

Rekey korisničkog certifikata

U roku od 30 dana prije isteka važećeg certifikata korisnik će primiti obavijest o skorom isteku. Procedura za obnavljanje certifikata razlikuje se od inicijalne samo u identifikaciji (**korak 9.**), jer korisnik ne mora osobno posjetiti RA osobu.

BITNO! Procedura u nastavku mora biti obavljena PRIJE isteka važećeg certifikata. U suprotnom korisnik mora proći [punu proceduru](#), koja uključuje osobnu posjetu RA osobi.

1. Pomoću preglednika Firefox otvoriti [sučlje SRCE CA](#).
2. U izborniku odabrati **My Certificates** -> **Request a Certificate**
3. Na stranici odabrati link **Browser Certificate Request**
4. Odabrati **Continue**
5. Na sljedećem ekranu ponovo odabrati **Continue** (polje FQDN ostaje prazno)
6. Unijeti i **zapamtiti** (za korak 9.) pin od barem 5 znakova te potom odabrati **Continue**
7. Na sljedećem ekranu prihvatiti dogovor odabiranjem tipke **Continue**
8. Odabirom tipke **Generate request** zahtjev će biti generiran. Privatni ključ je spremljen u web pregledniku. Nakon izdavanja certifikata (korak 10.) korisnik mora dohvatiti certifikat koristeći **isti** preglednik. Na trenutnoj stranici korisnik će dobiti podatke o zahtjevu koji se koriste u sljedećem koraku.
9. Identifikacija zahtjeva ostvaruje se na način da korisnik pošalje starim certifikatom [digitalno potpisan](#) mail na SRCE CA ili da pokrene skriptu **requestVerify.pl** na [UI čvoru](#). Na zahtjev za unos potrebno je unijeti podatke sa stranice u koraku 8. Predložak texta koji treba unijeti naveden je u nastavku. Nakon unosa potrebno je stisnuti **ENTER** pa **CTRL-D**. Potom treba unijeti lozinku kojom ste zaštitili privatni ključ.

```
ADDITIONAL_ATTRIBUTE_ADDRESS      ...
ADDITIONAL_ATTRIBUTE_EMAIL         ...
ADDITIONAL_ATTRIBUTE_INSTITUTE     ...
ADDITIONAL_ATTRIBUTE_REQUESTERCN   ...
ADDITIONAL_ATTRIBUTE_TELEPHONE     ...
NOTBEFORE                         ...
PIN                               ...
RA                                ...
ROLE                              ...
SERIAL                            ...
SUBJECT_ALT_NAME                   ...
TYPE                               ...
```

BITNO! Identifikacija mora biti ostvarena najkasnije 7 dana nakon podnošenja zahtjeva. U suprotnom zahtjev se briše te je potrebno podnijeti novi.

10. SRCE CA izdaje certifikat i obavještava korisnika putem maila da je certifikat objavljen na web stranici [SRCE CA](#). Po dobivanju maila korisnik može dohvatiti izdani certifikat putem web sučelja.
11. Po dobivanju certifikata korisnik mora poslati mail **potpisan sa novim certifikatom** na SRCE CA adresu navedenu u mailu s obavijesti u certifikatu. Korisnici trebaju poslati [potpisani odgovor](#) na prvi mail "SRCE CA Certificate Statement" naveden u obavijesti. Drugi mail se koristi isključivo kod izdavanja poslužiteljskih certifikata i **nije** ga potrebno slati.