DNSSEC validacija

Vladimir Rančev
IT Infrastructure Expert

subota, novembar 26, 2016

Top 10 AS čiji korisnici koriste DNSSEC validaciju

Rank	AS	DNSSEC Use	DNSSEC Users	Clients Tested	AS Name / Country
1	**AS44143**	**100%**	**67**	**67**	**VIPMOBILE-AS Vip mobile d.o.o. Serbia**
2	AS31343	99%	121	122	INTERTELECOM Intertelecom Ltd Ukraine
3	AS198471	98%	73	74	Linkem spa Italy
4	AS44034	98%	121	123	HI3G Hi3G Access AB Sweden
5	AS12849	97%	79	81	HOTNET-IL Hot-Net internet services Ltd. Israel
6	AS7657	96%	575	593	VODAFONE-NZ-NGN-AS Vodafone NZ Ltd. New Zealand
7	AS12912	96%	186	192	ERA Polska Telefonia Cyfrowa S.A. Poland
8	AS48161	96%	335	347	NG-AS SC NextGen Communications SRL Romania
9	AS22047	96%	800	832	VTR BANDA ANCHA S.A. Chile
10	AS34779	95%	292	305	T-2-AS set propagated by T-2 Slovenia

Source: https://labs.ripe.net/Members/gih/counting-dnssec

1. Koliko DNS zona koje koriste DNSSEC postoji?

2. Koji broj DNS upita je DNSSEC validiran?

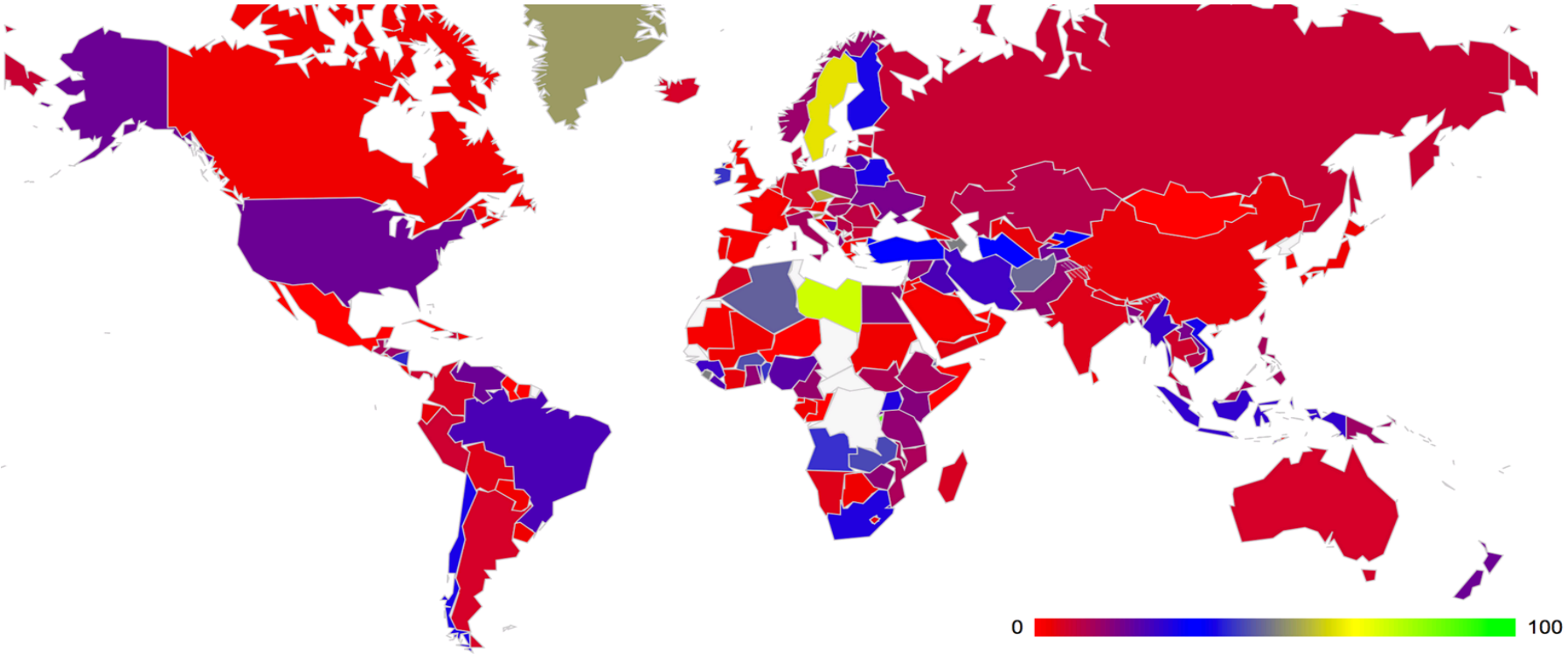
3. Koji broj DNS resolving servera koristi DNSSEC validaciju?

   2,316/57,267 **~4.0%**

4. Koliko korisnika interneta koristi servere sa DNSSEC validacijom?

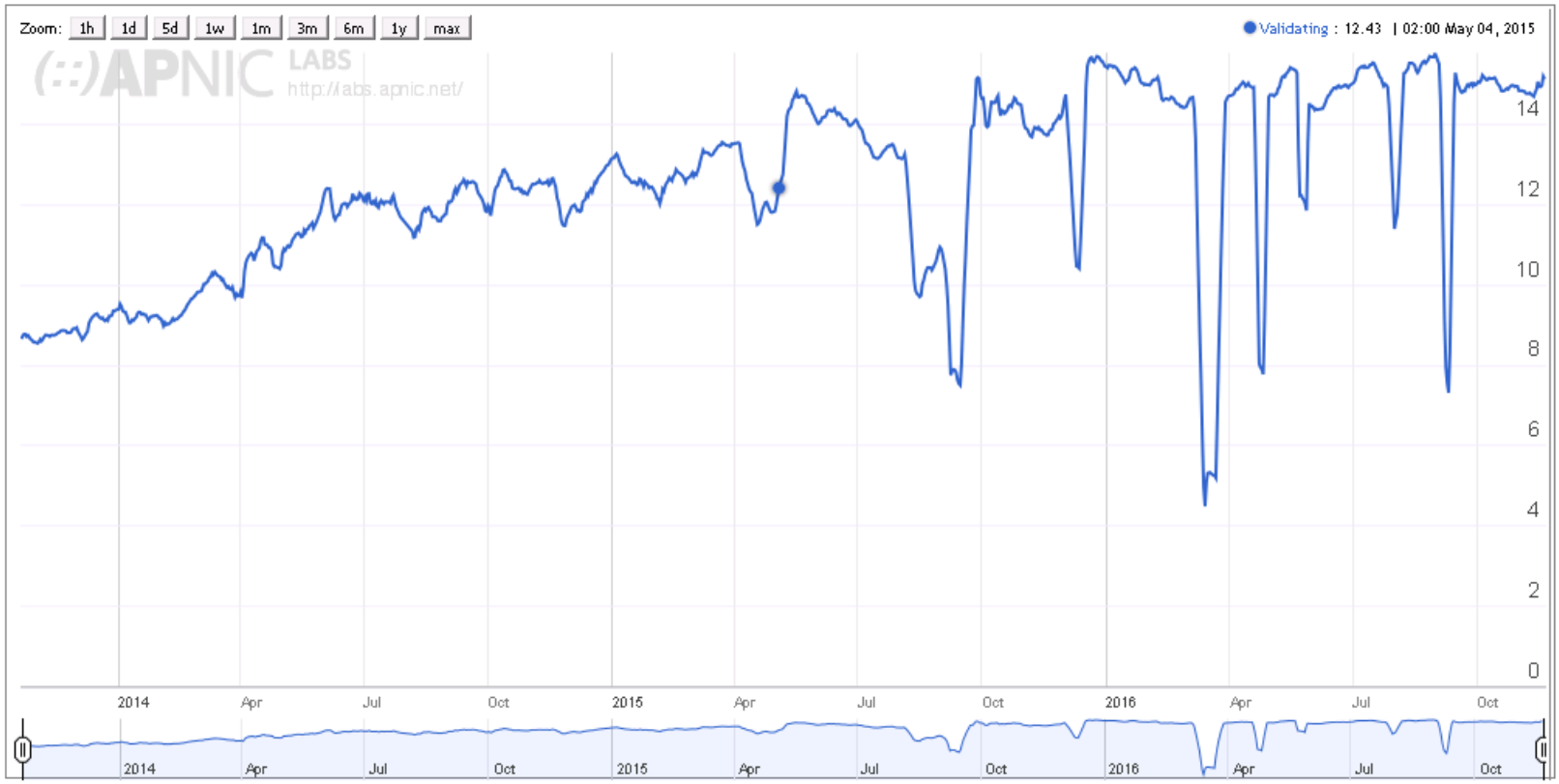
   269,560/770,934 **~9.0%**

Korisnici interneta koji koriste servere sa DNSSEC validacijom 2012



Country Code	Number of unique End Users	Number of DNSECC-validating End Users	Percent of Users using DNS resolvers that perform DNSSEC Validation
RS	**4607**	**440**	**9,55%**

Korisnici interneta koji koriste servere sa DNSSEC validacijom 2016



CC	Country	DNSSEC Validates	Uses Google PDNS
RS	Serbia, Southern Europe, Europe	28.31%	12.05%

Source: http://stats.labs.apnic.net/dnssec/XA

Šta DNSSEC radi?

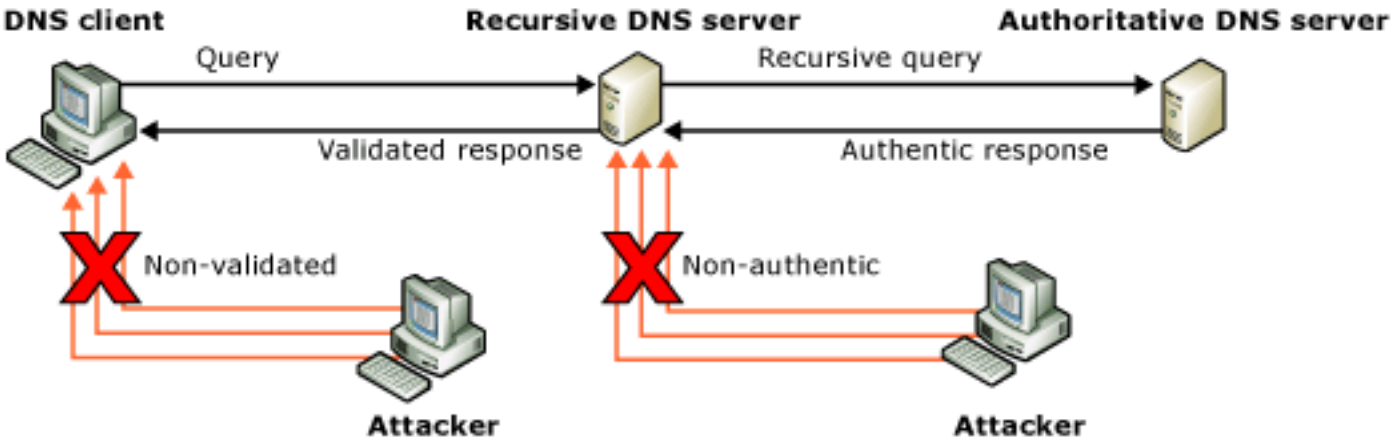
DNSSEC koristi public-key kriptografiju i digitalne potpise da potvrdi:

Integritet podataka

Da li je napadač (npr. man-in-the-middle) modifikovao podatke u odgovoru?

Autentičnost porekla podataka

Da li je DNS odgovor stvarno došao iz .COM DNS zone?



Šta DNSSEC ne radi?

Ne omogućava poverljivost DNS komunikacije

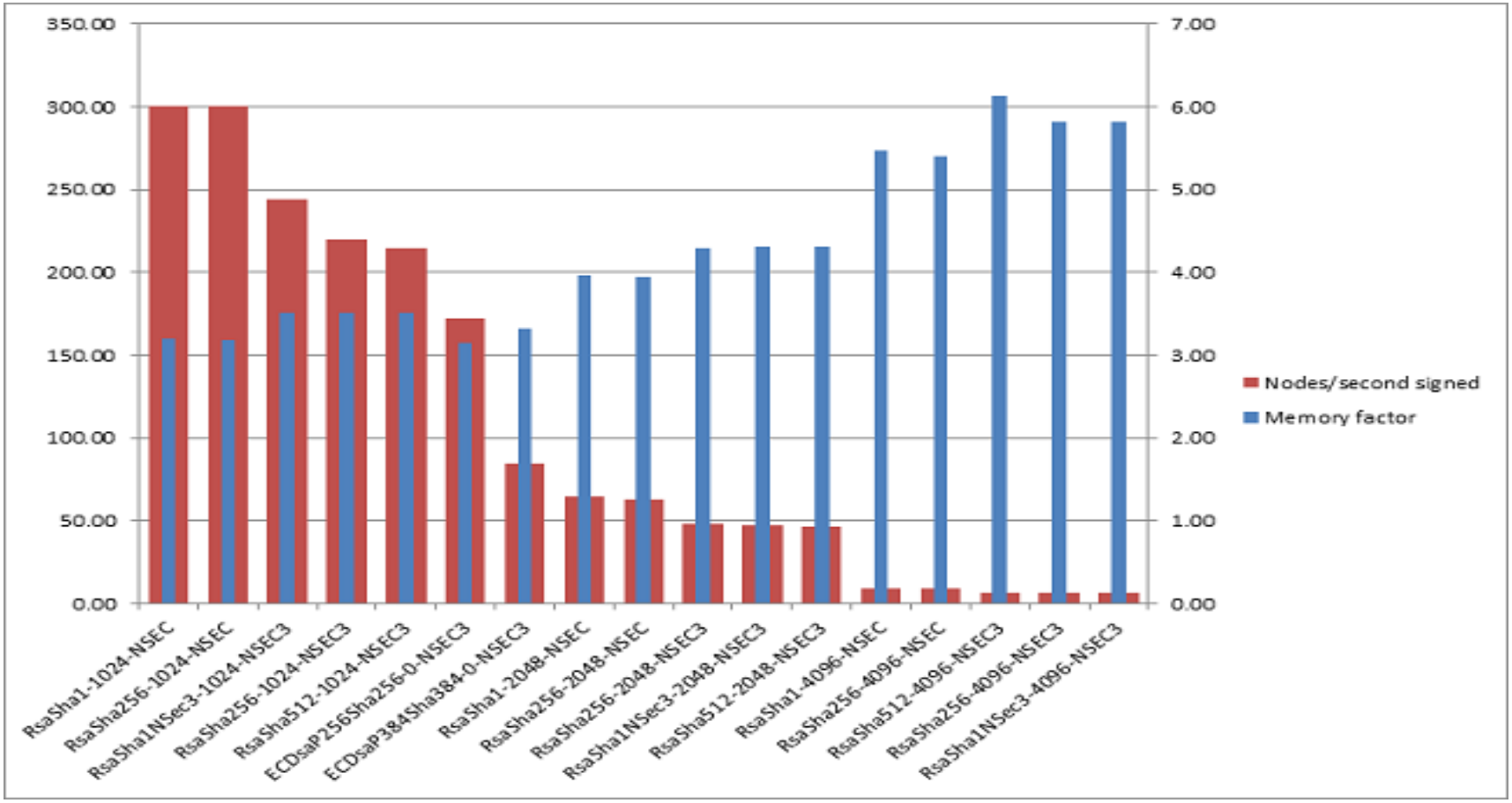
- DNS rekordi su javni i svima dostupni
- Nema enkripcije
- Ne osigurava privatnost client-server ili server-server saobraćaja

Ne sprečava bilo kakve napade na same DNS servere

- Ne pruža zaštitu od DDOS, DNS tunneling, idr. napada

DNSSEC elementi:

Key pairs	public key	Nalazi se u **DNSKEY** rekordu
	private key	Čuva se offline ili HSM
Digital Signatures	Privatni key potpisuje svaki DNS podatak u zoni	
	Svaki potpis se nalazi u **RRSIG** rekordu	
Dodatno	**KSK** key-signing keys	Potpisuje samo DNSKEY
	ZSK zone-signing keys	Potpisuje ostatak zone
	DS delegation signer	Upućuje na zone key child domena
	Trust anchor	Public key parenta kom se veruje



Performanse i iskorišćenje memorije u zavisnosti od tipa algoritma i dužine ključeva

za autoritativne DNS servere

Šta bi trebalo uzeti u obzir:

Sadržaj zone

- Broj potpisanih rekorda
- Broj KSK i ZSK ključeva
- Dodatne sekcije u DNS zonama

Kriptografski algoritmi

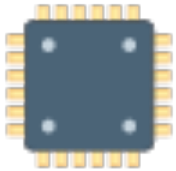
- Algoritmi bazirani na RSA su po pravilu brži od EC (Elliptical Curve)

Dužina ključa

- Što je dužina ključeva veća - potpisi su veći
- Potrebno je više CPU i memorije za verifikaciju

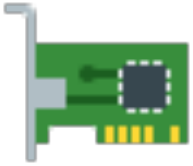
Ponašanje korisnika

HW i SW zahtevi za autoritativne DNS servere



CPU **X4**

RAM **X4**



Network **X15**

Linux

Bind 9.8

Instalacija nove instance BIND 9.8 sa DNSSEC validacijom

Konfiguracija BIND-a

/etc/named.conf

```
dnssec-enable yes;
dnssec-validation auto; (yes <bind 9.8)
dnssec-lookaside auto;

/* Path to ISC DLV key */
bindkeys-file "/etc/named.iscdlv.key";
```

Konfiguracija BIND-a

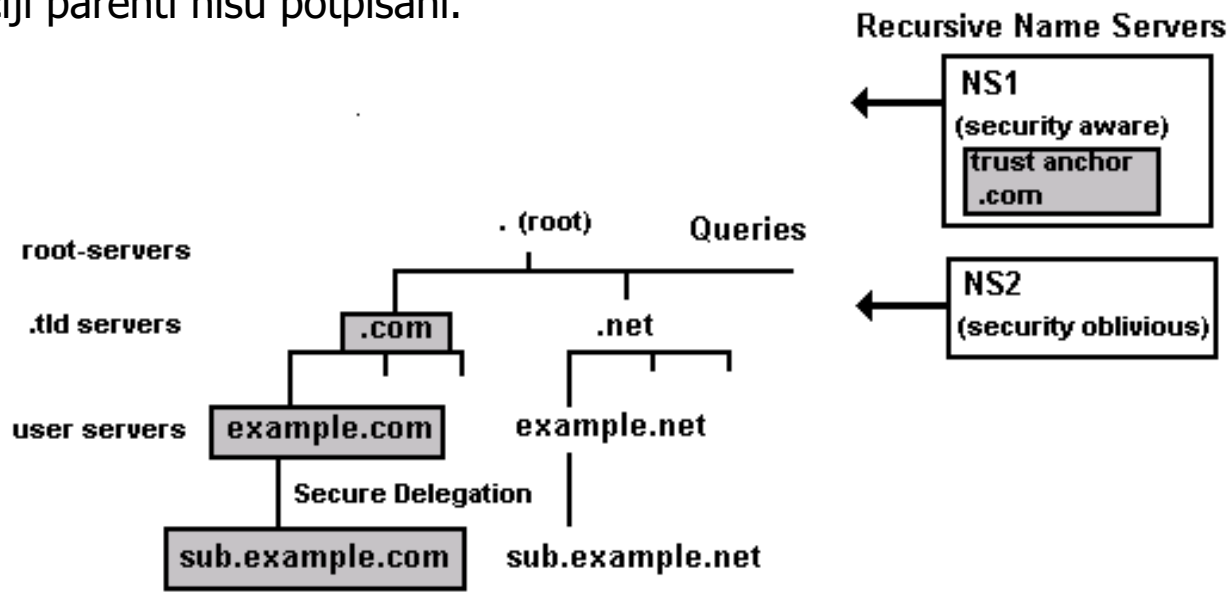
/etc/named.iscdlv.key

```
managed-keys {
        # ISC DLV: See https://www.isc.org/solutions/dlv for details.
        # NOTE: This key is activated by setting "dnssec-lookaside auto;"
        # in named.conf.
        dlv.isc.org. initial-key 257 3 5
"BEAAAAPHMu/5onzrEE7z1egmhg/WPO0+juoZrW3euWEn4MxDCE1+lLy2
                brhQv5rN32RKtMzX6Mj70jdzeND4XknW58dnJNPCxn8+jAGl2FZLK8t+
                1uq4W+nnA3qO2+DL+k6BD4mewMLbIYFwe0PG73Te9fZ2kJb56dhgMde5
                ymX4BI/oQ+cAK50/xvJv00Frf8kw6ucMTwFlgPe+jnGxPPEmHAte/URk
                Y62ZfkLoBAADLHQ9IrS2tryAe7mbBZVcOwIeU/Rw/mRx/vwwMCTgNboM
                QKtUdvNXDrYJDSHZws3xiRXF1Rf+al9UmZfSav/4NWLKjHzpT59k/VSt
                TDN0YUuWrBNh";

        # ROOT KEY: See https://data.iana.org/root-anchors/root-anchors.xml
        # for current trust anchor information.
        # NOTE: This key is activated by setting " dnssec-validation auto;"
        # in named.conf.
        . initial-key 257 3 8 "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
                FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
                bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
                X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
                W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
                Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
                QxA+Uk1ihz0=";
};
```

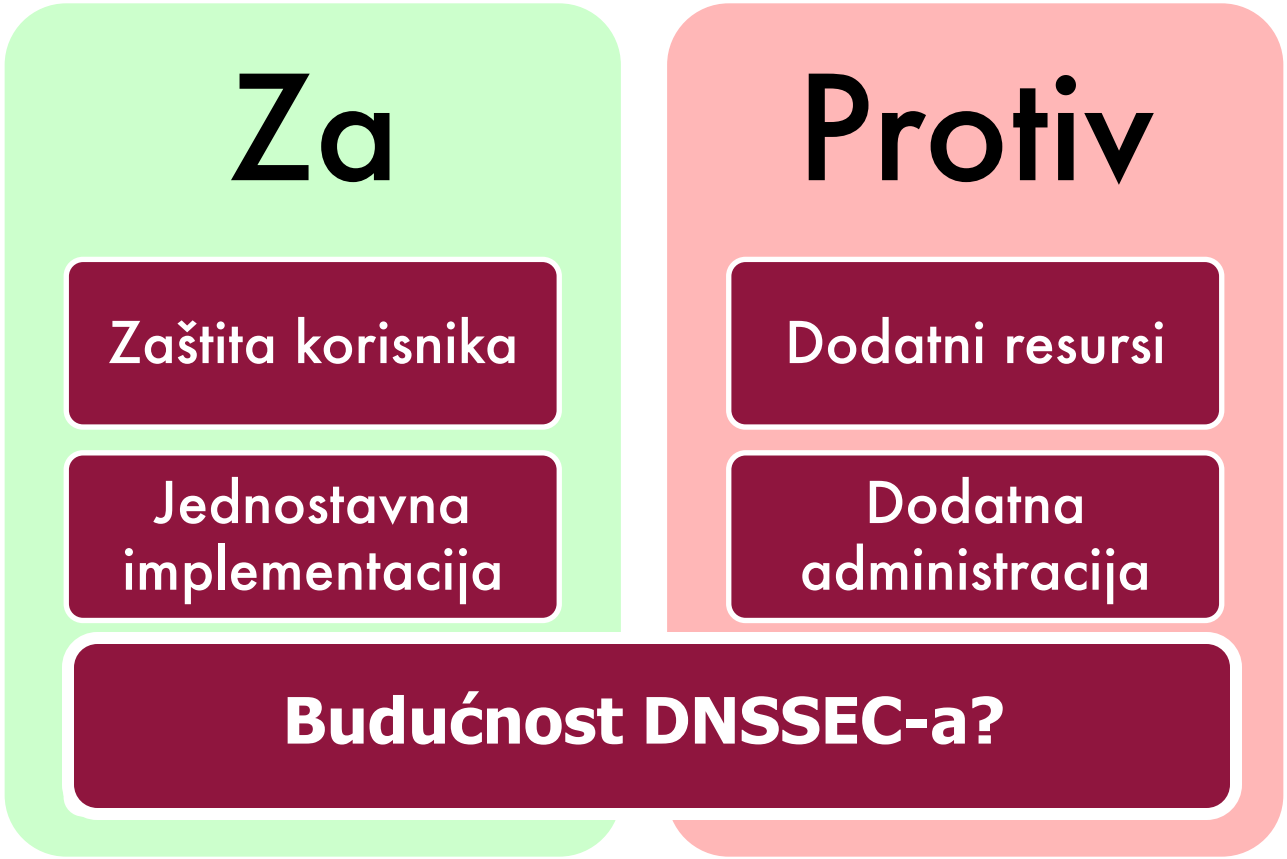
DLV (DNSSEC Look-aside Validation)

DLV je ekstenzija DNSSEC protokola sa ciljem da omogući potpisivanje i validaciju domena čiji parenti nisu potpisani.



Započet 2006 → Zatvoren za nove domene Jul 2016 → Gašenje servisa 2017

Zaključak


Za
Protiv
Zaštita korisnika
Dodatni resursi
Jednostavna implementacija
Dodatna administracija
Budućnost DNSSEC-a?

Hvala

v.rancev@vipmobile.rs

subota, novembar 26, 2016