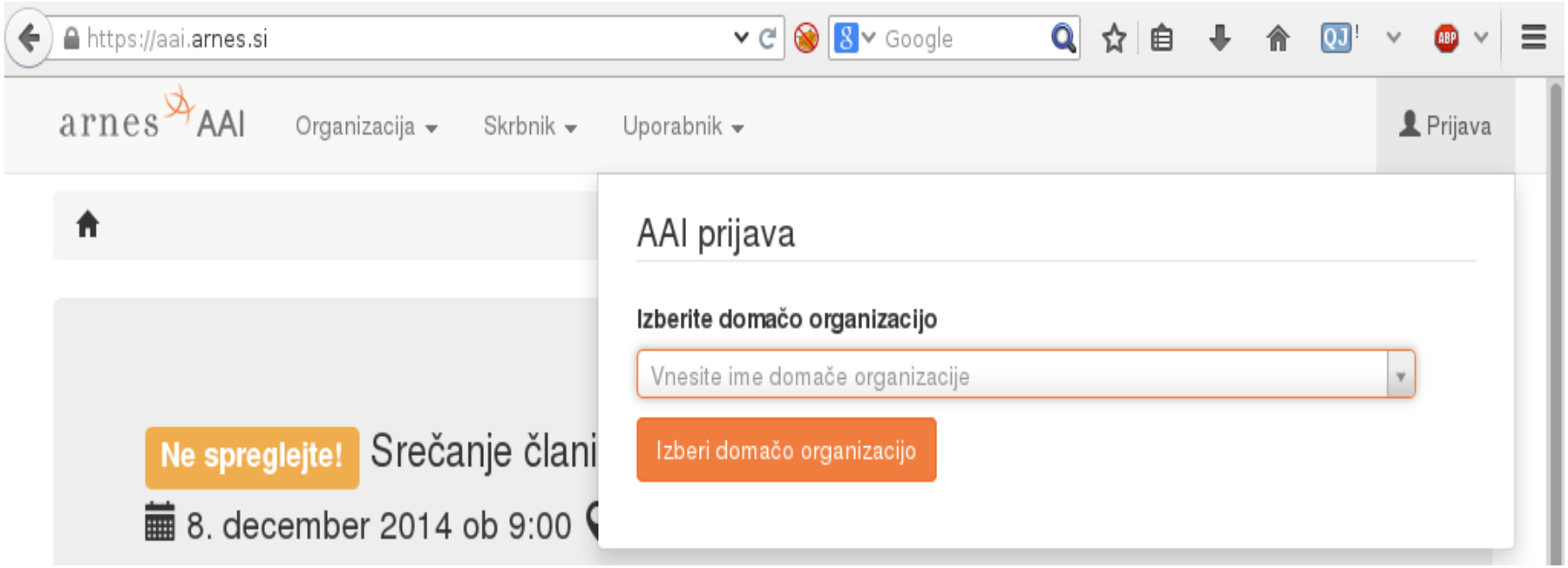
Uporaba certifikatov v eduroamu



Varen prenos gesla do strežnika na domači organizaciji

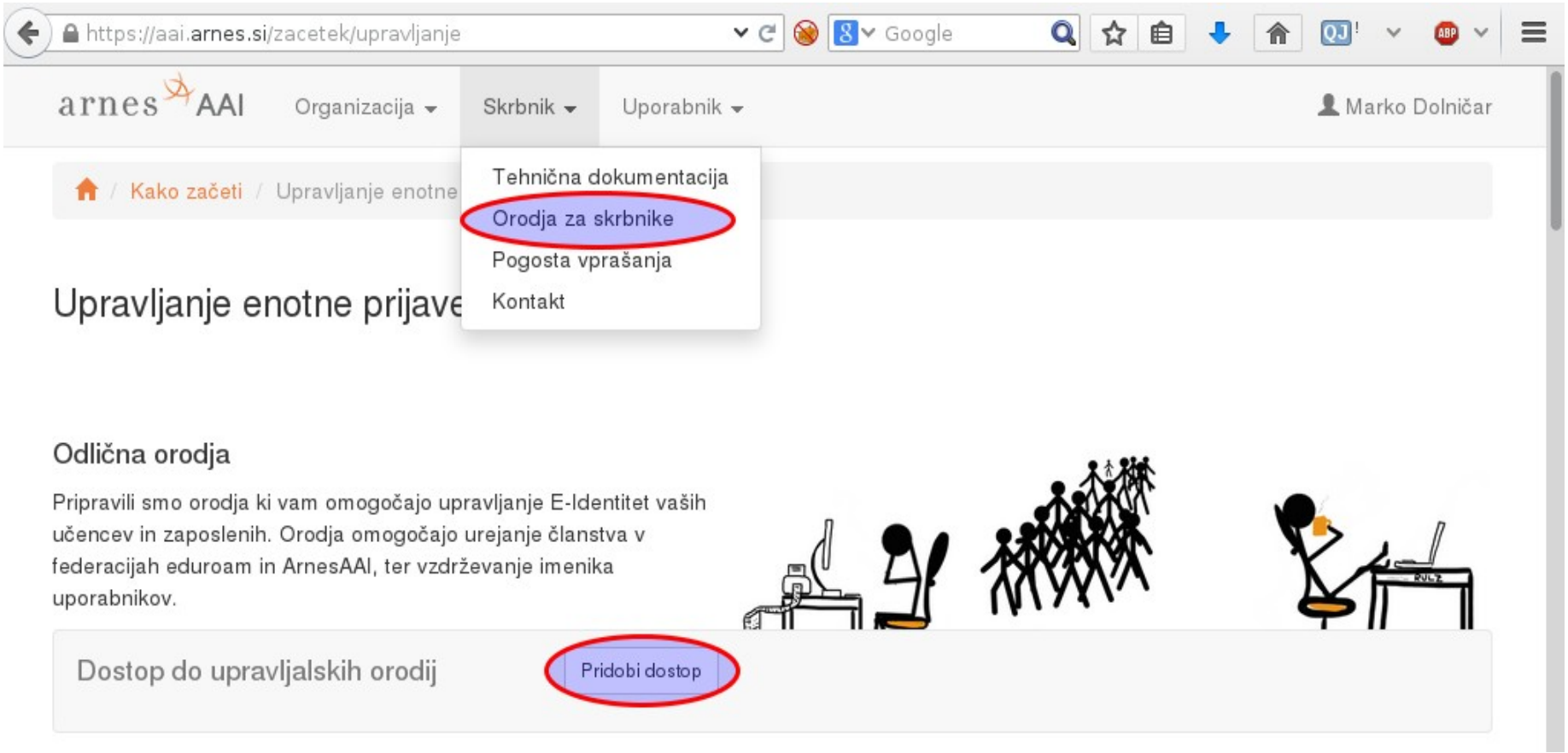
Upravljanje s certifikati
(https://aai.arnes.si)

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



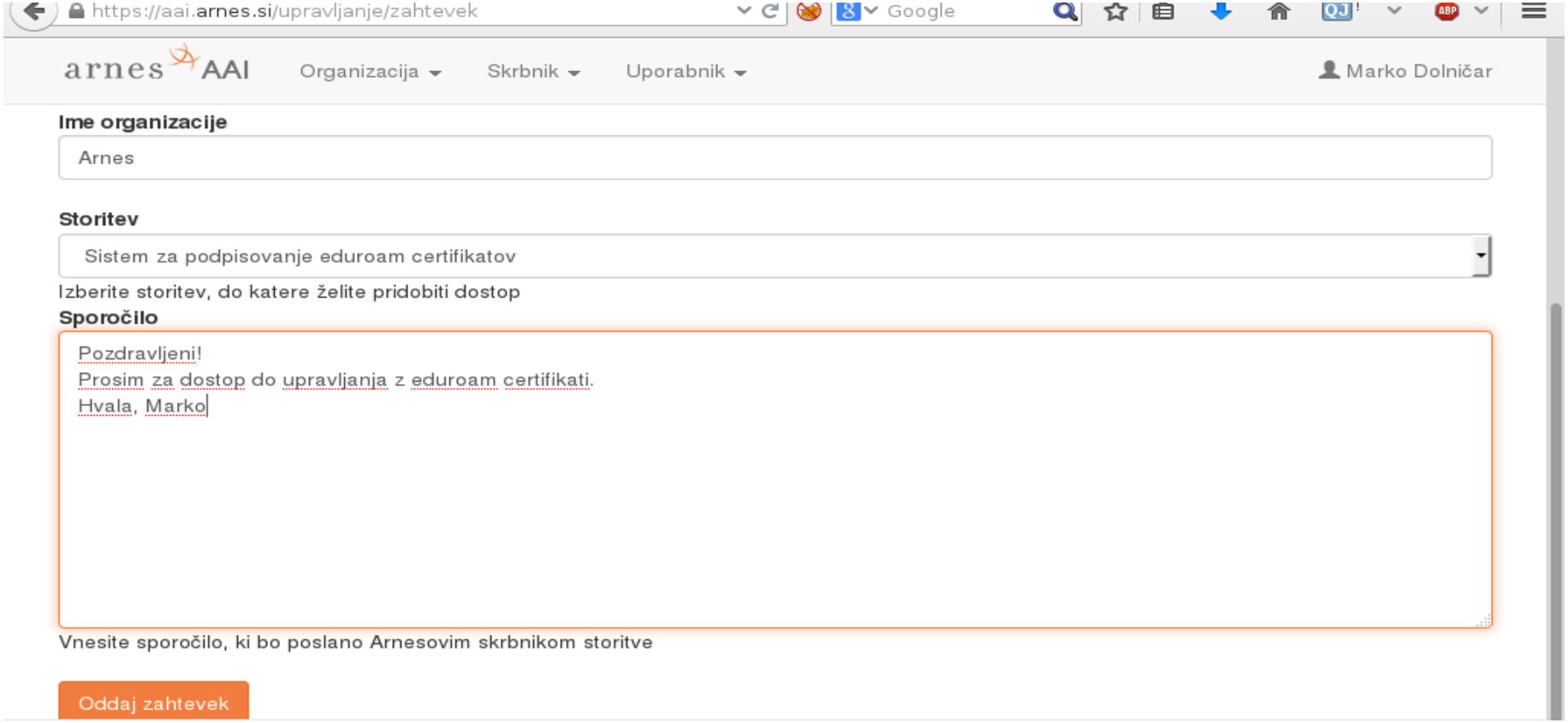
Upravljanje s certifikati
(https://aai.arnes.si)

2. Dostop do upravljanja



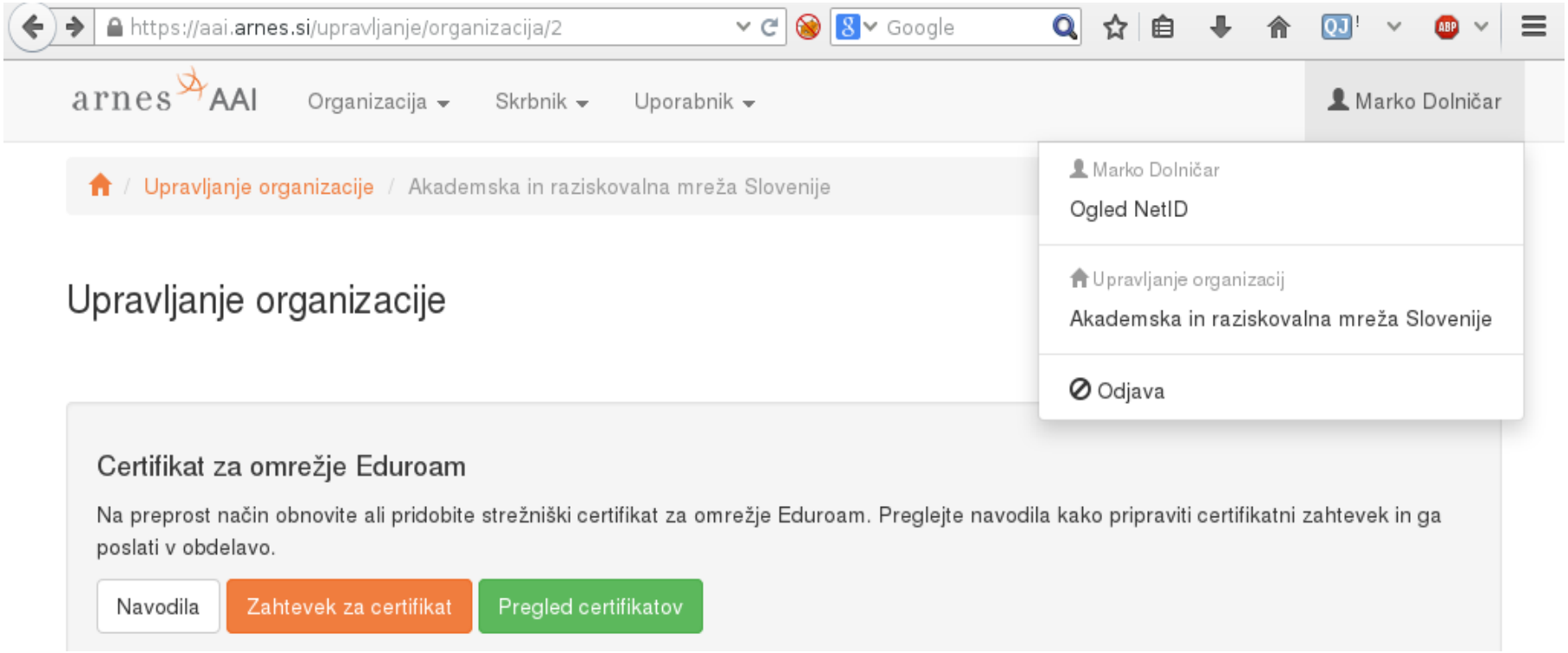
Upravljanje s certifikati
(https://aai.arnes.si)

3. Dostop do upravljanja (nadaljevanje)



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

4. Priprava certifikatnega zahtevka



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

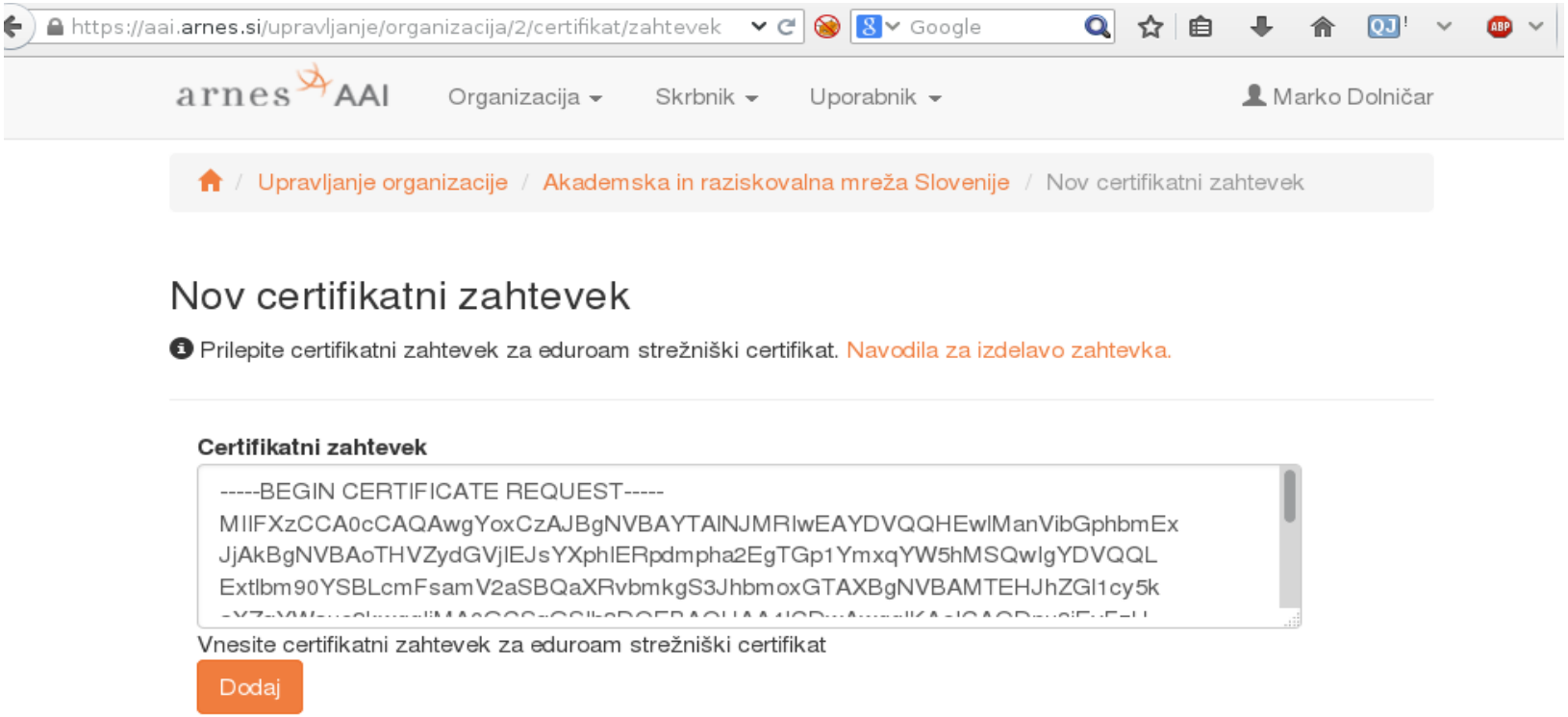
5. Priprava certifikatnega zahtevka (nadaljevanje)

```
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
```

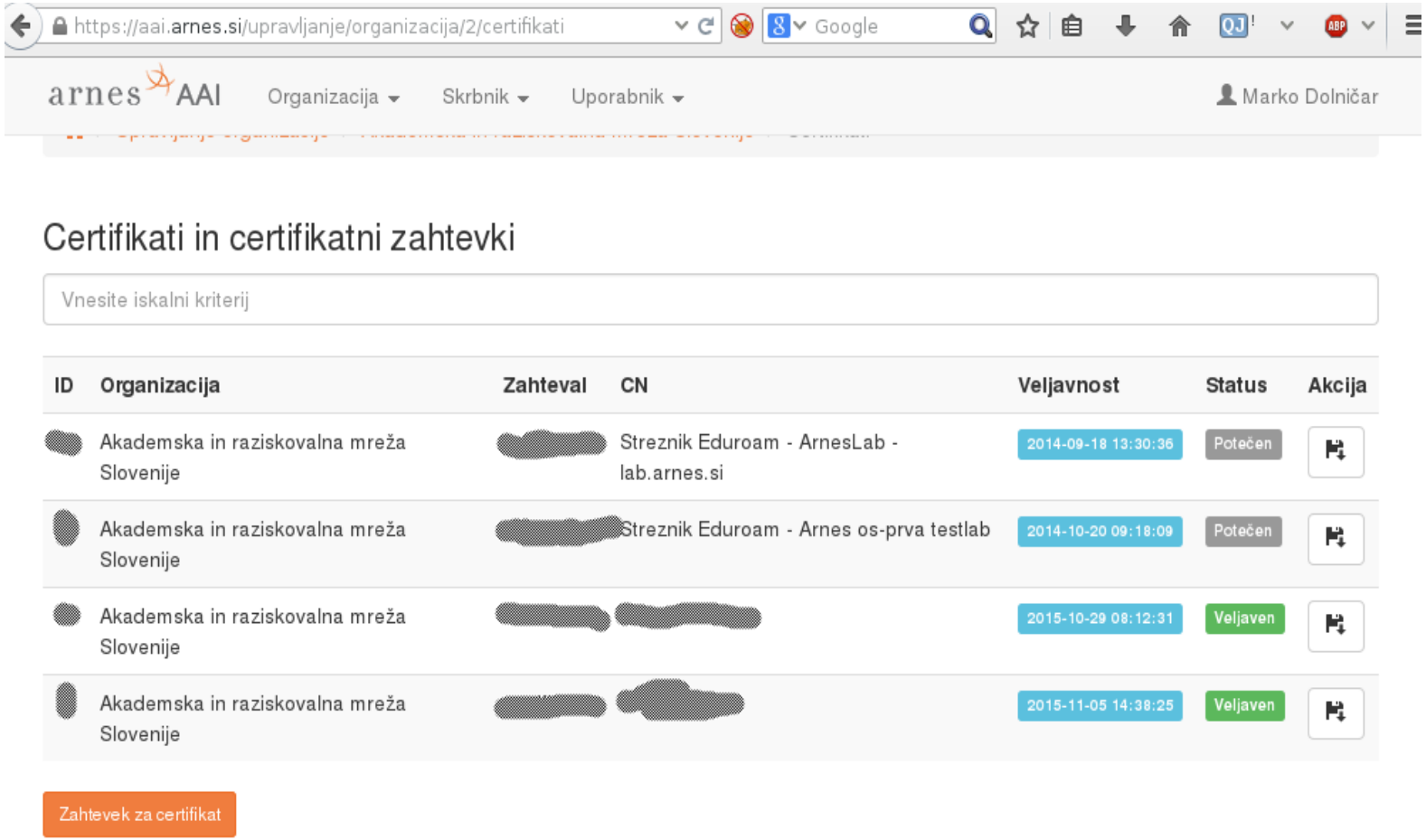
Upravljanje s certifikati
(https://aai.arnes.si)

6. Prenos certifikatnega zahtevka



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

7. Pregled certifikatov



arnes

Srečanje članic federacije 2014

8. december 2014, Ljubljana

Hvala!

Marko Dolničar

Arnes

aaa-podpora@arnes.si

https://aai.arnes.si