

Implementacija bezbednosnog rešenja u okviru školskog centra kompanije CPU d.o.o.

– Diplomski rad –

Mentor:

doc. dr Aleksandar Jevremović

Student:

Ljubomir Ivaniš

Broj indeksa:

2011/202218

Beograd, 2013.

IZJAVA O VALIDNOSTI AKADEMSKOG RADA

Ime i prezime Ljubomir Ivaniš
Broj indeksa 2011/202218
Naslov rada Implementacija bezbednosnog rešenja u okviru školskog centra
 kompanije CPU d.o.o.
Mentor doc. dr Aleksandar Jevremović
Datum predaje rada _____

Izjava o akademskoj validnosti

Izjavljujem da u priženom akademskom radu nisam predstavio niti pokušao da predstavim tuđi rad kao svoj, osim na mestima na kojima je to izričito naglašeno. Jasno mi je da bi takvo postupanje bilo jednako plagijat, čemu se Fakultet/Univerzitet javno izjasnio. Razumem da čaju slintelektualne dela mogu biti ačizbas Fakulteta/Univerziteta, te da sam dužan da budem upoznat sa fakultetskim/univerzitetskim propisima o plagijatu.

Ovim potvrđujem svoju aglasnost da Fakultet/Univerzitet ima pravo da raspože mojim radom u bilo kojoj formi; Fakultet/Univerzitet ima pravo da konsultuje i tre stranu (koja se može nalaziti unutar ili izvan Srbije) kako bi se ustanovi lo moguće kršenje propisa i proverilo da li moj rad sadimaterijal koji je plagijat, kao i da bi se utvrdio autorski kvalitet rada.

Upoznat sam sa pravnim posledicama koje su propisane za predaju akademskog rada sa zakšnenjem. Izjavljujem da sam sagl asan da Fakultet može da zadži moj diplomski rad, magistarski rad, odnosno doktorat, do daljeg. Seminarski radovi se vraju studentima.

Potpis studenta _____

Overava studentska služba _____

Datum _____

Implementacija bezbednosnog rešenja u okviru školskog centra kompanije CPU d.o.o.

Sažetak:

U ovom radu opisan je projekat implementacije rešenja bezbedne komunikacije kreirane u okviru školskog centra kompanije CPU d.o.o., koji se sastoji iz više delova. Svaki od ovih segmenata sadrži određen broj elemenata koji se instaliraju i konfigurišu u fazama. U ovom radu opisana su objašnjenja i procedure konfiguracije instalacija. Ove procedure i bezbednosne mere oslanjaju se na iskustva stečena tokom implementacije projekta **.RS** domen.

Ključne reči: *Microsoft, AD, DC, DNS, IPSec, Firewall, grupne polise*

Implementing security solutions for CPU Ltd. Learning Center

Abstract:

This paper describes solutions implementation project designed to secure communications within the CPU Ltd. Learning Center, which consists of several parts. Each section contains a number of elements that are installed and configured in stages. This paper contains configuration procedures of installations with explanations. These procedures and security measures rely on experiences gained during implementation of the **.RS** domain project.

Keywords: Microsoft, AD, DC, DNS, IPSec, Firewall, group policy

SADRŽAJ

1.	UVOD.....	- 1 -
1.1.	Kratak opis projekta i angažovanja	- 1 -
2.	Osnovni postulati aktivnog direktorijuma.....	- 3 -
2.1.	Odabir <i>Namespace</i> hijerarhije	- 3 -
2.2.	Odabir broja domena	- 5 -
2.3.	Odabir tipa instalacije domenskih kontrolera	- 6 -
3.	Postupak instalacije AD-a.....	- 7 -
4.	Kreiranje hijerarhije CA (<i>Certification Authority</i>).....	- 11 -
4.1.	Osnovna podela CA servera	- 13 -
4.2.	Procedura instalacije CA	- 15 -
4.3.	Instalacija <i>Subordinate</i> CA servera.....	- 20 -
5.	Automatska distribucija sertifikata računarima neophodnih za IPSec komunikaciju.....	- 26 -
6.	Konfiguracija i implementacija bezbednosnih IPSec polisa	- 28 -
7.	Konfiguracija WEB servisa za bezbednu komunikaciju.....	- 36 -
8.	Bezbedna komunikacija DNS servisa.....	- 40 -
8.1.	Primer zaštite DNS-a uz pomoć zaštite DNS keša od promena.....	- 40 -
8.2.	Zaštita DNS-a slučajnim izborom portova za odgovor klijentu.....	- 41 -
8.3.	Zaštita DNS servisa koristeći DNSSEC	- 42 -
8.4.	Procedura konfiguracije DNS-a	- 43 -
9.	Zaključak	- 48 -
10.	LITERATURA.....	- 49 -

1. UVOD

U ovom radu biće predstavljena iskustva i koncepti dizajna i implementacije projekta kreiranja rešenja bezbedne komunikacije u okviru školskog centra kompanije CPU d.o.o. Ovi koncepti proizašli su iz iskustava stečenih prilikom implementacije rešenja bezbedne komunikacije koja je implementirana u projektu **.RS** domena, a prilagođena je novim bezbednosnim trendovima i mogućnostima koje donose novi operativni sistemi.

Ovo je jedno od mogućih rešenja potrebe za višestrukom autentifikacijom, kao i stvaranja izuzetno bezbednog rešenja autentifikacije domenskih i spoljnih korisnika prilikom pristupa resursima u lokalnoj mreži. U radu će biti opisani višestruki bezbednosni sistemi, njihova konfiguracija, implementacija, kao i njihova međusobna integracija u jednu celinu.

Projekat opisan u ovom radu zasniva se na Majkrosoftovoj server-klijent platformi. U radu su korišćeni virtuelni računari pokrenuti na Majkrosoftovoj *Hyper-V* platformi.

1.1. Kratak opis projekta i angažovanja

Prvo bih predočio zahteve koji su bili postavljeni prilikom kreiranja rešenja **.RS** domena.

Zahtev projekta bio je da se omogući bezbedna komunikacija između registara i centrale **.RS** domena prilikom registracije novih domenskih zona.

Neophodni uslovi bili su:

- da se sva komunikacija obavlja šifrovano,
- da se zahtevi za promene mogu izvršiti samo sa računara registara (predefinisani skup računara u različitim kompanijama) uz prethodnu autentifikaciju samih računara iz predefinisnog skupa,
- da se aplikacija koja se koristi od strane registara autentifikuje (i prepozna kao validna i autorizovana); aplikacija bi bila distribuirana registrima kada budu autorizovani od strane centrale,
- da se tačno zna osoba koja je tražila zahtev za promenom ili unosom novih podataka u bazu,
- da se centrali pristupa preko WEB portala na portu 80 (uz najviši mogući nivo bezbednosti),
- da se osmisli način distribucije i implementacije ovog rešenja,
- da se kreira set uputstava za implementaciju i korišćenje rešenja.

Projekat je sponzorisan od strane kompanije *Microsoft* Srbija. Segment mog angažovanja bio je dizajn i projektovanje bezbednosnog rešenja za bezbednu komunikaciju, pružanje pomoći pri implementaciji rešenja, kao i kreiranje prilagođenih (*custom*) rešenja prema zadatim uslovima, kao i direktna saradnja sa timom programera koji su razvijali aplikaciju i bazu

podataka. Projekat je završen četiri meseca nakon početka i mesec dana posle uspešnog prelaska na **.RS** domen.

Zahtev koji je postavljen firmi CPU d.o.o. bio je da lokalnim klijentima omogući bezbedan izlazak na internet, kao i da se objavljeni resursi (*web*, *mejl*, ...) mogu razlučiti sa interneta. Pošto firma poseduje nekoliko domenskih okruženja, ovo je predstavljalo malo veći problem. Prvi korak bio je konfiguracija i podizanje bezbednosti unutrašnjih domenskih zona. U sledećem koraku su konfigurisane i obezbeđene spoljne zone.

Takođe treba napomenuti da su domenske zone nazvane imenima koja nisu validna na internetu, što je još jedan dodatni uslov prilikom konfiguracije rešenja. Da bi traženi zahtevi bili ostvareni, primenjena je konfiguracija zvana *Split DNS*. Ovakav vid konfiguracije podrazumeva posedovanje privatnih i javnih DNS servera. Zbog potreba zaštite od gore navedenih tipova napada, prilikom konfigurisanja DNS rešenja, u prvom koraku se odvajaju DNS servisi na različite DNS servere. Tako su domenski DNS serveri sa *Active Directory* zonom ostali u privatnoj mreži, dok su serveri sa javnim zonama prebačeni na DNS servere u *perimeter* mrežu.

Domenski DNS serveri zaštićeni su tako što je primenjena zaštita od napada na keš, zaštita korišćenjem slučajnog porta za komunikaciju sa klijentom, kao i digitalni potpis odgovora koji se šalje klijentu. Što se spoljnih DNS servera tiče, na njima je primenjena zaštita od promene sadržaja keša, kao i zaštita korišćenjem slučajnog porta za komunikaciju sa klijentom.

Koristeći iskustva stečena u projektovanju **.RS** domenske bezbednosti i sagledavajući aspekte zahteva koji su tada bili postavljeni kao i zahteve koji su nam postavljeni, a vezani su za implementaciju bezbedne komunikacije u okviru školskog centra kompanije CPU d.o.o, može se povući paralela između ovih projekata u pogledu dizajna i implementacije bezbednosnih rešenja.

U daljem tekstu biće opisani sistemi koji su korišćeni da bi traženi zahtevi bili postignuti.

2. Osnovni postulati aktivnog direktorijuma

Polazeći od traženih zadataka koji su pred nama i obzirom da kreiramo novu infrastrukturu, moramo početi od osnove koju čini aktivni direktorijum. Aktivni direktorijum, kao jednu od svoji prednosti, nosi centralizovanu autentifikaciju korisnika koja je ujedno i uslov koji je pred nama. Da bismo taj uslov ispunili, neophodno je kreirati okruženje aktivnog direktorijuma (*AD DS Active Directory Domain Services*). Ovo rešenje ujedno omogućava nekoliko dodatnih bezbednosnih aspekata, koji će biti opisani u daljem tekstu. Primer može predstavljati AD (*Active Directory*) integrisan sa DNS-om (*Domain Name System*) koji omogućava *multimaster* replikaciju baze. Takođe, sama implementacija CA (*Certificate Authority*) servera donosi posebne mogućnosti, kao što su kreiranje posebnih kalupa (*template*) sertifikata.

Zarad boljeg razumevanja AD infrastrukture, kako fizičke tako i logičke, neophodno je objasniti sledeće aspekte. AD (*Active Directory*) predstavlja jednu centralizovanu bazu različitih tipova objekata, kao što su korisnici, računari, kontakti, grupe, štampači, organizacione jedinice, prava i dozvole, kao i drugi objekti. Primer fizičkih komponenti mogu da predstavljaju računari na koje se instalira uloga domenskog kontrolera, bez obzira na to da li su u pitanju pravi ili virtuelni računari. Logičke komponente su, npr. domeni, stabla, sajtovi, organizacione jedinice itd. Logičku osnovu svakog AD-a čini šuma koja se sastoji iz više stabala u kojima se nalaze domeni. Ovo je ujedno osnova *Name Space* hijerarhije koja se zasniva na DNS infrastrukturi.

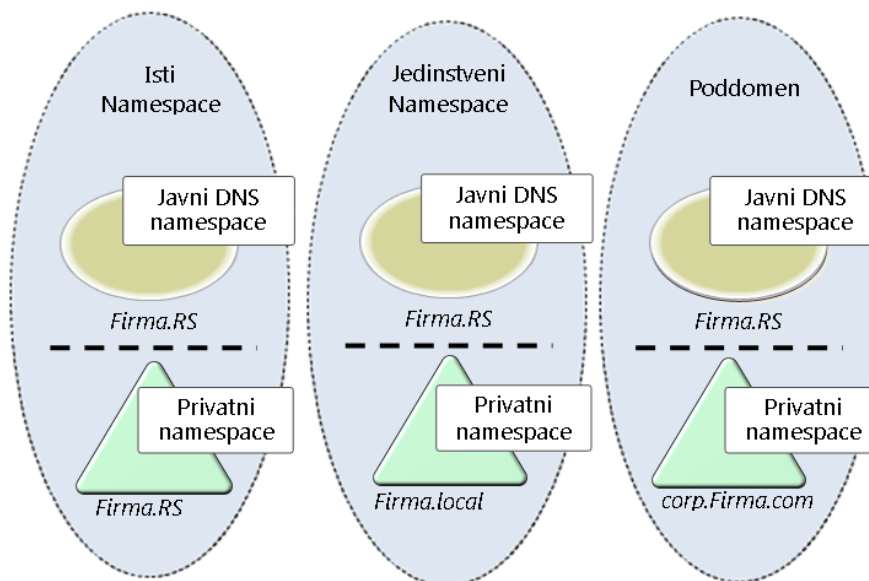
Takođe, jako je bitno napomenuti da se AD zasniva na DNS *Name Space* hijerarhiji, a da sam DNS servis može da funkcioniše i bez potrebe za aktivnim direktorijumom. Potreba AD-a za DNS servisom ogleda se u tome da se imenovanje domena i objekata u samom AD-u zasniva na principu internet *naming* hijerarhije. Pored ovoga, DNS servis je neophodan i prilikom autentifikacije računara i korisnika u samom AD servisu, pošto se u njemu nalaze servisni (SRV) rekordi koji omogućavaju pronalaženje odgovarajućeg domenskog kontrolera, na kome se obavlja autentifikacija i autorizacija pristupa resursima AD-a.

2.1. Odabir *Namespace* hijerarhije

Prilikom kreiranja aktivnog direktorijuma, odlučuje se za ime prvog domena koje će ujedno predstavljati ime prvog stabla i cele šume. Prilikom odabira imena mora se obratiti pažnja na to da postoje takozvana "javna" i "privatna" imena, kao što postoje privatne i javne IP adrese. Javnim imenima bavi se organizacija IANA-a (*Internet Assigned Numbers Authority*). Ta imena su razlučiva na internetu zahvaljujući DNS hijerarhiji. Privatna imena odabiraju se samostalno prema potrebama kompanije i ona nisu razlučiva na internetu.

Pošto svaka kompanija ima potrebu da ostvari prisustvo na internetu (objavljivanje javnih informacija i razmena *mail* poruka), potrebno je odlučiti se za odgovarajuću *Namespace* infrastrukturu.

Postoje tri osnovna principa za odabir *Namespace* infrastrukture, a to su: isti *Namespace*, jedinstveni *Namespace* i poddomen (slika 1).

Slika 1: Primeri *Namespace* hijerarhije

- **Isti *Namespace*** podrazumeva da se koristi isto ime za spoljne resurse i za aktivni direktorijum. Ovaj slučaj predstavlja jednu od najproblematičnijih situacija. Pošto postoji jedinstven *Namespace*, otvara se mogućnost da svi rekordi budu publikovani u okviru jednog DNS servera i jedne DNS zone. Međutim, u tom slučaju se pojavljuje problem bezbednosti unutrašnjih rekorda.

U slučaju da je odlučeno da se svi rekordi drže na jednom DNS serveru i da se ta zona objavi na internetu (što je ujedno preduslov za objavljivanje javnih resursa), tada su objavljeni ne samo javni resursi, njihova imena i IP adrese već i svi privatni AD rekordi. Ovo predstavlja ogroman bezbednosni problem, pošto zlonamerni korisnici mogu doći do informacija o kompletnoj infrastrukturi korporativne mreže.

Da bi se to izbeglo, potrebno je implementirati *Split DNS* infrastrukturu. Ovo znači da je neophodno postojanje odvojenih DNS servera sa javnim i DNS servera sa privatnim imenima. S obzirom da se radi o istim *Namespace*-ovima potrebno je potpuno odvojiti i sprečiti bilo kakvu komunikaciju između tih DNS servera. Na taj način bi kompanija posedovala interne DNS servere koji bi na sebi držali AD zonu i najverovatnije bili instalirani na domenskim kontrolerima i u sebi sadržali sve rekorde iz aktivnog direktorijuma.

Ovi DNS serveri na internet bi izlazili nezavisno zarad potrebe razlučivanja internet imena. Pored ovih DNS servera, bilo bi neophodno posedovati i dodatne DNS servere koji bi sadržali javnu zonu, kao i rekorde za javne sadržaje. Ovi DNS serveri bili bi dostupni sa interneta i oni bi omogućavali spoljnim korisnicima da pristupe objavljenim resursima.

- **Jedinstveni *Namespace*** podrazumeva potpuno različite *Namespace*-ove za privatne i javne resurse. Sa tačke bezbednosti, ovo je jedan od najbezbednijih načina za imenovanje domena iz veoma jednostavnog razloga, a to je da domensko ime nije validno i razlučivo na internetu. Ovo ujedno stvara potrebu za kreiranjem odvojenih javnih i privatnih DNS zona. Obe zone mogu se nalaziti na jedinstvenom DNS serveru, Međutim, iz razloga bezbednosti, ipak je neophodno razdvojiti ove zone na odvojene DNS servere. Ovakva konfiguracija dodatno komplikuje konfiguraciju većine servisa koji moraju da komuniciraju sa internetom, kao što su *Exchange Server* ili *System Center Configuration Manager*, ali je sa bezbednosne strane najbezbednija.
- **Poddomen** kao *Namespace* za AD koristi se usled potrebe da se obezbedi isto ime AD šume, kako za spoljna imena tako i za AD resurse. Ovo znači da se u javnim DNS zonama nalaze javni rekordi, a da se AD *Namespace* predstavlja kao poddomen javnog *Namespace*-a. Upotreba ovakvog rešenja je praktična za velike kompanije i kompanije kojima su javni i privatni resursi mapirani javnim IP adresama. Na taj način se postiže veoma lako publikovanje resursa koji se nalaze u okviru AD okruženja. Neke od kompanija koje koriste ovaj princip su *Microsoft*, UN, HP, itd.

Obzirom da je u ovom radu opisano rešenje koje ima odvojenu privatnu i javnu infrastrukturu, kao i veoma visoke zahteve za bezbednošću informacija, odabrano je rešenje jedinstvenog *Namespace*-a. Ime koje je odabrano za AD zonu je **CPU.local** dok je za javnu zonu odabrano ime **CPU.rs**.

2.2. Odabir broja domena

Posle odabira imena, odlučuje se koliko je domena neophodno za novo okruženje aktivnog direktorijuma. Ova odluka se donosi prema potrebama za samom administracijom objekata kao i prema potrebama za delegacijom prava i dozvola. Prilikom donošenja ove odluke važno je znati da je domen administrativna granica prava i dozvola. To bi značilo da ako neko poseduje privilegovana prava i dozvole u jednom domenu, po automatizmu ih ne poseduje u drugim domenima. Na ovu odluku utiče i sam proizvodni proces kompanije, kao što je njena geografska lokacija. Još jedan uslov koji je uticao na veći broj domena predstavljaju i *password* polise (moguće je implementirati samo jednu *password* polisu u domenu). Međutim, ovaj faktor je izgubio na značaju pojavom *Windows Servera 2008*, uz pomoć koga je moguće kreirati PSO (*Password Security Object*) objekte koji se mogu pridružiti korisnicima ili grupama i na taj način se postižu različite potrebe za *password* polisama u okviru jednog domena.

Pored ovih podela, još jedan od bitnih faktora predstavlja veličina same kompanije, tako da je za mala i srednja preduzeća u najvećem broju slučajeva potreban samo jedan domen.

2.3. Odabir tipa instalacije domenskih kontrolera

Ovakva logička infrastruktura ne može postojati bez fizičke infrastrukture, tj. servera na kojima je instaliran AD. Ti serveri se nazivaju domenski kontroleri. Do pojave virtuelizacije, domenski kontroleri su bili fizički serveri. Međutim, sama uloga (rola) domenskog kontrolera nije hardverski zahtevna, tako da se postavljalo pitanje zašto je neophodno “žrtvovati” relativno skup ili veoma funkcionalan server za tu ulogu. Tako su se domenski kontroleri našli prvi na listi servera koje je trebalo virtuelizovati. Usled nedostataka koji su postojali u virtuelizacionim rešenjima svih proizvođača, preporuka Majkrosofta bila je da se za svaki slučaj ostavi po barem jedan DC po domenu na fizičkom računaru.

Situacija se promenila pojavom *Hyper-V* servisa 3.0 u *Windows Serveru 2012*, koji je sa sobom doneo veliki broj poboljšanja kada je u pitanju aktivni direktorijum i njegova administracija. Pored ovoga, poboljšanja u virtuelizaciji koja su došla sa *Windows Serverom 2012* i *Hypervisor-om 3.0* posebno se ogledaju u povećanoj podršci za virtuelne domenske kontrolere. Najveće poboljšanje ogleda se u tome da je sada sam operativni sistem (*Windows Server 2012* i *Windows 8* klijent) svestan virtualizacije. Drugim rečima, OS prepoznaje da li je instaliran na fizičkom ili virtuelnom računaru. Kada su u pitanju domenski kontroleri, ovo se ogleda u činjenici da svaki put kada se startuje DC koji je instaliran na virtuelnom računaru on proverava svoje stanje kao i stanje baze AD-a i upoređuje ga sa stanjem baze ostalih domenskih kontrolera na mreži. U slučaju da postoji razlika, uzima se stanje sa najvećim GUID-om kao relevantno stanje i od njega kreću dalje promene. Na ovaj način su izbegnute moguće korupcije baze AD-a nastale usled slučajnog vraćanja nekog od virtuelnih domenskih kontrolera na raniji *Snapshot*.

Zahvaljujući ovim poboljšanjima, koja se ogledaju u tome da je sada i sam OS svestan da li je instaliran na fizičkom hardveru ili je instaliran kao virtuelna mašina, moguće je virtuelizovati sve domenske kontrolere bez bojazni da će doći do slučajne korupcije AD-a usled slučajnog/namernog vraćanja nekog od domenskih kontrolera na prethodno stanje.

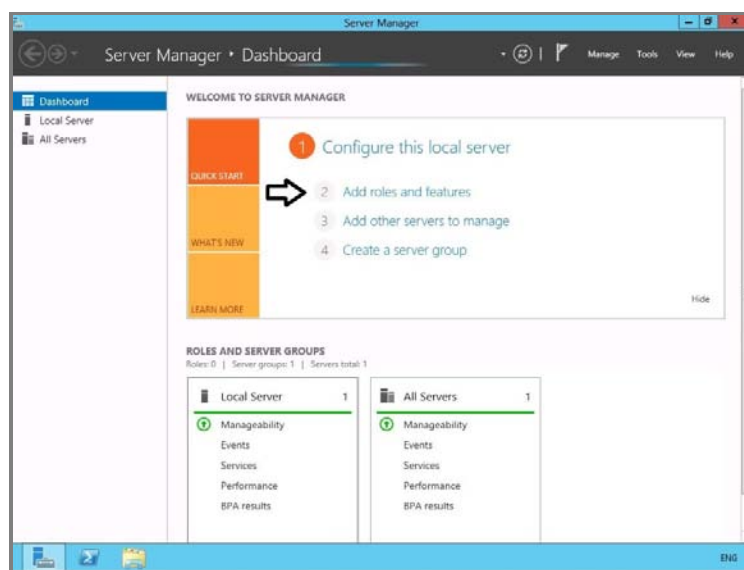
Promovisanje servera u domenski kontroler i instalacija AD DS servisa suštinski su identični kao i u prethodnim verzijama *Windows Servera*, počevši od verzije *Windows Server 2000*, ali se donekle proceduralno razlikuju u verziji *Windows Server 2012* u odnosu na prethodne verzije. Razlika je u tome što više nije moguće odmah pokrenuti promovisanje servera u domenski kontroler komandom „*dcpromo*,” već je prvo neophodno pokrenuti čarobnjak za instalaciju AD DS servisa, a zatim na kraju tog čarobnjaka izabrati opciju za konfigurisanje domenskog kontrolera.

U našem primeru koristićemo domensko okruženje koje će se sastojati od jednog domena sa imenom **CPU.local** koji poseduje dva domenska kontrolera. Potrebno je najmanje dva domenska kontrolera od kojih su oba DNS serveri i *Global* katalozi da bi se ostvarila visoka dostupnost.

3. Postupak instalacije AD-a

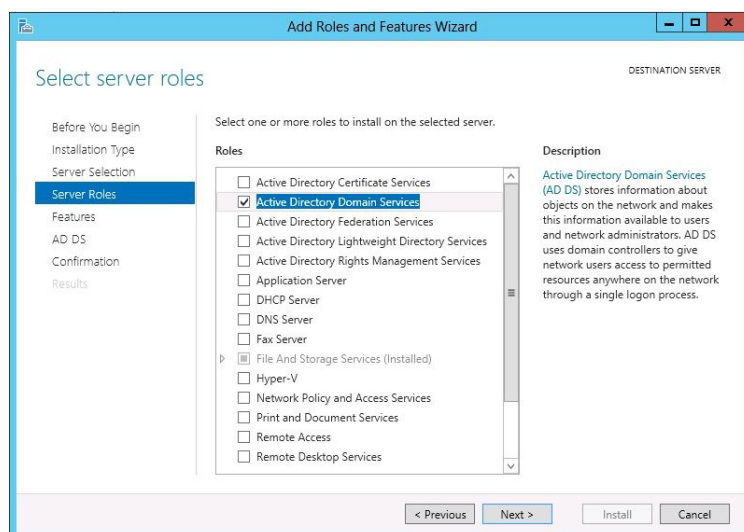
Da bi se aktivni direktorijum instalirao, neophodno je da se prvo instalira serverski operativni sistem na nekom računaru bez obzira da li je u pitanju fizički ili virtuelni računar. Po završetku instalacije i konfiguracije, takođe je neophodno da se nad tim računarom poseduju administrativna prava lokalnog administratora. Veoma je bitno naglasiti da mora da se definiše ime računara i statička IP adresu, obzirom da će te informacije biti upisane u novi aktivni direktorijum.

Kada se ovo završi, pokreće se konzola *Server Manager* u okviru koje se dodaje rola *Active Directory Domain Services* (slika 2).



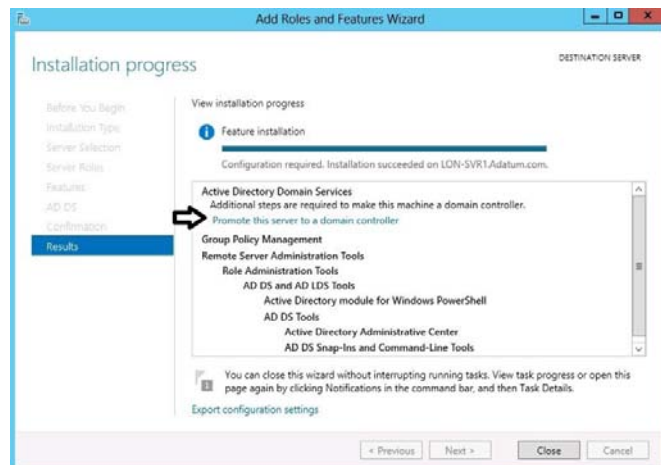
Slika 2: Server menadžer

Potom je potrebno odabrati ulogu (rolu) koju želimo da instaliramo na serveru (slika 3).



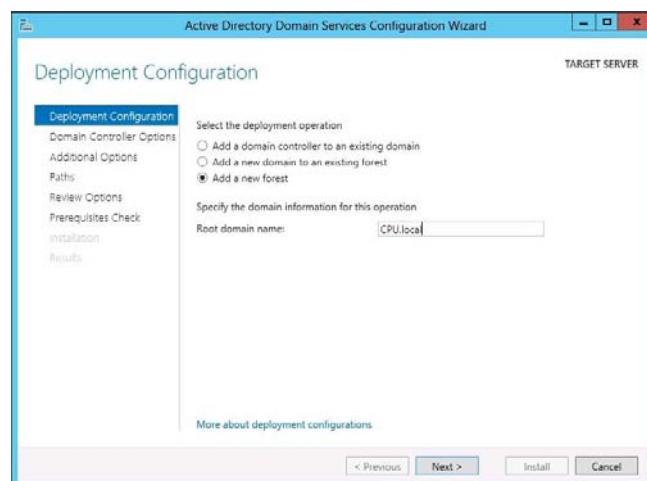
Slika 3: Odabir role za instalaciju

Posle izbora role pokrećemo samu instalaciju (slika 4).



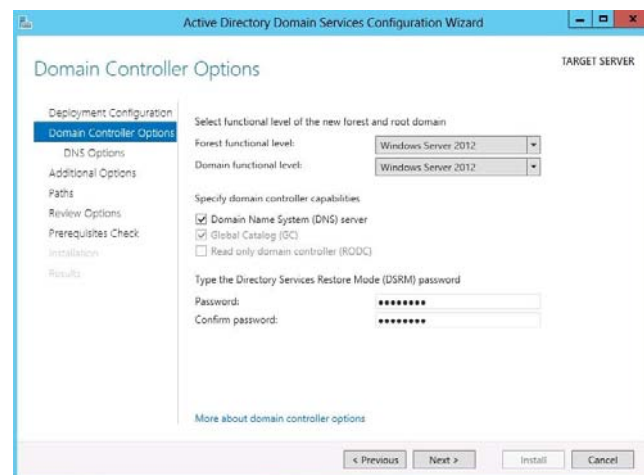
Slika 4: Početak promovisanja domenskog kontrolera

Po završetku instalacije neophodno je konfigurisati budući domen i sam domenski kontroler. Prvi korak predstavlja unos imena domena (slika 5).



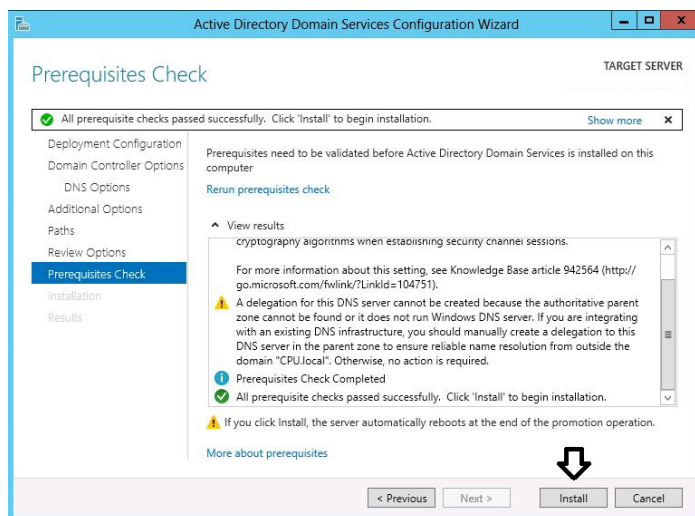
Slika 5: Unos imena domena

Sledeći korak je odabir nivoa domena i šume (slika 6).



Slika 6: Odabir nivoa domena i šume

U poslednjem koraku može se proveriti kompletna konfiguracija i u slučaju da zadovoljava naše potrebe može da se implementira (slika 7).

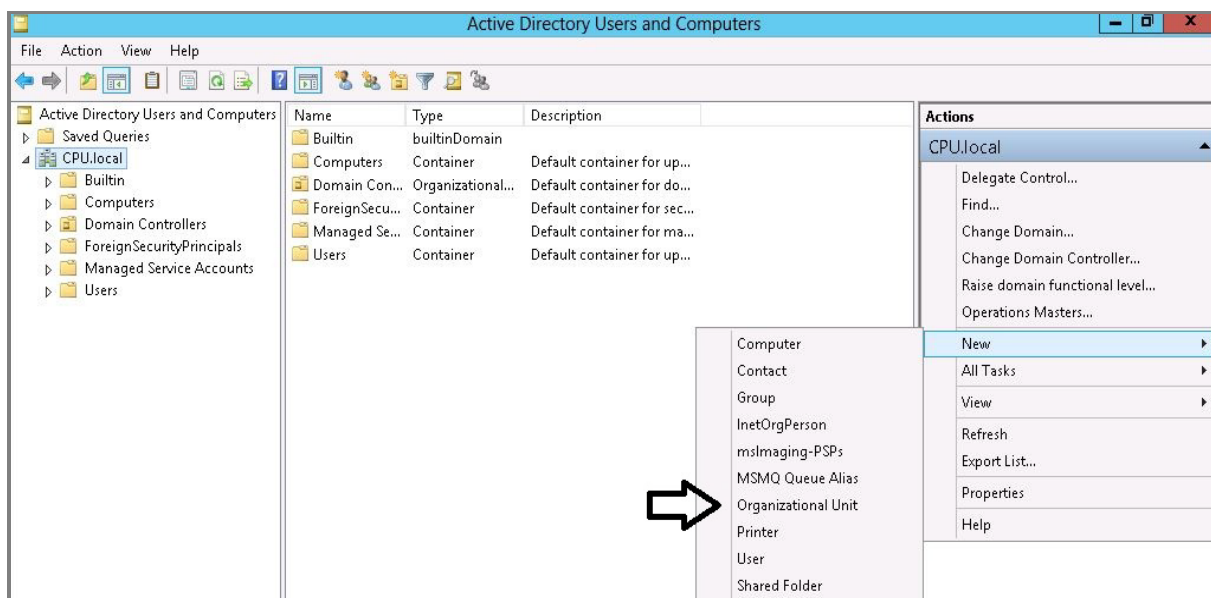


Slika 7: Kraj čarobnjaka

Po završetku instalacije aktivnog direktorijuma, potrebno je kreirati hijerarhiju organizacionih jedinica prema potrebama kompanije.

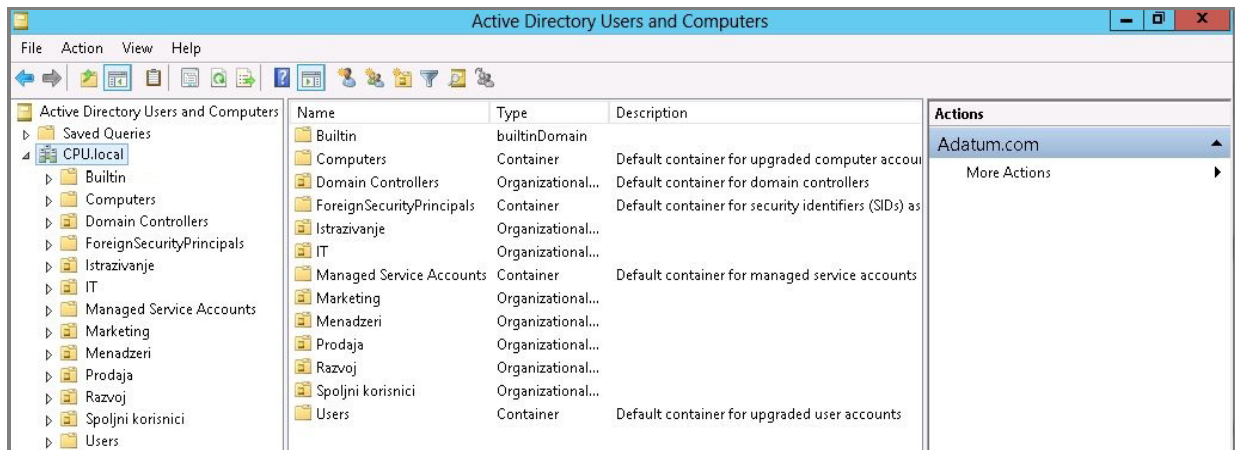
Faktori koji utiču na izbor hijerarhije raznovrsni su i razlikuju se od kompanije do kompanije. Najznačajniji faktori su implementacija GPO objekata (*Group Policy Object*), delegacija prava putem hijerarhije kao i grupisanje objekata sličnih karakteristika.

U ovom slučaju mogu se kreirati barem dve *PARENT* organizacione jedinice, jedna za AD korisnike i jedna u kojoj će se nalaziti korisnički nalozi za korisnike van kompanije sa ograničenim pravima pristupa (slika 8).



Slika 8: Početak kreiranja organizacionih jedinica

Po završetku konfiguracije organizacionih jedinica naš AD će izgledati kao na slici 9.

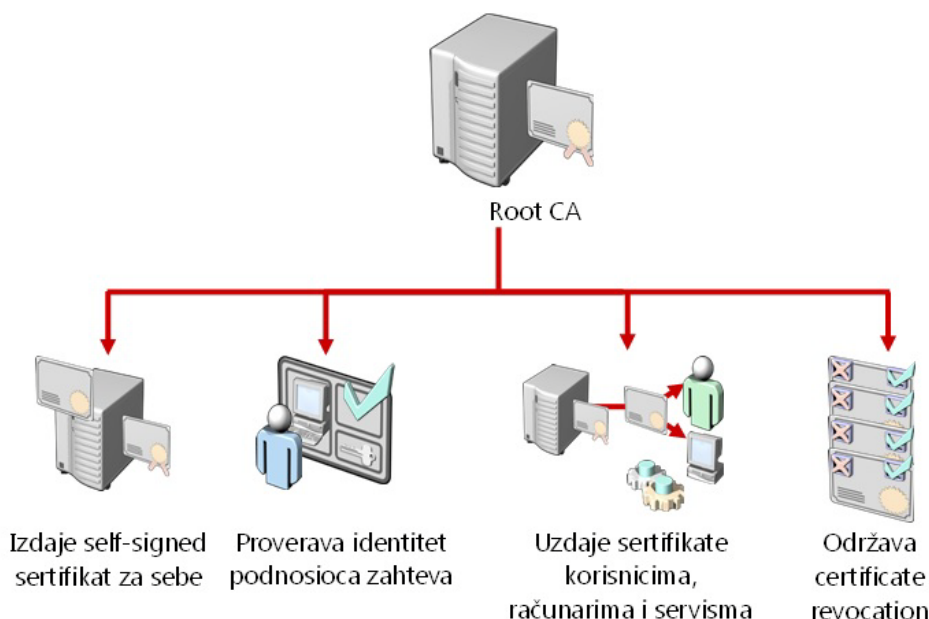


Slika 9: Finalni izgled aktivnog direktorijuma

4. Kreiranje hijerarhije CA (*Certification Authority*)

Pored instalacije i konfiguracije AD-a, u našem slučaju je potrebno instalirati i konfigurisati CA infrastrukturu.

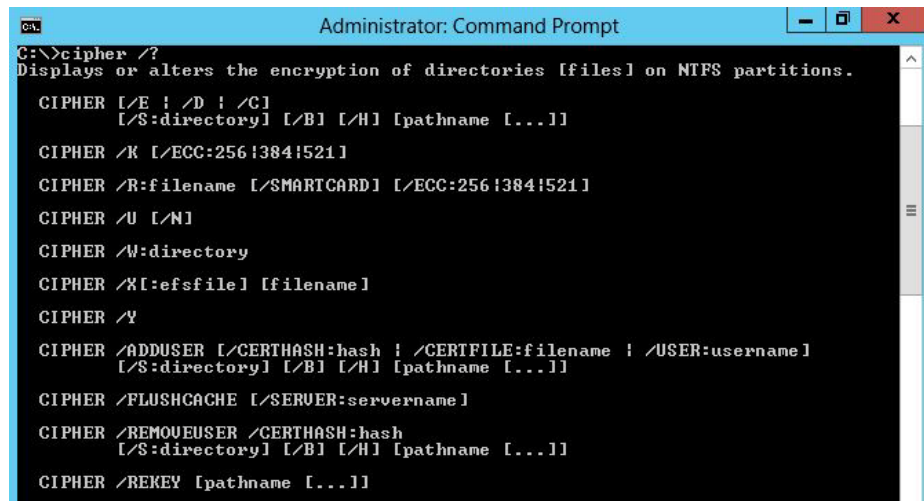
Uslov koji iziskuje posedovanje centralizovane PKI infrastrukturu nameće potrebu da se instalira CA okruženje. Da bi ovo bilo jasnije, prvo mora da se razmotri kako funkcioniše kreiranje para ključeva koji se koriste za enkripciju podataka i digitalno predstavljanje, tj. autentifikaciju. Na slici 10 prikazane su funkcionalnosti CA (*Certification Authority*) servera.



Slika 10: Funkcije CA servera

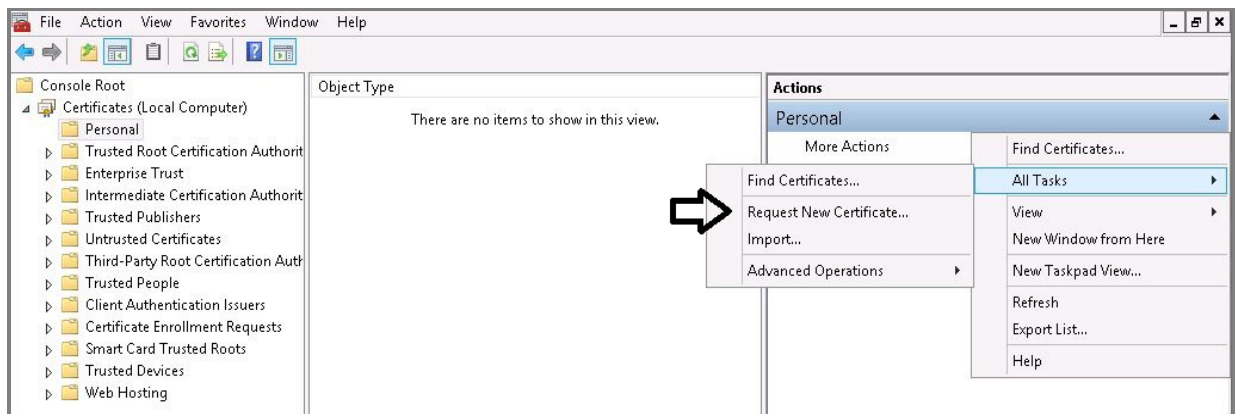
Kad se na klijentu pojavi potreba za sertifikatom, bez obzira na to da li se radi o automatskom ili manuelnom zahtevu za izdavanje sertifikata, klijent prvo proverava da li poseduje digitalni sertifikat. U slučaju da ga poseduje, iz njega iščitava informacije o CRL (*Certification Revocation List*) i proverava da li je taj sertifikat na listi povučenih sertifikata. Ako se sertifikat ne nalazi na listi povučenih sertifikata, klijent počinje da koristi taj sertifikat prema potrebi.

U slučaju da ne poseduje nikakav sertifikat, računar mora da ga dobije tako što će administrator da ga generiše lokalno ili uz pomoć CA servera ili će mu sertifikat automatski biti izdat u slučaju da je u pitanju računar koji je član domenskog okruženja. Primer automatskog zahteva predstavljao bi potrebu računara da komunicira uz pomoć IPsec-a, a primer manuelnog zahteva predstavlja pokretanje, npr. komande “*cipher*” ili pokretanje MMC konzole za generisanje sertifikata (slika 11). U svakom od tih momenata, na klijentu se pokreće servis CSP (*Cryptographic Service Provider*) koji generiše par ključeva (privatni i javni).



Slika 11: Cipher komanda

Ovo je takođe moguće uraditi i kroz MMC konzolu (slika 12).



Slika 12: Izdavanje sertifikata uz pomoć MMC konzole

Međutim, sledeći korak zavisi od toga da li postoji CA infrastruktura. U slučaju da je nema, klijent sam sebi potpisuje sertifikate i počinje da ih koristi. Ovo ujedno predstavlja problem, pošto su to takozvani *Self Sign* sertifikati, kojima veruje jedino sam klijent, dok ostatak mreže smatra ovaj sertifikat nevalidnim pošto se ne nalazi u pouzdanoj (*trusted*) hijerarhiji. Pošto se ovakvim sertifikatima ne veruje, znači da se oni ne mogu koristiti za ozbiljne namene.

U slučaju da postoji CA infrastruktura, klijent svoj javni ključ šalje CA serveru na overu. Po dobijanju zahteva od klijenta, CA server proverava ključ koji je dobio od klijenta i upoređuje ga sa *template*-ovima koje poseduje, kao i sa pravima osobe, računara ili servisa koji zahteva overu sertifikata. U slučaju da su svi uslovi zadovoljeni, CA server potpisuje javni ključ klijenta svojim privatnim ključem i klijentu izdaje digitalni sertifikat. Pošto je ovakav sertifikat izdat od strane sertifikacionog tela, njemu se veruje u hijerarhiji tog sertifikacionog tela.

4.1. Osnovna podela CA servera

Zarad boljeg razumevanja CA infrastrukturu, mora se napomenuti da postoje dva osnovna segmenta sertifikacionih tela, javna CA tela i privatna CA tela.

Javna CA tela predstavljaju kompanije kao što su *Verisign*, *Geo Trust*, itd. Poverenje prema ovim sertifikacionim telima ostvareno je tako što se javni ključevi tih CA servera nalaze u samim operativnim sistemima u segmentu koji se zove *Trusted ROOT Certification Authority*.

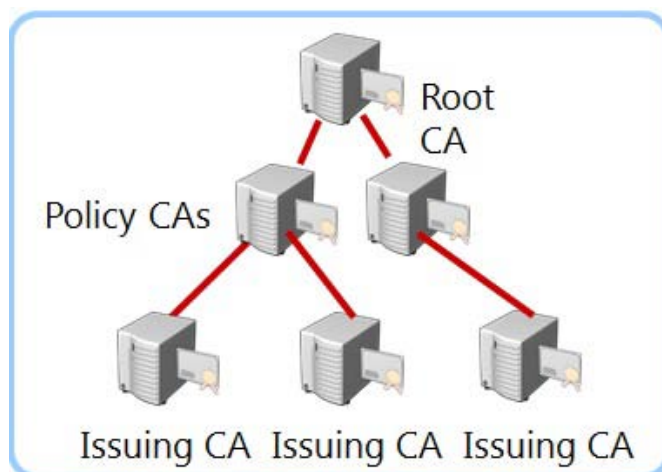
Ovo ujedno znači da svi sertifikati koje oni izdaju spadaju u grupu sertifikata od poverenja. Na ovaj način već je predefinisana grupa javnih CA servera u samoj instalaciji operativnog sistema. Međutim, da bi se naš CA server našao u ovoj grupi, potrebno je ispuniti brojne složene zahteve i procedure koje se moraju ispoštovati, kao i obezbediti relativno veliku količinu novca. Pošto je to komplikovan proces koji je finansijski neisplativ, kompanije se često odlučuju za instalaciju i konfiguraciju privatnih CA tela.

Privatna CA tela ne zahtevaju dodatna sredstva za instalaciju i konfiguraciju i ne moraju zadovoljavati sve međunarodne standarde, tako da mogu kreirati sertifikate prema potrebama kompanije.

Sledeća jako bitna stvar je bezbednost CA okruženja. Drugim rečima, svim sertifikatima koji su izdati od nekog CA servera neograničeno se veruje osim ako nisu povučeni (*revoked*). Ovo znači da, u slučaju da neko kompromituje CA server, dolazi do kompromitovanja svih sertifikata koje je on izdao. Ujedno ovo znači da kompletno svi sertifikati i sam CA server moraju da povuku sa mreže i da se kreira nova CA infrastruktura. Da bi se to izbeglo, neophodno je posedovati više CA servera u nekom okruženju tako da, u slučaju da je jedan kompromitovan, ostali mogu nesmetano da nastave sa radom.

Prema njihovom položaju u hijerarhiji, CA serveri se dele na **ROOT CA servere** i **Subordinate CA servere**. Za prosečnu kompaniju, sasvim je dovoljan samo jedan CA server za skoro sve njene potrebe. Međutim, prilikom kreiranja hijerarhije CA infrastrukture, neophodno je obratiti pažnju na to da li je moguće instalirati samo jedan *ROOT* CA server u hijerarhiji. Ovakva instalacija može dovesti do dva problema. Prvi predstavlja nedostatak visoke dostupnosti (u slučaju otkazivanja tog CA servera, cela PKI infrastruktura se ruši), a drugi problem predstavlja mogućnost kompromitovanja tog CA servera od strane zlonamernih lica ili softvera, što opet uzrokuje pad celokupne PKI infrastrukture.

Usled ovih razloga, neophodno je imati više CA servera u infrastrukturi, kako zbog visoke dostupnosti tako i da bi se smanjila šteta u slučaju kompromitovanja nekog od CA servera u hijerarhiji. Ovo se postiže instalacijom podređenih CA servera (*Subordinate CA*), kojih može postojati neograničen broj za svaki pojedinačni *ROOT* CA. Na ovaj način se kreira *Trusted* hijerarhija koja omogućava da se veruje svim sertifikacionim telima i sertifikatima koje su oni overili (slika 13).



Slika 13: Hijerarhija CA servera

Sledeća podela CA servera odnosi se na CA servis koji se može kreirati na platformi *Windows Servera*. Na *Windows* serverima, CA kao servis može se konfigurisati u dve varijante prema funkcionalnosti, i to kao **samostalni** (*Standalone*) i **član AD-a** (*Enterprise*), bez obzira na to da li se radi o serveru *ROOT CA* ili *Subordinate CA*. Svaki od ova dva načina instalacije ima svoje prednosti i mane (slika 14).

<i>Standalone CA</i>		<i>Enterprise CA</i>	
	Mora se koristiti u slučaju da je CA (<i>root/intermediate/policy</i>) offline, zato što samostalni CA ne mora biti član ni jednog AD domena		Neophodno je posedovati AD okruženje
	Korisnici moraju samostalno da obezbede neophodne informacije i odaberu tip sertifikata		Možete koristiti <i>Group Policy</i> za izdavanje sertifikata od <i>trusted root</i> CA servera
	Ne koristi <i>template</i> sertifikata		Izdaje sertifikate zasnovane na <i>template</i> -ovima
	Svi zahtevi za sertifikatima su u stanju <i>pending</i> -a dok ih administrator ne odobri		Podržava <i>autoenrollment</i> za izdavanje sertifikata

Slika 14: Samostalni i *Enterprise* CA serveri

Prilikom odabira načina i verzije instalacije CA servera mora se obratiti pažnja na buduću upotrebu ovog servisa. U slučaju da su potrebni prilagođeni *template*-ovi sertifikata, bira se *Enterprise* instalacija sa integracijom u AD. Međutim, ovo otvara novi rizik koji se ogleda u tome da takav *ROOT CA* server mora s vremena na vreme da bude na mreži, pošto je integrisan u AD. Ovo sa sobom nosi povećanje rizika da dođe do kompromitovanja tog servera, a samim tim i celokupne CA i PKI infrastrukture.

Radi povećanja bezbednosti CA rešenja i zaštite od kompromitovanja, neophodno je da *ROOT CA* server bude skinut sa mreže i ugašen, a potom da se uključuje po potrebi. Ovo se postiže

tako što se *ROOT CA* servis instalira na serveru koji je član radne grupe uz odabir *Standalone ROOT CA* server opcije. Potom se njegov javni sertifikat importuje u AD, a zatim publikuje kao *Trusted ROOT CA* sertifikat. Na ovaj način je postignuto da se takvom CA serveru veruje u AD-u kompanije, kao i da on istovremeno ne bude priključivan na mrežu. Po završetku ove procedure, a usled potrebe da se prave prilagođeni *template*-ovi sertifikata, neophodno je da se instalira *Enterprise* verzija CA servera u AD-u koja će konstantno biti dostupna domenskim klijentima. Ovo se postiže uz pomoć instalacije *Enterprise Subordinate* CA servera koju podržava *Windows Server 2012*.

Proceduru importovanja i publikovanja javnog ključa CA servera neophodno je ponoviti na svim mrežama ili radnim stanicama partnerskih firmi.

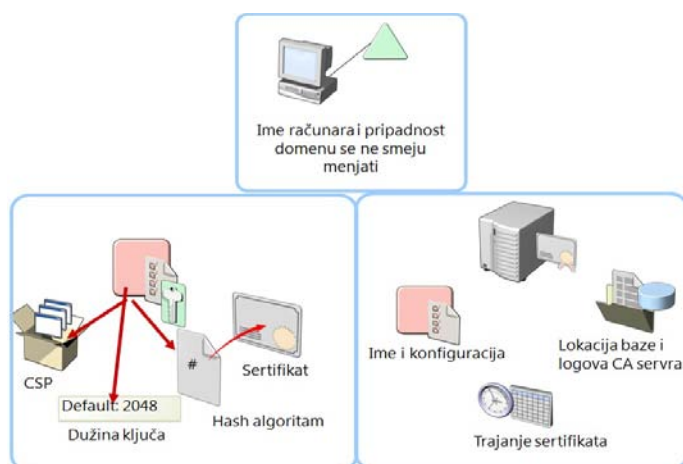
Ovom procedurom kreirana je sopstvena CA infrastruktura kojoj se veruje u potrebnom okruženju.

4.2. Procedura instalacije CA

Prvi korak u instalaciji je odabir instalacija serverskog operativnog sistema. U prethodnim verzijama serverskih operativnih sistema, pre pojave *Windows Servera 2012*, odabir prave verzije bio je ključan. Na primer, u slučaju da je instaliran CA server na *Windows Server Standard 2003/2008* platformi, kompanija bi bila uskraćena za IPsec *template*-ove sertifikata, dok u *Enterprise* verziji taj problem nije postojao. Sa pojavom *Windows Servera 2012*, ova i druge razlike između serverskih verzija su ukinute, tako da sada ne postoje funkcionalne razlike između različitih edicija servera. Razlika se, osim u ceni, ogleda samo u broju licenciranih virtuelnih računara koji se na njima mogu pokretati.

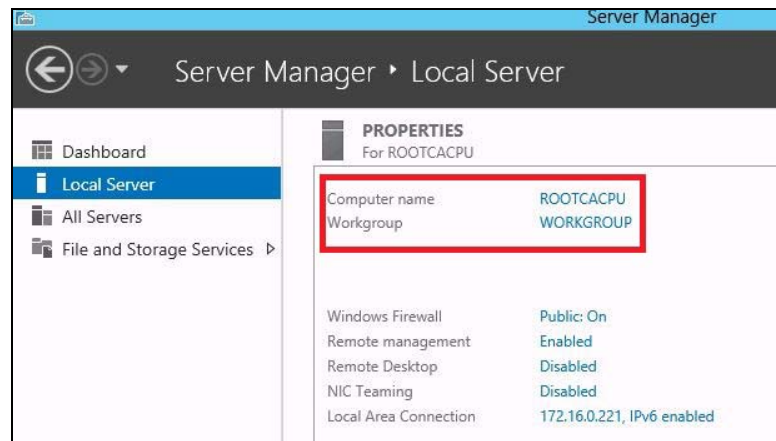
U našem slučaju, za potrebe okruženja **CPU.local**, za *ROOT CA* server odabraćemo *Windows Server 2012 Standard* koji će biti instaliran na virtuelnom računaru, s obzirom da će ovaj računar veliki deo vremena biti *offline* i ugašen.

Sledeći bitan korak je odabir imena samog CA servera, pošto po završetku instalacije uloge CA servera na nekom računaru njegovo ime i pripadnost domenu ili radnoj grupi više se ne mogu menjati. Ovde je takođe važno obratiti pažnju na to da ime našeg CA servera treba da ima veze sa našom firmom (slika 15).



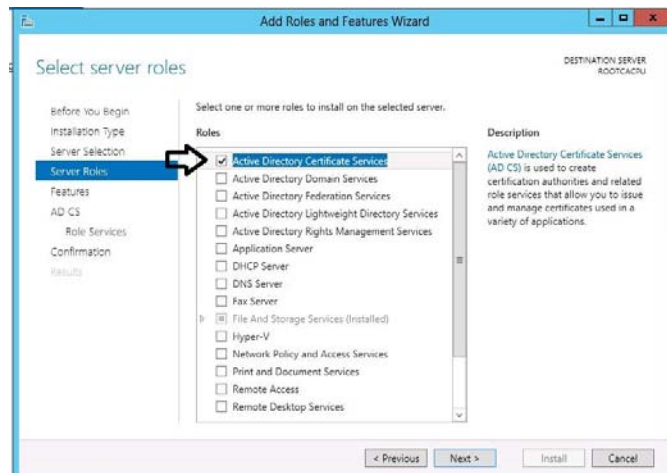
Slika 15: Planiranje *ROOT CA* servera

Po odabiru imena iz konzole server menadžera, pokreće se čarobnjak za instalaciju (slika 16).



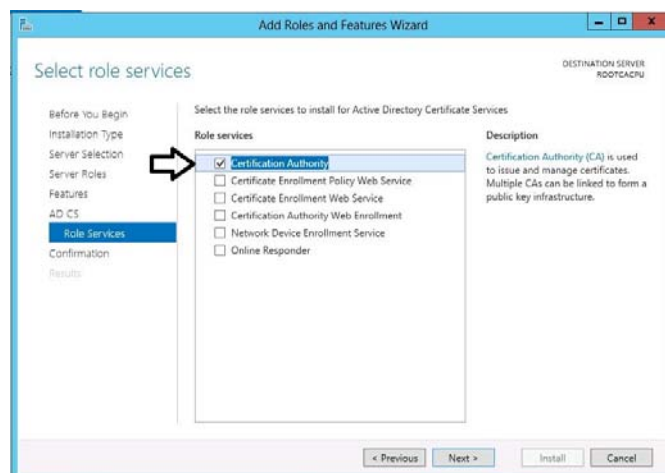
Slika 16: Odabir imena računara na kom se instalira CA server

Pošto smo odabrali korektno ime budućeg CA servera, po pokretanju čarobnjaka za instalaciju rola neophodno je odabrati odgovarajuću ulogu (slika 17).



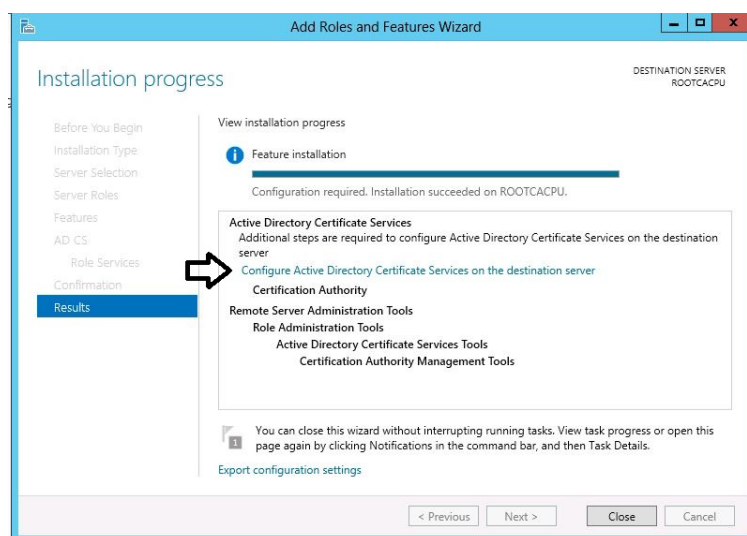
Slika 17: Odabir uloge CA servera

Zatim je potrebno odabrati dodatne opcije instalacije samog CA servera koje će ujedno predstavljati i njegove buduće moguće upotrebe (slika 18).



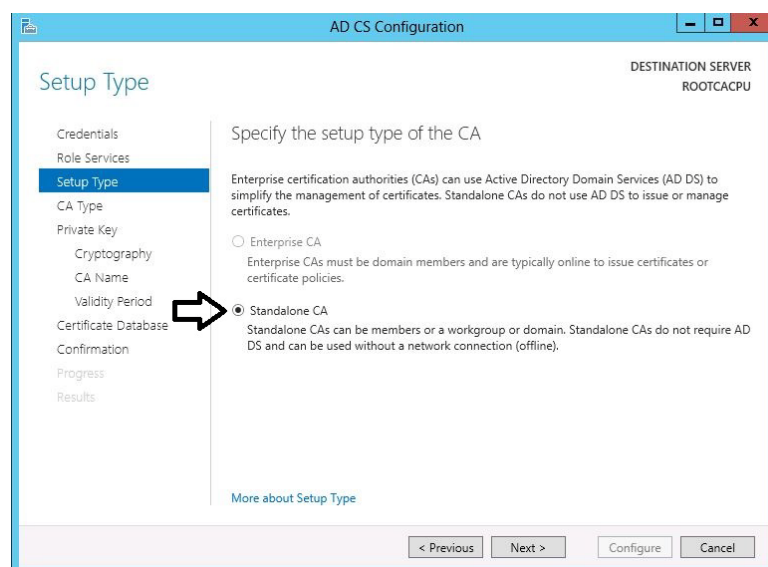
Slika 18: Odabir pratećih opcija CA servera

Po završetku inicijalne instalacije neophodno je konfigurisati CA servis (slika 19).



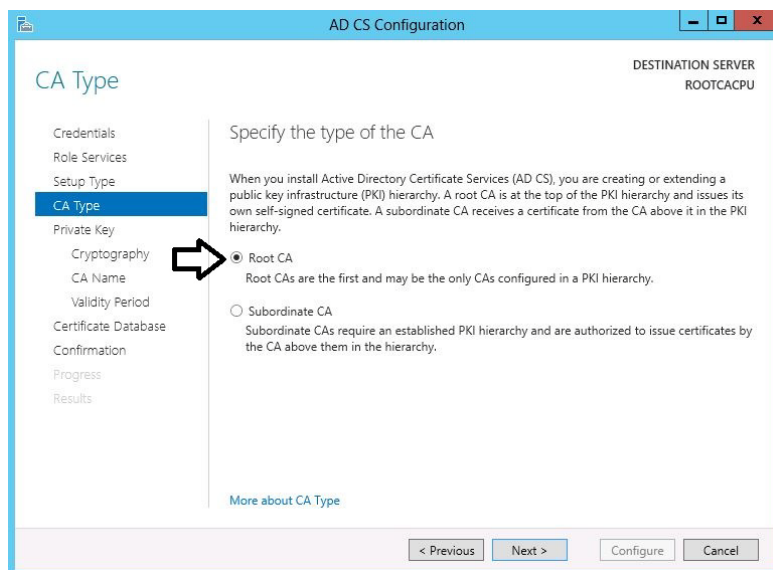
Slika 19: Kraj osnovne instalacije i pokretanje konfiguracije

Po završetku osnovne instalacije, na redu je konfiguracija CA servera. U okviru ovog dela konfiguracije neophodno je podesiti kompletnu konfiguraciju samog servisa. Prvo što je potrebno uraditi je odlučiti se da li se koristi *Enterprise* ili samostalni CA server, kao i da li se instalira *ROOT* ili *Subordinate* CA server i odabrati njegovo javno ime. Potom je neophodno kreirati novi par ključeva za sam CA server, kao i odlučiti se za veličinu ključa, način šifrovanja, veličinu HASH vrednosti kao i dužinu trajanja samog ključa (slika 20).



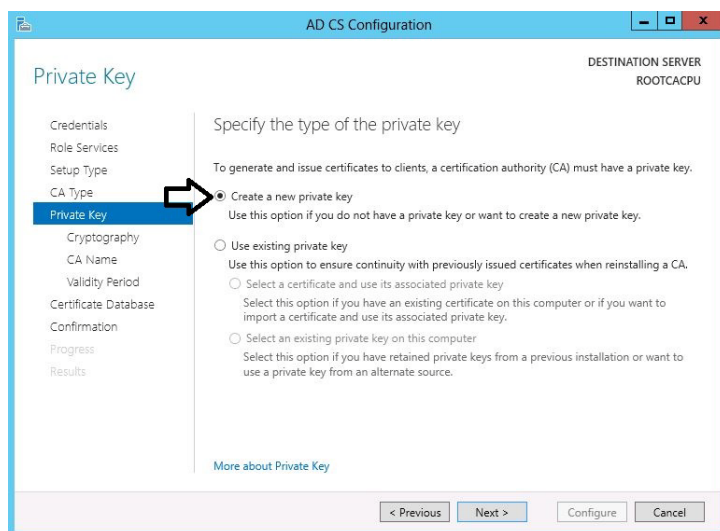
Slika 20: Odabir tipa instalacije CA servera

Po odabiru tipa instalacije CA servera, neophodno je odabrati hijerarhijski položaj tog CA servera (slika 21).



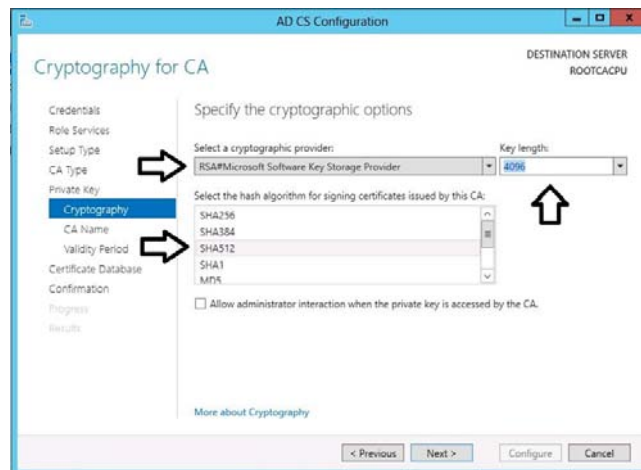
Slika 21: Odabir tipa instalacije CA servera

Potom se odabira kreiranje novog ključa za CA server. Ovo je neophodno zato što ne posedujemo druge CA servere koji bi mogli da izdaju ključ za naš ROOT CA server. U slučaju da smo dobili ključ od nekog drugog CA servera, kreirali bi *Cross Certificate Authentication*. Ovo se koristi u slučaju da jedna kompanija izdaje ključ drugoj kompaniji za njihov ROOT CA server. Ovim se uspostavlja automatsko poverenje u sertifikaciona tela između kompanija (slika 22).



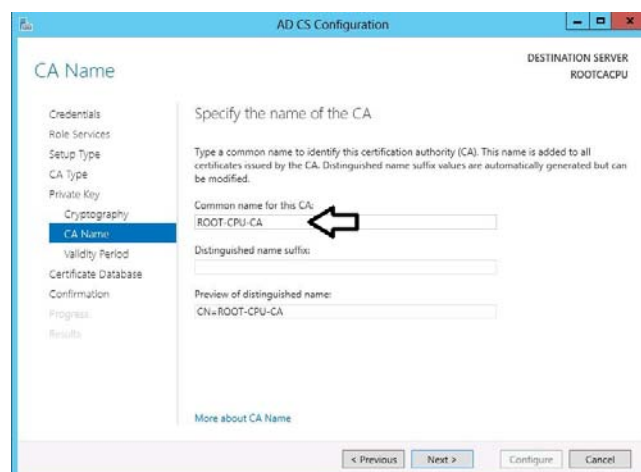
Slika 22: Odabir kreiranja privatnog ključa

Sledi odabir tipa kriptografije, *hash* algoritma i veličine ključa (slika 23).



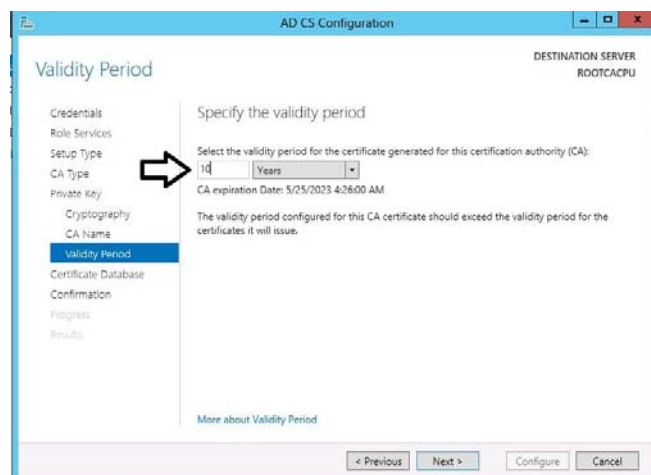
Slika 23: Izbor kriptografije za privatni ključ

Važno je da se obrati pažnja na pravilan odabir imena koje će se pojaviti u ROOT sertifikatu (slika 24).



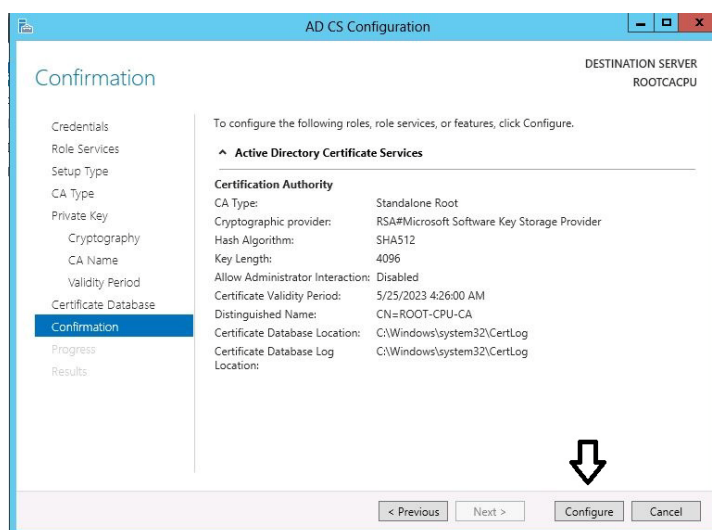
Slika 24: Odabir javnog imena CA servera

Potom se bira dužina trajanja ROOT sertifikata (slika 25).



Slika 25: Odabir vremenskog trajanja javnog ključa CA servera

Na kraju konfiguracija može da se pregleda i potom da se implementira (slika 26).



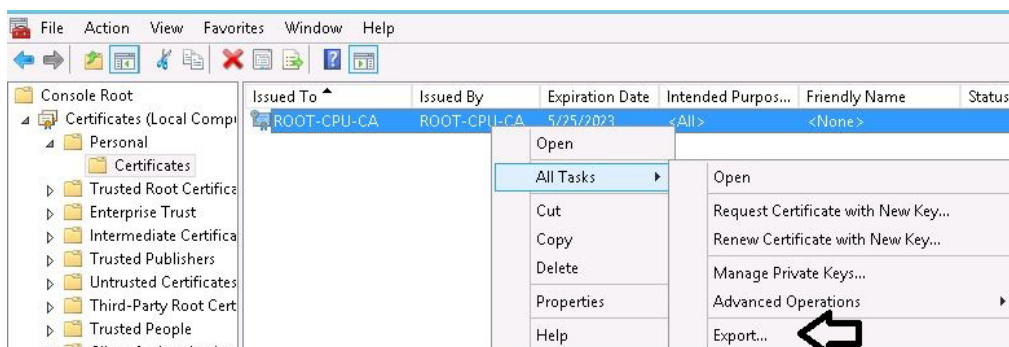
Slika 26: Kraj konfiguracije

Nakon ovoga se, u okviru *ROOT* CA servera, konfiguriše CRL distributivnu lista kao i vreme u kome će se ona ažurirati. Pošto je ovaj CA server *offline*, mora da se definiše mrežna putanja servera koje je stalno dostupan i na kojoj će CRL biti objavljen.

4.3. Instalacija *Subordinate* CA servera

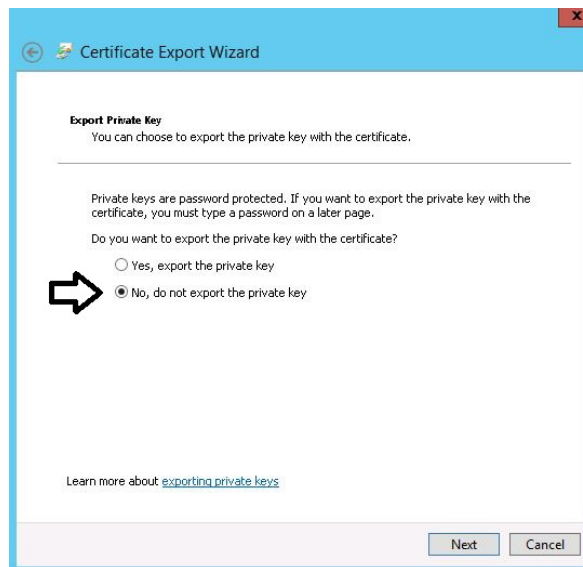
Po završetku konfiguracije i provere da je sve korektno instalirano i konfigurisano, neophodno je ostvariti verovanje našeg AD-a konkretnom CA serveru. Ovo je potrebno zato što je ovaj server van našeg AD-a, kao i zato što je to privatni CA server. Da bi se ovo postiglo, neophodno je uvesti sertifikat *ROOT* CA servera u naš domen **CPU.local**.

Ovo se postiže tako što će se prvo izvesti javni ključ *ROOT* CA servera u fajl i taj fajl uvesti u AD. Da bi se taj ključ uvezao u AD i objavio na svim računarima, poželjno je koristiti grupne polise i to prvenstveno domensku polisu (slika 27).



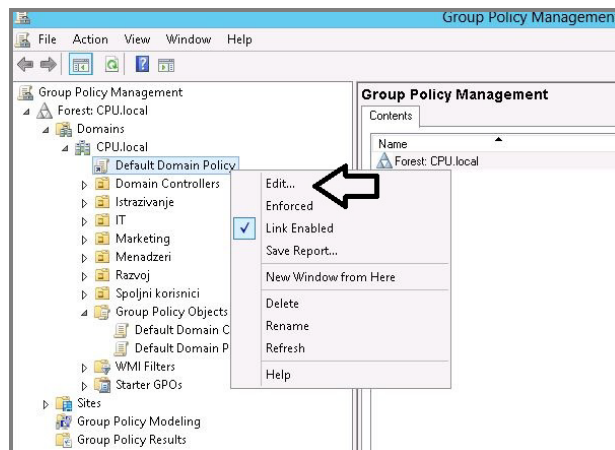
Slika 27: Izvoz javnog ključa sa CA servera

Zatim odabiramo koji se sertifikat eksportuje (slika 28).



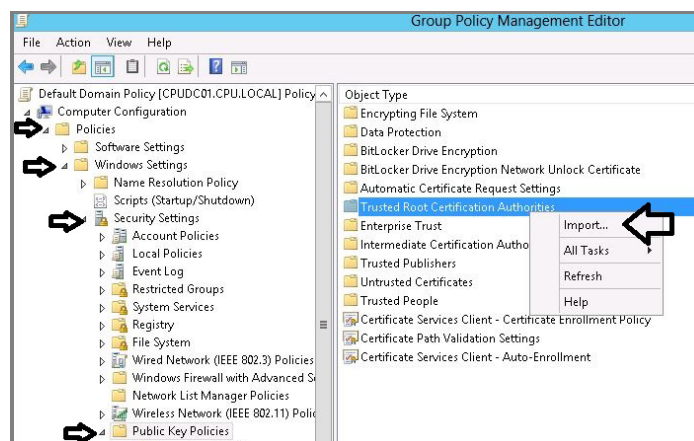
Slika 28: Javni ključ se izvozi

Po eksportu sertifikata neophodno je editovati domensku politisu (slika 29).



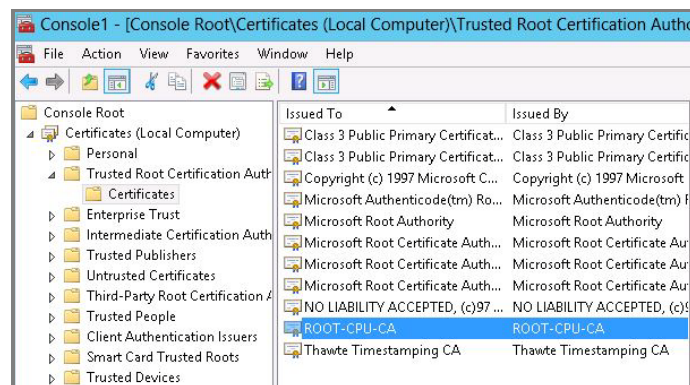
Slika 29: Editovanje domenske grupne politise

Zatim sertifikat uvozimo u domensku politisu (slika 30).



Slika 30: Uvoz ključa ROOT CA servera u domensku politisu

Možemo proveriti da li se odgovarajući ključ pojavio u *Trusted ROOT Certification Authority* segmentu naših računara koristeći MMC konzolu na klijentu, što ujedno znači da je željeni cilj postignut (slika 31).



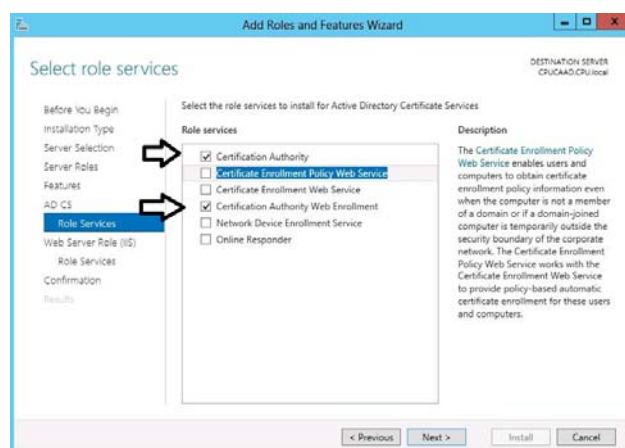
Slika 31: Rezultat uspešne konfiguracije

Po završetku ovog segmenta konfiguracije, uspešno sam uradio propagaciju novog *ROOT CA* server našem AD okruženju. Sada na red dolazi kreiranje radnog (*Issuing*) CA servera koji će se svakodnevno koristiti u radnom okruženju za sve moguće potrebe upotrebe PKI rešenja. Pored ovoga, na njemu će se kreirati prilagođeni *template*-ovi sertifikata.

Kao i u prethodnom slučaju, neophodno je instalirati i konfigurisati serverski operativni sistem na budućem CA serveru i pokrenuti inicijalnu instalaciju CA servisa.

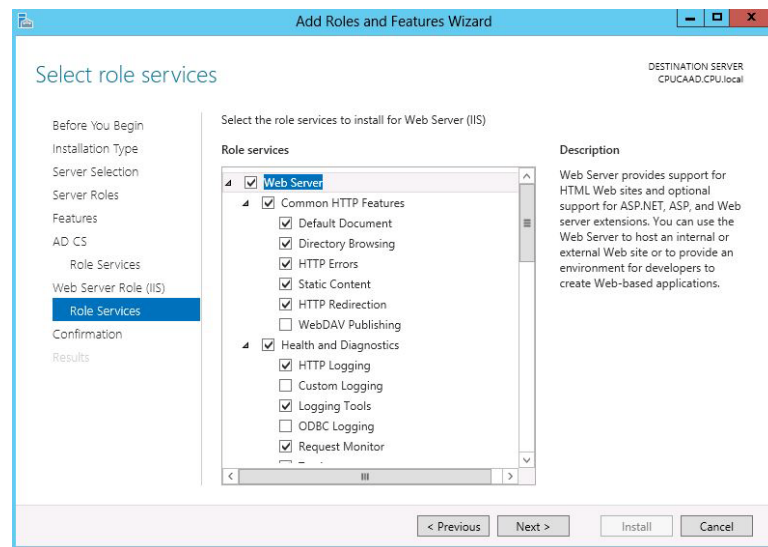
Međutim, sada u okviru konfiguracije treba odabrati *Enterprise* opciju pošto je *Issuing CA* server član AD **CPU.Local** i postoji potreba za kreiranjem modifikovanih *template*-ova sertifikata. Takođe se bira opcija *Subordinate CA* server, pošto se on u hijerarhiji CA servera u našem okruženju nalazi na drugom mestu.

Mora se obratiti pažnja na to da li je *ROOT CA offline*, kao i da ne može direktno da se potražuje sertifikat koji je neophodan za kreiranje *Subordinate CA* servera. Ovo konkretno znači da je u samoj instalaciji *Subordinate CA* server neophodno napraviti *offline* zahtev koji se potom fizički odnosi na *ROOT CA* server i tamo se overava i izdaje sertifikat. Po završetku ove procedure, izdati sertifikat se instalira na *Subordinate CA* server posle čega on počinje sa radom. Odabir funkcija radnog CA servera u okviru instalacionog čarobnjaka prikazan je na slici 32.



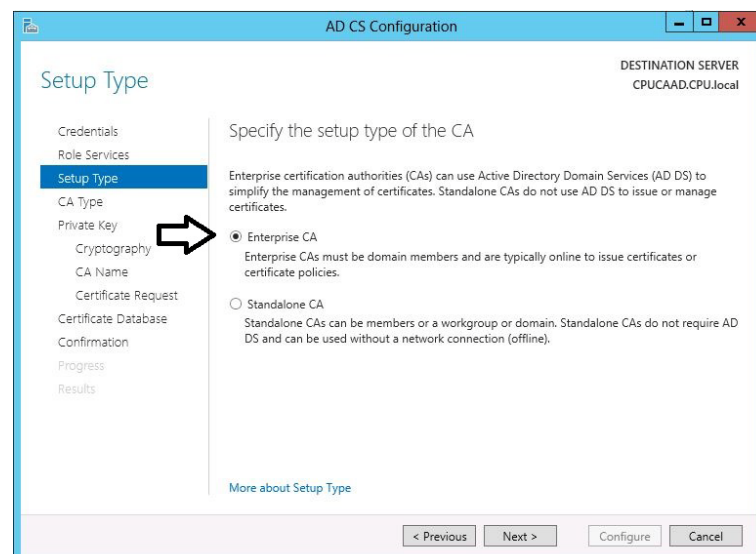
Slika 32: Odabir rola *Subordinate CA* servera

Pošto je odabrana uloga izdavanja sertifikata kroz WEB interfejs, neophodno je konfigurisati i WEB server. Ovakav vid izdavanja sertifikata neophodan je zbog povećanja kompatibilnosti sa različitim tipovima klijenata kojima se izdaju sertifikati (slika 33).



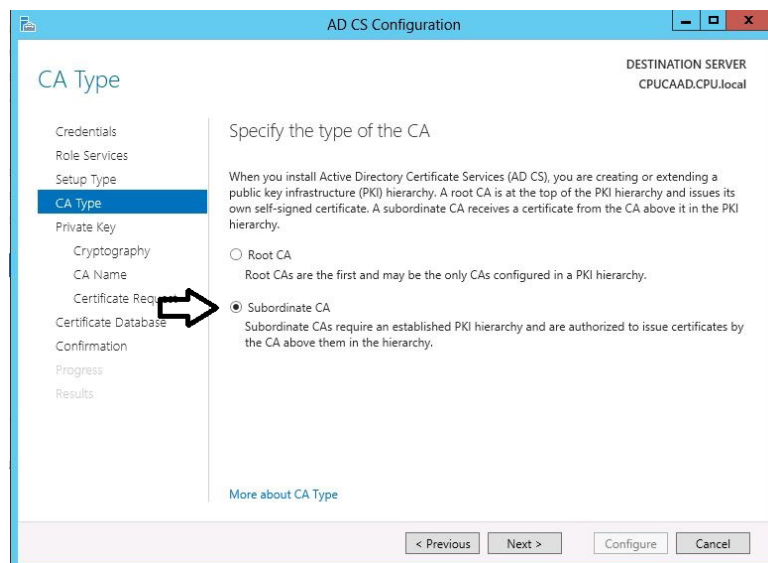
Slika 33: Dodatne funkcije uključuju instalaciju IIS servisa

Potom je neophodno odabrati tip instalacije CA servera. Obzirom da želimo da kreiramo prilagođene sertifikate, odabraćemo *Enterprise* CA server (slika 34).



Slika 34: Odabir tipa CA servera

Sledi izbor pozicije CA servera u hijerarhiji. U ovom slučaju se bira *Subordinate* CA server (slika 35).



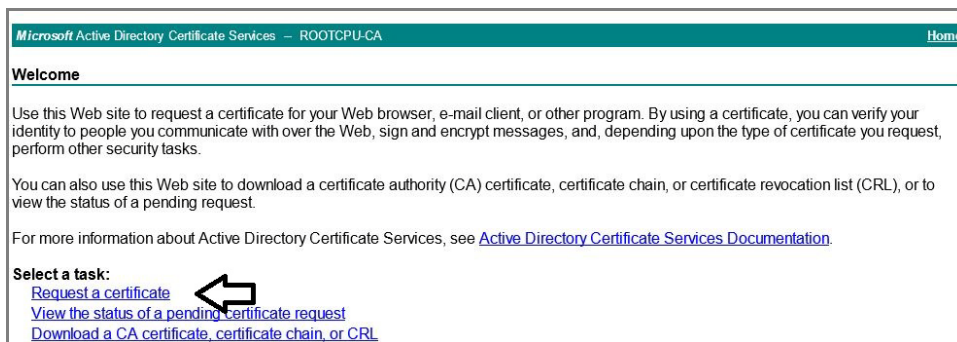
Slika 35: Pozicioniranje CA servera u hijerarhiji

Obzirom da je *ROOT CA offline* neophodno je da se zahtev za sertifikat novog CA servera odigra *offline*. Da bismo ovo postigli neophodno je da se kreira "*offline certificate request*" uz pomoć *hash* vrednosti (slika 36).



Slika 36: Zahtev za izdavanje *Subordinate* CA sertifikata

Potom se taj zahtev fizički prenosi na *ROOT* CA server gde se procedura nastavlja (slika 37).



Slika 37: Početak izdavanja *Subordinate* CA sertifikata

Prethodno generisana *hash* vrednost unosi se u zahtev (slika 38).

Microsoft Active Directory Certificate Services – ROOTCPU-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDIZCCAgsCAQAwRTEVMBMGCGmSUmT81xkARKW
LQGBGRYDQ1BVMRcwFQYDVQDEwSDUFUUtQ1BVQ0FB
AQEBBQADggEPADCCAQoCggEBANM57adcXC5RjbE3
g7hQJcTKBnHPZouYDnnjbeC+fVWKf+gmDU8CCjhy
R3F9kGmqZoxGDrkQjfiI+j5dZuhbSwpm0a8AML8H
-----
```

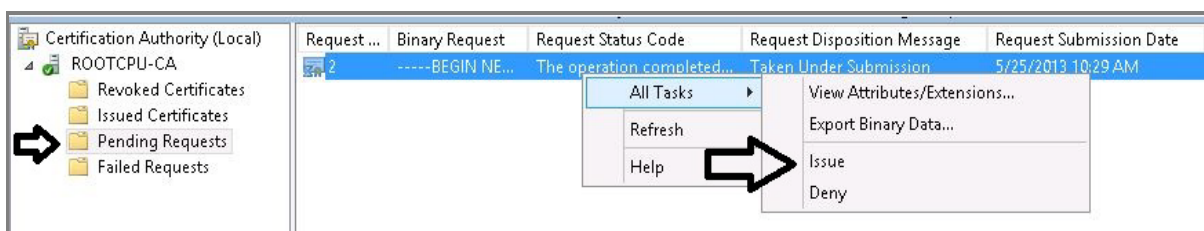
Additional Attributes:

Attributes:

Submit >

Slika 38: Unos HASH vrednosti dobijene prilikom instalacije

Obzirom da je ROOT CA server instaliran kao *standalone* server, ne postoji mogućnost automatskog odobravanja zahteva za sertifikatima, zato je neophodno manuelno odobriti zahtev u samom ROOT CA serveru (slika 39).



Slika 39: Odobravanje sertifikata od strane ROOT CA servera

Po odobrenju sertifikata neophodno je uraditi njegov *download* (slika 40).

Microsoft Active Directory Certificate Services – ROOTCPU-CA

Certificate Issued

The certificate you requested was issued to you.

☒ DER encoded or ☐ Base 64 encoded

 [Download certificate](#)

[Download certificate chain](#)

Slika 40: Odobren sertifikat za *Subordinate* CA servera spreman za preuzimanje

Kad se dobije fajl sa sertifikatom za radni CA server, potrebno ga je preneti nazad na server i instalirati na *Subordinate* CA server, posle čega on počinje sa radom. Pošto je sada domenska CA infrastruktura osposobljena, može se početi sa izdavanjem sertifikata korisnicima i računarima u domenu.

5. Automatska distribucija sertifikata računarima neophodnih za IPSec komunikaciju

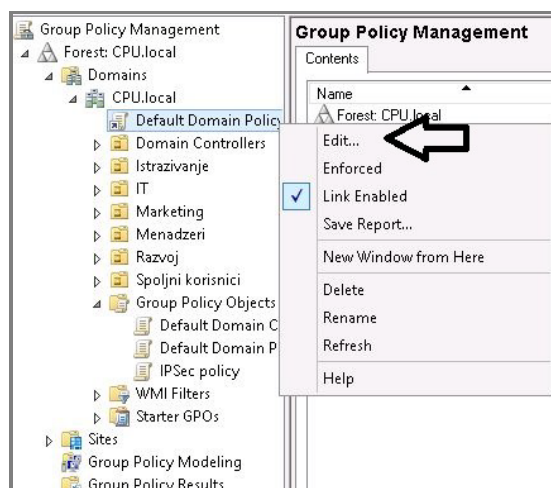
Po završenoj instalaciji CA okruženja, a zarad potrebe da se ostvari bezbedna komunikacija računara u okviru domenskog okruženja koristeći IPSec, neophodno je izdati odgovarajuće sertifikate računarima u domenu.

Za potrebe IPSec komunikacije, u ovom slučaju ćemo koristiti kompjuterske sertifikate kao jedan od mogućih načina autentifikacije strana u komunikaciji.

Sama procedura izdavanja sertifikata računarima moguća je na više načina. Ovi načini izdavanja sertifikata mogu se podeliti u manuelne i automatske.

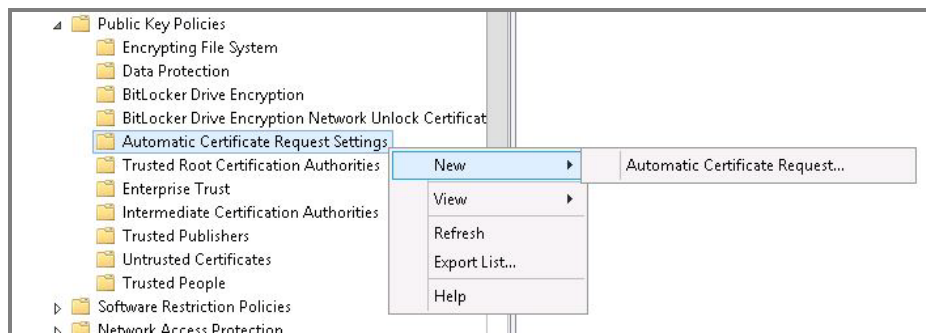
- Manuelni podrazumevaju akciju korisnika koja zahteva izdavanje kompjuterskog sertifikata, kroz web interfejs ili kroz MMC konzolu. Ovakvi zahtevi su relativno jednostavni, međutim zahtevaju dosta posla što se ogleda u vremenu potrebnom za izdavanje pojedinačnog sertifikata. Pored ovoga, da bi korisnik uopšte mogao da zatraži i instalira kompjuterski sertifikat, neophodno je da poseduje prava lokalnog administratora. Ako bi se opredelili za ovakve pristupe ovo bi ujedno značilo da, ako želimo da koristimo bezbednu komunikaciju, svi korisnici računara moraju da poseduju prava lokalnog administratora ili da sam administrator za njih danih instalira sertifikate na klijentskim računarima. U slučaju da su računari članovi radne grupe, ova opcija je jedina moguća.
- Druga opcija je automatizacija izdavanja sertifikata, koja je moguća u domenskom okruženju uz pomoć grupnih politika. Ovaj način podrazumeva automatsko izdavanje i instaliranje kompjuterskih sertifikata bez obzira na to koja su prava korisnika koji koristi taj računar. Takođe, na ovaj način se angažovanje administratora svodi na minimum, tj. samo na kreiranje politike pošto se njeno izdavanje odigrava automatski prilikom procesiranja grupe politike ili kada računar pokuša da ostvari bezbednu komunikaciju.

Procedura za automatsko izdavanje sertifikata sastoji se iz modifikacije centralne domenske politike ili politike koja je vezana za organizacionu jedinicu u kojoj se nalaze računari koji treba da koriste bezbednu komunikaciju (slika 41).



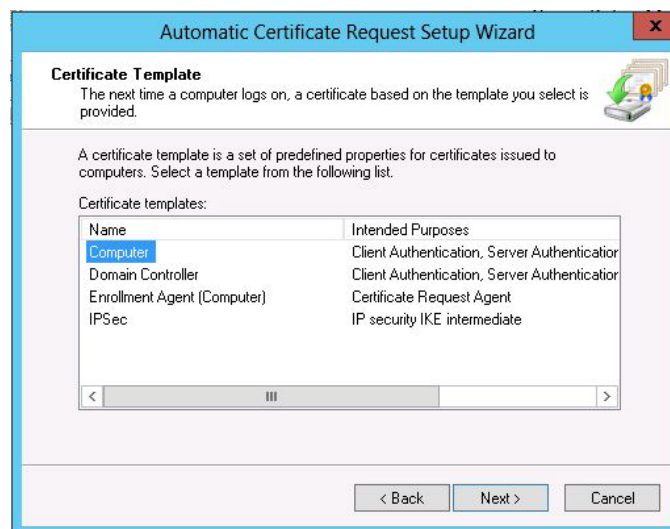
Slika 41: Domenska politika

Potom je u okviru grupne polise neophodno odabrati segment *Public Key Policies* i u okviru njega automatsko izdavanje sertifikata (slika 42).



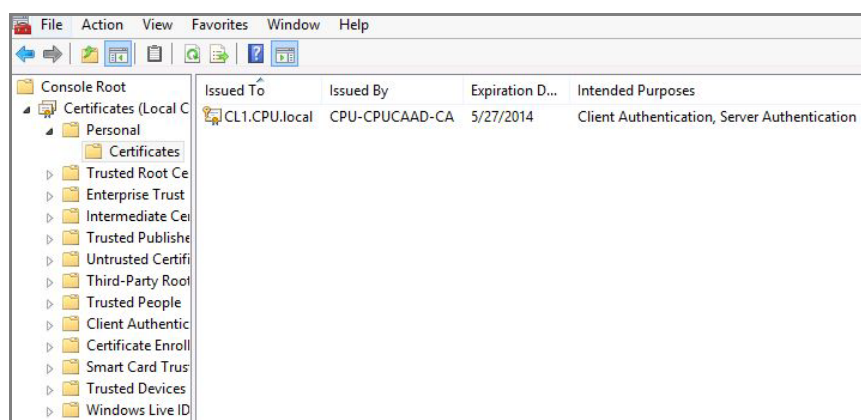
Slika 42: Konfiguracija grupne polise

Zatim u čarobnjaku treba odabrati kompjuterski sertifikat (slika 43).



Slika 43: Čarobnjak za automatsko izdavanje sertifikata

Po završetku čarobnjaka potrebno je sačekati da se grupna polisa procesira u okviru domena i da se pojave računarski sertifikati na samim računarima (slika 44).



Slika 44: Automatski izdat kompjuterski sertifikat

Kada svi računari u domenu dobiju kompjuterske sertifikate može se početi sa kreiranjem i implementacijom bezbednosnih IPSec polisa.

6. Konfiguracija i implementacija bezbednosnih IPSec polisa

Po završetku instalacije i konfiguracije grupnih polisa neophodnih za izdavanje sertifikata računarima može se preći na sledeći korak, a to je podešavanje *Firewall*-a i prilagođenih IPSec polisa u AD-u koje će obezbediti bezbednu komunikaciju između klijenata.

IPSec u svojoj osnovi omogućava sledeće prednosti kada je bezbednost u pitanju:

- uzajamna autentifikacija pre i tokom komunikacije između klijenata,
- poverljivost kroz enkripciju IP saobraćaja,
- integritet IP saobraćaja odbacivanjem modifikovanog saobraćaja,
- zaštita od *Replay* napada.

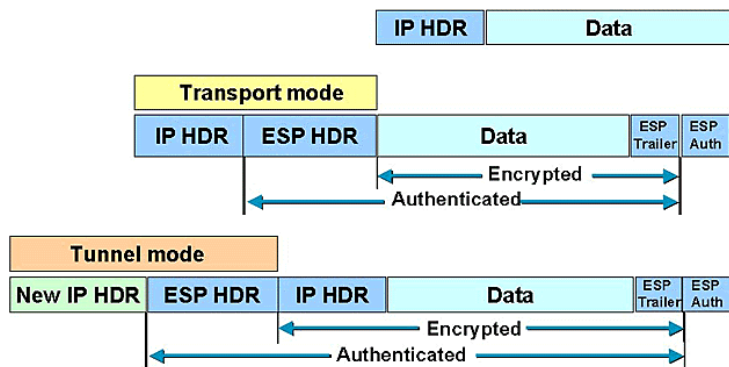
Ovo se postiže tako što IPSec koristi šifrovanje podataka i to na dva načina, digitalnim potpisivanjem zaglavlja AH (*Authentication Header*) i šifrovanjem sadržaja ESP (*Encapsulating Security Payload*). Zahvaljujući ovim mogućnostima postoje dva osnovna načina upotrebe IPSec-a (slika 45):

- Transportni režim (*Transport mode*)

U transportnom režimu samo je sadržaj IP paketa šifrovan ili autentifikovan, što podrazumeva upotrebu ESP segmenta IPSec-a. Ovakav vid transporta ne utiče na rutiranje paketa, pošto se IP zaglavlje ne menja. Međutim, kada se koristi potpisivanje zaglavlja IP adrese ne može se koristiti NAT jer će to poništiti *hash* vrednost zaglavlja paketa.

- Tunelski režim (*Tunnel mode*)

U tunelskom režimu ceo IP paket je šifrovan i autentifikovan. Takav paket se zatim ubacuje u novi IP paket sa novim IP zaglavljem i potom šalje na destinaciju. Tunelski režim se najčešće koristi za kreiranje virtuelnih privatnih mreža koje omogućavaju veze između lokacija kao i za komunikaciju između računara ili udaljeni pristup. Tunelski režim takođe podržava i NAT-T (NAT traversal).



Slika 45: Izgled transportnog i tunelskog režima IPSec komunikacije

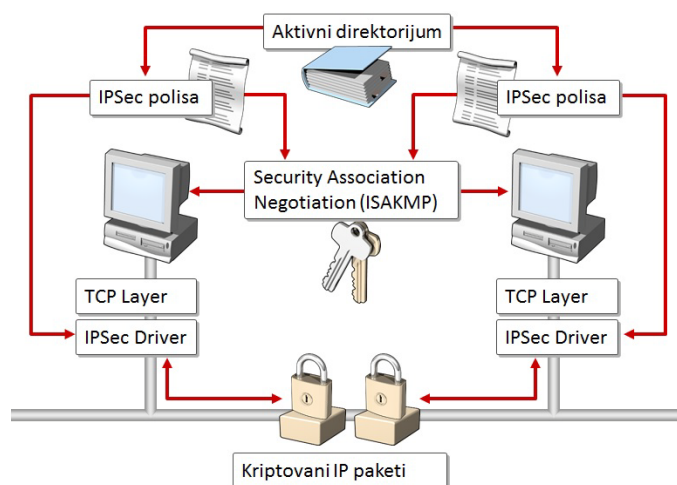
Iz prethodnog teksta veoma je očigledno da IPSec podrazumeva šifrovanje sadržaja paketa kao i digitalnu autentifikaciju. Kada su Majkrosoftovi operativni sistemi u pitanju, postoji više načina na koje je ovo moguće postići. Osnovna četiri metoda autentifikacije koji se koriste za IPSec u okviru Microsoft operativnih sistema su:

- kompjuter Kerberos V5
- kompjuter NTLM V2
- kompjuterski sertifikat
- deljeni ključ

Prva dva metoda podrazumevana su u slučaju posedovanja aktivnog direktorijuma i koriste standardnu AD autentifikaciju, dok su druga dva namenjena korišćenju u mešovitom okruženju radne grupe i aktivnog direktorijuma. Po pitanju bezbednosti, najsigurniji način autentifikacije je korišćenje deljenog ključa. Međutim, ovo je relativno komplikovano za podešavanje i implementaciju, pošto postoji potreba da se svaki put kreira novi ključ za bezbednu komunikaciju što dodatno usložnjava ceo proces.

Zbog svega ovoga i zbog potrebe da se ostvari IPSec komunikacija, kako između domenskih tako i računara koji se nalaze u radnoj grupi, ostaje samo jedna mogućnost, a to je upotreba digitalnih sertifikata za autentifikaciju.

Takođe je važno naglasiti da za upotrebu IPSec-a mora da postoji saglasnost obe strane u komunikaciji, kako po pitanju korišćenja IPSec-a uopšte tako i oko načina razmene ključeva i same enkripcije sadržaja (slika 46).



Slika 46: Princip funkcionisanja IPSec-a

Do sada su postojale tri osnovne IPSec polise:

- **Klijent**
Klijent normalno komunicira nešifrovanom komunikacijom dok se od njega ne zatraži da koristi IPSec komunikaciju.
- **Server**
Prilikom svakog uspostavljanja komunikacije, klijent prvo pokušava da uspostavi bezbednu IPSec komunikaciju. U slučaju da druga strana nema mogućnost bezbedne komunikacije, klijent spušta nivo bezbednosti i uspostavlja nešifrovanu komunikaciju.

- *Secure server*

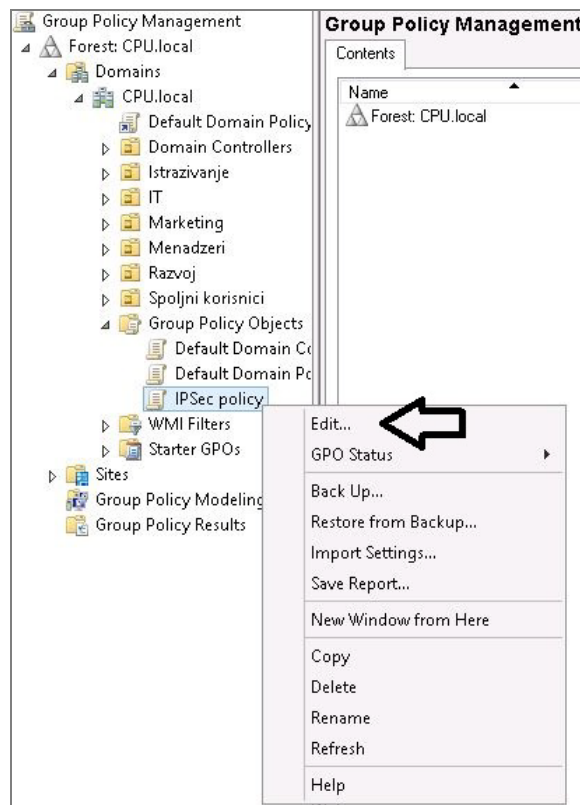
Ova polisa insistira na korišćenju šifrovane komunikacije i odbija bilo koji pokušaj nešifrovane komunikacije.

Međutim, pojavom *Windows Servera 2008* i *Windows Vista* klijenta, konfiguracija i sama lokacija IPSec polisa je promenjena, pošto je IPSec sada postao sastavni deo *Firewall* klijenta. Ovo ujedno znači da je *Firewall* sada sastavni deo svake komunikacije između klijenata. Iako prethodne tri polise više nisu u upotrebi, kada su u pitanju novije verzije Windows-a, polise koje se konfigurišu su slične i koriste iste principe.

IPSec polise koje se odnose na sve verzije *Windowsa* posle *Windows Servera 2008* i *Windows Vista* klijenta konfigurišu se kroz segment *Firewall* koji se zove *Connection Security Rules*.

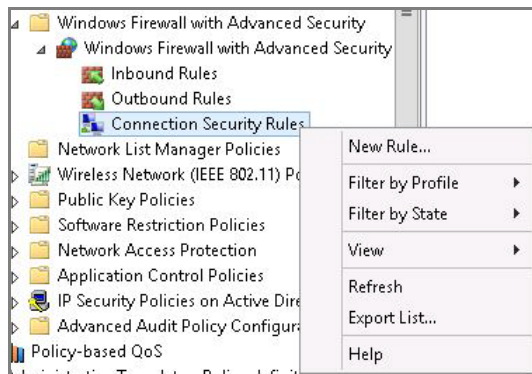
Procedura konfiguracije i instalacije IPSec polisa u aktivnom direktorijumu počinje kreiranjem nove grupne polise u domenu.

Pošto smo kreirali novu grupnu polisu i adekvatno je nazvali, možemo je prilagoditi našim potrebama (slika 47).



Slika 47: Konfiguracija IPSec polise

Potom je u segmentu *Windows Firewall* potrebno kreirati novi *Security Rule* u okviru koga sledi odabir tipa komunikacije koji želimo da osiguramo (slika 48).



Slika 48: *Connection Security Rules*

Postoje već predodređene mogućnosti za obezbeđivanje komunikacije u zavisnosti od njene namene i to su:

- Izolacija (*Isolation*)

Ovo pravilo izoluje računare na osnovu uslova kao što su pripadnost domenu ili postojanje odgovarajuće IPSec polise. Ovo pravilo omogućava kreiranje posebne izolovane komunikacione grupe u kojoj se komunicira samo uz pomoć IPSec-a.

- Izuzetak autentifikacije (*Authentication exemption*)

Koristiti se za izuzeće određenih računara od autentifikacije u slučaju da je ona neophodna. Primer predstavlja situacija u kojoj računari koji su izolovani prema prethodnoj polisi (*Isolation*) imaju potrebu da komuniciraju sa računarima koji nemaju konfigurisanu bezbednu komunikaciju ili nemaju tako visok nivo bezbednosti. Takođe, ovde se mogu definisati posebni opsezi IP adresa, sabneti ili ruteri prema kojima nije potrebna bezbedna komunikacija. Resursi mogu biti definisani kroz jedinstvene IP adrese ili kroz mrežne sabnete.

- *Server-to-server*

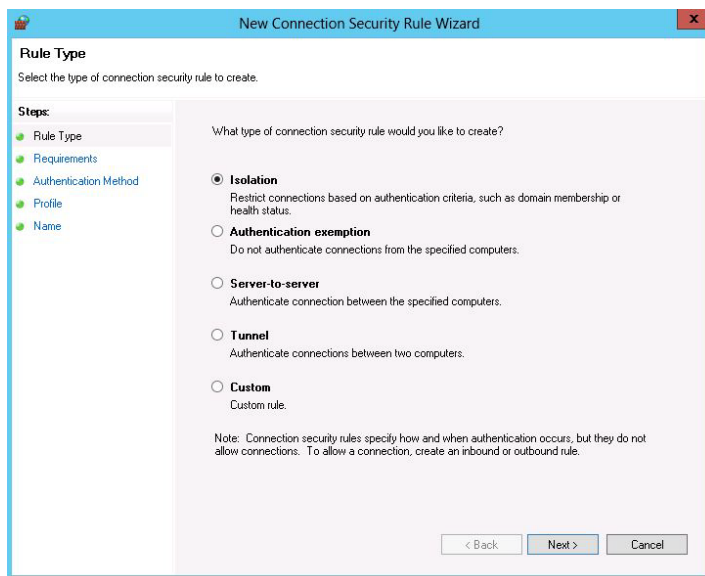
Server-to-server pravilo kreira vezu između određenih računara. Obično se koristi za direktno povezivanje servera.

- Tunel (*Tunnel*)

Tunel pravilo omogućava zaštitu veze između spoljnih rutera koji služe za povezivanje lokacija preko interneta između udaljenih delova mreže.

- Prilagođeno pravilo (*Custom*)

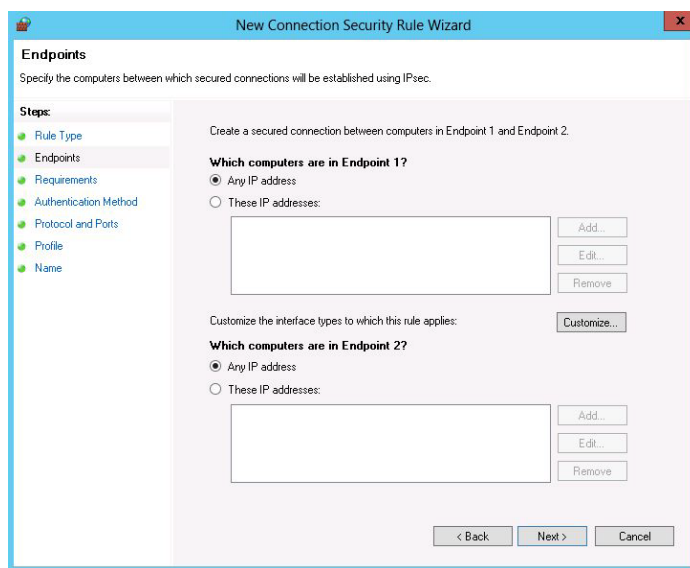
Ovo pravilo omogućava da sami korisnici kreiraju IPSec pravilo prema svojim potrebama (slika 49).



Slika 49: Tipovi bezbednosnih pravila

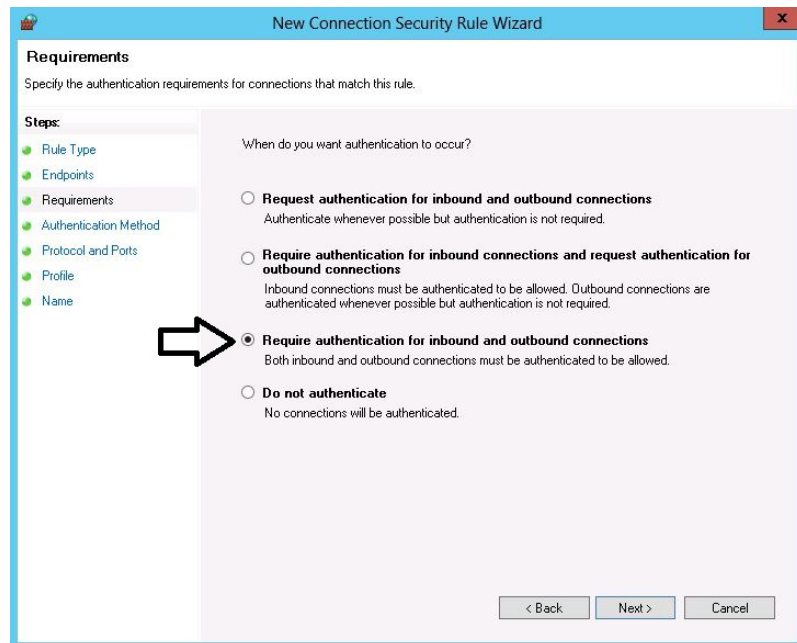
Međutim, kada bi IPSec komunikaciju implementirali na kompletan saobraćaj u mreži, on bi direktno rezultovao na usporen rad celokupne mreže. Ovo bi se ogledalo, ako ništa drugo, onda samo u povećanju količine mrežnog saobraćaja ogledanog kroz povećanje veličine paketa koji bi bili uvećani za AH i ESP hedere. Isto tako, retko gde postoji potreba da kompletan saobraćaj na mreži bude šifrovan i zato je neophodno kreirati prilagođene IPSec polise za posebne potrebe. Primeri mogu biti komunikacija po posebnim portovima između računara, za potrebe pojedinih aplikacija koje same nemaju mogućnost šifrovanja sadržaja ili komunikacija ka određenim serverima i resursima ili implementacija tih kombinacija.

Posle odabira prilagođenog pravila neophodno je da sledeći korak bude odabir izvorišnih i destinacionih IP adresa na koje će se ovo pravilo odnositi. Na primer, može se konfigurisati IPSec polisa u kojoj klijenti otvaraju sve WEB sajtove, kako internet tako i lokalne, koristeći nešifrovanu komunikaciju, ali ako žele da pristupe konkretnom WEB serveru na specifičnoj IP adresi, tog momenta ovo pravilo se aktivira i počinje bezbedna šifrovana komunikacija (slika 50).



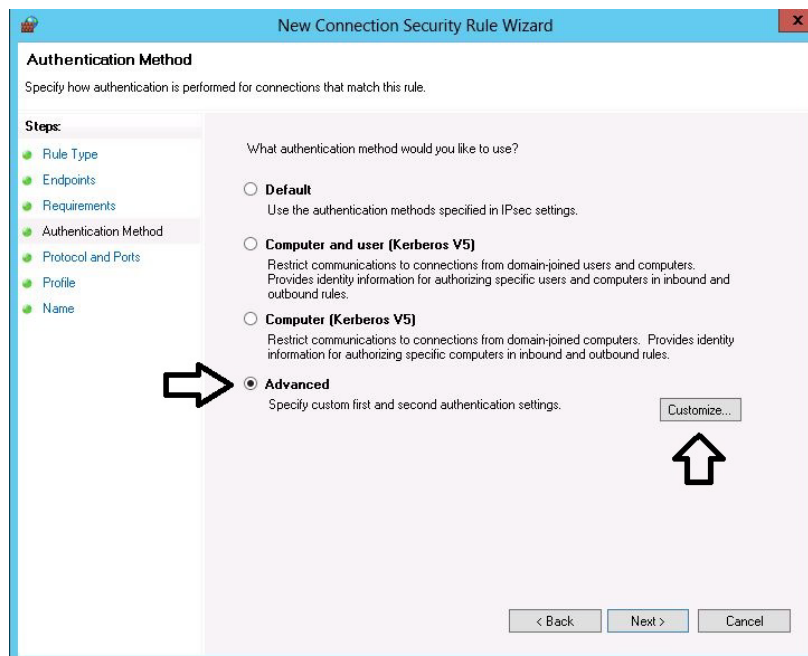
Slika 50: Odabir izvorišnog i destinacionog saobraćaja

Sledeći korak je odabir zahteva za predstavljanje strana koje učestvuju u komunikaciji (slika 51).



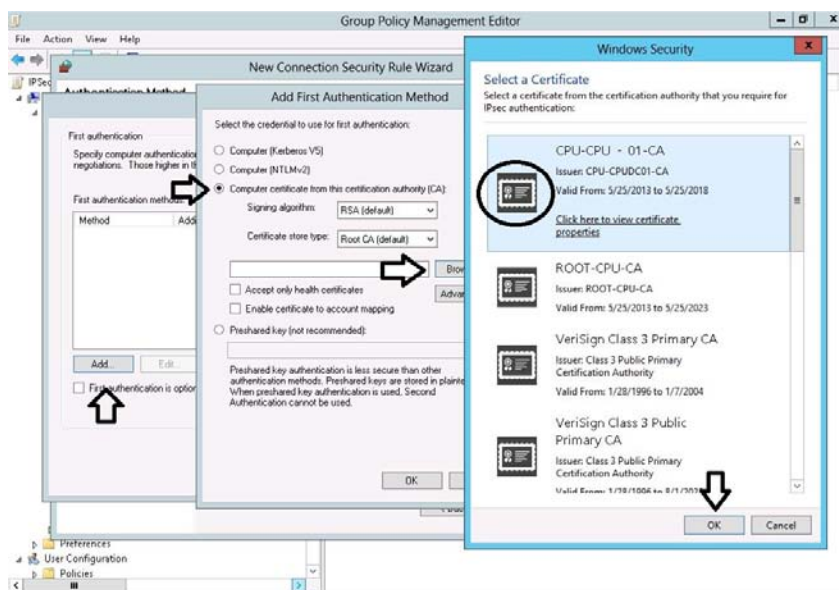
Slika 51: Odabir zahteva za bezbednom komunikacijom

Sledi odabir načina autentifikacije koristeći postojeće metode. Pošto u našem slučaju postoji potreba za mešovitom autentifikacijom, biramo naprednu konfiguraciju i dodatna podešavanja (slika 52).



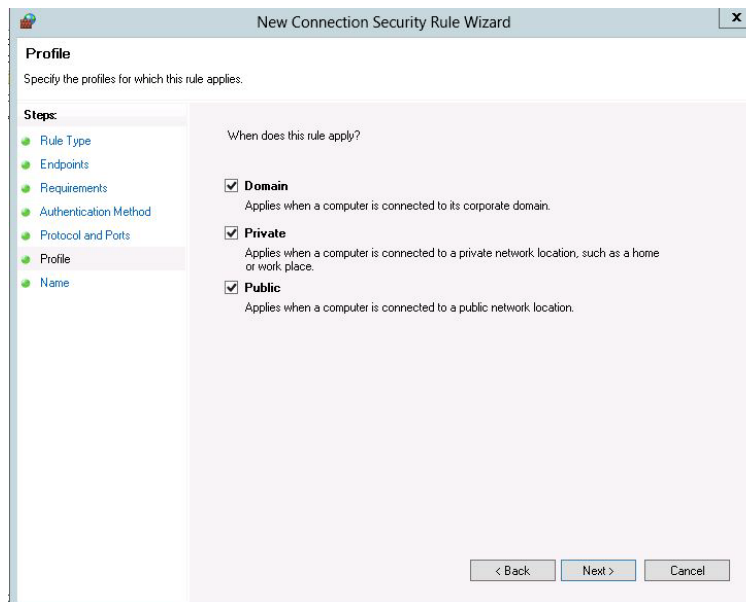
Slika 52: Odabir načina autentifikacije

Po otvaranju novih prozora možemo odabrati da li želimo samo autentifikaciju računara ili korisnika i računara (takozvani *two-step authentication*). Zatim se dodaje željeni način autentifikacije. U našem slučaju biramo sertifikate izdate od CA servera iz postojeće CA infrastrukture (slika 53).



Slika 53: Odabir načina autentifikacije

Neophodno je definisati i tip komunikacije, portove po kojima se ta komunikacija odvija, kao i na koje se mrežne profile ta komunikacija odnosi (slika 54).



Slika 54: Mrežni profili

Pravila koja su na ovaj način konfigurisana automatski se primenjuju na domenske računare. Da bi se ista podešavanja primenila i na računare u radnim grupama, ova podešavanja mogu se izvesti u fajl, a zatim preneti na željeni računar i potom primeniti.

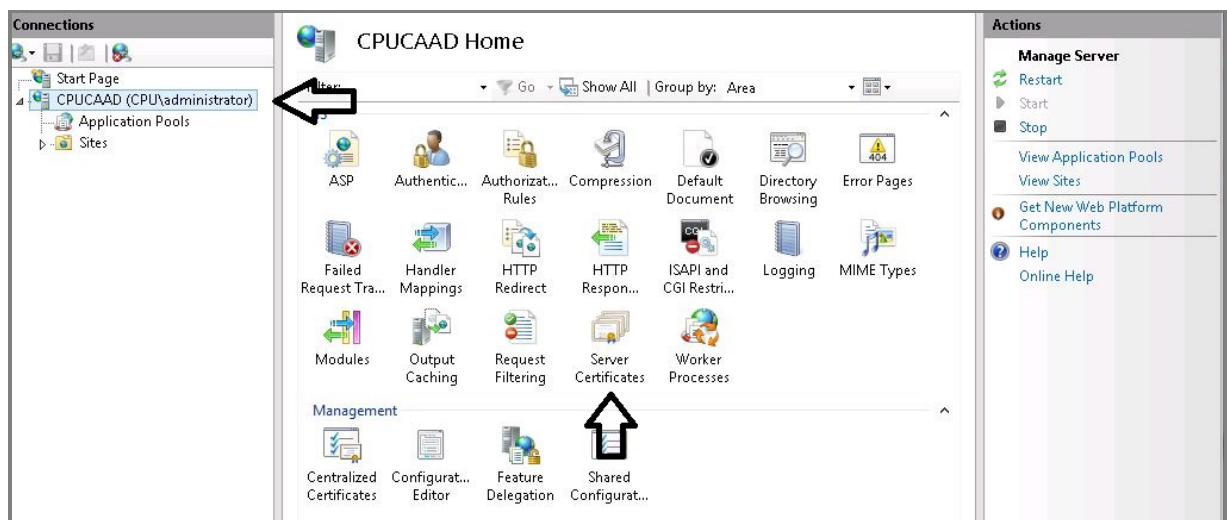
Međutim, još uvek ostaje problem izdavanja sertifikata računarima koji nisu članovi **CPU.local** domena. Prema potrebama projekta, neophodno je i da računari van **CPU.local** domena bezbedno komuniciraju sa pojedinim resursima koristeći IPSec polise i šifrovanu komunikaciju. Da bi se ovaj problem rešio, potrebno je izdavanje sertifikata i tim računarima. Ovo se može postići tako što će se sa tih računara zahtevati sertifikati kroz WEB interfejs koristeći SSL (*Secure Sockets Layer*) komunikaciju ka WEB serveru za izdavanje sertifikata.

7. Konfiguracija WEB servisa za bezbednu komunikaciju

Prilikom instalacije *Subordinate* CA servera i njegove konfiguracije, odabrali smo i opciju WEB *Enrollment-a*. Ovo ujedno znači da je na tom CA serveru već uključen i konfigurisan WEB server kao i WEB sajt za izdavanje sertifikata. Međutim, problem je u tome što, po predefinisanim opcijama, ovaj server prima komunikaciju koja nije šifrovana na portu 80. Da bi se postigla bezbedna SSL komunikacija i osiguralo izdavanje sertifikata, neophodno je da se konfiguriše IIS i WEB sajt za izdavanje sertifikata na način da prihvata samo komunikaciju koja je bezbedna i šifrovana.

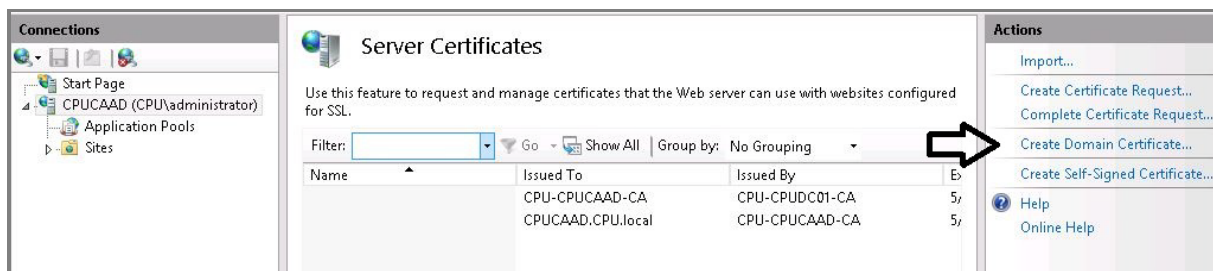
Da bi se ovo postiglo, prvo treba kreirati sertifikat za sam WEB server prema predefinisanom DNS imenu (npr. **www.cpu.local** ili **www.cpu.rs**) u zavisnosti da li tom WEB serveru treba da se omogući pristup iz privatne ili spoljne mreže. Ovo je neophodno pošto će to biti definisano u samom setifikatu kojim će se taj WEB server predstavljati klijentima i da bi se izbegle neželjene poruke kako se ime WEB servera i URL ime razlikuju. Potom se taj sertifikat koristiti za bezbednu komunikaciju koristeći SSL komunikaciju po portu 443. Zatim je još neophodno definisati i insistiranje na bezbednoj komunikaciji ka virtuelnom direktorijumu CA servisa na samom WEB sajtu.

Procedura se sastoji u tome da se prvo iz IIS konzole odabere WEB server i u centralnoj konzoli odabere opcija serverski sertifikati (slika 55).



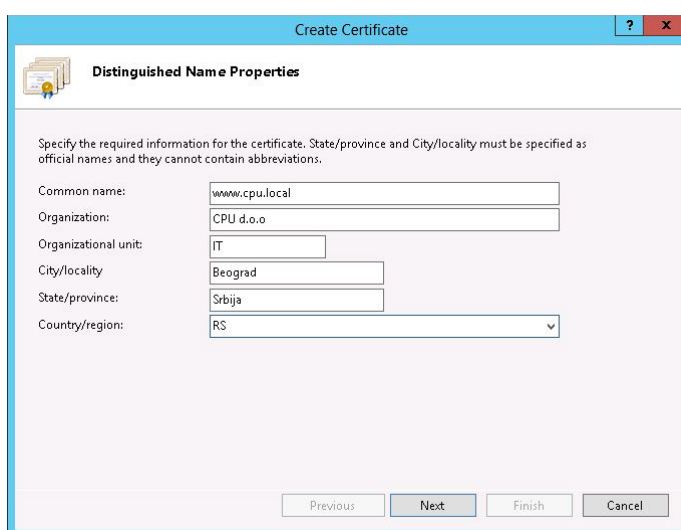
Slika 55: IIS konzola, konfiguracija serverskih sertifikata

Zatim je potrebno odabrati zahtev za domenskim sertifikatom. Kreiranje ovog zahteva je moguće pošto posedujemo domenski CA server koji je *online* i kome se veruje (slika 56).



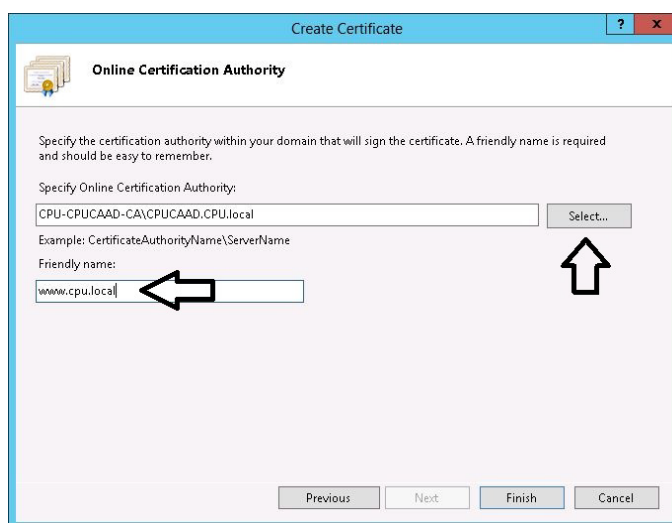
Slika 56: Odabir zahteva za domenski sertifikat

U zahtevu za sertifikatom neophodno je popuniti sve relevantne parametre da bi klijenti koji pristupaju tom WEB sajtu sa sigurnošću znali o kome se radi (slika 57).



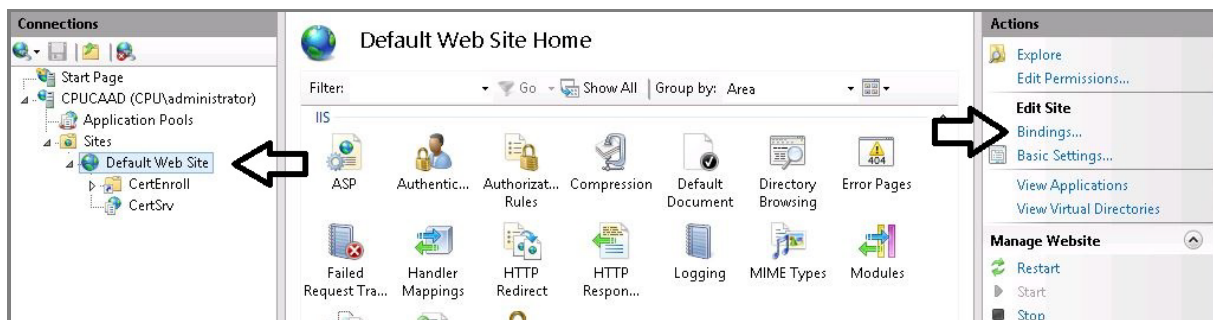
Slika 57: Zahtev sertifikata

Potom sledi odabir CA servera, u ovom slučaju *Subordinate* CA servera domena **CPU.local**. Važno je obratiti pažnju da *friendly name* koji se unosi treba da bude isto kao ime WEB sajta koje je unešeno na početku samog zahteva (slika 58).



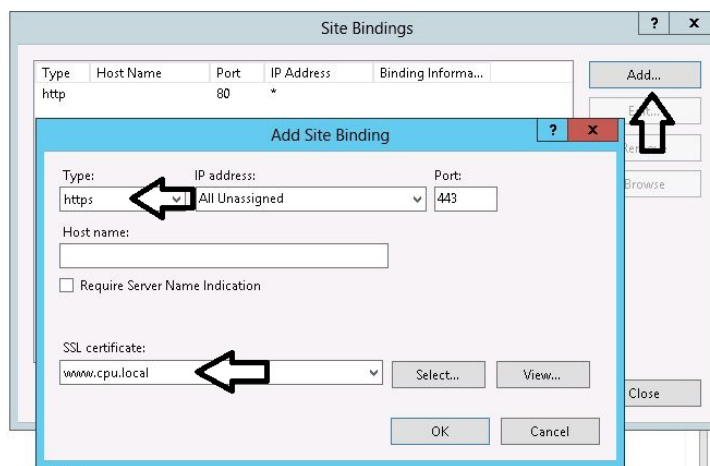
Slika 58: Odabir CA servera

Po uspešnom dobijanju sertifikata, na red dolazi konfiguracija SSL komunikacije u okviru kompletnog WEB servisa. Ovo se postiže kroz takozvano povezivanje (*Bindings*) (slika 59).



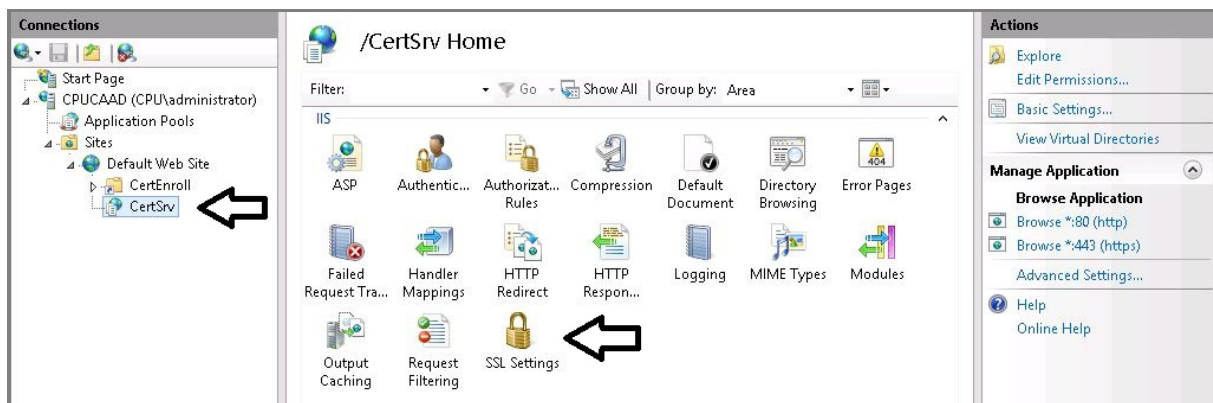
Slika 59: Konfiguracija SSL-a

Pošto su predefinisana podešavanja svakog novog instaliranog WEB servera takva da se koristi samo otvorena HTTP komunikacija preko porta 80, potrebno je dodati bezbednu komunikaciju. Ovo se postiže uz HTTPS koji koristi SSL na portu 443 i digitalne sertifikate za autentifikaciju i šifrovanje sadržaja (slika 60).

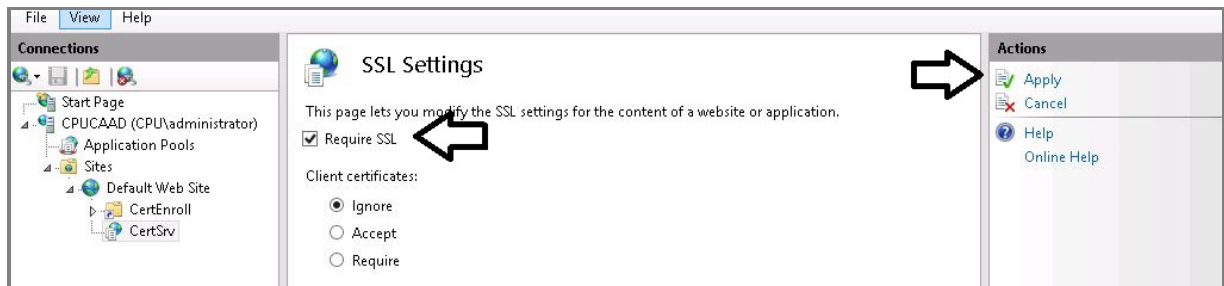


Slika 60: Dodavanje SSL-a i sertifikata

Kad je bezbedna komunikacija omogućena korišćenjem SSL-a, neophodno je konfigurisati i insistiranje na korišćenju bezbedne komunikacije. Ovo se postiže tako što se za određeni virtuelni direktorijum ili za ceo Web sajt, u okviru njegovih SSL podešavanja, uključi opcija za insistiranje na bezbednoj komunikaciji (slike 60 i 61).

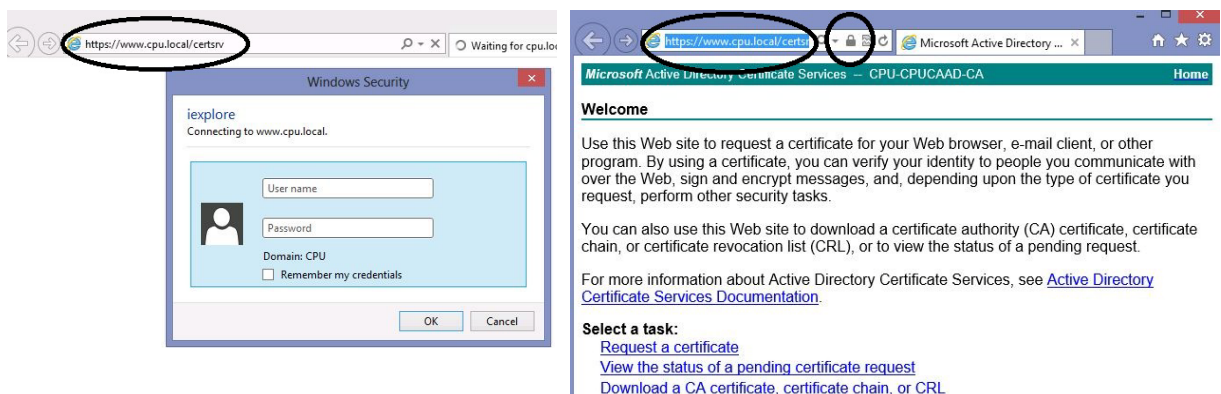


Slika 60: Podešavanje SSL-a



Slika 61: Odabir virtuelnog direktorijuma i bezbedne komunikacije

Ostalo je još samo da se pristupi bezbednom WEB sajtu i da se svim klijentima koji imaju potrebu za bezbednom komunikacijom izdaju potrebni sertifikati (slika 62).



Slika 62: Bezbedan pristup CA serveru kroz WEB konzolu

Na ovaj način osigurano je bezbedno izdavanje sertifikata koristeći WEB interfejs za potrebe kako domenskih računara i korisnika, tako i korisnika koje se ne nalaze u aktivnom direktorijumu **CPU.local**.

8. Bezbedna komunikacija DNS servisa

Sledeći korak u implementaciji traženog rešenja je obezbeđivanje DNS servisa i kreiranje bezbedne komunikacije s njim.

Polazeći od samog početka upotrebe DNS servisa, on je funkcionisao kao veoma robustan servis. Sa svakom novom verzijom, DNS servis je poboljšavan, kako funkcionalno tako i sa bezbednosnog aspekta. Vremenom su počeli da se uočavaju nedostaci u funkcionalnosti i bezbednosti. Međutim, kako je DNS servis napredovao tako su se pojavljivali i novi načini da se on zloupotrebi, tako da napade na DNS servis možemo podeliti u dve grupe.

Prva grupa napada svodi se na onemogućavanje servisa da funkcioniše, a primer bi mogao biti neki vid DoS napada. Ovi napadi predstavljaju problem sa te strane što sprečavaju klijente da razlučuju imena i predstavljaju opasnost kao i svaki drugi *Denial of Service* napad.

Međutim, druga grupa napada predstavlja mnogo veći problem pošto se radi o napadima koji menjaju informacije u samom DNS servisu ili omogućavaju napadačima da se predstavljaju kao autorizovani DNS serveri. Ovakvi napadi mogu da prouzrokuju mnogo veću štetu nego DoS napadi. Ova činjenica se zasniva na tome da, ako napadač može da promeni informacije o konkretnom *web* sajtu ili mejl serveru, sav saobraćaj može da preusmeri u njemu željenom smeru što predstavlja ogroman problem. Neki od primera ovih napada su *Name-Jacking* i *DNS Cache Poisoning*.

8.1. Primer zaštite DNS-a uz pomoć zaštite DNS keša od promena

Svaki DNS, kao sastavnu komponentu, koristi *Cache* da bi smanjio količinu nepotrebnog saobraćaja. Ovo funkcioniše tako što se rezultati razlučenih pretraga smeštaju u keš i dobijaju TTL (*Time to Live*). Samim tim se ne proveravaju ponovo do isteka samih rekorda koji su keširani. Međutim, i tu postoji mogućnost zloupotrebe koja se ogleda u tome što maliciozni softver ili korisnik menja sadržaj keša (*Cache Poisoning* tip napada) i na taj način preusmerava tok saobraćaja u neželjenom smeru.

Jedan način zaštite predstavljao bi zaštitu keširanih rezultata pretraga. Što se *Windows* servera tiče, ova opcija postala je standard sa verzijom *Windows Server 2008R2*. Ovim putem omogućeno je da se rezultati pretraga DNS-a koji se keširaju, zaštite zaključavanjem prema našim potrebama. To se može postići komandom koja služi za menadžment DNS-a "*dnscmd*" pokrenutom iz komandnog prompta, ili iz *powershell*-a koristeći komandu "*Set-DnsServerCache*."

Koristeći ova saznanja, firma CPU d.o.o. je, svakom ponaosob, na domenskim i javnim DNS serverima, zaključala promene na keširanim vrednostima na 100% vremenskog limita (TTL-a). U primeru su date dve komande, prva koja se pokreće iz komandnog prompta i druga koja se pokreće iz *powershell*-a.

dnscmd /Config /CacheLockingPercent 100

Set-DnsServerCache –LockingPercent 100

U konkretnom slučaju, korišćene su samo promene uz pomoć *powershell*-a koji je sastavni deo operativnog sistema.

8.2. Zaštita DNS-a slučajnim izborom portova za odgovor klijentu

Predefinisano stanje DNS servisa je da koristi isti port za prijem i odgovor na upite. Međutim, ta funkcionalnost DNS-a koristi se i za *Cache Poisoning* tip napada. Zato bi bilo dobro da se portovi randomizuju, tako da se ne koristi predodređeni port za odgovor kao što je i port za zahtev.

Ovakav tip zaštite funkcioniše tako što se svaki put kada se DNS servis pokrene, bira različit port za komunikaciju sa klijentima iz predefinisano opsega portova, umesto da se koriste predefinisani portovi. Ovo ujedno smanjuje mogućnost *Cache Poisoning* tipa napada pošto napadač sada mora da pogodi izvorni port DNS upita kao i *transaction ID* da bi izvršio uspešan napad. Podrazumevana količina portova koje DNS servis može da koristi je 2.500 portova, ali se ovu vrednost možemo podići do 10.000 portova. Mogućnost da DNS server koristi slučajan izbor portova veći od 10.000 postoji od verzije servera 2008R2. Primer korišćenja ove mogućnosti dat je u komandi "*dnscmd*" u okviru koje <vrednost> predstavlja broj portova koje ostavljamo DNS servisu na korišćenje.

dnscmd /Config /SocketPoolSize 10000

Koristeći ovu mogućnost, firma CPU d.o.o. konfigurisala je domenske i javne DNS servere na maksimalne vrednosti i tako su smanjili mogućnost slučajnog pogađanja portova od strane napadača, mada je to bilo moguće uraditi komandom kao u primeru.

Odlučeno je da se koristi promena baze registra (*registry*) na svim DNS serverima. Za potrebe implementacije promene baze registra, korišćene su grupne polise za domenske DNS servere i lokalne polise na javnim DNS serverima.

Izmene primenjene na domenskim DNS serverima ogledaju se u podešavanju veličine *pool*-a na 10.000 kao i otvaranju slučajnih portova u rasponu između 1 - 65.535. Međutim, promene koje su implementirane na javnim DNS serverima donekle se razlikuju. Npr. veličina *pool*-a podignuta je na 10.000 ali je broj portova koji se koriste smanjen i limitiran na poseban opseg koji mora dinamički da se otvori na *firewall*-u.

Firma CPU d.o.o. odlučila se za implementaciju kroz promenu baze registra, kao i implementaciju kroz polise iz razloga uniformnosti rešenja, kako za lokalne tako i za javne DNS servere. U tabeli je dat primer mogućih promena.

Tabela 1: Raspored portova koji se koriste u DNS komunikaciji

Setting name	Location	Type	Default value	Possible values
SocketPoolSize	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\DNS\Parameters	REG_DWORD	2500	0 to 10000
SocketPoolExcludedPortRanges Windows Server 2008 R2 only.	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\DNS\Parameters	REG_MULTI_SZ	N/A	1 to 65535 Configured as a port range (ex: 4000-5000). To specify a single port, use the same start and end value.
 Conseil				
To apply changes to settings for the Socket Pool, you must restart the DNS service.				

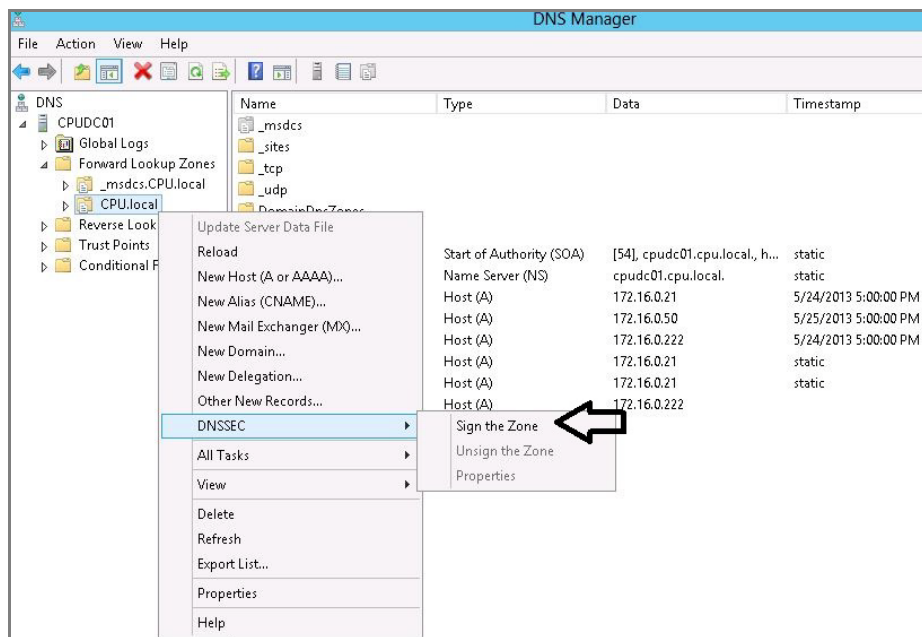
8.3. Zaštita DNS servisa koristeći DNSSEC

Kao i u prethodnim slučajevima, napadi na DNS predstavljaju veliki problem i svaka promena rekorda ili lažno predstavljanje mogu napraviti problem u razlučivanju imena. Ovakvi napadi naročito mogu imati nesagledive posledice kada su u pitanju napadi na *web*-prodavnice ili mejl servere. Kada je komunikacija između klijenata i servera u pitanju, upotreba digitalnih potpisa je metoda koje se koristi u toj ili sličnim situacijama. Upotreba digitalnih potpisa u DNS servisu postala je moguća od verzije *Windows Server 2008R2*, ali je tek u verziji *Windows Server 2012* dobila potpunu funkcionalnost.

Digitalni potpisi u DNS servisu funkcionišu tako što se generiše par ključeva sa strane DNS servisa za svaku DNS zonu ponaosob. Prilikom kreiranja zona koje se potpisuju, kreiraju se ključevi KSK (*Key Signing Key*) i ZSK (*Zone Signing Key*). Ovi ključevi se kasnije mogu koristiti za potpisivanje višestrukih zona ili kreirati ponaosob za svaku zonu. Ovi ključevi se zajedničkim imenom nazivaju DNSKEY. Prilikom potpisivanja zone kreira se i novi tip DNS rekorda sa imenom *resource RRSIG (Resource Record Signature)*. Međutim, da bi se ostvarila puna funkcionalnost ovog rešenja potrebno je i da klijentski operativni sistemi budu svesni ovih mogućnosti. Klijentski operativni sistemi koji su svesni DNSSEC-a su *Windows 7* i kasniji klijenti, kao i *Windows Server 2008R2* i kasnije verzije. Takođe je bitno razumeti da je neophodno konfigurisati servere i klijente da koriste DNSSEC u slučaju da poseduju podršku za ovo rešenje. Ovo se postiže tako što se implementira NRPT (*Name Resolution Policy Table*) koji predstavlja set pravila vezanih za postavljanje upita kao i validacije odgovora dobijenih od DNS servisa.

8.4. Procedura konfiguracije DNS-a

Procedura instalacije i konfiguracije digitalnog potpisivanja DNS zona odvija se na sledeći način. Prvi korak je odabir DNSSEC opcije u okviru DNS konzole (slika 63).



Slika 63: Digitalno potpisivanje DNS zone

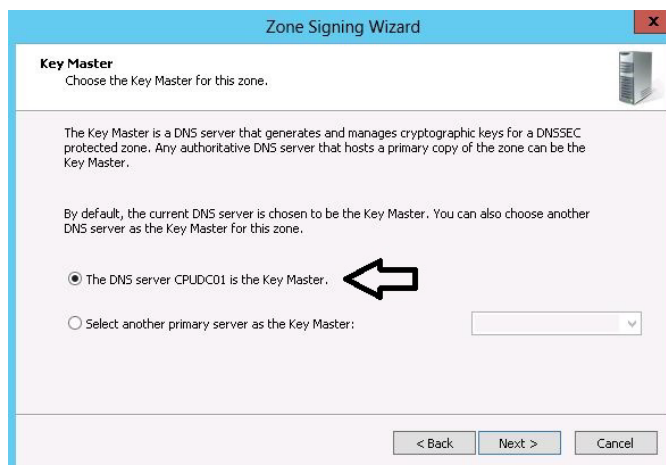
Potom je potrebno odabrati koji će se ključ koristiti za potpisivanje DNS zone, drugim rečima da li se kreira novi ili se koristi postojeći ključ. U našem slučaju, pošto ne posedujemo *Zone Signing Key*, moramo da kreiramo novi (slika 64).



Slika 64: Zone Signing Key

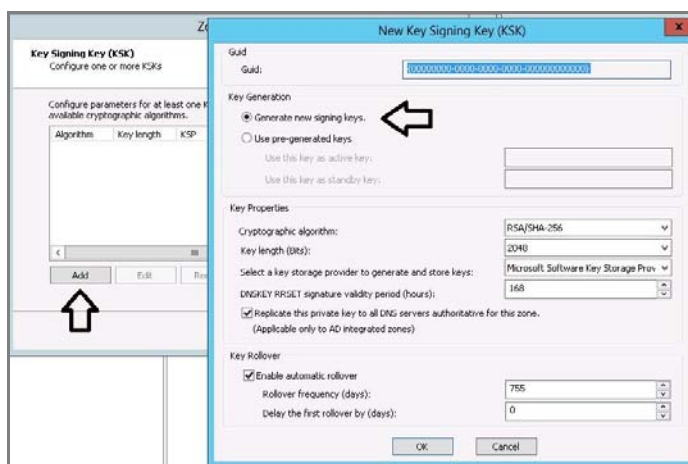
U sledećem koraku se definiše koji će DNS server biti nosilac ključeva (*Key Master*). Ova uloga obično je namenjena DNS serveru na kome se nalazi primarna zona za odgovarajući *Namespace*.

Obzirom da je DNS server na kome smo pokrenuli čarobnjak za potpisivanje zone, odabraćemo opciju da se ključevi čuvaju na njemu (slika 65).



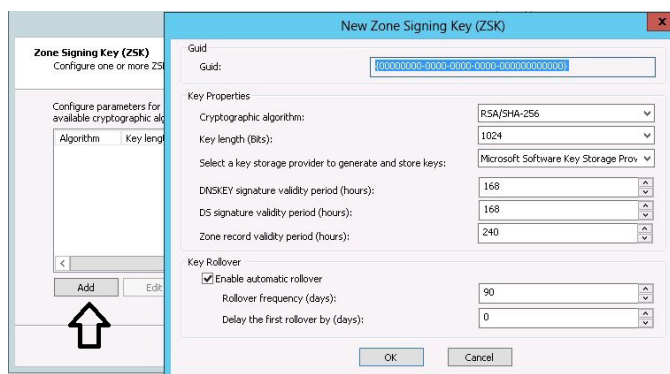
Slika 65: Odabir *Key Master-a*

Sledi generacija KSK (*Key Signing Key*) ključa, odabir njegove dužine, načina šifrovanja kao i dužina regeneracije (obnavljanja) istog. Ovaj ključ ujedno autentifikuje autorizovani DNS server (slika 66).



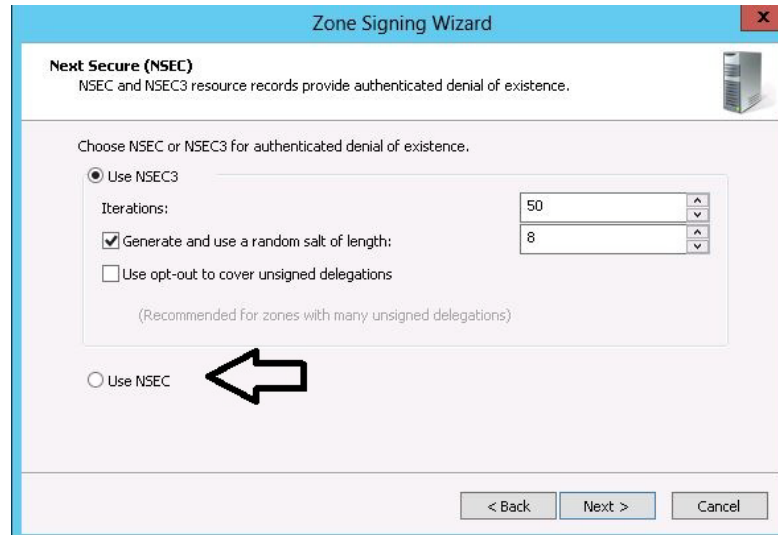
Slika 66: Kreiranje KSK ključa

Potom se generiše ZSK (*Zone Signing Key*) koji će služiti za digitalni potpis same zone (slika 67).



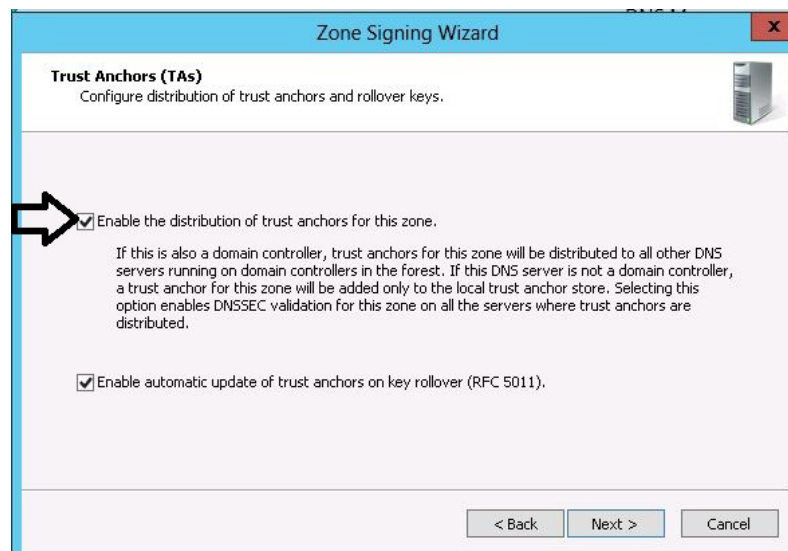
Slika 67: Kreiranje ZSK ključa

Sledi odabir kompatibilnosti digitalnog potpisa prema tipu klijenata koji će moći da koriste usluge ovog digitalnog potpisa. NSEC3 je moguće implementirati samo na *Windows Serveru 2012* i kasnijim, a podržavaju ga klijenti *Windows 8* i kasniji. Obzirom da u postojećem okruženju imamo i starije verzije operativnih sistema, neophodno je da odaberemo NSEC opciju za digitalni potpis (slika 68).



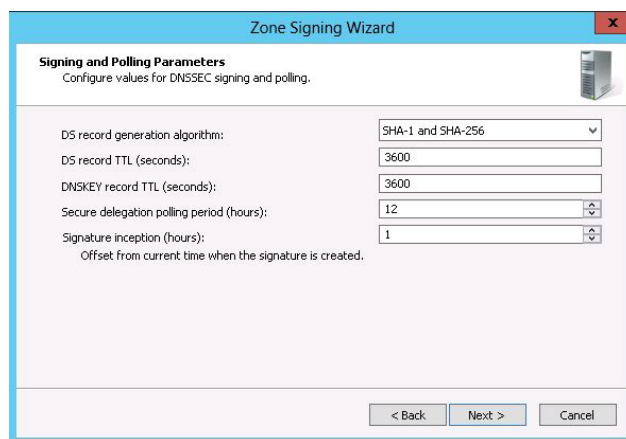
Slika 68: Konfiguracija kompatibilnosti

Pošto se DNS zona **CPU.local** nalazi na domenskom kontroleru i uzevši u obzir da u aktivnom direktorijumu postoji *multimaster* replikacija informacija aktivnog direktorijuma između domenskih kontrolera u koju je uključen i *Active Directory Integrated DNS Zone*, neophodno je da svi domenski kontroleri budu na listi DNS servera koji mogu da potpišu zonu digitalnim ključem (slika 69).



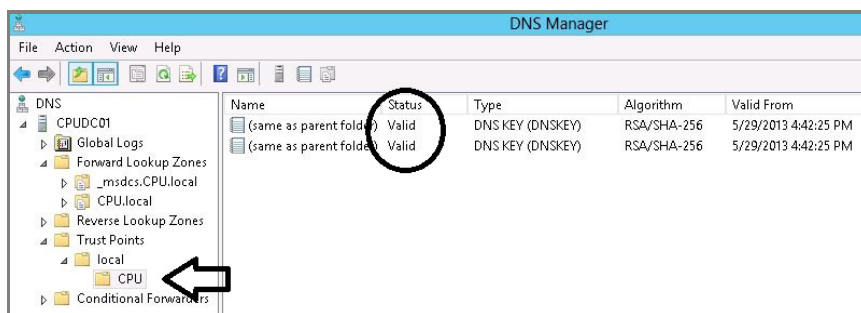
Slika 69: Smeštanje ključa u AD

Sledi sumarizovana informacija o konfiguraciji (slika 70).



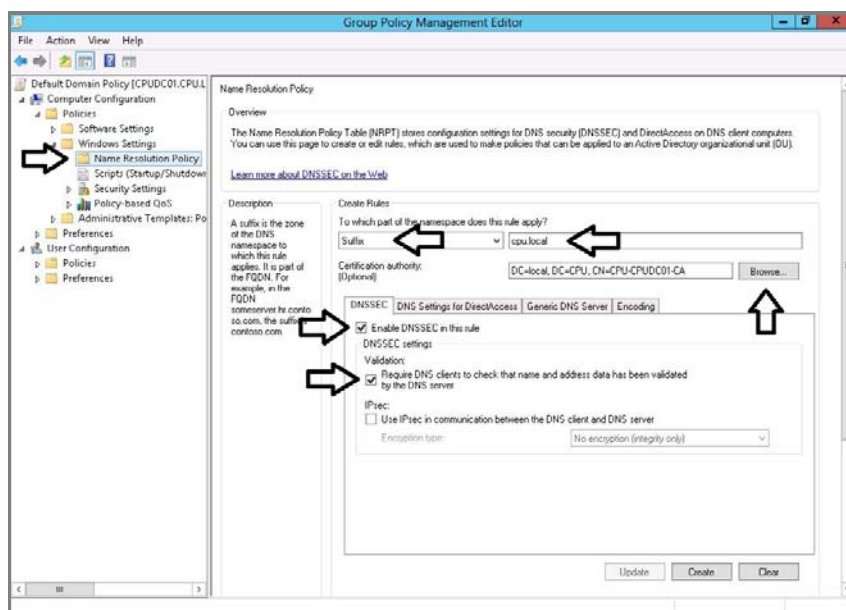
Slika 70: Kraj čarobnjaka

Po završetku konfiguracije digitalnog potpisivanja DNS zone, možemo proveriti da li su kreirani neophodni ključevi, kao i da li su oni funkcionalni (slika 71).



Slika 71: Provera validnosti DNS ključeva

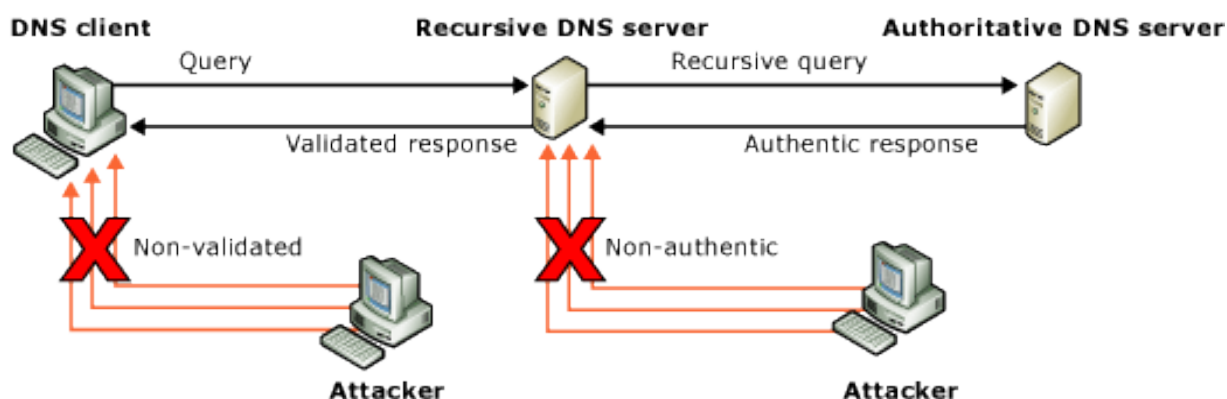
Pošto smo konfigurisali digitalno potpisivanje zona na DNS serverima, sledi konfiguracija klijenata. Drugim rečima, sada je neophodno klijentima propagirati informacije na koji način da komuniciraju sa DNS serverima na bezbedan način (slika 72).



Slika 72: Konfiguracija Name Resolution polise

Pored informacija o digitalnom potpisivanju, ovde je takođe moguće konfigurisati i šifrovanje zone uz pomoć IPsec-a. Ovako konfigurisan DNS server i klijenti trenutno nude jedan od najviših modova zaštite u okviru razlučivanja imena, a samim tim podižu nivo bezbednosti komunikacije na viši nivo.

Na slici 73 prikazan je upit klijenta ka DNS servisu koji poseduje digitalno potpisanu zonu. Po prijemu upitu od klijenta, DNS servis vraća informaciju o RRSIG rekordu koja klijentu ukazuje da je zona digitalno potpisana i potom šalje traženu informaciju koja je potpisana sa DNSKEY ključem DNS servisa. Po dobijanje odgovora od DNS servisa, klijent proverava da li je odgovor potpisan odgovarajućim ključem i, u slučaju da je to istina, klijent prihvata odgovor kao validan i počinje sa uspostavljanjem veze sa traženom adresom.



Slika 73: Bezbedna komunikacija uz pomoć digitalno potpisanih DNS zona

Kako je ovo trenutno jedan od najboljih vidova zaštite, u kompaniji CPU d.o.o. koristi se sledeći skup operativnih sistema, koji je prikazan u tabeli.

Tabela 2: Struktura računara u okviru školskog centra kompanije CPU d.o.o.

Serverski operativni sistem	Procenat	Klijentski operativni sistem	Procenat
Windows Server 2012	95%	Windows 8	70%
Windows Server 2008R2	4%	Windows 7	28%
Windows Server 2003	1%	Windows XP/Windows Vista	2%

Takođe, uzevši u obzir informacije iz prethodne tabele, možemo primetiti da postoje klijenti i serveri koji direktno ne podržavaju ovo rešenje, kao što su *Windows Server 2003* i *XP/Vista*. Ovi klijenti i serveri mogli bi predstavljati problem u implementaciji ukoliko bi postojala potreba da se uključe u dato rešenje. Međutim, zahvaljujući dodatnim informacijama o upotrebi ovih klijenata samo za posebna test okruženja koja su nezavisna u komunikaciji, može se zaključiti da oni neće praviti problem prilikom implementacije rešenja.

Za samu implementaciju rešenja bitno je da svi klijenti i serveri imaju operativne sisteme koji su kompatibilni sa ovim rešenjem, što je istina u ovom slučaju. Zahvaljujući ovim saznanjima, firma CPU d.o.o. odlučila je da implementira digitalno potpisivanje zona na domenskim DNS serverima i to samo za domenske zone. Tako su iskorišćeni benefiti novih mogućnosti koje donosi *Windows Server 2012* koji se ogledaju u novim čarobnjacima (*wizard*-ima) ubačenim u DNS konzolu i grupne polise.

9. Zaključak

Bezbednost računarske mreže u celini mora da se gleda kao skup pojedinačnih bezbednosti svih subjekata koji učestvuju u komunikaciji. Veoma je bitno da zaštita svakog pojedinačnog subjekta, servisa ili aplikacije pojedinačno, ali i u celini, podiže nivo bezbednosti celokupnog rešenja.

Implementacija domenskog rešenja i aktivnog direktorijuma, pored prednosti centralizovane autentifikacije, nosi i prednost povećanja bezbednosti kada je pristup resursima u pitanju. Ovo se postiže kroz višestruke provere kako korisnika, tako i računara, što ujedno podiže nivo bezbednosti celokupnog rešenja.

Curenje informacija i zloupotreba pristupa predstavljaju ogroman rizik za svaku kompaniju. Postupcima koji su ovde primenjeni, kao što su upotreba IPSec-a za šifrovanje komunikacije, omogućava da se sadržajima koji se nalaze u okviru kompanije bezbedno pristupa iznutra i spolja, a ujedno se smanjuje mogućnosti zloupotreba i curenja poverljivih informacija.

Bezbedan pristup sadržajima i nepromenljivost čine bitne faktore za sve resurse koji se objavljuju na WEB serverima za lokalne i za spoljne korisnike. Upotrebom digitalnih sertifikata sigurnih portova i IPSec komunikacije, postizemo bezbednost kako samih servera, tako i sadržaja koji su na njima objavljeni.

Napadi na DNS servis predstavljaju veliku opasnost i otvaraju mnogo mogućnosti za zloupotrebu. Zbog toga postoji potreba za podizanjem nivoa zaštite. Svako dodatno povećanje zaštite, koliko god ono bilo jednostavno ili kompleksno za implementaciju, smanjuje mogućnost zloupotrebe datog servisa. Kada je DNS servis u pitanju, implementacija jednog ili više ponuđenih rešenja može da pomogne u podizanju nivoa bezbednosti razlučivanja na jedan sasvim prihvatljivo visok nivo. Samim tim se ujedno smanjuju, ili skoro u potpunosti onemogućavaju, mogućnosti zloupotrebe samog servisa.

U konkretnom primeru kompanije CPU d.o.o treba napomenuti da su ispunjeni svi zahtevi koji su stavljani pred nas, da se ostvari bezbedna komunikacija i bezbedno razlučivanje imena. Ovim rešenjem, kao i drugim koja su implementirana zarad povećanja nivoa bezbednosti komunikacije i podataka, zadovoljeni su veoma visoki standardi bezbednosti među kojima je i ISO 27001 standard.

10. LITERATURA

1. Rad za konferenciju

Načini zaštite DNS servisa

Autor: Ljubomir Ivaniš, 2012

2. Knjiga:

„Računarske mreže“

Autori: Mladen Veinović, Aleksandar Jevremović. ISBN 978-86-7912-368-8;

COBBIS.SR-ID, 2011

3. Knjiga:

20410B: Installing and Configuring Windows Server® 2012

Autori: Stan Reimer, Damir Dizdarević, Gary Dunlop i drugi, 2012

4. Knjiga:

20411B: Administering Windows Server® 2012

Autori: Andrew J. Warren, Jason Kellington i drugi, 2012

5. Knjiga:

20412B: Configuring Advanced Windows Server® 2012 Services

Autori: Stan Reimer, Damir Dizdarević, Orin Thomas, 2012

6. Knjiga:

20417A: MCT Prep - Upgrading Your Skills to MCSA Windows Server 2012

Autor: Microsoft, 2012

7. Knjiga:

6406B: First Look: Getting Started with Security and Policy Control in Windows Server® 2008

Autor: Microsoft, 2008

8. Knjiga:

6436A: Designing Active Directory® Infrastructure and Services in Windows Server® 2008

Autor: Microsoft, 2008

9. Knjiga:

6415A: Updating your Network Infrastructure Technology Skills to Windows Server 2008

Autor: Microsoft, 2007

10. Knjiga:

2830A: Designing Security for Microsoft® Networks

Autor: Microsoft, 2002

11. Knjiga:

2277C: Implementing, Managing, and Maintaining a Microsoft® Windows Server.

2003 Network Infrastructure: Network Services

Autor: Microsoft, 2005

12. Knjiga:

2823B: Implementing and Administering Security in a Microsoft® Windows Server. 2003 Network

Autor: Microsoft, 2005

13. Online izvori - web strana:

Windows Firewall with Advanced Security and IPsec [online]. Dostupno na:

[http://technet.microsoft.com/en-us/library/cc732283\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc732283(v=ws.10).aspx)

[pregledano 25.05.2013]

14. Online izvori - web strana:

Secure DNS Deployment Guide [online]. Dostupno na:

[http://technet.microsoft.com/en-us/library/ee649266\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee649266(v=ws.10).aspx)

[pregledano 25.05.2013]