

	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	1/15

SADRŽAJ:

1. Svrha i cilj.....	2
2. Područje primjene	2
3. Pojmovi i skraćenice.....	2
4. Preuvjeti za preuzimanje ssl digitalnih certifikata.....	2
5. Pristup CMS web portalu.....	3
6.1 OpenSSL.....	6
6.2 Microsoft IIS	10

	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	2/15

1. Svrha i cilj

Ovom se uputom prikazuje način preuzimanja SSL digitalnih certifikata pomoću CMS web portala.

2. Područje primjene

Radna uputa se primjenjuje za sve fizičke osobe i poslovne subjekte koji trebaju preuzeti SSL/poslužiteljski digitalni certifikat pomoću Fina CMS sustava za izdavanje certifikata.

3. Pojmovi i skraćenice

Skraćenica	Puni naziv	Objašnjenje
Digitalni certifikat	Digitalni certifikat	Elektronički identitet u raznim elektroničkim interakcijama
CMS	Credential Management System	Finin sustav za upravljanje certifikatima
SSL	Secure Socket Layer	Transportni protokol koji omogućava sigurnu komunikaciju pomoću interneta
CSR	Certificate Signing Request	Poruka koja se šalje izdavatelju certifikata za certifikaciju javnog ključa
pkcs#10	Certification Request Standard	Standard koji određuje format poruke koja se šalje izdavatelju certifikata za dobivanje certifikata temeljem dostavljenog javnog ključa
LRA	Local Registration Authority	Služba za registraciju korisnika

4. Preduvjeti za preuzimanje ssl digitalnih certifikata

Da bi se preuzeli SSL certifikati, potrebno je imati instalirane CA certifikate izdavatelja (Fina Root CA i Fina RDC 2015). Certifikate je moguće preuzeti i instalirati sa stranice Fine (<https://rdc.fina.hr/Root/FinaRootCA.cer> i <https://rdc.fina.hr/Root/FinaRDCCA.cer>).

Instalacija Root CA certifikata se provodi prema uputi:

[https://rdc.fina.hr/upute/Uputa za instalaciju FINA RDC CA certifikata.pdf](https://rdc.fina.hr/upute/Uputa%20za%20instalaciju%20FINA%20RDC%20CA%20certifikata.pdf)

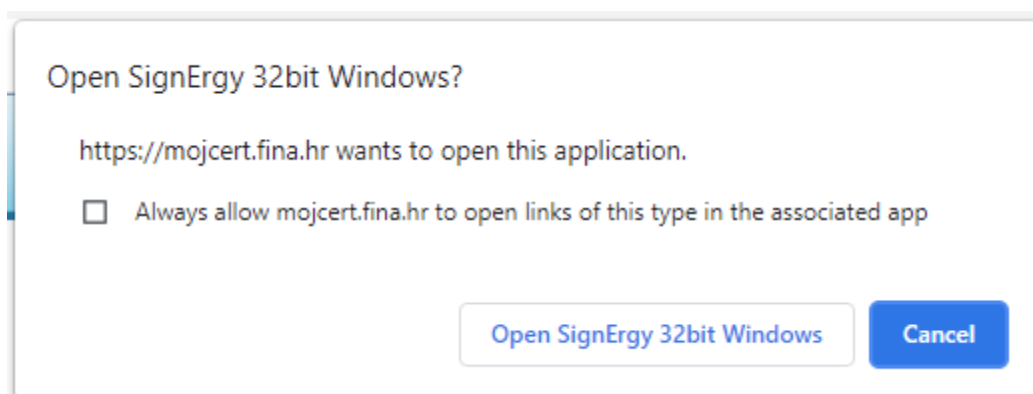
Za preuzimanje certifikata u cer obliku nužno je na strani korisnika koristiti neki od alata za generiranje ključeva i CSR zahtjeva. U uputi je prikazan način kreiranja CSR-a pomoću openssl alata i Internet Information Services alata.

	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	3/15

5. Pristup CMS web portalu

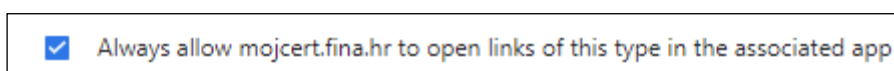
U adresnu liniju potrebno je upisati: <https://mojcert.fina.hr/finacms/>

Ukoliko se ne koristi Internet preglednik koji podržava izvođenje Java appleta, pojaviti će se sljedeći prozor upozorenja da se pokreće aplikacija potreban za rad CMS portala:



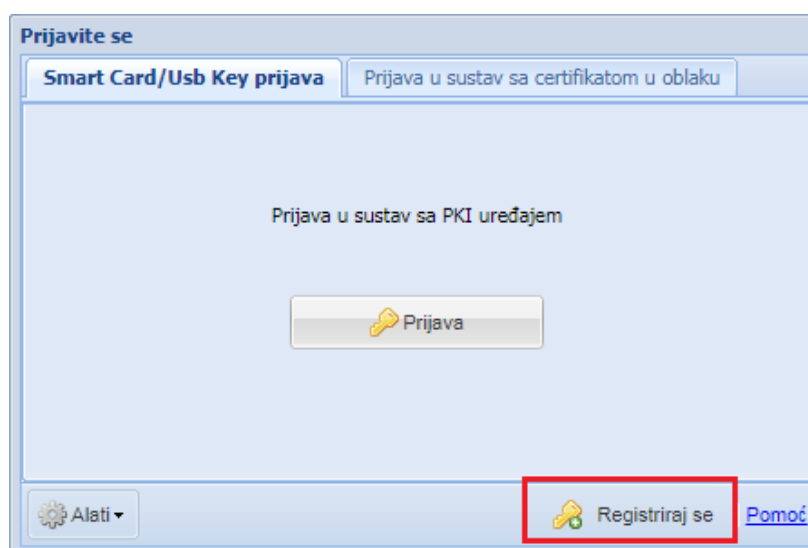
Slika 5.1. Pokretanje aplikacije

Na tom je prozoru potrebno odabrati tipku „Open SignErgy 32bit Windows“ i eventualno staviti oznaku da se prozor upozorenja više ne pojavljuje:



Slika 5.2.

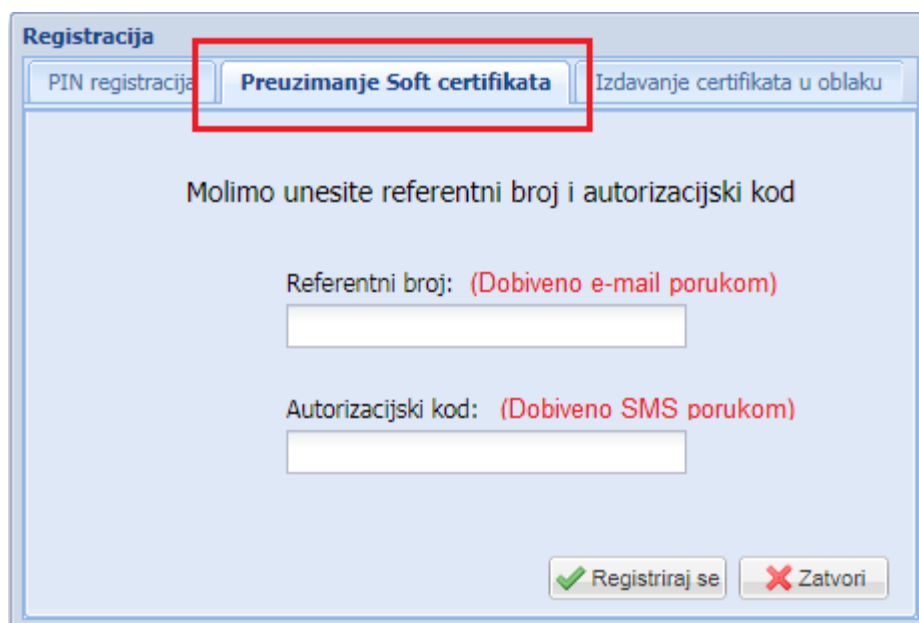
Pojavljuje se prozor za registraciju/prijavu na sustav na kojem je potrebno odabrati „Registriraj se“:



Slika 5.3. Registracija na sustav za preuzimanje certifikata

	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	4/15

Nakon prijave potrebno je odabrati „Preuzimanje soft certifikata“:

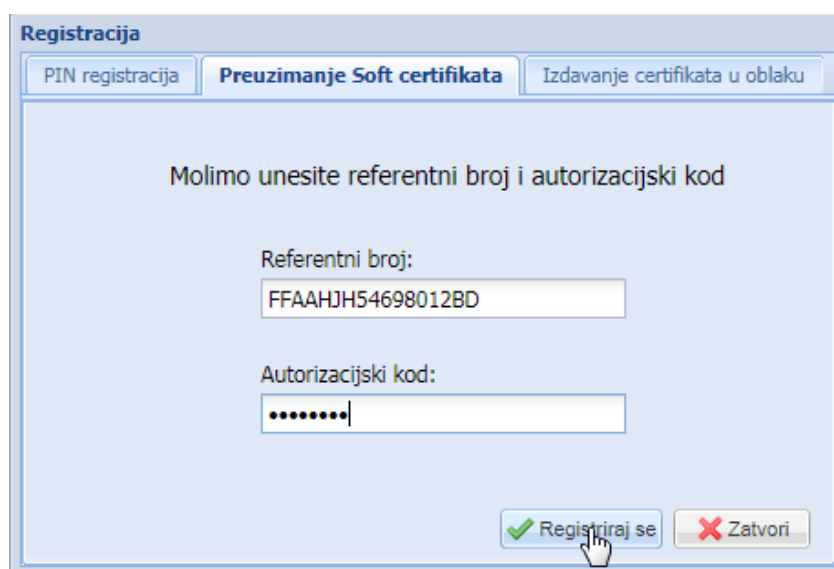


Slika 5.4. Preuzimanje soft certifikata

Referentni broj i autorizacijski kod dostavljaju se preko dva odvojena kanala gdje se koriste podaci o e-mail poruci i broju mobilnog uređaja iz obrasca zahtjeva za izdavanje SSL certifikata.

Ove podatke moguće je zatražiti i od LRA službenika gdje je zatražen certifikat.

Nakon unosa dostavljenih podataka potrebno je odabrati „Registriraj se“:



Slika 5.5. Nastavak registracije u CMS

	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	5/15

Pojaviti će se ekran sa prikazanim podacima gdje je potrebno označiti certifikat za izdavanje:

☐ Certifikati	Ključevi	Zahtjev	Izdavanje	Pohrana	Status
☒ CN=test.nrw2.hr,L=ZAGREB,O=FINA HR85821130368,C=HR	×	×	×	×	Spreman

Prvi korak: označavanje certifikata

Drugi korak: odabir tipke "Izdaj označene"

 Izdaj označene

Slika 5.6. Priprema preuzimanja certifikata

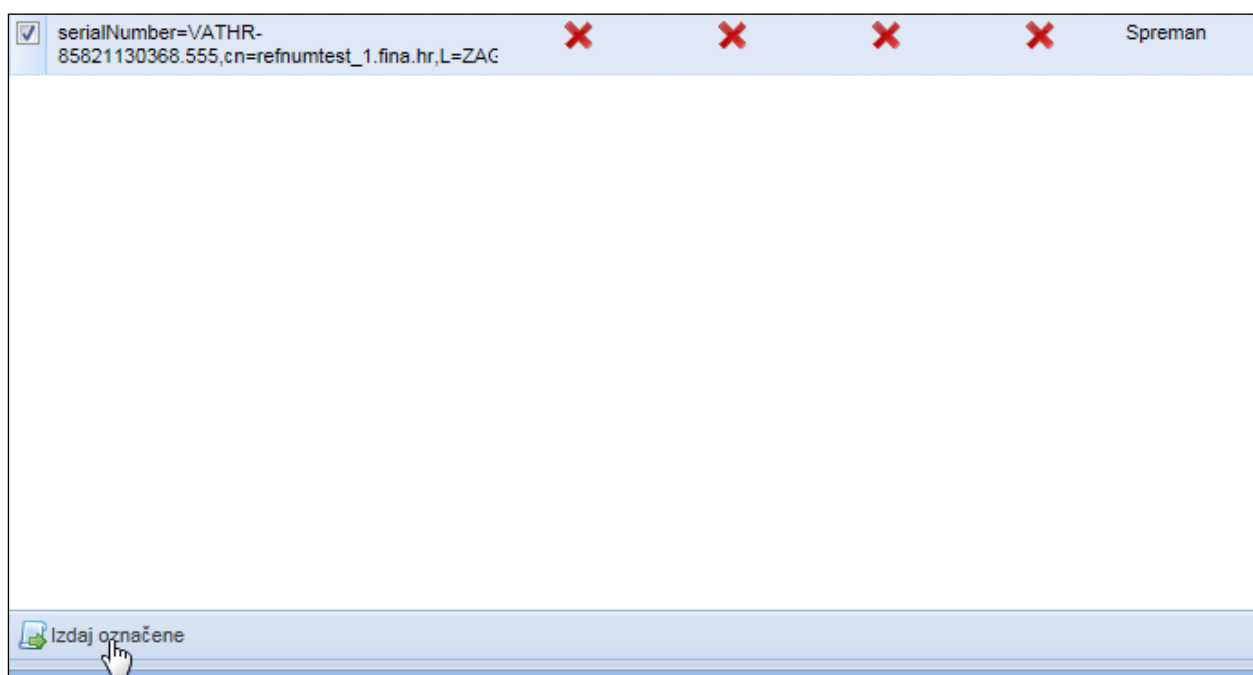
	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	6/15

6.1 OpenSSL

U sklopu ovog dijela upute biti će opisan postupak izdavanja SSL certifikata koji će se koristiti za potrebe Apache web poslužitelja. Za potrebe kreiranja privatnog ključa i CSR zahtjeva koristiti će se program *openssl* koji se može preuzeti sa stranice

<https://www.openssl.org/source/>

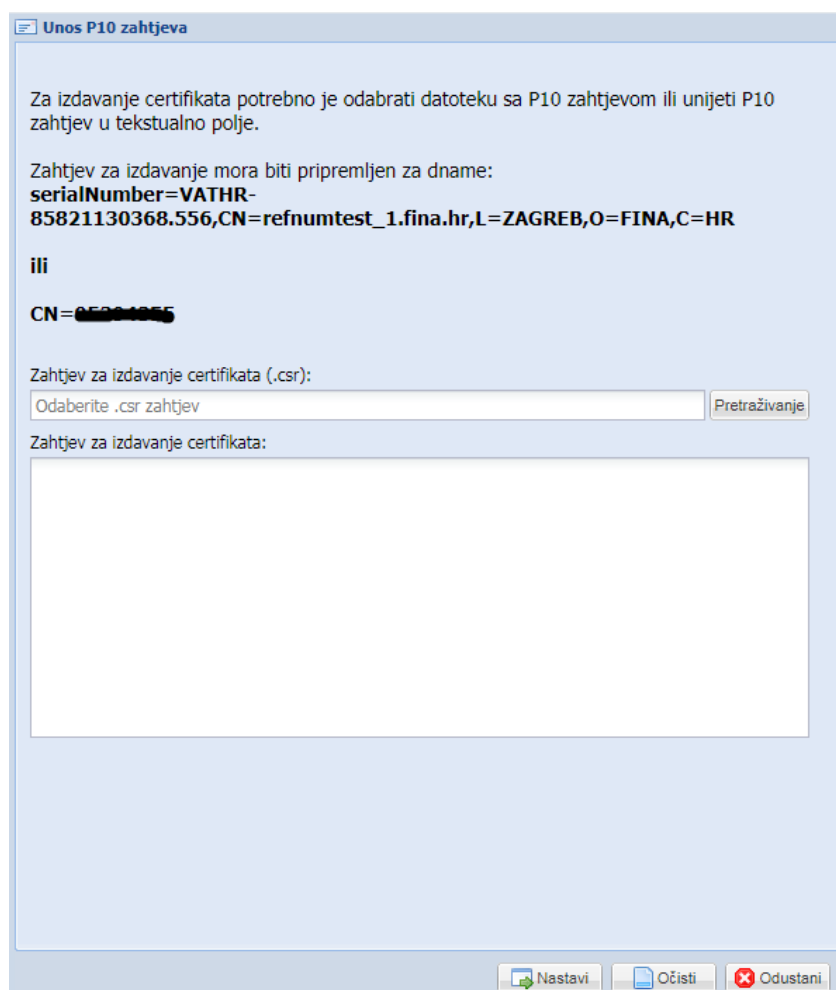
U ovom dijelu upute koristi se testni certifikat iz Fina okruženja CN=refnumtest_1.fina.hr



Slika 6.1. Preuzimanje certifikata

	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	7/15

Nakon odabira tipke „Izdaj označene“ pojavit će se ekran gdje je potrebno odabrati csr zahtjev ili napraviti copy/paste sadržaja zahtjeva u predviđeni prozor:



Slika 6.2. Unos csr-a za certifikat

Sada je na web poslužitelju potrebno pokrenuti naredbe za generiranje RSA privatnog ključa modula duljine 2048 bita te za generiranje CSR zahtjeva za certifikat. Nakon pokretanja naredbe

openssl genrsa -out key.pem 2048

dobiva se izlaz prikazan na donjoj slici:

```
linux-0e51:~ # openssl genrsa -out key.pem 2048
Generating RSA private key, 2048 bit long modulus
...+++
.....
e is 65537 (0x10001)
```

Nakon toga na web poslužitelju potrebno je pokrenuti sljedeću naredbu za generiranje CSR zahtjeva:

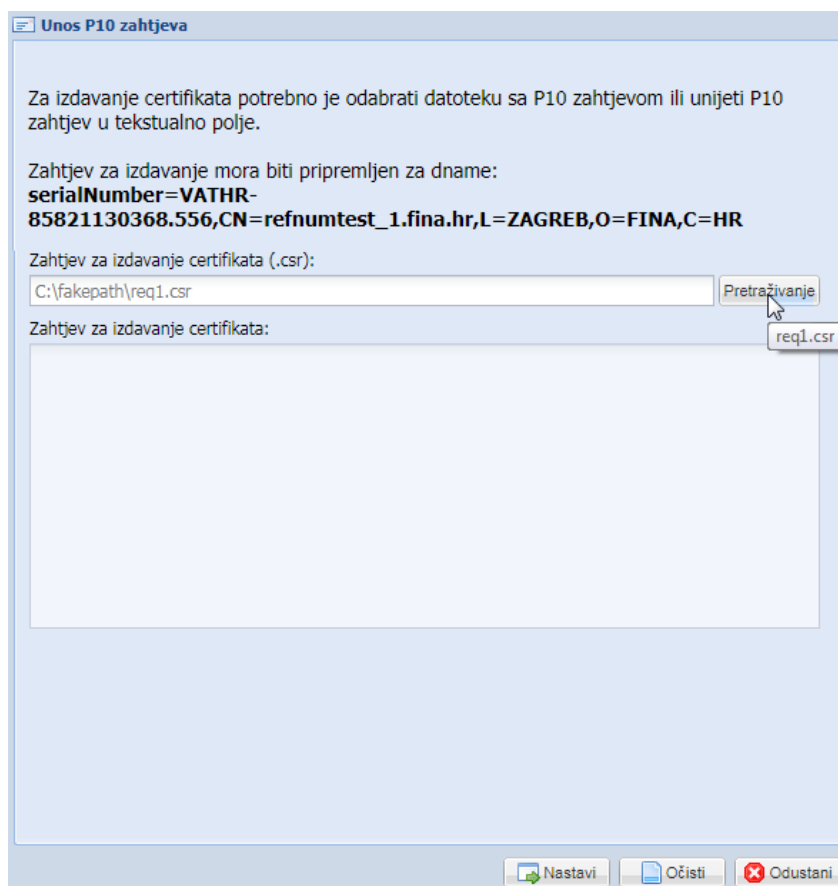
```
linux-0e51:~ # openssl req -new -sha256 -nodes -key key.pem -out req1.csr -subj "/CN=refNum"
linux-0e51:~ # █
```

	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	8/15

*refNum je broj koji je dobiven u e-mail poruci.

Ovime se dobio CSR zahtjev u datoteci req1.csr te ga je potrebno učitati u CMS:

Vraćamo se na CMS sučelje gdje se može ili otvoriti csr datoteka u notepadu ili odabrati cijela datoteka. U ovom prikazu odabrana je datoteka zahtjeva req1.csr



Slika 6.3. Odabran CSR

	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	9/15

Nakon odabira tipke „Nastavi“ započinje proces preuzimanja certifikata koji završava ekranom na kojem se može odabrati format datoteke za preuzimanje. Ponuđeni su cer, p7b i p7b sa certifikatima izdavatelja.



Slika 6.4. Preuzimanje izdanog ssl certifikata

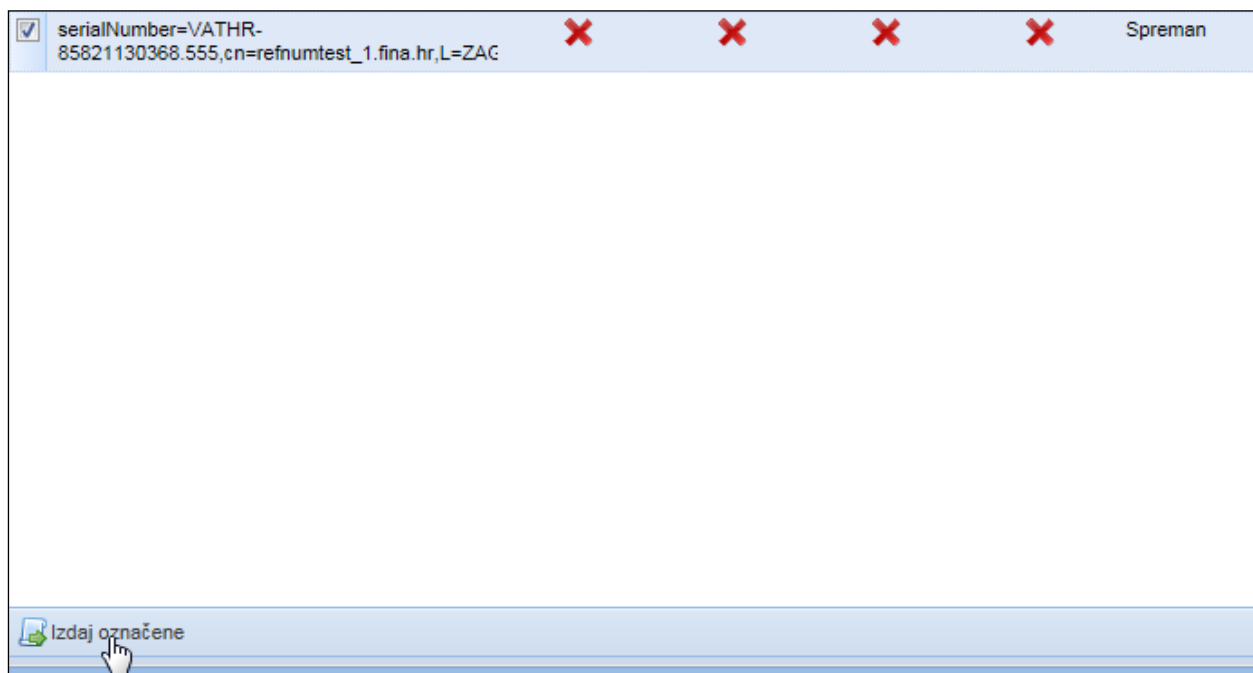
Ovime je završeno preuzimanje certifikata od strane klijenta.

	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	10/15

6.2 Microsoft IIS

U sklopu ovog dijela upute biti će opisan postupak izdavanja SSL certifikata koji će se koristiti za potrebe MS Internet Information Services alata. U postupku naručivanja certifikata biti će potrebno kreirati CSR preko IIS-a.

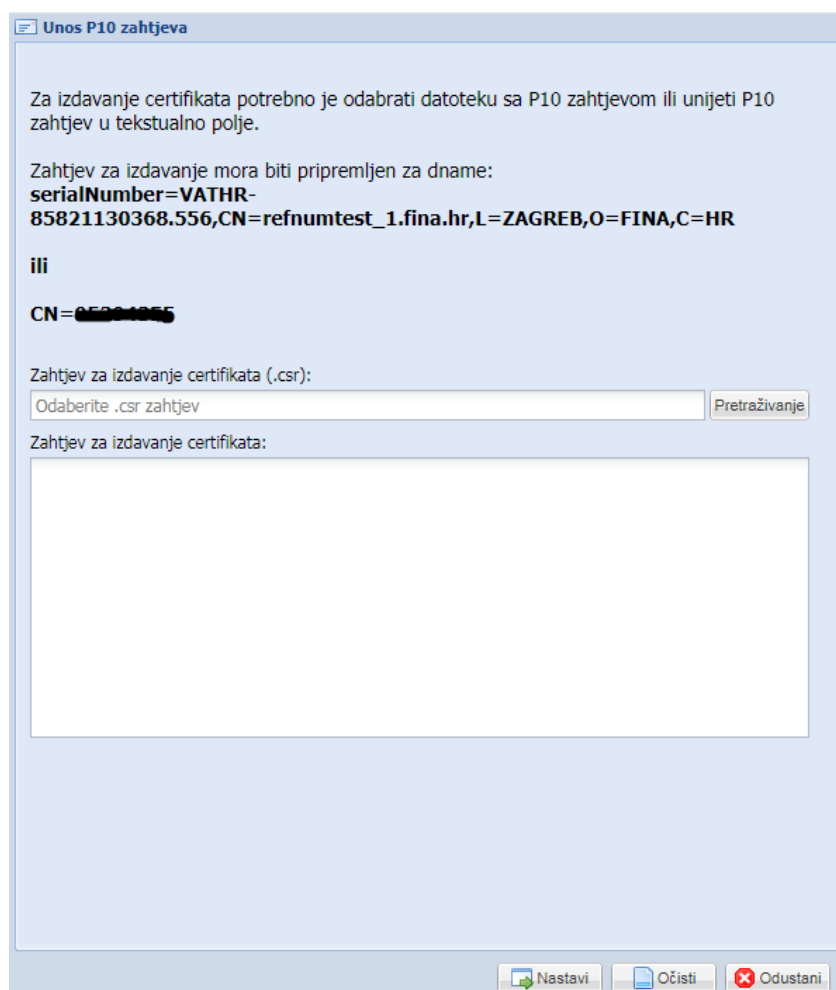
U ovom dijelu upute koristi se testni certifikat iz Fina okruženja CN=refnumtest_1.fina.hr



Slika 6.5. Preuzimanje certifikata

	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	11/15

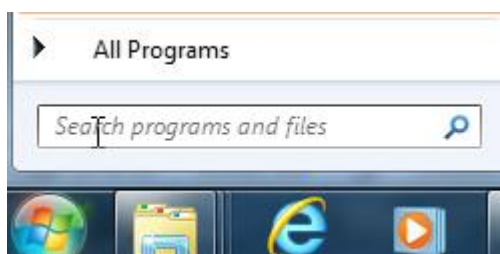
Nakon odabira tipke „Izdaj označene“ pojavit će se ekran gdje je potrebno odabrati csr zahtjev ili napraviti copy/paste sadržaja zahtjeva u predviđeni prozor:



Slika 6.6. Unos csr-a za certifikat

Temeljem dostavljenih podataka u e-mail poruci potrebno je u IIS-u napraviti csr na sljedeći način:

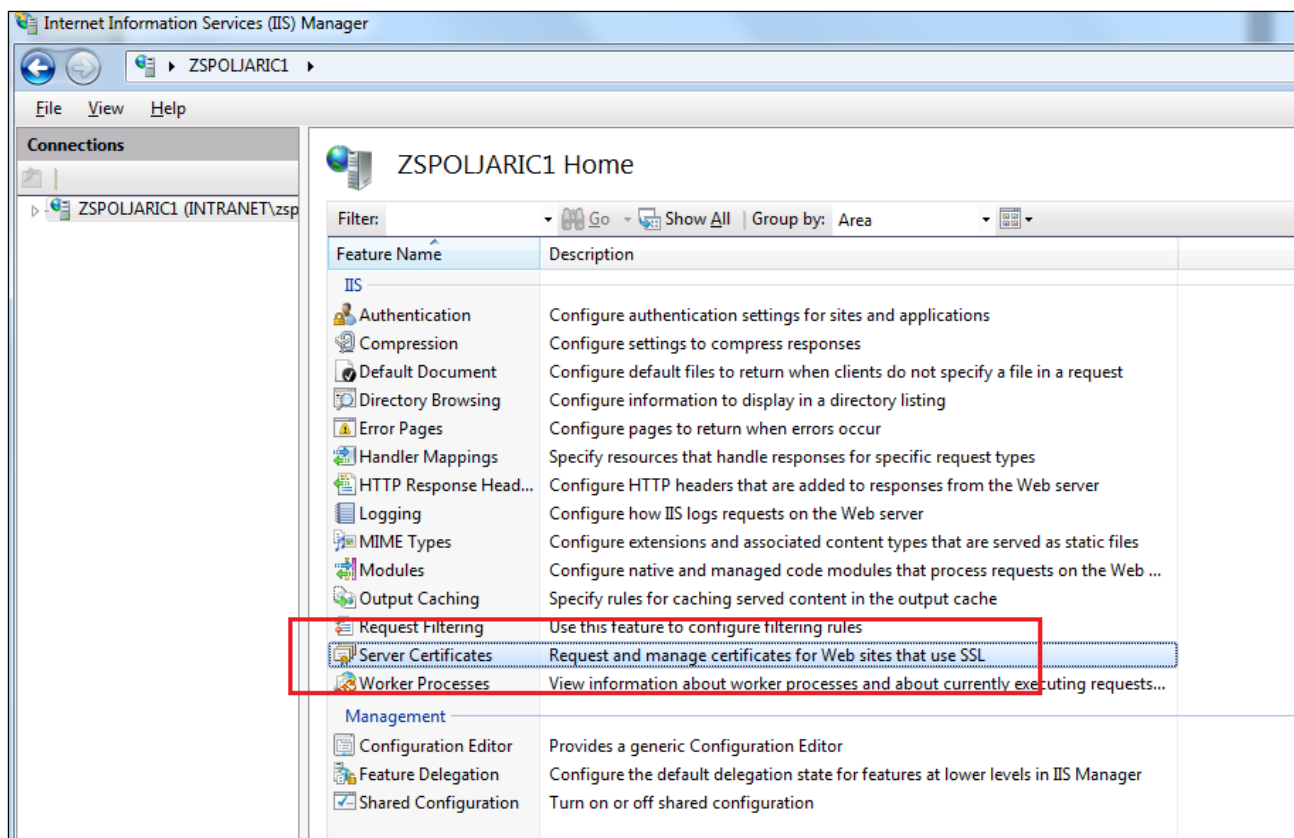
Pronaći IIS upisivanjem „iis“ unutar prozora za pretraživanje certifikata:



Slika 6.7. Pokretanje IIS-a

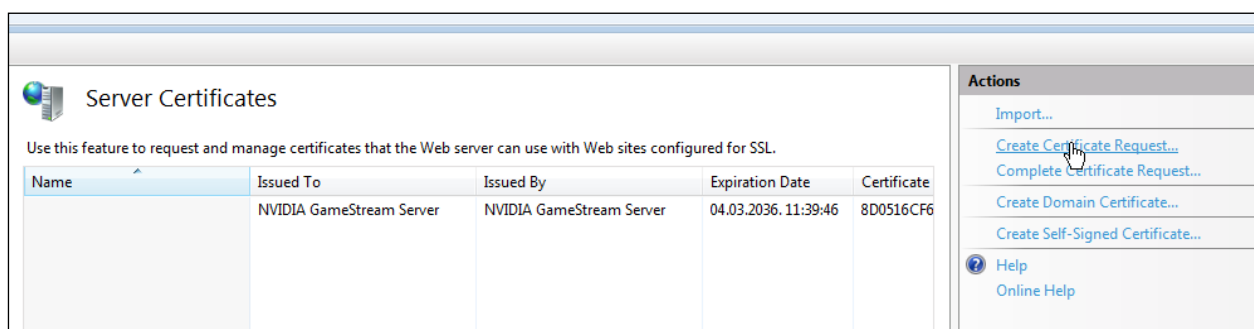
	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	12/15

Prikazuje se sljedeći ekran:



Slika 6.8. Odabir dijela za upravljanje certifikatima

Dvostrukim klikom dobiva se ekran na kojem je potrebno odabrati „Create certificate request...”

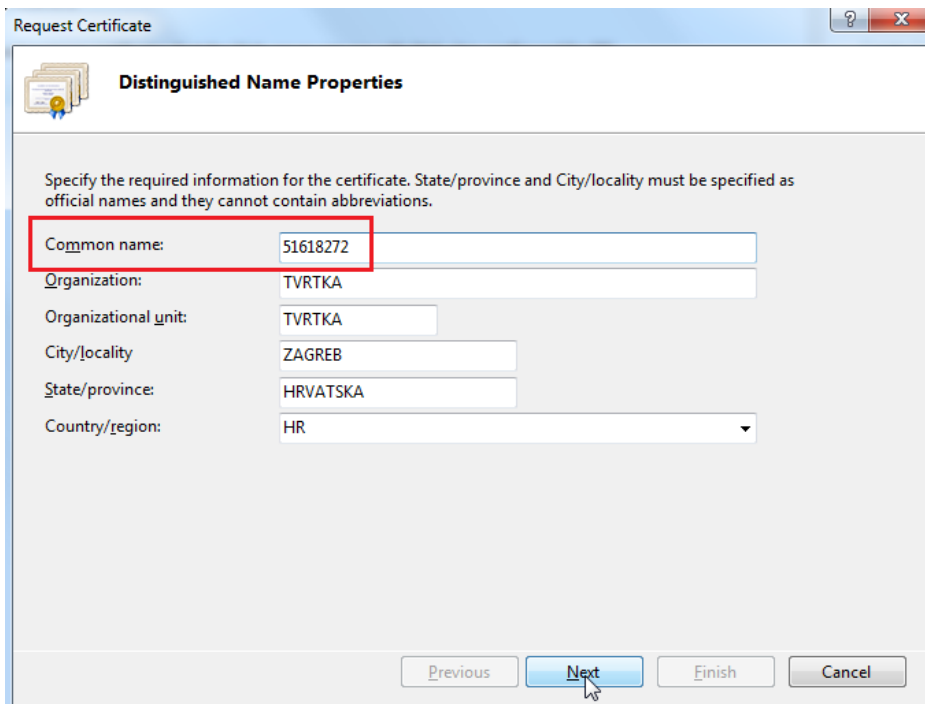


Slika 6.9. Pokretanje procesa izrade CSR-a

	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	13/15

U prozoru „Common name“ upisuje se podatak za kreiranje p10 (csr) zahtjeva dobiven u e-mail poruci:

Podatak za kreiranje p10 zahtjeva za certifikat je: CN=51618272



Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: 51618272

Organization: TVRTKA

Organizational unit: TVRTKA

City/locality: ZAGREB

State/province: HRVATSKA

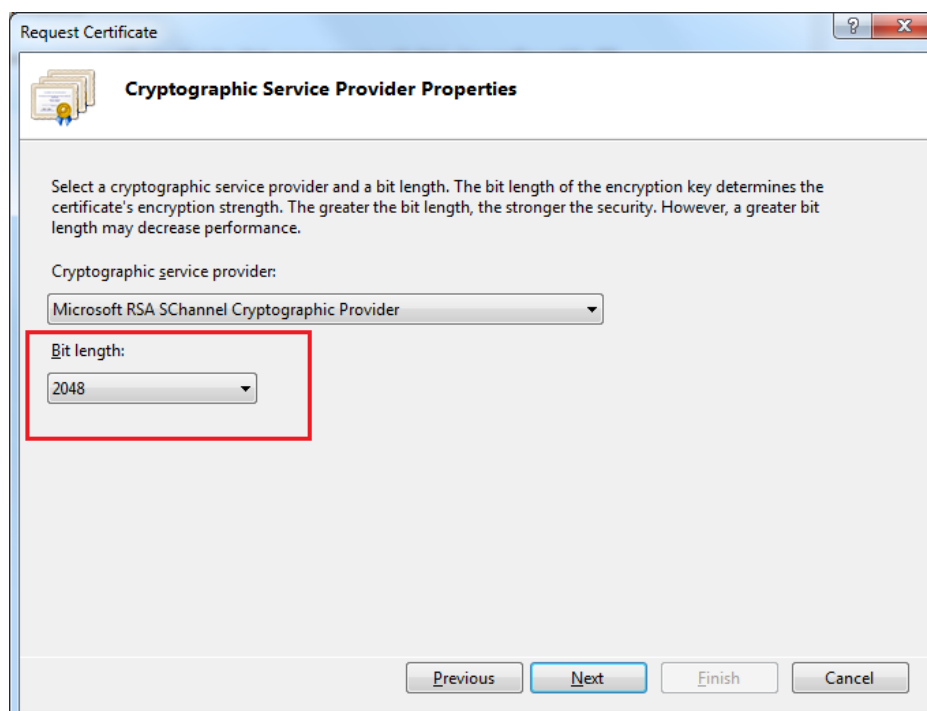
Country/region: HR

Previous Next Finish Cancel

Slika 6.10. Pokretanje procesa izrade CSR-a

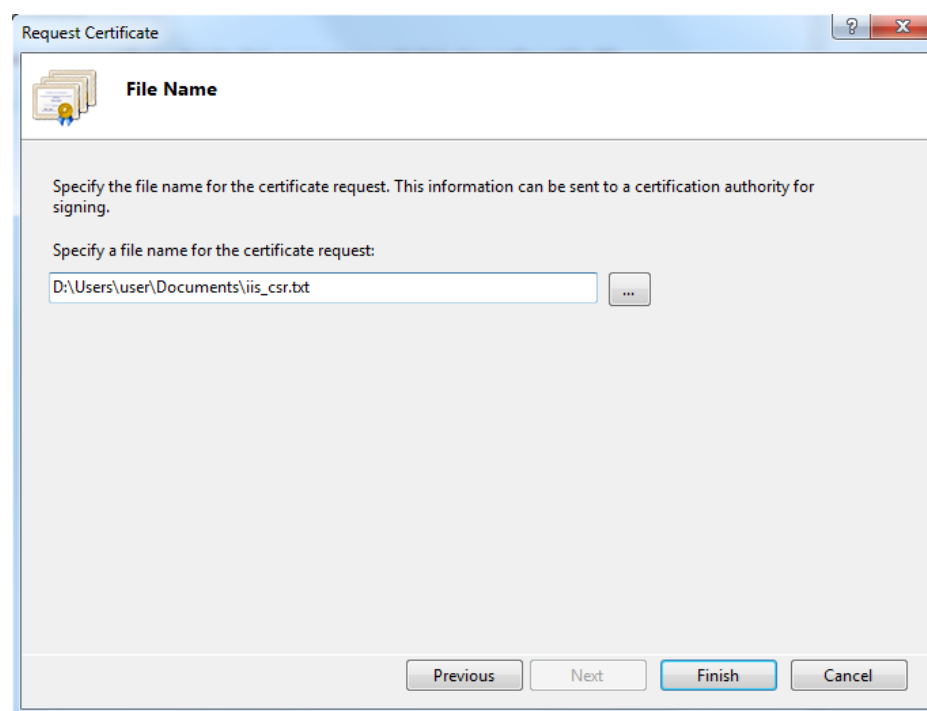
	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	14/15

Nakon toga pojavljuje se ekran gdje je potrebno odabrati algoritam i duljinu ključa. Potrebno je obratiti pažnju da je i dalje na Win7 ponuđena duljina ključa od 1024 umjesto 2048 pa to treba posebno odabrati:



Slika 6.11. Definiranje algoritma i duljine ključa

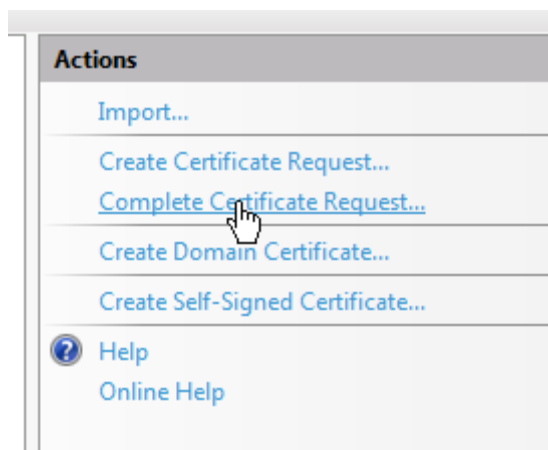
Sada je potrebno postaviti lokaciju i naziv datoteke koja će se kreirati:



Slika 6.12. Lokacija i naziv kreirane datoteke

	Radna uputa za preuzimanje SSL certifikata pomoću FINA CMS web portala	klasifikacija:	
		oznaka:	63370006
		revizija:	7-09/2021
		strana:	15/15

Nakon što se datoteka kreira, potrebno se vratiti u CMS i tamo priložiti csr datoteku isto kao i u prethodnom primjeru. Nakon izdavanja certifikata temeljem csr zahtjeva, isti je potrebno preuzeti u cer obliku te nakon toga napraviti akciju „Complete Certificate Request...” u IIS na sljedećem ekranu:



Slika 6.13. Završavanje postupka dobivanja certifikata