RNIDS
Registar nacionalnog internet domena Srbije

.rs .срб

DNSSEC u Srbiji

Žarko Kecić

RSNOG / novembar 2017. Beograd

Ako kontrolišem vaš DNS...

... mogu da kontrolišem vaš svet.

Koristite online banking? Trgujete na Amazonu ili eBay-y? Šaljete i primate važne poslovne e-mail poruke?

U 2016. 51% ukupne trgovine obavljeno je online.

(Izvor: http://fortune.com/2016/06/08/online-shopping-increases/)

Poslovi vredni stotine hiljada milijardi $ oslanjaju se na DNS sistem koji je definisan početkom 80tih bez razmišljanja o bezbednosti.

Ako neko kontroliše vaš DNS može vas preusmeriti gde god želi!

Da li zaista možete da verujete DNS sistemu?

Većina Internet korisnika ne razume DNS, pre svega, jer im nije potrebno da razumeju kako radi da bi koristili Internet. ***DNS jednostavno funkcioniše i korisnici mu veruju!***

DNS je dizajniran da podaci budu dostupni.

- DNS podaci se repliciraju na više servera.
- DNS zona „radi“ ako je samo jedan server dostupan.

DNS ne uključuje proveru autentičnosti i tačnosti podataka.

- Bilo koji DNS odgovor se prihvata.
- Nema načina da resolver razlikuje ispravne od neispravnih odgovora.

Zašto nam je potreban DNSSEC?

U međuvremenu pojavilo se mnogo korisnika, a neki od ih nemaju baš dobre namere.

- **Man in the middle** – presretanje i izmena DNS odgovora.
- **Cache poisoning** – ubacivanje pogrešne informacije u DNS podatke koje „resolveri“ čuvaju lokalno.
- **Malware** – destruktivni programi koji mogu da izmene **host** fajl ili podatke o DNS serverima.
- **DoS, DDoS i rDDoS napadi** – DNS predstavlja jednu od najkorišćenijih tehnologija za sprovođenje napada na druge sisteme (botnet command and control)

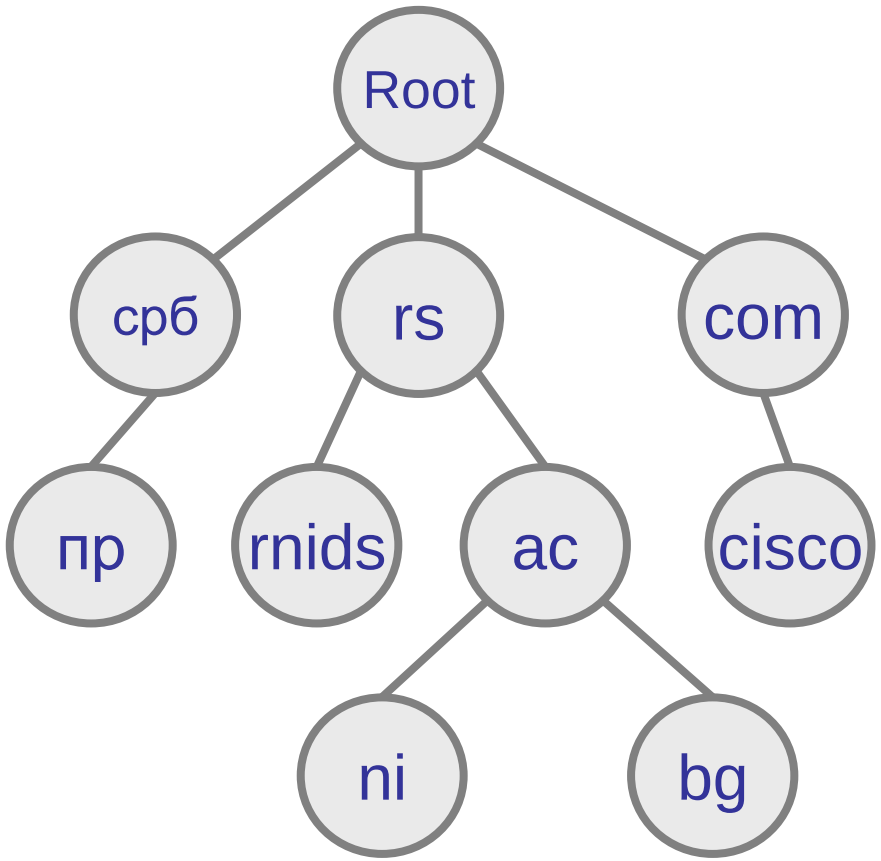
DNS sistem

Osnovni zadatak DNS sistema je mapiranje naziva domena u IP adresu:

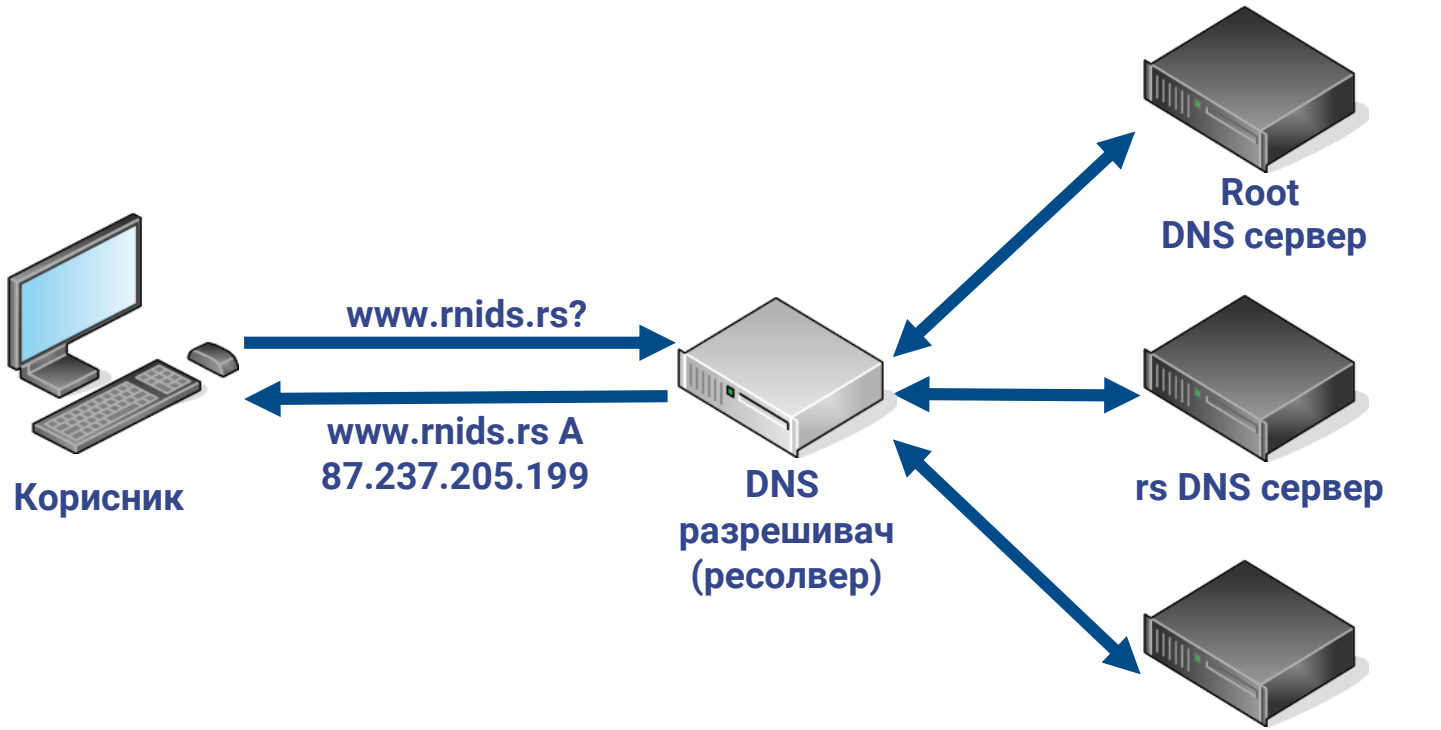
- www.rnids.rs = *87.237.205.199*
- Kao i mnoga druga mapiranja (e-mail servis (MX), IPv6 (AAAA), inverzno mapiranje…)

DNS je hijerarhijski organizovan

- Svaka zona ima autoritativnu DNS strukturu i sadrži lokalne podatke.

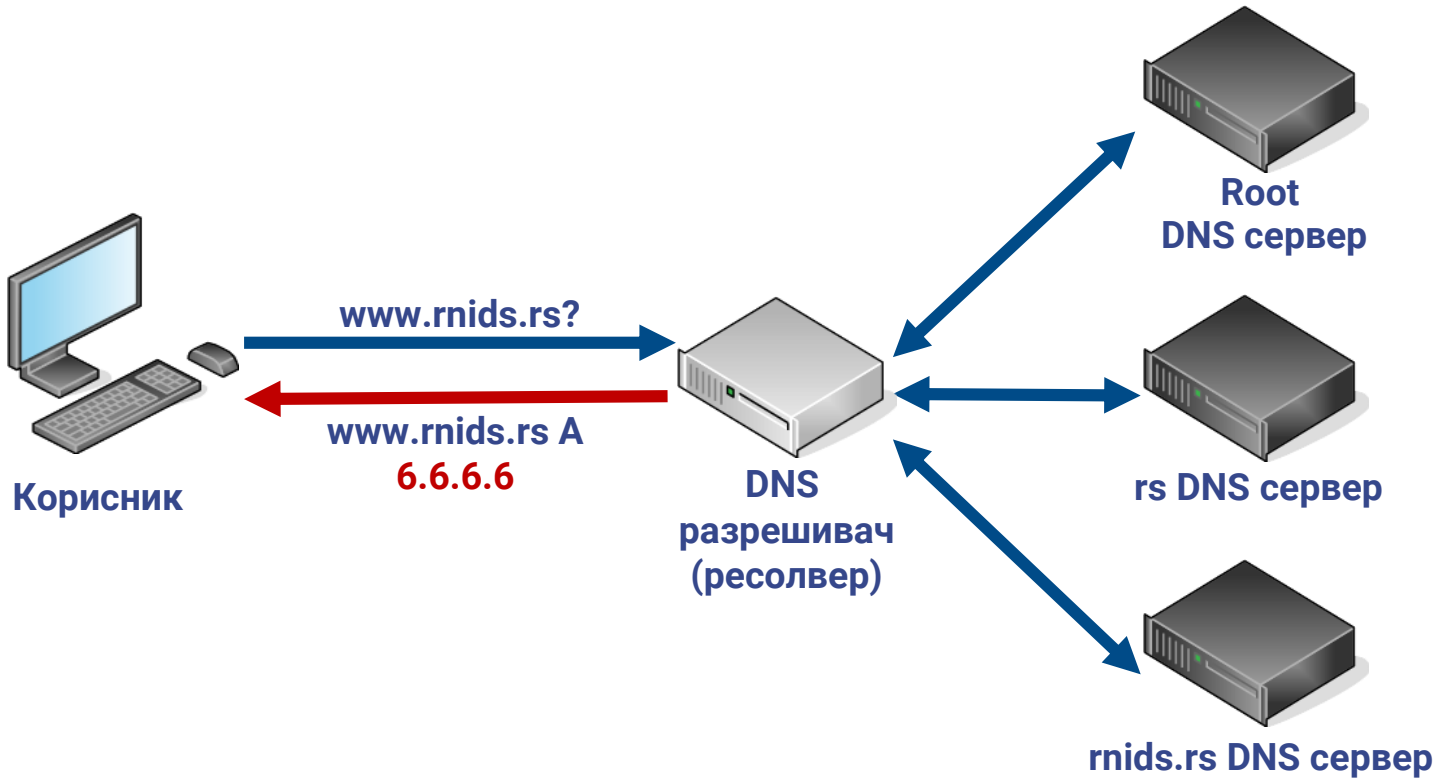


Kako radi DNS



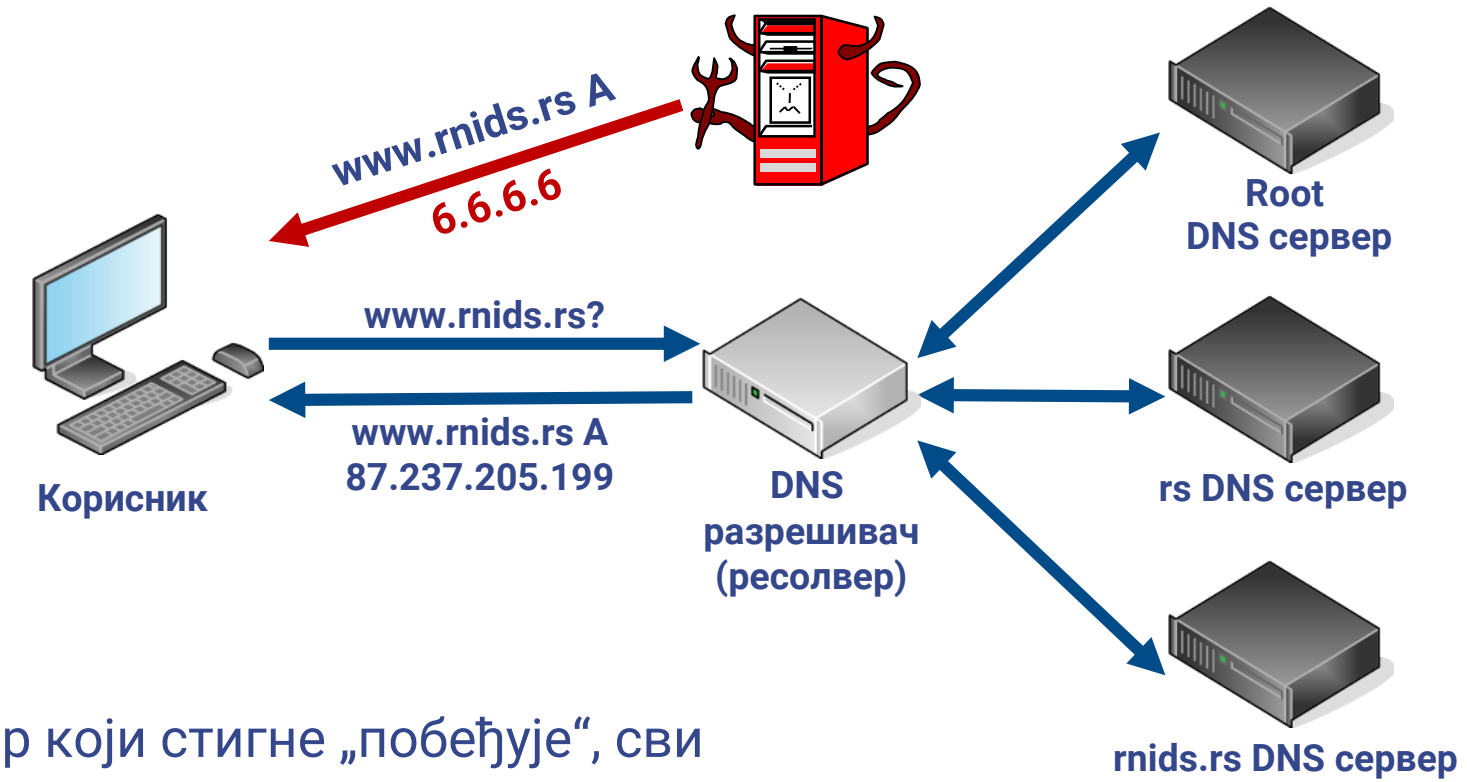
DNS упити се разрешавају у неколико корака – од хијерархијски виших нивоа ка нижим.

Može li odgovor da izgleda ovako?



www.rnids.rs = 87.237.205.199

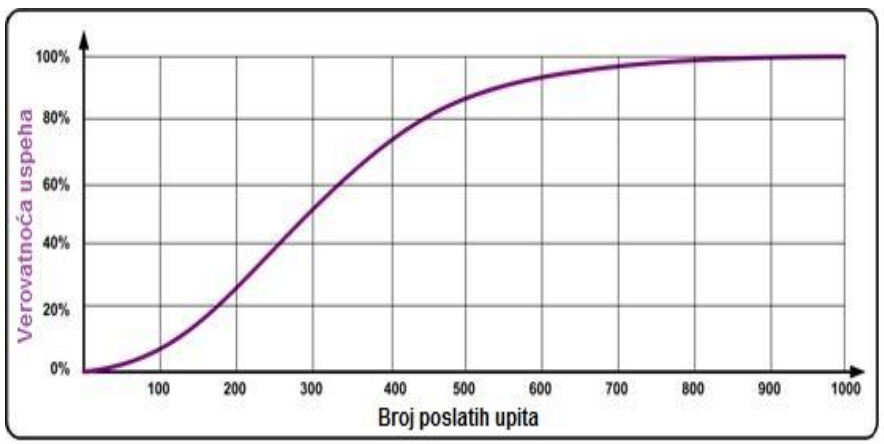
Jednostavan MITM napad

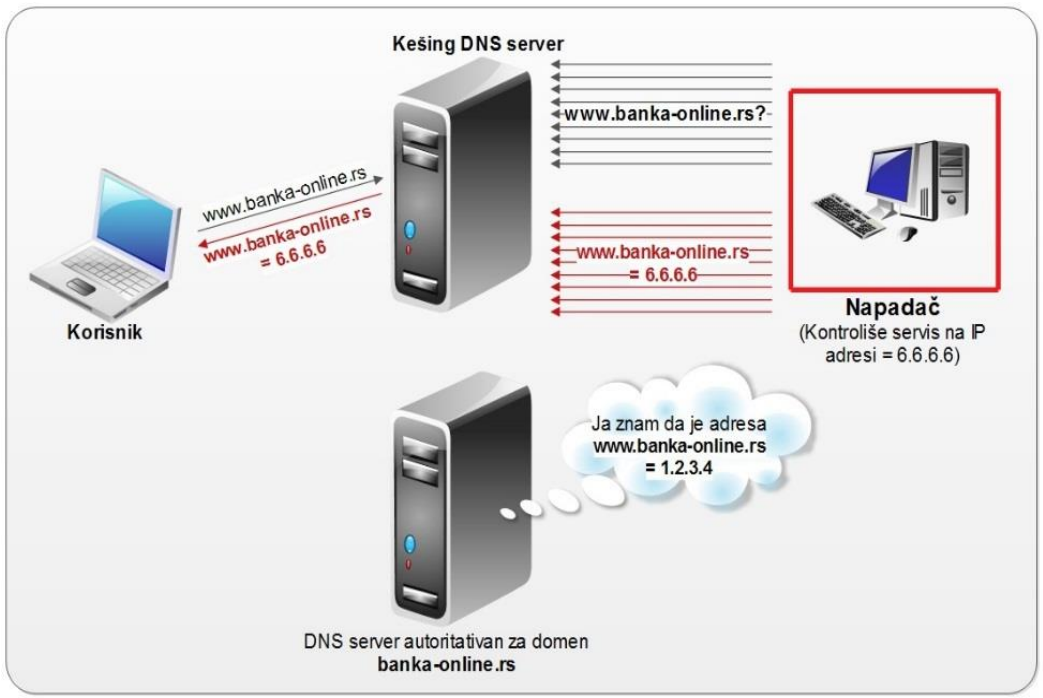


Prvi odgovor koji stigne „pobeđuje“, svi stali su odbačeni!

Cache poisoning napad

$$\text{Вероватноћа} = 1 - \left(1 - \frac{1}{t}\right)^{\frac{n\,(n-1)}{2}}$$





Сви корисници „зараженог“ DNS сервера добијају погрешан одговор!

DNSSEC

DNSSEC (Domain Name System Security Extensions) je proširenje DNS-a koje implementira digitalne potpise DNS podataka koji su podloćni napadima.

DNSSEC omogućava da Internet postane mnogo bezbednije okruženje.

Prednosti DNSSEC-a

DNSSEC omogućava:

- **Autentičnost podataka** – resolver može da odredi da li DNS odgovor potiče od autoritativnog DNS servera.
- **Integritet podataka** – resolver može da utvrdi da li je DNS odgovor menjan u toku prenosa.
- **Autentičnost nepostojanja** – resolver može da potvrdi da ne postoji DNS zapis na autoritativnom serveru (NXDOMAIN).

Da bi sve ovo bilo ispunjeno, resolver mora da bude konfigurisan da vrši validaciju DNSSEC odgovora!

UKLJUČITE DNSSEC VALIDACIJU!

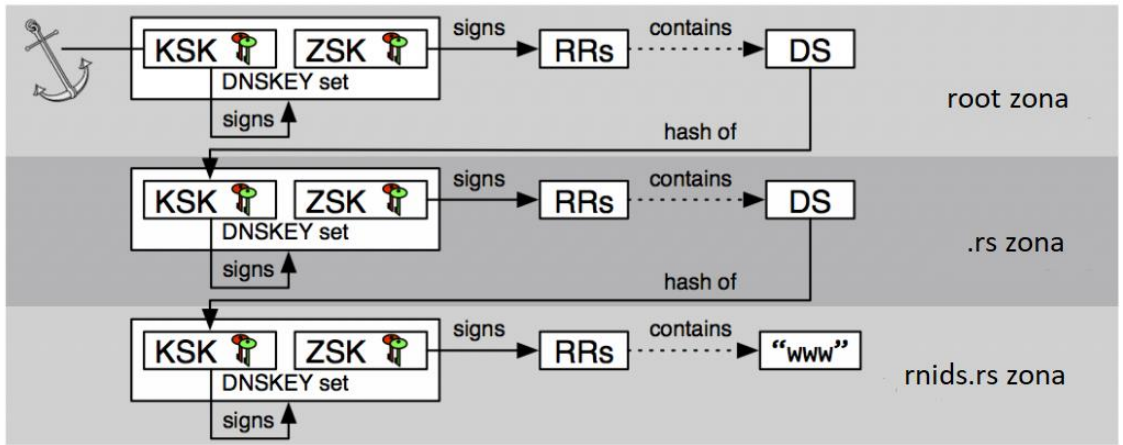
Kako DNSSEC funkcioniše

DNSSEC koristi dva tipa ključeva: ključeve za potpisivanje ključeva (Key Signing Keys – KSK) i ključeve za potpisivanje zone (Zone Signing Keys – ZSK).

Javni KSK ključ se u zonskom fajlu pojavljuje kao DNSKEY zapis, ali se njegov privatni ključ koristi samo za potpisivanje DNSKEY zapisa zone.

Privatni ZSK ključ se koristi za potpisivanje i potvrdu zapisa u zoni, a njegov odgovarajući javni ključ se objavljuje u vidu DNSKEY zapisa.

1. DNS operater generiše KSK i ZSK parove ključeva
2. Javni ključevi se dodaju u zonski fajl kao DNSKEY tip recorda
3. Potpisivanjem zone se kreiraju dva nova tipa zapisa (RRSIG & NSEC3)za svaki autoritativni zapis u zoni.
4. RRSIG je potpis odgovarajućeg zapisa
5. NSEC3 zapis daje sledeći siguran zapis i omogućava potvrdu nepostojanja zapisa.
6. DNS operater prosleđuje DS (Delegation Signer) zapis koji se upisuje u roditeljsku zonu (hijerarhijski viša zona) i potpisuje se odgovarajućim ZSK
7. Sada je zona potpisana i resolveri koji rade validaciju mogu da imaju poverenje u dobijeni odgovor.



DNSSEC nakon 15 godina

- Skoro 80% TLD zona je potpisano.
- Broj potpisanih domena po TLD-u je veoma nizak (prosek ispod 15%)
- Broj resolvera koji vrše validaciju DNSSEC zapisa je oko 13%

DNSSEC u Srbiji

Code	Region	DNSSEC Validates	Uses Google PDNS	Samples	Weight	Weighted Samples
XA	World	11.96%	11.40%	864,194,167	1	864,194,167
XE	Europe	20.67%	9.78%	178,149,136	0.81	143,653,267

Code	SubRegion	DNSSEC Validates	Uses Google PDNS	Samples	Weight	Weighted Samples
QN	Southern Europe, Europe	14.93%	11.45%	61,575,697	0.44	27,198,264

CC	Country	DNSSEC Validates	Uses Google PDNS	Samples	Weight	Weighted Samples
PT	Portugal, Southern Europe, Europe	62.68%	9.81%	4,612,449	0.38	1,759,049
SI	Slovenia, Southern Europe, Europe	54.80%	7.50%	1,033,108	0.37	379,732
RS	Serbia, Southern Europe, Europe	36.28%	15.33%	6,653,329	0.18	1,206,838
MK	The former Yugoslav Republic of Macedonia, Southern Europe, Europe	33.49%	41.59%	1,283,159	0.29	367,088
BA	Bosnia and Herzegovina, Southern Europe, Europe	29.36%	13.02%	2,991,023	0.2	594,905
VA	Holy See, Southern Europe, Europe	22.69%	51.16%	692	0	0
GI	Gibraltar, Southern Europe, Europe	16.93%	75.15%	22,172	0	0
GR	Greece, Southern Europe, Europe	16.32%	7.11%	12,300,245	0.15	1,797,342
ME	Montenegro, Southern Europe, Europe	15.57%	20.75%	777,806	0.13	98,867
HR	Croatia, Southern Europe, Europe	14.48%	9.98%	1,983,484	0.4	795,387
AL	Albania, Southern Europe, Europe	14.29%	17.09%	2,388,572	0.19	465,562
ES	Spain, Southern Europe, Europe	8.45%	12.74%	7,734,167	1.25	9,642,764
IT	Italy, Southern Europe, Europe	6.75%	8.87%	18,663,759	0.54	9,988,529
AD	Andorra, Southern Europe, Europe	4.93%	7.50%	57,496	0.29	16,887
SM	San Marino, Southern Europe, Europe	4.80%	12.36%	4,499	0	0
MT	Malta, Southern Europe, Europe	3.38%	4.04%	1,069,737	0.08	85,233

DNSSEC u RNIDS-u

Krajem 2012. instalirano okruženje za testiranje DNSSEC-a. Avgusta 2017. urađena nova instalacija i obavljeno testiranje različitih varijanti DNSSEC-a.

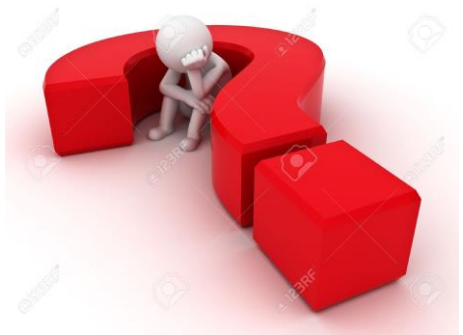
Potpisivanje TLD zona - januar 2018. Produkciono okruženje i dokumentacija će biti spremni početkom decembra.

Do sredine 2018. godine biće stvoreni uslovi za potpisivanje domena drugog i trećeg nivoa od strane DNS operatera. Ovo podrazumeva razvoj DNSSEC funkcionalnosti aplikacije za registraciju domena i EPP protokola.

Početak II kvartala biće organizovana DNSSEC radionica za DNS operatere u Srbiji.

RNIDS će pšripremiti i svim zainteresovanim staviti na raspolaganje DNSSEC uputstva radi lakše i sveobuhvatnije implementacije kod većine DNS operatera u Srbiji.

Hvala na pažnji!



www.rnids.rs
рнидс.срб

www.domen.rs
домен.срб