



## KATEDRA ZA OPERACIJSKE SUSTAVE

# Operacijski sustavi: mrežna infrastruktura i servisi

---

### Lab 08 – Certifikacijski servisi



## Sadržaj

Uvod .....	2
EFS .....	3
Prije vježbe .....	4
Konfiguracija AD CS uloge .....	5
Instalacija uloge .....	5
Online responder .....	7
Certifikat za IIS poslužitelj .....	8
IIS konfiguracija .....	9
SSL kriptiranje veze .....	10
Konfiguracija mehanizma za opoziv certifikata .....	11
Pristup preko web-servisa .....	12
Zahtjev za certifikatom .....	12
Opoziv certifikata .....	14
Automatsko izdavanje certifikata .....	15
Enkripcija na razini datotečnog sustava .....	18
Pričuvne kopije i oporavak .....	21
Rezultat vježbe .....	22
Što treba znati nakon ove vježbe? .....	23
Dodatna literatura .....	23



## Uvod

### -----UPOZORENJE-----

Prije nego počnemo s uvodom, naglasimo važnost današnje vježbe. Certifikacijski su servisi osnova za iduće vježbe. Stoga današnju vježbu morate savršeno točno odraditi i na kraju izraditi *snapshot* svih korištenih virtualnih računala. Bez funkcionalne infrastrukture za certifikacijske servise NAP mehanizmi koje konfiguriramo u idućim vježbama neće i ne mogu funkcionirati. Sljedeću ćemo vježbu izravno nastaviti na ovu. Zato savjesno pratite upute i u slučaju bilo kakvih nejasnoća ili pogrešaka pri izvođenju vježbe zamolite asistenta za pomoć. Nikako nemojte zaboraviti izraditi *snapshot* na kraju vježbe!

Tema današnje vježbe jesu **Active Directory certifikacijski servisi** (eng. *Certificate services*) – **AD CS**. Oni su skup uloga koje instalirate na Windows Server 2012, a implementiraju **PKI** (eng. *Public Key Infrastructure*) infrastrukturu. PKI je skup mehanizama za potvrdu identiteta svakog člana koji sudjeluje u kriptiranoj mrežnoj komunikaciji. PKI infrastruktura može biti vrlo jednostavna (s jednim samostalnim poslužiteljem) ili vrlo složena, s mnogo hijerarhijski organiziranih poslužitelja integriranih u Active Directory.

Odlučiti kakvu certifikacijsku infrastrukturu želite nipošto nije lagan zadatak. U produkcijskom okruženju nije nimalo dobro „na blef“ odabrati jedan poslužitelj i na njega instalirati *Enterprise RootCA* certifikacijske servise. Naime, ispad ili sigurnosna kompromitacija tog poslužitelja može imati katastrofalne posljedice na cijelu infrastrukturu. Jedan od čestih pristupa pri dizajniranju certifikacijske infrastrukture jest uporaba samostalnog *RootCA* poslužitelja s kojim povežete nekoliko *Enterprise* podređenih (eng. *Subordinate*) CA poslužitelja. Tada samostalni poslužitelj isključite (fizički ga ugasite) i maksimalno osigurajte. Ponovno ćete ga uključiti tek kad podređeni CA poslužitelji moraju obnoviti vlastite certifikate.

U današnjoj ćemo vježbi raditi s jednim poslužiteljem, ali će on svakako biti vezan za AD. Opišimo infrastrukturu koju želimo postići.

- **SERVERDC**: domenski kontroler na koji danas instaliramo certifikacijske servise. Ovo nije u skladu s preporukama u prošlim vježbama, gdje smo naglasili da je domenski kontroler uloga za sebe. Ipak, certifikacijski servisi nisu pretjerano zahtjevna uloga (iako može imati posljedice na domenski kontroler – vidi dodatnu literaturu) pa je u našem testnom okruženju možemo instalirati na domenski kontroler. Time smo računalo SERVER1 ostavili neopterećeno, što će nam odgovarati u idućoj vježbi.
- **SERVER1**: ovim se računalom danas nećemo koristiti, osim na samom kraju vježbe kako bismo mu izdali certifikat. Nemojte ga niti uključivati dok upute ne kažu drugačije.
- **CLI1**: klijentsko računalo s kojeg ćemo testirati funkcionalnost certifikacijskih servisa.

Ponovimo ukratko pojmove certifikacijskih servisa koje ćemo danas upoznati:

- **predložci**: certifikati u AD CS-u pojedinom se računalu, korisniku ili nekom drugom objektu izdaju na osnovi predložaka (eng. *Templates*). Za svaku vrstu objekta postoji predefinirani predložak, u kojem je definirana namjena certifikata, vrijeme ispravnosti i sl. Nije preporučljivo



(iako je moguće) znatno modificirati ugrađene predloške. Radije kopirajte predložak i onda tu kopiju prilagodite svojim potrebama. Takvom ćemo se koncepcijom koristiti u vježbi.

- **CRL popis:** certifikat izdan na osnovi predloška ima vrijeme valjanosti – „rok trajanja“. Vrijeme valjanosti certifikata varira od predloška do predloška – npr. 5 godina za RootCA, 1 godina za korisnika itd. Certifikat kojem je isteklo vrijeme valjanosti opoziva se, tj. dodaje se na **popis za opoziv certifikata** (eng. *Certificate Revocation List*) – **CRL**. Popis za opoziv u pravilnim se vremenskim intervalima objavljuje u cijeloj domeni, kako bi informacija o neispravnom certifikatu stigla do svih objekata koji sudjeluju u enkriptiranoj komunikaciji. CRL popis nakon instalacije AD CS-a predefinirano se objavljuje jednom tjedno. U svakom je trenutku moguće ručno objaviti popis za opoziv, izvan predodređenog intervala. Tada su dostupne opcije za objavu cijelog popisa za opoziv ili samo razlika koje su se pojavile prošle objave popisa. Popis s razlikama označuje se terminom **DeltaCRL**, a predefinirano se objavljuje jednom dnevno.
- **Online responder:** komponenta koja odgovara na klijentske upite o ispravnosti certifikata. Rabi se u kompleksnim ili velikim mrežama.
- **Certifikacijski Web servis:** web-servis koji korisnicima i računalima omogućuje prijavu za izdavanje certifikata uz pomoć http(s) protokola. Funkcionalno se svodi na korištenje webstranicom i preuzimanje (eng. *Download*) traženog certifikata.

## EFS

**EFS** (eng. *Encrypting File System*) jest naziv za ugrađenu tehnologiju enkripcije na razini NTFS datotečnog sustava. EFS rabi 256-bitnu enkripciju kako bi korisnik mogao osigurati svoje važne podatke. Savjetujem da enkripciju datotečnog sustava ne uključujete bez prijekne potrebe. Enkriptirani se podaci potpisuju certifikatom za svakog korisnika. Prije nego uopće pomislite svojim korisnicima ponuditi mogućnost enkripcije, konfigurirajte metodu povrata kriptiranih podataka. Metoda se zove **EFS Recovery Agent**, a načelno se svodi na izradu (ili odabir postojećeg, kao što ćemo mi učiniti) korisničkog računa s certifikatom koji je valjan za dekrpciju svih kriptiranih podataka u domeni. EFS Recovery Agent cijenit ćete kad korisnik ostane bez računala, kad mu reinstalirate operacijski sustav, kad mu istekne certifikat ili, drugim riječima, u svim situacijama kada korisnik ne može do vlastitih podataka.

Postavlja se pitanje: u kojoj je situaciji uopće potrebno kriptirati podatke? Banalan odgovor jest: onda kada sve ostale metode zaštite podataka (dozvole pristupa, fizička sigurnost) mogu lako zakazati. Jedan od čestih primjera jest korisnik s prijenosnim računalom. Korisnik prijenosnog računala može vrlo lako postati metom lopova. Ako mu prijenosnik ukradu, dozvole pristupa postavljene na važne podatke ne pružaju nikakvu zaštitu. Naime, lopov može čvrsti disk prijenosnika prebaciti u drugo računalo na kojem ima prava lokalnog administratora. S tim pravima lopov može bez problema promijeniti sve dozvole pristupa i pristupiti podacima. U takvoj je situaciji jedina zaštita podataka enkripcija.

Ovime završava današnji uvod. Krenimo s vježbom.



## Prije vježbe

1. Prijavite se na računalo kao **Administrator** s lozinkom **Pa\$\$w0rd**.
2. Kliknite na **Start-> Administrative Tools-> Hyper-V Manager**.
3. Provjerite jesu li sva virtualna računala isključena. Podsjetimo se, isključena računala kao oznaku statusa imaju **Off** ili **Saved**. Uključena računala imaju oznaku **Running**.
4. Primijenite *snapshot* Start na virtualnom računalu **KZOS-SERVERDC**.
5. Primijenite *snapshot* Start na virtualnom računalu **KZOS-SERVER1**.
6. Primijenite *snapshot* Start na virtualnom računalu **KZOS-CLI1**.



## Konfiguracija AD CS uloge

Kako je opisano u uvodu, CS ćemo implementirati na računalu SERVERDC. To će računalo sadržavati i sve dodatne uloge koje su preduvjet za određene komponente certifikacijskog servisa, kao što je IIS (eng. *Internet Information Services*) **poslužitelj**. U sljedećih ćemo nekoliko cjelina instalirati i konfigurirati certifikacijski servis.

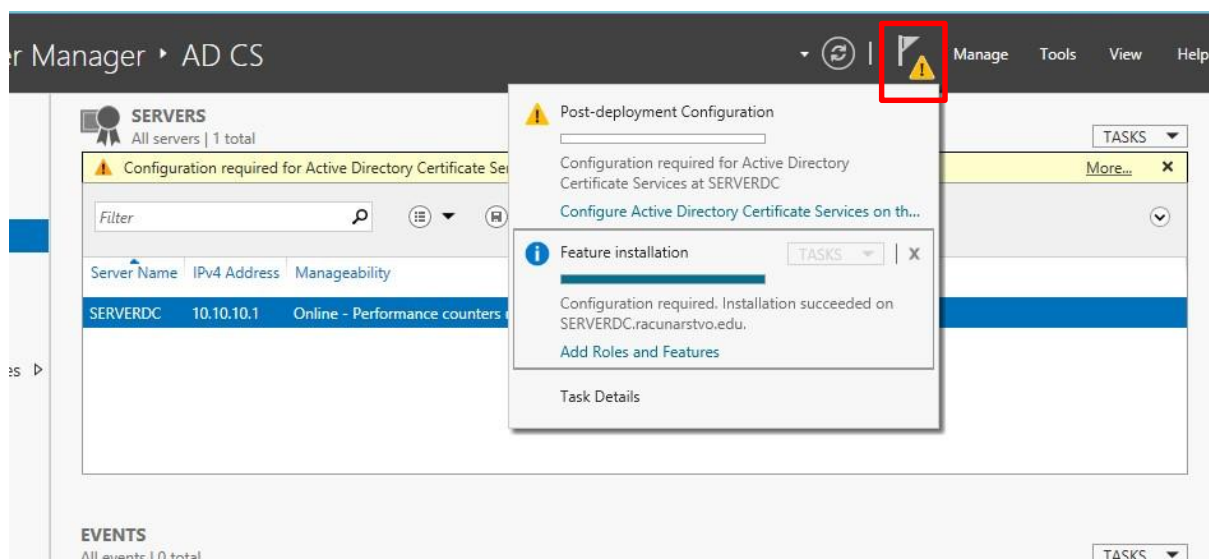
## Instalacija uloge

CA je uloga koju instaliramo preko **Server Manager** konzole. Koristi se klasični čarobnjak (koji smo vidjeli već mnogo puta), a u jednom ćemo trenutku morati instalirati i dodatnu ulogu – IIS poslužitelj. IIS poslužitelj nužan je za *Online Responder* i *Web enrollment* komponente certifikacijskog servisa. Krenimo s instalacijom:

1. Prikažite **Hyper-V Manager** konzolu.
2. Pokrenite virtualno računalo **KZOS-SERVERDC**
3. Prijavite se na računalo **SERVERDC** kao **RACUNARSTVO\Administrator** s lozinkom **Pa\$\$wOrd**
4. Prikažite ekran **Start** i kliknite na **Server Manager**.
5. Prikazuje se **Server Manager** konzola. Kliknite na izbornik **Manage-> Add Roles and Features**.
6. Prikazuje se ekran **Before you begin**. Kliknite gumb **Next**.
7. Prikazuje se ekran **Select installation type**. Ostavite predefinirane opcije i kliknite gumb **Next**.
8. Prikazuje se ekran **Select destination server**. Ostavite predefinirane opcije i kliknite gumb **Next**.
9. Prikazuje se ekran **Select Server Roles**. Označite stavku **Active Directory Certificate Services**.
10. Prikazuje se ekran s informacijom o potrebi instalacije dodatnih komponenti. Kliknite gumb **Add Features**.
11. Vraćate se na ekran **Select server roles**. Kliknite gumb **Next**.
12. Prikazuje se ekran **Select features**. Ostavite predefinirane opcije i kliknite gumb **Next**.
13. Prikazuje se ekran **Active Directory Certificate Services**. Kliknite gumb **Next**.
14. Prikazuje se ekran **Select Role Services**. Označite stavke:
  - a. **Certification Authority**
  - b. **Certification Authority Web Enrollment** (pojavit će se prozor s dodatnim zahtjevima, kliknite gumb **Add Features**)
  - c. **Online Responder** (pojavit će se prozor s dodatnim zahtjevima, kliknite gumb **Add Features**).
15. Prikazuje se ekran **Web Server Role (IIS)**. Kliknite gumb **Next**.
16. Prikazuje se ekran **Select Role Services**. Iz kategorije **Security** označite stavke **Client Certificate Mapping Authentication** i **IIS Client Certificate Mapping Authentication**. Kliknite gumb **Next**.
17. Prikazuje se sažetak odabranih opcija. Kliknite gumb **Install**.
18. Pričekajte završetak instalacije i kliknite gumb **Close**.
19. Ne zatvarajte **Server Manager** konzolu!

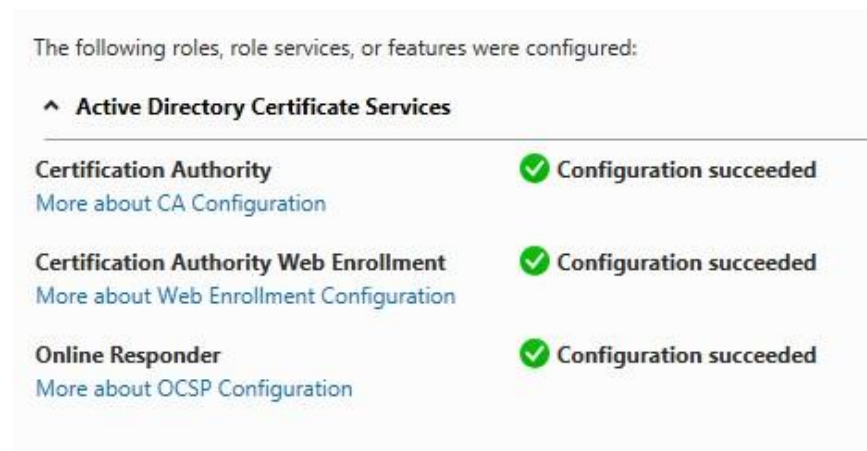
Instalirali smo CA ulogu. Konfigurirat ćemo certifikacijski autoritet:

1. Sa alatne trake **Server Manager** konzole kliknite na ikonu zastavice i iz izbornika odaberite opciju **Configure Active Directory Certificate Services on the destination Server**, kako prikazuje donja slika.



Slika 1 Pristup konfiguracijskom čarobnjaku

2. Prikazuje se **Credentials** ekran. Ostavite predefinirane postavke i kliknite gumb **Next**.
3. Prikazuje se ekran **Role Services**. Označite stavke **Certification Authority**, **Certification Authority Web Enrollment** i **Online Responder**. Kliknite gumb **Next**.
4. Prikazuje se **Setup Type** ekran. Označite opciju **Enterprise CA** i kliknite gumb **Next**.
5. Prikazuje se **CA Type** ekran. Označite opciju **Root CA** i kliknite gumb **Next**.
6. Prikazuje se ekran **Private Key**. Označite opciju **Create a new private key** i kliknite gumb **Next**.
7. Prikazuje se **Configure Cryptography for CA** ekran. Ostavite predefinirane postavke i kliknite gumb **Next**.
8. Prikazuje se **Configure CA Name** ekran. U polje **Common name for this CA** upišite **SERVERDC-CA** i kliknite gumb **Next**.
9. Prikazuje se **Validity Period** ekran. Ostavite predefinirane postavke i kliknite gumb **Next**.
10. Prikazuje se **Configure Certificate Database** ekran. Ostavite predefinirane postavke i kliknite gumb **Next**.
11. Prikazuje se ekran sa sažetkom odabranih opcija. Kliknite gumb **Configure** i pričekajte kraj konfiguracije. Konfiguracija se mora izvršiti bez pogrešaka, kao na donjoj slici.





## Slika 2 Početna konfiguracija CA

12. Kliknite gumb **Close** i zatvorite **Server Manager** konzolu.

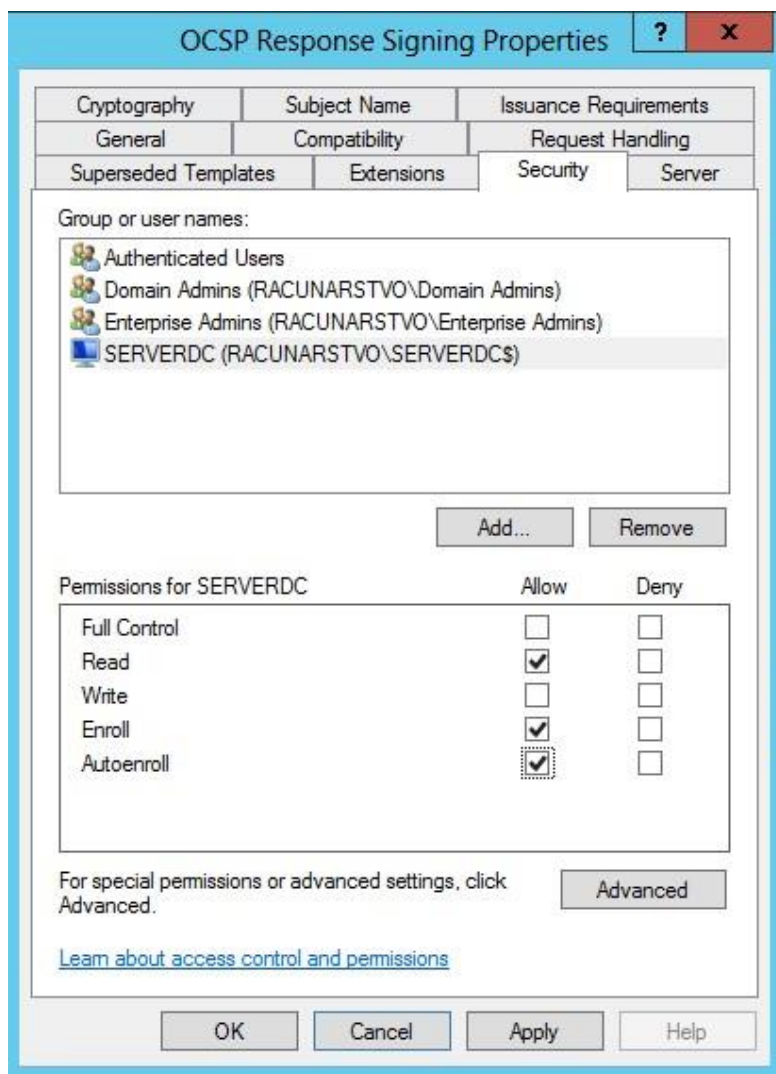
U nastavku vježbe ćemo konfigurirati predloške, *online responder* i IIS poslužitelj.

### Online responder

*Online responder* klijentima će pružiti informacije o opozvanim certifikatima na osnovi CRL liste. Odgovori koji se šalju klijentu moraju biti potpisani certifikatom. Izdat ćemo ga na temelju predloška za OCSP protokol.

1. Prikažite ekran **Start** i kliknite na **Certification Authority**.
2. Prikazuje se **Certification Authority** konzola. Unutar lijevog okna proširite poslužitelj **SERVERDC-CA**.
3. Desnim gumbom miša kliknite na **Certificate Templates** mapu i iz kontekstualnog izbornika odaberite opciju **Manage**.
4. Prikazuje se **Certificate Templates** konzola. Desnim gumbom miša kliknite na **OCSP Response Signing** predložak i iz kontekstualnog izbornika odaberite opciju **Properties**.
5. Prikazuje se **OCSP Response Signing Properties** ekran. Kliknite na karticu **Security**.
6. Kliknite gumb **Add**.
7. Prikazuje se ekran za odabir objekata. Kliknite gumb **Object Types**.
8. Prikazuje se ekran **Object Types**. Označite stavku **Computers** i kliknite **OK**.
9. Vraćate se na ekran za odabir objekata. U polje **Enter the object names to select** upišite **SERVERDC** i kliknite gumb **OK**.
10. Vraćate se na **OCSP Response Signing Properties** ekran. Dodijelite dozvole **Enroll** i **Autoenroll**, kao što je prikazano na sljedećoj slici.





Slika 3. Dozvole računala SERVERDC

11. Kliknite gumb **OK** i zatvorite **Certificate Templates** konzolu.
12. Prikažite **Certification Authority** konzolu.
13. Unutar lijevog okna desnim gumbom miša kliknite na **Certificate Templates** mapu i iz kontekstualnog izbornika odaberite **New-> Certificate Template to Issue**.
14. Označite predložak **OCSP Response Signing** i kliknite gumb **OK**.
15. Ne zatvarajte **Certification Authority** konzolu!

### Certifikat za IIS poslužitelj

IIS poslužitelj na kojem se nalazi *online responder* također mora imati odgovarajući certifikat. Kao i u prethodnom slučaju, izdajemo ga na osnovi predloška. Predložak najprije moramo konfigurirati.

1. Unutar lijevog okna desnim gumbom miša kliknite na **Certificate Templates** mapu i iz kontekstualnog izbornika odaberite opciju **Manage**.
2. Prikazuje se **Certificate Templates** konzola. Desnim gumbom miša kliknite na **Web Server** i iz kontekstualnog izbornika odaberite opciju **Properties**.
3. Prikazuje se **Web Server Properties** ekran. Kliknite na karticu **Security**.



4. Kliknite gumb **Add**.
5. Prikazuje se ekran za odabir objekata. Kliknite gumb **Object Types**.
6. Prikazuje se **Object Types** ekran. Označite stavku **Computers** i kliknite **OK**.
7. Vraćate se na ekran za odabir objekata. U polje **Enter the object names to select** upišite **SERVERDC** i kliknite gumb **OK**.
8. Dodijelite dozvolu **Enroll** i kliknite gumb **OK**.
9. Vraćate se u **Certificate Templates** konzolu. Desnim gumbom miša kliknite na **Web Server** predložak i iz kontekstualnog izbornika odaberite opciju **Duplicate Template**.
10. Prikazuje se **Properties of New Template** ekran. Kliknite na karticu **General** i u polje **Template display name** upišite **SERVERDC-IIS-CERT**.
11. Označite opciju **Publish certificate in Active Directory** i kliknite gumb **Apply**.
12. Kliknite na karticu **Security**.
13. U kategoriji **Group or user names** označite računalo **SERVERDC**.
14. Dodijelite dozvole **Enroll** i **Autoenroll** i kliknite gumb **Apply**.
15. Kliknite na karticu **Superseded Templates**.
16. Kliknite gumb **Add**.
17. Prikazuje se **Add Superseded Template** ekran. Označite **Web Server** predložak i kliknite gumb **OK**.
18. Vraćate se na ekran **Properties of New Template**. Kliknite gumb **OK** i zatvorite **Certificate Templates** konzolu.

Zatim izdajemo predložak.

1. Prikažite **Certification Authority** konzolu.
2. Unutar lijevog okna desnim gumbom miša kliknite na **Certificate Templates** mapu i iz kontekstualnog izbornika odaberite **New-> Certificate Template to Issue**.
3. Prikazuje se ekran **Enable Certificate Templates**. Označite predložak **SERVERDC-IIS-CERT** i kliknite gumb **OK**.
4. Minimizirajte **Certification Authority** konzolu.

Ostatak konfiguracije događa se na IIS poslužitelju.

## IIS konfiguracija

Nakon što smo izradili certifikat, na IIS poslužitelju asociramo ga s odgovarajućim web-servisom. Najprije ćemo izraditi certifikat za cijelu racunarstvo.edu domenu.

1. Prikažite ekran **Start** i kliknite na **Internet Information Services (IIS) Manager**.
2. Prikazuje se **IIS Manager** konzola. Unutar lijevog okna kliknite na **SERVERDC** poslužitelj.
3. U središnjem oknu dvostrukim klikom otvorite **Server Certificates** mapu.
4. U desnom oknu (traka **Actions**) kliknite na opciju **Create Domain Certificate**.
5. Prikazuje se **Distinguished Name Properties** ekran. Popunite podatke o novom certifikatu:
  - a. **Common name:** serverdc.racunarstvo.edu
  - b. **Organization:** racunarstvo.edu

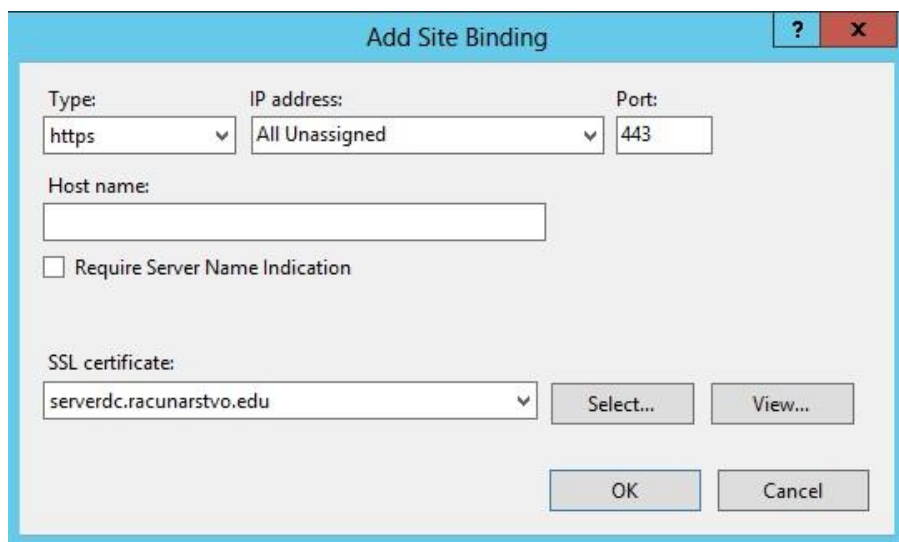


- c. **Organizational Unit:** CoreServeri
  - d. **City/locality:** Zagreb
  - e. **State/province:** Zagreb
  - f. **County/region:** ostavite predefiniranu HR opciju.
6. Kliknite gumb **Next**.
  7. Prikazuje se **Online Certification Authority** ekran. Kliknite gumb **Select**.
  8. Prikazuje se ekran **Select Certification Authority**. Označite **SERVERDC-CA** i kliknite gumb **OK**.
  9. Vraćate se na **Online Certification Authority** ekran. U polje **Friendly name** upišite **serverdc.racunarstvo.edu** i kliknite gumb **Finish**.
  10. Ne zatvarajte **IIS Manager** konzolu!

### SSL kriptiranje veze

Sada uključujemo SSL (eng. *Secure Sockets Layer*) kriptiranje komunikacije za web-servise IIS poslužitelja.

1. Unutar lijevog okna proširite mapu **Sites**.
2. Unutar lijevog okna desnim gumbom miša kliknite na **Default Web Site** i iz kontekstualnog izbornika odaberite opciju **Edit Bindings**.
3. Prikazuje se **Site Bindings** ekran. Kliknite gumb **Add**.
4. Prikazuje se **Add Site Binding** ekran. Postavite opcije:
  - a. **Type:** odaberite vrijednost **https**
  - b. **SSL certificate:** odaberite vrijednost **serverdc.racunarstvo.edu**.
5. Usporedite izgled svog ekrana s onime na donjoj slici.



Slika 4 Odabir certifikata za SSL protokol

6. Kliknite gumb **OK**.
7. Vraćate se na **Site Bindings** ekran. Kliknite gumb **Close**.
8. Vraćate se u **IIS Manager** konzolu. Unutar lijevog okna proširite **Default Web Site** mapu i označite opciju **CertSrv**.
9. U središnjem oknu dvostrukim klikom otvorite stavku **SSL Settings**.



10. Označite opciju **Require SSL**.
11. Vrijednost unutar kategorije **Client Certificates** postavite na **Require**.
12. Unutar desnog okna kliknite na opciju **Apply**.
13. Zatvorite **IIS Manager** konzolu.

## Konfiguracija mehanizma za opoziv certifikata

I za kraj osnovne konfiguracije definiramo autoritet koji će opozvati certifikate.

1. Prikažite ekran **Start** i kliknite na **Online Responder Management**.
2. Prikazuje se Online Responder konzola. Unutar lijevog okna desnim gumbom miša kliknite na opciju **Revocation Configuration** i iz kontekstualnog izbornika odaberite opciju **Add Revocation Configuration**.
3. Prikazuje se početni ekran čarobnjaka **Add Revocation Configuration**. Kliknite gumb **Next**.
4. Prikazuje se **Name the Revocation Configuration** ekran. U polje **Name** upišite **SERVERDCCA-REV** i kliknite gumb **Next**.
5. Prikazuje se **Select CA Certificate Location** ekran. Označite opciju **Select a certificate for an Existing enterprise CA** i kliknite gumb **Next**.
6. Prikazuje se **Choose CA Certificate** ekran. Označite opciju **Browse CA certificate published in Active Directory** i kliknite gumb **Browse**.
7. Prikazuje se **Select Certification Authority** ekran. Označite **SERVERDC-CA** i kliknite gumb **OK**.
8. Vraćate se na **Choose CA Certificate** ekran. Kliknite gumb **Next**.
9. Prikazuje se **Select Signing Certificate** ekran. Označite opciju **Automatically select a signing certificate**.
10. Označite opciju **Auto-Enroll for an OCSP signing certificate**. Opcije za CA i predložak postaviti će se same, kao na slici u nastavku. Kliknite gumb **Next**.

The screenshot shows the 'Add Revocation Configuration' wizard window. The title bar says 'Add Revocation Configuration'. The main window has a left sidebar with a tree view containing: 'Getting started with addi...', 'Name the Revocation Co...', 'Select CA Certificate Loca...', 'Choose CA Certificate', 'Select Signing Certificate' (which is highlighted), and 'Revocation Provider'. The main area is titled 'Select Signing Certificate'. It contains the following text: 'Revocation information is signed before it is sent to a client. The Online Responder can select a signing certificate automatically, or you can manually select a signing certificate for each Online Responder.' There are three radio button options: 1. 'Automatically select a signing certificate' (selected), which includes a checked checkbox for 'Auto-Enroll for an OCSP signing certificate'. Below this, there is a text box for 'Certification authority:' containing 'SERVERDC.racunarstvo.edu\SERVERDC-CA' and a 'Browse...' button. There is also a dropdown for 'Certificate Template:' with 'OCSPResponseSigning' selected. 2. 'Manually select a signing certificate' (unselected), with a note: 'Note: You will need to specify a signing certificate for each member in the Online Responder Array.' 3. 'Use the CA certificate for the revocation configuration' (unselected). At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.



#### Slika 5. Opcije opoziva certifikata

11. Prikazuje se **Revocation Provider** ekran. Kliknite gumb **Finish**.
12. Zatvorite **Online Responder Management** konzolu.

Pogledajmo kako izgleda certifikacijski web-servis s klijentske strane.

#### Pristup preko web-servisa

Web-servisu preko kojeg korisnik može zatražiti certifikat pristupamo uz pomoć **https** protokola:

1. Pokrenite virtualno računalo **KZOS-CLI1**.
2. Prijavite se na računalo **CLI1** kao **RACUNARSTVO\marko.tomic** s lozinkom **Pa\$\$w0rd**.
3. Pokrenite **Internet Explorer**. Na poruci o postavkama Internet Explorera kliknite gumb **Ask me later**.
4. Upišite adresu **https://serverdc/certsrv** (svakako upišite punu adresu s oznakom protokola, točno kako piše u ovom koraku).
5. Prikazuje se poruka o neispravnom certifikatu. Kliknite opciju **Continue to this website (not recommended)**.
6. Prikazuje se greška **403: Access Denied**. Korisnik Marko Tomić nema odgovarajući klijentski certifikat za pristup web-servisu. Zatvorite **Internet Explorer**.

#### -----NAPOMENA-----

Greška certifikata u 5. koraku prikazuje se zbog različite web-adrese. Naime, u adresnu traku Internet Explorera upisali ste **https://serverdc/certsrv**, a preusmjereni ste na stranicu čiji je certifikat povezan s adresom **https://serverdc.osmis.edu/certsrv**. Internet Explorer razliku između tražene i stvarne stranice percipira kao pokušaj *phishinga*, tj. preusmjerenja korisnika na lažni web-servis. Kako je riječ o zaštitnom mehanizmu koji mnogo znači za sigurnost korisnika, na Internetu nije ga preporučljivo isključiti. Certifikat smo mogli konfigurirati za obje web-adrese (uz znatno više koraka – u produkcijskom okruženju nebitno). Ako vas greška certifikata smeta, pristupite certifikacijskom web-servisu preko ispravne adrese. Na upit o korisničkom imenu i lozinci unesite podatke s kojima ste se prijavili na virtualno računalo. U ostatku vježbe pretpostavljam da upisujete skraćenu adresu zbog koje se javlja greška o neispravnom certifikatu. Savjetujem da se ne opterećujete pogreškom certifikata (naravno, samo u ovom slučaju).

U idućoj ćemo cjelini vidjeti kako korisnik može zatražiti certifikat.

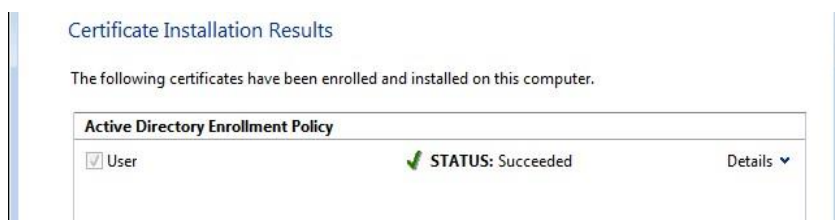
#### Zahtjev za certifikatom

Certifikacijska infrastruktura koju smo do sada implementirali nije praktična. Korisnici će morati ručno zatražiti certifikat kako bi pristupili uslugama koje ih zahtijevaju. Pokažimo postupak iz perspektive korisnika.

1. Prikažite ekran **Start**, upišite **mmc** i pritisnite tipku **Enter**.
2. Prikazuje se **MMC** konzola. Kliknite na izbornik **File-> Add/Remove Snap-In**.



3. Prikazuje se **Add or Remove Snap-ins** ekran. U kategoriji **Available snap-ins** (lijevo okno) označite stavku **Certificates** i kliknite gumb **Add**.
4. Kliknite gumb **OK**.
5. Vraćate se u **MMC** konzolu. Unutar lijevog okna proširite mapu **Certificates**.
6. Unutar lijevog okna desnim gumbom miša kliknite na mapu **Personal** i iz kontekstualnog izbornika kliknite opciju **All Tasks-> Request New Certificate**.
7. Prikazuje se **Certificate Enrollment** čarobnjak. Kliknite gumb **Next**.
8. Prikazuje se **Select Certificate Enrollment Policy** ekran. Kliknite gumb **Next**.
9. Prikazuje se **Request Certificates** ekran. Označite stavku **User** i kliknite gumb **Enroll**.
10. Pričekajte dok se certifikat ne izda. Oznaka statusa mora biti **Succeeded**, kako prikazuje sljedeća slika.

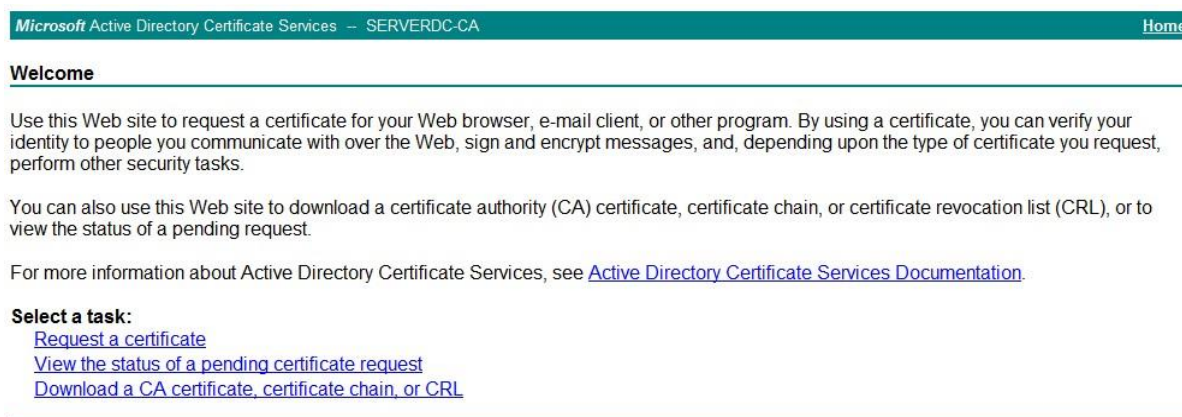


Slika 6. Uspješno izdan certifikat

11. Kliknite gumb **Finish** i zatvorite **MMC** konzolu. Ne spremajte izmjene u MMC konzolu.

Provjerimo može li Marko sada pristupiti web-servisu za certifikate:

1. Pokrenite **Internet Explorer** i upišite adresu **https://serverdc/certsrv** (svakako upišite punu adresu s oznakom protokola, točno kako piše u ovom koraku).
2. Prikazuje se greška o neispravnom certifikatu. Kliknite opciju **Continue to this website (not recommended)**.
3. Prikazuje se naslovna stranica certifikacijskog web sučelja:



Slika 7. Web-sučelje certifikacijskog servisa

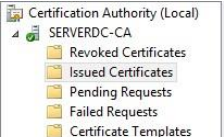
4. Iz ovog sučelja korisnici mogu zatražiti dodatne certifikate (npr. za enkripciju datotečnog sustava, e-poštu...), provjeriti status zahtjeva za izdavanje certifikata i sl.
5. Zatvorite **Internet Explorer** i sve otvorene prozore na računalu **CLI1**.



## Opoziv certifikata

Izdani certifikat možemo opozvati. Time ga dodajemo na CRL popis. Pokažimo kako!

1. Prebacite se na računalo **SERVERDC** i prikažite **Certificate Authority** konzolu.
2. Unutar lijevog okna kliknite na mapu **Issued Certificates**. U desnom se oknu prikazuju svi izdani certifikati. Uočite certifikat izdan za korisnika Marka Tomića kako prikazuje slika u nastavku:



Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiration Date
2	RACUNARSTVO\Administrator	-----BEGIN CERTI...	Web Server (WebSer...	75000000027e1...	3.6.2014. 16:41	2.6.2016. 16:41
3	RACUNARSTVO\SERVERDCS	-----BEGIN CERTI...	OCSP Response Sign...	750000000393d...	3.6.2014. 16:49	17.6.2014. 16:49
4	RACUNARSTVO\SERVERDCS	-----BEGIN CERTI...	Domain Controller (m...	7500000004dfc...	3.6.2014. 16:55	3.6.2015. 16:55
5	RACUNARSTVO\marko.tomic	-----BEGIN CERTI...	User (User)	7500000005541...	3.6.2014. 16:57	3.6.2015. 16:57

Slika 8. Certifikat za Marka Tomića

3. Desnim gumbom miša kliknite na certifikat izdan za Marka Tomića i iz kontekstualnog izbornika kliknite **All Tasks-> Revoke Certificate**.
4. Prikazuje se **Certificate Revocation** ekran. Iz izbornika **Reason Code** odaberite opciju **Certificate Hold** i kliknite gumb **Yes**.
5. Ne zatvarajte **Certificate Authority** konzolu!

### -----NAPOMENA-----

**Certificate Hold** jedini je razlog opoziva certifikata koji možete poništiti (naravno, sve dok certifikat ne istekne). Koristi se kada niste sigurni je li integritet certifikata zaista narušen pa ga stavljate „na mirovanje“ dok ne istražite situaciju.

Opozvani certifikat neće odmah biti dojavljen ostalim računalima. Ipak, postupak objave popisa opozvanih certifikata možemo ubrzati na sljedeći način.

1. Unutar lijevog okna desnim gumbom miša kliknite na mapu **Revoked Certificates** i kliknite **All Tasks-> Publish**.
2. Prikazuje se **Publish CRL** ekran. Označite opciju **Delta CRL only** i kliknite gumb **OK**.

Provjerimo je li informacija o isteklom certifikatu registrirana.

1. Prebacite se na računalo **CLI1**.
2. Pokrenite **Internet Explorer** i upišite adresu **https://serverdc/certsrv** (svakako upišite punu adresu s oznakom protokola, točno kako piše u ovom koraku).
3. Prikazuje se greška o neispravnom certifikatu. Kliknite opciju **Continue to this website (not recommended)**.
4. Prikazuje se greška **403: Access Denied**. Marko nema ispravan certifikat i ne može pristupiti web-servisu dok ne zatraži novi ili mu administrator ne poništi opoziv starog.
5. Zatvorite sve prozore na računalo **CLI1** i odjavite se s istog.



Na kraju ovog dijela vježbe poništimo opoziv certifikata.

1. Prebacite se na računalo **SERVERDC** i prikažite **Certificate Authority** konzolu.
2. Unutar lijevog okna kliknite na mapu **Revoked Certificates**.
3. U desnom oknu desnim gumbom miša kliknite na certifikat za Marka Tomića i iz kontekstualnog izbornika odaberite opciju **All Tasks-> Unrevoke Certificate**.
4. Unutar lijevog okna desnim gumbom miša kliknite na mapu **Revoked Certificates** i kliknite **All Tasks-> Publish**.
5. Prikazuje se ekran **Publish CRL**. Označite opciju **Delta CRL only** i kliknite gumb **OK**.
6. Ne zatvarajte **Certification Authority** konzolu!

Ovime je Markov certifikat ponovno valjan i on opet može pristupiti web-servisu. U nastavku vježbe konfigurirat ćemo praktičniji način izdavanja certifikata.

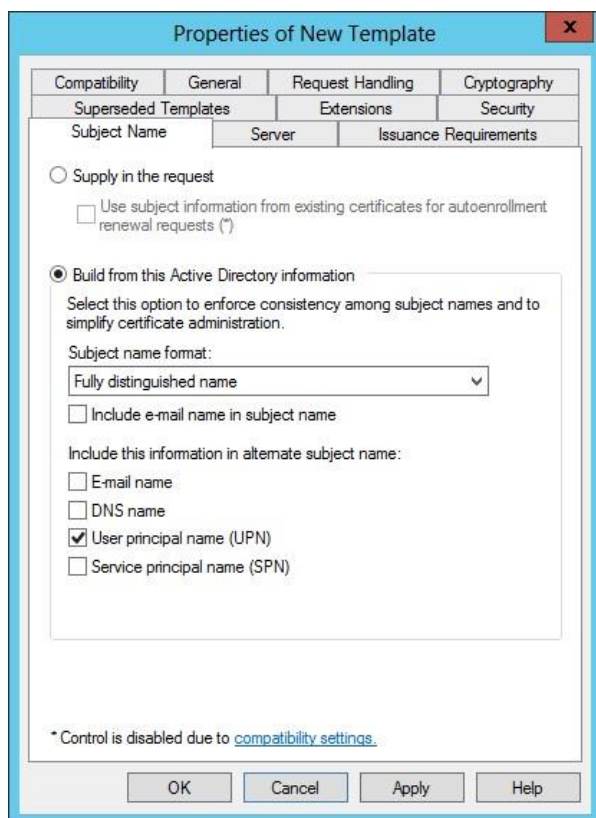
## Automatsko izdavanje certifikata

Način izdavanja certifikata koji smo do sad implementirali prilično je nepraktičan. Naime, korisnik mora ručno zatražiti certifikat preko MMC konzole. Nama je korištenje MMC konzolom već postalo prirodno, ali budite sigurni da prosječni korisnik neće razumjeti rečenicu: „Samo zatraži klijentski certifikat preko *Certificates snap-ina* u MMC konzoli, u čemu je problem?“

Kada tu rečenicu ponovite petom ili desetom korisniku, shvatit ćete da mora postojati jednostavniji način. I postoji – pokažimo kako konfigurirati **automatsko izdavanje certifikata** (eng. *Autoenroll*) korisnicima i računalima. Kao i kod web-poslužitelja, najprije konfiguriramo odgovarajući predložak:

1. Unutar lijevog okna desnim gumbom miša kliknite na mapu **Certificate Templates** i iz kontekstualnog izbornika odaberite opciju **Manage**.
2. Prikazuje se **Certificate Templates** konzola. Desnim gumbom miša kliknite na predložak **User** i iz kontekstualnog izbornika odaberite opciju **Duplicate Template**.
3. Prikazuje se **Properties of New Template** ekran. Kliknite na karticu **General**.
4. U polje **Template display name** upišite **OSMIS korisnici**.
5. Označite opciju **Publish certificate in Active Directory** i kliknite gumb **Apply**.
6. Kliknite na karticu **Security**.
7. U kategoriji **Group or user names** označite grupu **Domain Users**.
8. Dodijelite dozvole **Enroll** i **Autoenroll** i kliknite gumb **Apply**.
9. Kliknite na karticu **Subject Name**.
10. Isključite opcije **Include e-mail name in subject name** i **E-mail name**, kako prikazuje donja slika.





Slika 9. Postavke novog predloška

11. Kliknite gumb **OK**.

Istim postupkom izrađujemo predložak za računala.

1. Desnim gumbom miša kliknite na predložak **Computer** i iz kontekstualnog izbornika odaberite opciju **Duplicate Template**.
2. Prikazuje se **Properties of New Template** ekran. Kliknite na karticu **General**.
3. U polje **Template display name** upišite **OSMIS racunala**.
4. Označite opciju **Publish certificate in Active Directory** i kliknite gumb **Apply**.
5. Kliknite na karticu **Security**.
6. U kategoriji **Group or user names** označite grupu **Domain Computers**.
7. Dodijelite dozvole **Enroll** i **Autoenroll** i kliknite gumb **OK**.
8. Zatvorite **Certificate Templates** konzolu.

Zatim izdajemo stvorene predloške.

1. Prikažite **Certification Authority** konzolu.
2. Unutar lijevog okna desnim gumbom miša kliknite na mapu **Certificate Templates** i iz kontekstualnog izbornika odaberite **New-> Certificate Template to Issue**.
3. Prikazuje se **Enable Certificate Templates** ekran. Označite predložak **OSMIS korisnici** i kliknite gumb **OK**.
4. Unutar lijevog okna desnim gumbom miša kliknite na mapu **Certificate Templates** i iz kontekstualnog izbornika odaberite **New-> Certificate Template to Issue**.



5. Prikazuje se **Enable Certificate Templates** ekran. Označite predložak **OSMIS racunala** i kliknite gumb **OK**.
6. Minimizirajte **Certification Authority** konzolu.

Stvorene ćemo predloške preko Group Policyja povezati s korisnicima i računalima.

1. Prikažite ekran **Start** i kliknite na **Group Policy Management**.
2. Prikazuje se **Group Policy Management** konzola. Unutar lijevog okna proširite mapu **Forest: racunarstvo.edu-> Domains-> racunarstvo.edu**.
3. Unutar lijevog okna desnim gumbom miša kliknite na domenu racunarstvo.edu i iz kontekstualnog izbornika izaberite opciju **Create a GPO in this domain, and Link it here...**
4. Prikazuje se **New GPO** ekran. U polje **Name** upišite **Certifikati** i kliknite gumb **OK**.
5. Unutar lijevog okna desnim gumbom miša kliknite na GPO **Certifikati** i iz kontekstualnog izbornika odaberite opciju **Edit**.
6. Prikazuje se **Group Policy Management Editor** konzola. Proširite mapu **Computer Configuration-> Policies-> Windows Settings-> Security Settings-> Public Key Policies**.
7. U desnom oknu dvostrukim klikom otvorite stavku **Certificate Services Client – Auto – Enrollment**.
8. Prikazuje se **Certificate Services Client Properties** ekran. Postavite vrijednosti:
  - a. **Configuration Model**: odaberite opciju **Enabled**
  - b. uključite opciju **Renew expired certificates, update pending certificates, and remove revoked certificates**
  - c. uključite opciju **Update certificates that use certificate templates**.
9. Kliknite gumb **OK**.
10. Unutar lijevog okna proširite mapu **User Configuration-> Policies-> Windows Settings-> Security Settings-> Public Key Policies**.
11. U desnom oknu dvostrukim klikom otvorite stavku **Certificate Services Client – Auto – Enrollment**.
12. Prikazuje se ekran **Certificate Services Client Properties**. Postavite vrijednosti:
  - a. **Configuration Model**: odaberite opciju **Enabled**
  - b. uključite opciju **Renew expired certificates, update pending certificates, and remove revoked certificates**
  - c. uključite opciju **Update certificates that use certificate templates**.
13. Kliknite gumb **OK**.
14. Zatvorite sve otvorene prozore na računalu **SERVERDC**.
15. Pokrenite **Command Prompt**.
16. Upišite naredbu **gpupdate /force**.
17. OPCIONALNO: Na pitanje o odjavi korisnika pritisnite **Y** i ponovno se prijavite kao **RACUNARSTVO\administrator** s lozinkom **Pa\$\$w0rd** Pogledajmo kako funkcionira izdavanje certifikata s korisničke strane.



1. Prebacite se na računalo **CLI1**.
2. Prijavite se na računalo **CLI1** kao **RACUNARSTVO\ana.ivic** s lozinkom **Pa\$\$w0rd**.
3. Pokrenite **Command Prompt** i upišite naredbu **gpubdate /force**.
4. OPCIONALNO: Na pitanje o odjavi korisnika pritisnite **Y** i ponovno se prijavite kao **RACUNARSTVO\ana.ivic** s lozinkom **Pa\$\$w0rd**.
5. Pokrenite **Internet Explorer** i upišite adresu **https://serverdc/certsrv** (svakako upišite punu adresu s oznakom protokola, točno kako piše u ovom koraku).
6. Prikazuje se poruka o neispravnom certifikatu. Kliknite opciju **Continue to this website (not recommended)**.
7. Prikazuje se naslovna stranica certifikacijskog web-sučelja. Ani je uspješno izdan certifikat.
8. Zatvorite sve otvorene prozore na računalu **CLI1**.

## Enkripcija na razini datotečnog sustava

U sljedećim ćemo cjelinama konfigurirati metodu povrata kriptiranih podataka – **EFS Recovery Agent**. Kao što je opisano u uvodu, EFS Recovery Agent apsolutno je nužan u okruženju u kojem korisnici imaju mogućnost enkripcije podataka (ova se opcija može isključiti preko Group Policyja). Najprije izradimo dijeljenu mapu u koju korisnici spremaju podatke.

1. Prebacite se na računalo **SERVERDC**.
2. U korijenskoj mapi diska **C** izradite mapu **EFS**.
3. Desnim gumbom miša kliknite na mapu **EFS** i iz kontekstualnog izbornika odaberite opciju **Properties**.
4. Prikazuje se **EFS Properties** ekran. Kliknite na karticu **Sharing** i zatim kliknite gumb **Advanced Sharing**.
5. Prikazuje se **Advanced Sharing** ekran. Označite opciju **Share this folder** i kliknite gumb **Permissions**.
6. Prikazuje se **Permissions for EFS** ekran. Grupi **Everyone** dodijelite **Full Control** dozvolu i kliknite gumb **OK**.
7. Vraćate se na **Advanced Sharing** ekran. Kliknite gumb **OK** i zatim gumb **Close**.
8. Zatvorite sve otvorene prozore na računalu **SERVERDC**.

Sada konfiguriramo račun za povrat podataka – EFS Recovery Agent.

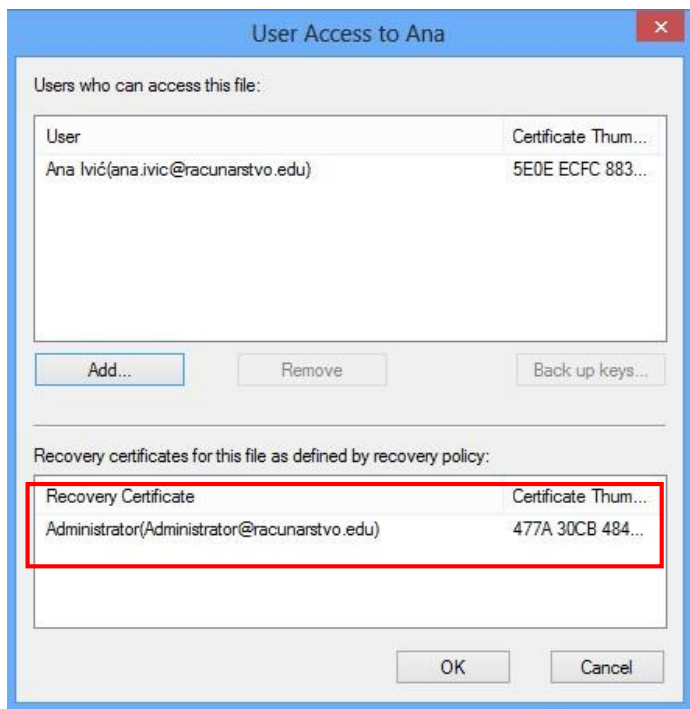
1. Prikažite ekran **Start** i kliknite na **Group Policy Management**.
2. Prikazuje se **Group Policy Management** konzola. Unutar lijevog okna proširite mape **Forest: racunarstvo.edu-> Domains-> racunarstvo.edu**.
3. Unutar lijevog okna desnim gumbom miša kliknite na GPO **Certifikati** i iz kontekstualnog izbornika odaberite opciju **Edit**.
4. Prikazuje se **Group Policy Management Editor** konzola. Proširite mapu **Computer Configuration-> Policies-> Windows Settings-> Security Settings-> Public Key Policies**.



5. Unutar desnog okna desnim gumbom miša kliknite na mapu **Encrypting File System** i iz kontekstualnog izbornika odaberite opciju **Create Data Recovery Agent**.
6. Otvorite mapu **Encrypting File System** i uočite da sadrži certifikat za korisnika **RACUNARSTVO\Administrator**.
7. Zatvorite sve otvorene prozore na računalu **SERVERDC**.
8. Pokrenite **Command Prompt** i upišite naredbu **gpupdate /force**.
9. OPCIONALNO: Na pitanje o odjavi korisnika pritisnite Y i ponovno se prijavite kao **RACUNARSTVO\administrator** s lozinkom **Pa\$\$w0rd**

Sada možemo uključiti enkripciju.

1. Prebacite se na računalu **CLI1** i otvorite **Command Prompt**.
2. Upišite naredbu **net use Z: \\SERVERDC\EFS**.
3. Zatvorite **Command Prompt**.
4. Otvorite lokaciju **Computer** i zatim otvorite mrežni disk **EFS**. U njemu izradite mapu **Ana**.
5. Unutar mape **Ana** izradite novu tekstualnu datoteku imena **Ana.txt** sa sadržajem **Tajni tekst**.
6. Vratite se u korijensku mapu mrežnog diska Z:.
7. Desnim gumbom miša kliknite na mapu **Ana** i iz kontekstualnog izbornika odaberite opciju **Properties**.
8. Prikazuje se **Ana Properties** ekran. Kliknite na karticu **General** i zatim kliknite gumb **Advanced**.
9. Prikazuje se **Advanced Attributes** ekran. Označite opciju **Encrypt contents to secure data** i kliknite gumb **OK**.
10. Vraćate se na **Ana Properties** ekran. Kliknite gumb **OK**.
11. Prikazuje se **Confirm Attribute Changes** ekran. Označite opciju **Apply changes to this folder, subfolders and files** i kliknite gumb **OK**.
12. Uočite da je mapa Ana promijenila boju u **zelenu**. Otvorite mapu **Ana**.
13. Desnim gumbom miša kliknite na datoteku **Ana.txt** i iz kontekstualnog izbornika odaberite opciju **Properties**.
14. Prikazuje se **Ana Properties** ekran. Kliknite na karticu **General** i zatim kliknite gumb **Advanced**.
15. Prikazuje se **Advanced Attributes** ekran. Kliknite gumb **Details**.
16. Prikazuje se **User Access to Ana** ekran. Uočite da je u kategoriji **Recovery certificates for this file as defined by recovery policy** certifikat za korisnika **RACUNARSTVO\Administrator**, kao na slici u nastavku.



Slika 10. EFS Recovery certifikat

17. Kliknite gumb **Cancel** i zatvorite sve prozore na računalu **CLI1**.

Budući da je korisnik **RACUNARSTVO\Administrator** definiran kao Recovery Agent, on mora moći dekriptirati Aninu datoteku. Provjerimo je li to zaista točno.

1. Prebacite se na računalu **SERVERDC**.
2. Otvorite mapu **C:\EFS**. Desnim gumbom miša kliknite na mapu Ana i iz kontekstualnog izbornika odaberite opciju **Properties**.
3. Prikazuje se **Ana Properties** ekran. Kliknite na karticu **General** i zatim kliknite gumb **Advanced**.
4. Prikazuje se **Advanced Atributes** ekran. Isključite opciju **Encrypt contents to secure data** i kliknite gumb **OK**.
5. Vraćate se na **Ana Properties** ekran. Kliknite gumb **OK**. Prikazuje se ekran **Confirm Attribute Changes**.
6. Označite opciju **Apply changes to this folder, subfolders and files** i kliknite gumb **OK**.
7. Uočite da mapa Ana više nije obojena zeleno.

-----NAPOMENA-----

Naravno, korisnik **RACUNARSTVO\Administrator** ima mogućnost dekripcije podataka bilo kojeg korisnika u domeni.



## Pričuvne kopije i oporavak

Kao i kod ostalih uloga do sada (npr. AD i DHCP), potrebno je redovito izrađivati pričuvnu kopiju baze certifikata kako bismo mogli oporaviti servis u slučaju kvara poslužitelja. Mi ćemo pričuvnu kopiju izraditi na računalu SERVERDC. Naravno, u produkcijskom ćete okruženju pričuvnu kopiju pohraniti na drugu lokaciju. Za kraj vježbe pokažimo postupak izrade pričuvne kopije.

1. Otvorite **Windows Explorer** i u korijenskoj mapi diska **C** izradite novu mapu imena **BackupCA**.
2. Prikažite ekran **Start** i kliknite na **Certification Authority**.
3. Prikazuje se **Certification Authority** konzola. Unutar lijevog okna desnim gumbom miša kliknite na **SERVERDC-CA** i iz kontekstualnog izbornika odaberite **All Tasks-> Backup CA**
4. Prikazuje se **Certification Authority Backup** čarobnjak. Kliknite gumb **Next**.
5. Prikazuje se **Items to Back Up** ekran. Postavite opcije:
  - a. označite **Private key and CA certificate**
  - b. označite **Certificate database and certificate database log** (opcija **Perform incremental backup** je nedostupna jer izrađujemo prvu ikad pričuvnu kopiju)
  - c. kliknite gumb **Browse** i označite mapu **C:\BackupCA**
6. kliknite gumb **Next**.
7. Prikazuje se **Select a Password** ekran. U oba polja upišite lozinku **Pa\$\$w0rd** i kliknite gumb **Next**.
8. Prikazuje se ekran sa sažetkom odabranih opcija. Kliknite gumb **Finish**.
9. Ne zatvarajte **Certification Authority** konzolu!

Povrat iz pričuvne kopije je jednostavan.

1. Unutar lijevog okna desnim gumbom miša kliknite na **SERVERDC-CA** i iz kontekstualnog izbornika odaberite **All Tasks-> Restore CA**.
2. Na ekranu s porukom o zaustavljanju certifikacijskih servisa kliknite **OK**.
3. Prikazuje se **Certification Authority Restore** čarobnjak. Kliknite gumb **Next**.
4. Prikazuje se **Items to Restore** ekran. Postavite opcije:
  - a. označite **Private key and CA certificate**
  - b. označite **Certificate database and certificate database log**
  - c. kliknite gumb **Browse** i označite mapu **BackupCA**.
5. Kliknite gumb **Next**.
6. Prikazuje se **Provide Password** ekran. Upišite lozinku **Pa\$\$w0rd** i kliknite gumb **Next**.
7. Prikazuje se sažetak odabranih opcija. Kliknite gumb **Finish**.
8. Na ekranu s porukom o pokretanju certifikacijskih servisa kliknite gumb **Yes**.
9. Zatvorite sve prikazane prozore na računalu **SERVERDC**.

Ovime završava današnja vježba. Sada izradite *snapshot* kako je opisano u cjelini **Rezultat vježbe**. Tek ćete nakon toga popuniti izvještaj.





## Rezultat vježbe

Rezultat današnje vježbe jesu instalirani certifikacijski servisi na računalu SERVERDC. Slijedi sažeti prikaz postavljenih opcija.

- Jedan *Enterprise RootCA* poslužitelj
- *Online Responder* s autoritetom za opoziv SERVERDC-CA-REV
- Web-servis konfiguriran za pristup s klijentskim certifikatima
- Domenski certifikat za domenu racunarstvo.edu
- Automatsko izdavanje certifikata računalima i korisnicima
- EFS Recovery Agent je račun RACUNARSTVO\Administrator

Današnja vježba zahtijeva *snapshot*. Izradite ga pomno prateći sljedeće korake.

1. Prebacite se na računalo **CLI1** i zatvorite sve prikazane prozore.
2. Računalo **CLI1** isključite regularnim putem (**Shut Down** izbornik unutar virtualnog računala).
3. Pokrenite računalo **SERVER1** i prijavite se kao **RACUNARSTVO\Admin1** s lozinkom **Pa\$\$w0rd** (ovo radimo kako bi se računalu SERVER1 i korisniku Admin1 izdali certifikati).
4. Računalo **SERVER1** isključite regularnim putem (**Shut Down** izbornik unutar virtualnog računala).
5. Prebacite se na računalo **SERVERDC** i zatvorite sve prikazane prozore.
6. Računalo **SERVERDC** isključite regularnim putem (**Shut Down** izbornik unutar virtualnog računala).
7. Prebacite se na **Hyper-V Manager** konzolu.
8. Istodobno označite sva tri računala.
9. Desnim gumbom miša kliknite na bilo koje od označenih računala i iz kontekstualnog izbornika odaberite opciju **Checkpoint**.
10. Pričekajte dok se *Checkpointi* ne izrade (pratite napredak u stupcu **Status**).
11. **OBAVEZNO** preimenujte *Checkpointe* na **LAB8 – Vaše ime i prezime – (DATUM i VRIJEME)**

Sad krenite s popunjavanjem izvještaja o vježbi.



## Što treba znati nakon ove vježbe?

1. Instalirati AD certifikacijske servise (Online responder, RootCA, opoziv)
2. Konfigurirati predloške
3. Konfigurirati automatsko izdavanje certifikata
4. Opozvati certifikat
5. Konfigurirati bilo koji korisnički račun kao EFS Recovery Agent
6. Izraditi pričuvnu kopiju certifikacijske baze

## Dodatna literatura

- Dio Technet dokumentacije za CS. Preporučujem barem ovo pročitati prije implementacije CS-a u produkcijskom okruženju:

[http://technet.microsoft.com/en-us/library/cc728203\(v=ws.10\)](http://technet.microsoft.com/en-us/library/cc728203(v=ws.10))

- Zanimljiv vodič (tutorial) za implementaciju hijerarhijskog CS okruženja s jednim *offline* RootCA poslužiteljem i *online* CA poslužiteljem:

<http://itbloggen.se/cs/blogs/kristoferohman/archive/2009/04/24/setting-up-a-tier-2-pki>  
<http://itbloggen.se/cs/blogs/kristoferohman/archive/2009/04/24/setting-up-a-tier-2-pki-structure.aspx>

- Zanimljiva rasprava o posljedicama instalacije AD CS-a na domenski kontroler:

<http://social.technet.microsoft.com/Forums/en-US/winserverDS/thread/ce9df65f-cf58-4c84-a969>  
<http://social.technet.microsoft.com/Forums/en-US/winserverDS/thread/ce9df65f-cf58-4c84-a969-3cd67d1c00423cd67d1c0042>