Univerzitet Singidunum

Bezbednosna proširenja DNS-a (DNSSEC)

Analiza standarda, iskustava i relevantnih dokumenata

Preporuke i smernice za implementaciju DNSSEC-a

Za potrebe Registra nacionalnog Internet domena Srbije

Jul 2014.

Postavljeni zahtevi

Izrada studije koja sadrži:

- Potrebne korake i spisak neophodnih propisa i pravila koje je potrebno doneti radi implementacije DNSSEC-a u okviru RS i SRB TLD-a
- Analiza relevantnih dokumenata i najbolje prakse:
  - Pregled i analiza standarda vezanih za DNSSEC
  - Pregled i analiza iskustava drugih registara po pitanju korišćenja DNSSEC-a
  - Pregled i analiza ostalih dokumenata javno dostupnih na Internetu koji obrađuju problematiku korišćenja DNSSEC

    (trenutni presek stanja u svetu po pitanju korišćenja DNSSEC-a)
- Osnovne preporuke o mogućim načinima implementacije DNSSEC-a:
  - Preporučenim načinima za kreiranje i čuvanje DNSSEC ključeva
  - Moguća rešenja za razmenu sigurnosnih podataka između DNS operatera – ovlašćenih registara – i RNIDS-a
  - Ostale preporuke
- Uloga RNIDS u procesu potpisivanja zonskih fajlova kod DNS operatera

Sadržaj

Uvod

1.1 Ukratko o DNSSEC-u

DNSSEC je standard koji modifikuje zapise resursa i protokole DNS-a da bi se obezbedila sigurnost za transakcije između razrešitelja i servera naziva. Uvođenjem podataka koji su kriptografski potpisani javnim ključem u DNS uz pomoć četiri nova zapisa resursa, DNSSEC obezbeđuje:

- Autentičnost izvora: Razrešitelj može da odredi da li odgovor potiče od autoritativnog servera naziva određene zone.
- Verifikaciju integriteta: Razrešitelj može da odredi da li je odgovor menjan u toku prenosa.
- Autentično poricanje postojanja: Razrešitelj može da potvrdi da je određeni upit nerazrešiv, ako ne postoji zapis resursa DNS-a na autoritativnom serveru naziva.

DNSSEC uvodi četiri nova tipa zapisa resursa: Potpis zapisa resursa (RRSIG), DNS Javni ključ (DNSKEY), Potpisnik delegiranja (DS) i Sledeći bezbedan (NSEC). DNSSEC Server naziva za određenu zonu drži Potpis zapisa resursa (RRSIG) za različite skupove zapisa resursa (RRset) koje se na njemu drže. RRSIG predstavlja digitalni potpis koji se formira uzimanjem hash-a određenog skupa zapisa resursa u zoni i njegovom enkripcijom uz pomoć privatnog ključa iz kompleta kriptografskih ključeva administratora te zone. Odgovarajući javni ključ iz ovog kompleta se čuva u zapisu DNSKEY. Po primanju potpisanog DNS odgovora od servera naziva, DNSSEC razrešitelj dešifruje RRSIG uz pomoću javnog ključa zone. Razrešitelj zatim generiše hash RRset dela odgovora i upoređuje ga sa hash-om dobijenim iz RRSIG dela odgovora. Na taj način se potvrđuje ili negira integritet i autentičnost porekla različitih tipova informacija.

Kako razrešitelj dolazi do autentičnog DNSKEY ključa za određenu zonu? Zapis resursa Potpisnik delegiranja (DS) se obezbeđuje od strane parent zone i predstavlja tačku delegiranja između parent i child zona koja se može autentifikovati. Da bi potvrdio DNSKEY child zone, razrešitelj preuzima odgovarajući DS, RRSIG(DS) i DNSKEY parent zone. DS se verifikuje pomoću dešifrovanog RRSIG(DS) i zatim se DS podaci koriste za autentifikaciju DNSKEY podatka child zone. Na ovaj način, potpisani DS funkcioniše kao “sertifikat” koji se autoritativno isporučuje iz parent zone i vezuje child zonu za svoj DNSKEY. Server naziva iz parent zone postaje, praktično, “pouzdano treće lice”, koje olakšava razmenu DNS informacija između razrešitelja i child zone. Niz ovakvih delegiranih odnosa formira lanac autentifikacije, koji predstavlja putanju koju razrešitelj može da prati od javnog ključa (tj. pouzdanog polazišta – trust anchor) DNS root-a. Na kraju, Sledeći bezbedan (NSEC) zapis resursa povezuje potpisane resurse, omogućavajući razrešitelju da pretražuje fajl zone i da odredi da li određeni domen postoji u DNS-u.

Ovde je važno napomenuti da se u praksi koriste dva tipa kriptografskih ključeva po zoni, ključevi za potpisivanje zone (Zone Signing Keys – ZSK) i ključevi za potpisivanje ključeva (Key

Signing Keys – KSK). Tajni ZSK ključ se koristi za potpisivanje svih podataka zone i njegov odgovarajući javni ključ se objavljuje u vidu DNSKEY zapisa. Javni KSK ključ se takođe pojavljuje kao DNSKEY zapis, ali se njegov tajni ključ koristi samo za potpisivanje DNSKEY zapisa.

Dva različita ključa se koriste iz bezbednosnih razloga. Opšte pravilo u kriptografiji je da što se više podataka šifruje određenim ključem, opasnost da se ključ sazna postaje sve veća. U ovom slučaju u pitanju je tajni ključ. U DNS-u se taj ključ koristi za potpisivanje velike količine podataka jer svaka promena u zoni zahteva ponovno potpisivanje. Što je zona veća, to ima više podataka koji su dostupni za kriptoanalizu. Iz tog razloga, praksa je da se ZSK ključevi menjaju relativno često. Kada bi se koristio samo jedan ključ, svaki put kada bi se on menjao, bilo bi neophodno slati DNSKEY parent zoni kako bi se u njoj zamenio i ponovo potpisao DS zapis za tu zonu. Da bi se ovo izbeglo, koriste se dva odvojena tipa ključeva, i parent zonu je potrebno kontaktirati samo pri promeni KSK ključeva, što se čini relativno retko (njime se potpisuje vrlo malo podataka). Održavanje jake bezbednosti sistema ovime postaje lakše i brže.

1.2 Struktura dokumenta

Dokument je podeljen na sedam poglavlja i dva dodatka. Struktura istovremeno predstavlja i redosled neophodnih koraka koje je potrebno pratiti radi implementacije DNSSEC-a.

U prvom poglavlju dat je kratak uvid u funkcionisanje DNSSEC-a kao i pregled strukture ovog dokumenta.

U drugom poglavlju je dat pregled dokumenata koji čine DNSSEC standard. Takođe, predstavljena je i kategorizacija mogućih DNSSEC rešenja po nivou automatizacije procesa i nivou bezbednosti pri upravljanju ključevima.

U trećem poglavlju se daju preporuke za implementaciju i bezbednosnu politiku. Obuhvaćeno je upravljanje ključevima, sistem potpisivanja, distribucija, validacija kao i preporuke o tehničkim parametrima.

U četvrtom poglavlju se vrši analiza DNSSEC rešenja tj. DNS serverskog softvera OpenDNSSEC i BIND.

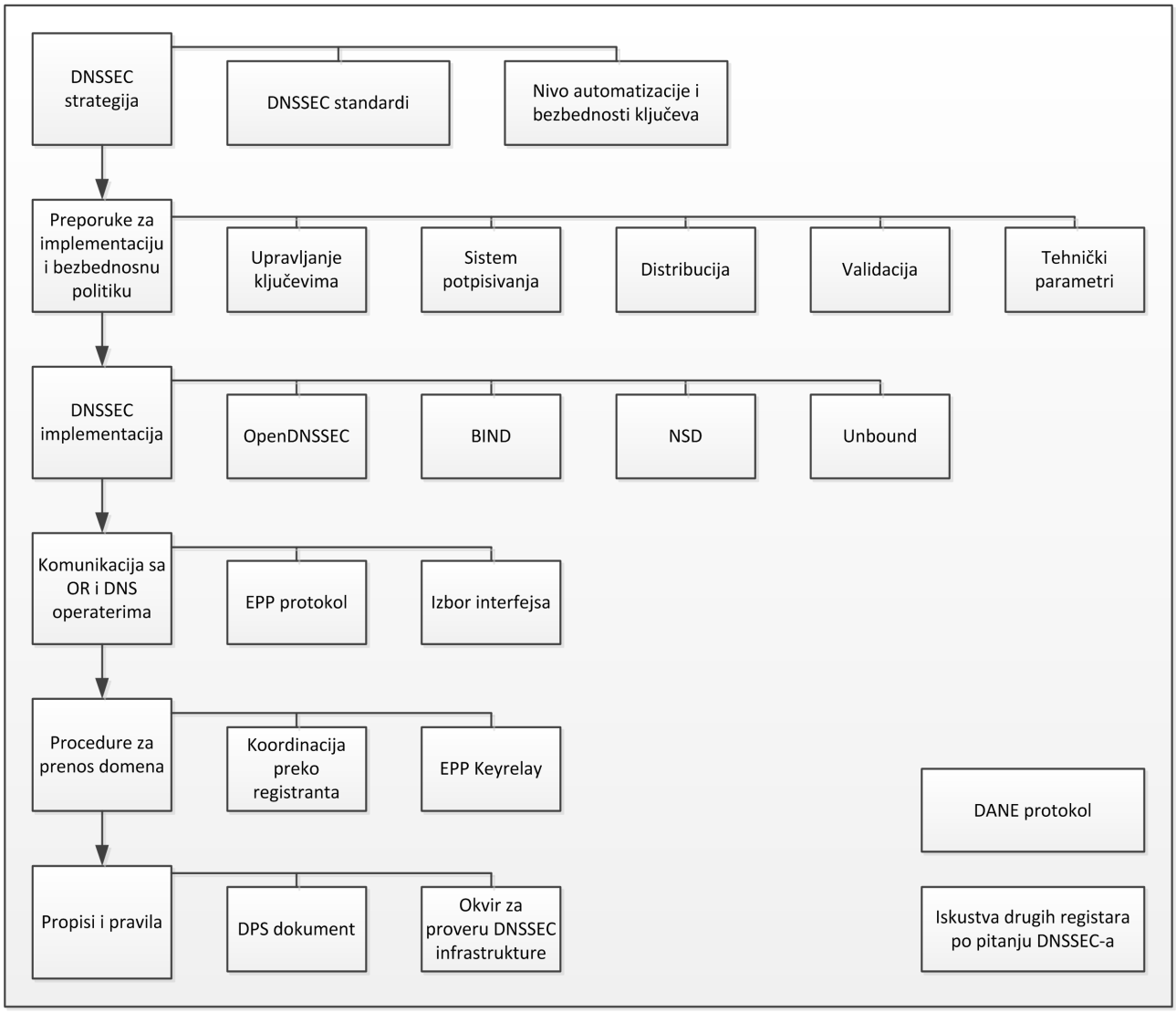
U petom poglavlju se razmatraju mogući načini komunikacije sa ovlašćenim registrima i DNS operaterima.

U šestom poglavlju su predstavljene procedure za prenos domena obezbeđenog DNSSEC-om.

Sedmo poglavlje predstavlja smernice za donošenje „DNSSEC Policy and Practice Statement“.

U dodatku A je dat pregled i analiza iskustava drugih nacionalnih registara po pitanju korišćenja DNSSEC-a, u dodatku B pregled TTL vrednosti DNSSEC zapisa kod registara domena najvišeg nivoa, a u dodatku C spisak poznatih hardverskih modula zaštite (HSM).

Šematski prikaz strukture dokumenta je dat na slici 1.



Slika 1. Struktura dokumenta

1. DNSSEC standardi i strategije

2.1 Pregled i analiza standarda vezanih za DNSSEC

DNSSEC standardi na koje se poziva ICANN su predstavljeni u sledećim dokumentima:

2.1.1 RFC 4033: „DNS Security Introduction and Requirements“

Kategorija: Standard

Sažetak: Bezbednosna proširenja sistema imenovanja domena (DNSSEC) uvode autentičnost izvora i integritet podataka u DNS. Ovaj dokument predstavlja ova proširenja i opisuje njihove mogućnosti i ograničenja. Takođe, ovaj dokument razmatra i koje usluge DNSSEC obavlja a koje ne. Na kraju, ovaj dokument opisuje međusobnu povezanost između dokumenata koji zajednički opisuju DNSSEC.[2]

- Definicije važnih DNSSEC termina
- Usluge koje DNSSEC obavlja
  - Autentičnost izvora podataka i integritet podataka
  - Autentično poricanje postojanja
- Usluge koje DNSSEC ne obavlja
  - Poverljivost podataka
  - Zaštita od DDoS napada
- Validirajući *resolver* može da odredi četiri stanja:
  - *Secure, Insecure, Bogus, Indeterminate*
- Razlika između TTL vrednosti i perioda važenja RRSIG
  - TTL funkcija se ne menja
  - Polja za početak i kraj važenja u RRSIG zapisu određuju period u toku koga se potpis može koristiti za validaciju RRSet na koji se odnosi. TTL vrednosti ne mogu da produže period važenja koji je određen ovim poljima.
- Vremenska zavisnost zona
  - Ponovnim potpisivanjem jednog ili više RRset u okviru zone menja se i jedan ili više RRSIG RR, što za sobom povlači i povećanje serijskog broja SOA da bi se označila promena, kao i ponovno potpisivanje SOA RRset.

2.1.2 RFC 4034: „Resource Records for the DNS Security Extensions“

Kategorija: Standard

Sažetak: Ovaj dokument opisuje sledeće zapise resursa: „javni ključ“ (DNSKEY), „potpisnik delegiranja“ (DS), „digitalni potpis zapisa resursa“ (RRSIG) i „autentifikovano poricanje postojanja“ (NSEC). Detaljno su opisani svrha i format a dat je i primer svakog od zapisa resursa.[3]

- DNSKEY zapis resursa
  - Autoritativni RRset-ovi u zoni se potpisuju tajnim ključem, čiji se odgovarajući javni ključ čuva u okviru DNSKEY RR. *Resolver*-i koriste ovaj javni ključ za validaciju potpisa koji pokrivaju RRset-ove u zoni, time ih autentifikujući.
- RRSIG zapis resursa
  - Digitalni potpisi se čuvaju u RRSIG zapisima resursa i koriste se u autentifikacionom procesu DNSSEC-a. RRSIG zapis sadrži potpis za određeni RRset, sa odgovarajućim imenom, klasom i tipom. Takođe, sadrži i interval važenja potpisa, algoritam, naziv potpisnika i oznaku ključa koji služe za određivanje DNSKEY RR koji sadrži javni ključ kojim se može verifikovati potpis.
  - TTL vrednost RRSIG RR MORA biti ista kao i TTL vrednost RRset-a na koji se odnosi.
- NSEC zapis resursa
  - NSEC RR sadrži:
    - Naziv vlasnika sledećeg RRset u kanoničkom redosledu zone i
    - komplet RR tipova koji postoje za taj naziv
  - NSEC RR bi trebalo da sadrži istu TTL vrednost kao i SOA minimum TTL.
- DS zapis resursa
  - DS zapis je povezan sa DNSKEY zapisom, čuvajući oznaku ključa, broj algoritma kao i sažetak DNSKEY RR. Autentifikacijom DS zapisa, resolver može da autentifikuje DNSKEY RR na koji DS zapis pokazuje.

2.1.3 RFC 4035: „Protocol Modifications for the DNS Security Extensions“

Kategorija: Standard

Sažetak: Ovaj dokument opisuje izmene DNSSEC protokola. Definiše se koncept potpisane zone zajedno sa zahtevima za isporučivanje i razrešavanje uz korišćenje DNSSEC-a. Ove tehnike omogućavaju sigurnosno svesnom razrešitelju da autentifikuje DNS zapise resursa kao i autoritativne indikacije o grešci.[4]

- DNSSEC uvodi koncept potpisane zone. Potpisana zona sadrži DNSKEY, RRSIG, NSEC i opciono DS RR.
    - DNSKEY RR za ključ zone MORA sadržati postavljen Zone Key bit.
    - Vrh zone MORA sadržati najmanje jedan DNSKEY RR koji služi kao *Secure entry point* za zonu.
    - RRSIG RR ne sme biti potpisan.
    - Za svaki autoritativni RRset u zoni, MORA postojati barem jedan RRSIG zapis sa identičnim: nazivom vlasnika, klasom, tipom, *Original TTL* vrednošću, TTL.
    - RRSIG *Labels* polje je jednako broju polja u RRset nazivu vlasnika.
    - Polje sa nazivom potpisnika u RRSIG je jednako nazivu zone koja sadrži RRset.
    - RRSIG polja za algoritam, naziv potpisnika i oznaku ključa određuju DNSKEY zapis ključa zone na vrhu zone.
    - NS RRset koji se pojavljuje na vrhu zone MORA biti potpisan, dok NS RRset-ovi na tačkama delegiranja NE SMEJU biti potpisani.
    - MORA postojati RRSIG za svaki RRset koji koristi najmanje jedan DNSKEY svakog algoritma iz DNSKEY RRset-a na vrhu zone. DNSKEY RRset na vrhu zone MORA biti potpisan svakim algoritmom koji se pojavljuje u DS RRset u roditeljskoj zoni.
    - Za svaki naziv vlasnika u zoni koja sadrži autoritativne podatke ili NS RRset tačku delegiranja, MORA postojati NSEC RR.
    - Svi DS RRset-ovi u zoni MORAJU biti potpisani i DS RRset-ovi se ne smeju pojavljivati u vrhu zone.
- Sigurnosno svestan DNS server MORA podržavati EDNS0 ekstenziju za veličinu poruke, MORA da podržava veličinu poruke od najmanje 1220 okteta, trebalo bi da podržava veličinu poruke od 4000 okteta. DNS *resolver* uz ovo MORA i da koristi *sender's UDP payload size* polje u ENDS OPT pseudo-RR da bi najavio veličinu poruke koju je u stanju da prihvati. IP sloj DNS *resolver*-a MORA pravilno da obradi fragmentovane UDP pakete, bez obzira da li su primljeni putem IPv4 ili IPv6.
- Da bi autentifikovao DNSKEY RRset na vrhu zone, *resolver* MORA:
    - Da verifikuje da se inicijalni DNSKEY RR pojavljuje u DNSKEY RRset-u na vrhu zone i da poseduje postavljen Zone Key fleg.
    - Da verifikuje da postoji RRSIG RR koji pokriva DNSKEY RRset na vrhu zone, i da kombinacija RRSIG RR i inicijalnog DNSKEY RR autentifikuje DNSKEY RRset.

2.1.4 RFC 4470: „Minimally Covering NSEC Records and DNSSEC On-line Signing“

Kategorija: Standard

Sažetak: Ovaj dokument opisuje kako formirati DNSSEC NSEC zapise resursa koji pokrivaju manji opseg imena nego što se zahteva u RFC 4034. Generisanjem i potpisivanjem ovih zapisa po potrebi, autoritativni serveri naziva mogu efektivno da spreče odavanje sadržaja zone, što je inače omogućeno praćenjem lanca NSEC zapisa u potpisanoj zoni.[5]

- U *next name* polju NSEC zapisa instanciranih naziva, umesto navođenja sledećeg instanciranog naziva u zoni, navodi se bilo koji naziv koji leksički dolazi posle naziva vlasnika NSEC imena a pre sledećeg instanciranog naziva u zoni
- Kad god se javi potreba za NSEC zapisom resursa radi dokazivanja nepostojanja naziva, dinamički se kreira i potpisuje novi NSEC zapis. Novi zapis poseduje naziv vlasnika koji je leksički pre QNAME ali nakon bilo kog postojećeg imena, sa *next name* koje leksički dolazi posle QNAME ali pre bilo kog postojećeg imena.

2.1.5 RFC 6781: “DNSSEC Operational Practices, Version 2“

Kategorija: Informativan

Sažetak: Ovaj dokument opisuje skup praksi za rad sa DNS-om uz DNSSEC. Ciljna publika su administratori zona koji uvode DNSSEC. Ovaj dokument razmatra operativne aspekte korišćenja ključeva i potpisa u DNS-u. Razmatraju se i pitanja generisanja ključeva, skladištenja ključeva, generisanja potpisa, prelaska između ključeva i srodnih politika.[6]

- Opisuju se procedure čiji je zadatak da održavanje zona, kao u slučaju ponovnog potpisivanja ili prelaska između ključeva, učine transparentnim za klijente koji obavljaju verifikaciju.
- Generisanje i čuvanje ključeva
    - Prelazak između KSK:
        - Često i redovno, da bi prelasci postali operativna rutina.
        - Često ali neredovno, sa velikom *jitter* vrednošću.
        - Jedino kada se sumnja ili zna da je ključ kompromitovan, ili prilikom promene politika i procedura.
        - Ne postoji široka saglasnost oko toga koja od ove tri politike je najbolja za različite implementacije DNSSEC-a. Razlozi mogu biti za potrebe stvaranja rutine, testiranja ili u slučaju stvarnog problema.
    - SEP fleg treba postavljati samo na KSK ključeve
    - Period efektivnosti ključa
        - KSK bi trebalo menjati svakih 12 meseci.
        - ZSK bi trebalo menjati svakog meseca.
    - Napomene o kriptografiji
        - Za potpisivanje se preporučuje korišćenje RSA/SHA-256 ili alternativno RSA/SHA-1. *Elliptic Curve* algoritmi (GOST, ECDSA) donose prednosti u smislu prostora koji potpisi zauzimaju, ali su trenutno u fazi

standardizacije i implementacije i nisu podržani od strane svih razrešitelja.
        - Preporučena veličina RSA ZSK ključa je 1024 bita, dok je za KSK 2048 bita.
        - Najbezbednije rešenje za upravljanje potpisivanjem u dinamičkoj zoni je rešenje sa skrivenim *master* serverom (nedostupnim na Internetu, nije u NS RRset-u), preko koga se ažuriranja dostavljaju javno dostupnim serverima, uz AXFR, IXFR i NOTIFY mehanizme.
        - Tehničke preporuke za generisanje ključeva se mogu naći u RFC 4086[37] i dokumentu NIST 800-90A[38]. HSM uređaji obezbeđuju dobru platformu za generisanje ključeva.
- Generisanje potpisa, prelasci između ključeva i politike
    - Prelasci između ključeva
        - *Pre-publish* metoda (preporučeno za ZSK)
        - *Double signature* metoda (preporučeno za KSK)
    - Prelasci između algoritama
        - „konzervativni“ pristup: Očekuje se da svaki RRset poseduje validan potpis za svaki algoritam koji se pojavljuje u DNSKEY RRset na vrhu zone, uključujući i keširane RRset-ove.
        - „liberalni“ pristup: Pomenuto pravilo je ograničeno na RRset-ove u zoni pri autoritativnim serverima.
        - NSEC na NSEC3 prelaz algoritma: obavlja se uobičajeni prelaz između algoritama, NSEC se koristi sve vreme, NSEC3 se implementira tek po okončanju prelaska. Procedure su opisane u RFC 5155[7].
    - Planiranje prelazaka između ključeva u slučaju nužde
        - Preporučuje se postojanje dokumentovane procedure
        - KSK – mogući prelasci uz narušavanje lanca poverenja i uz njegovo očuvanje
        - ZSK – važe ista pravila kao prilikom redovnog prelaska između ključeva
        - *Stand-by* ključevi: ZSK – ključ se objavljuje u okviru DNSKEY RR; KSK – DS RR se objavljuje u roditeljskoj zoni.
    - Politike u roditeljskoj zoni
        - Korišćenje samog DNS-a kao izvora DNSKEY materijala ima prednost u eliminisanju mogućnosti za ljudsku grešku. Ipak, *out-of-band* verifikacija je neophodna prilikom prve dostave sigurnosnih podataka.
        - Preporučuje se postojanje mogućnosti za prihvatanje DS zapisa, čak i uz postojanje mogućnosti za prihvatanje DNSKEY zapisa.
        - *Security lameness* – stanje u kome u roditeljskoj zoni postoje DS zapisi koji pokazuju na nepostojeće DNSKEY zapise. Ne sme se dozvoliti da svi DS zapisi budu u ovakvom stanju. Roditeljska zona može, u trenutku razmene ključeva, da vrši proveru postojanja odgovarajućih DNSKEY zapisa.
        - Preporučuje se period važenja potpisa za DS RR od najmanje nekoliko dana. Maksimalni preporučeni period važenja zavisi od toga koliko dugo su zone potomka spremne da provedu kao ranjive u slučaju kompromitacije ključeva.
        - Promena DNS operatera: U scenariju gde je stari operater voljan da sarađuje, koristi se *Pre-publish* ZSK prelaz (gde stari operater unapred objavljuje ZSK novog operatera) kombinovan sa *Double signature* KSK prelazom (gde dva operatera razmenjuju javne ključeve, nezavisno

generišu potpis nad tim kompletima ključeva i objavljuju u svojoj kopiji zone). U slučaju da stari operater nije voljan da sarađuje, zona mora na određeno vreme biti nebezbedna, dok se ne ukloni DS RR koji pokazuje na starog operatera, promeni NS RRset i uvede novi DS RR.

- DNSSEC uvodi pojam apsolutnog vremena u DNS, jer potpisi poseduju datum isteka nakon kojeg postaju nevažeći. Vremenske preporuke:
  - Maksimalna TTL vrednost podataka u zoni bi trebalo da bude manja od perioda važenja potpisa
  - Period u kome je potpis objavljen bi trebalo da se završava u trajanju od najmanje jedne maksimalne TTL vrednosti u zoni pre kraja perioda važenja potpisa.
  - Minimalna TTL vrednost u zoni bi trebalo da bude dovoljno velika da se preuzmu i verifikuju svi zapisi u lancu poverenja.
  - Slave serveri bi trebalo da mogu da preuzimaju novopotpisane zone dovoljno dugo pre nego što potpisi u zonama koje serveri opslužuju isteknu.
  - Maksimalno trajanje potpisa: U slučaju trajnih, stabilnih resursa, period važenja potpisa može biti više meseci.
  - Minimalno trajanje potpisa: Određuje se odabirom *Refresh* perioda (obično nekoliko dana), definisanjem *Re-Sign* perioda na takav način da je (*Refresh* period) – (*Re-Sign* period) – (maksimalna *jitter* vrednost) = vreme u okviru kog se mogu razrešiti operativni problemi.

- „*Next Record*“ tipovi
  - NSEC predstavlja čitljivu, sortiranu i povezanu listu naziva u zoni. NSEC3 koristi metodu heširanja zahtevanog naziva, uz višestruke iteracije i dodatak *salt* vrednosti.
  - NSEC se preporučuje za visoko strukturirane zone i male zone koje sadrže zapise samo u svom vrhu, da bi se olakšao rad. NSEC3 se preporučuje za velike zone, naročito uz pogodnosti koje pruža *Opt-out* mehanizam.
  - NSEC3 parametri:
    - Kao odbrana od *dictionary* napada, koriste se parametri iteracija i *salt*. Veći broj iteracija donosi veću otpornost na napade, uz veće opterećenje servera. Promena *salt* vrednosti smanjuje životni vek unapred izračunate heš vrednosti, samim tim skraćujući upotrebnu vrednost napadačevih tabela.
  - *Opt-out* mehanizam je namenjen za korišćenje samo na tačkama delegiranja i najviše koristi donosi zonama koje poseduju veliki broj nebezbednih delegiranja. Ovo je naročito važno za velike TLD zone.

2.1.6 RFC 5155: „DNS Security (DNSSEC) Hashed Authenticated Denial of Existence“

Kategorija: Standard

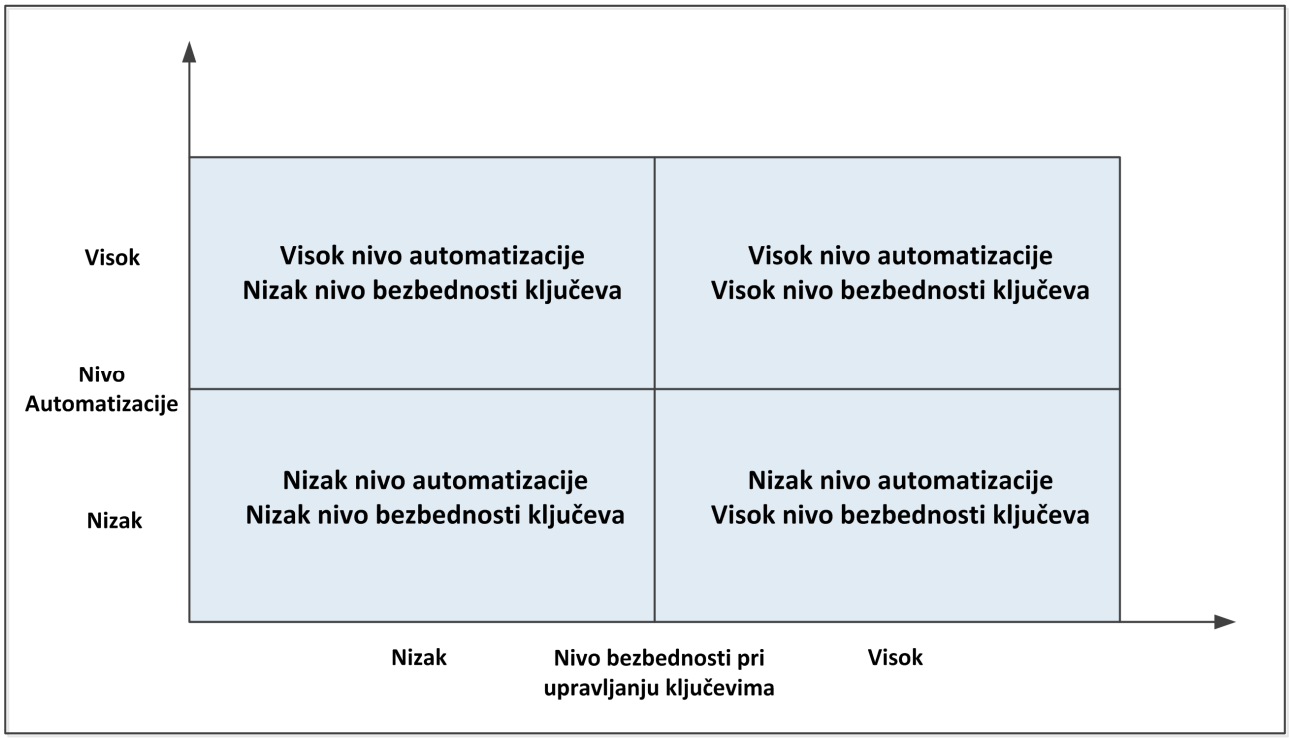
Sažetak: Bezbednosnim proširenjima DNS-a je uveden NSEC zapis resursa za autentifikovano poricanje postojanja. Ovaj dokument uvodi alternativni zapis resursa, NSEC3, koji na sličan način omogućava autentifikovano poricanje postojanja. Međutim, obezbeđuju se i mere protiv „nabrajanja“ zone („zone enumeration“) i omogućava se postepeno širenje zona koje su u najvećoj meri okrenute delegiranju.[7]

- Kompatibilnost
  - Bezbednosno svesni razrešitelji na kojima nije implementiran NSEC3 mogu videti odgovore sa primenjenim NSEC3 kao neispravne. Da bi se ovo izbeglo, koristi se signalizacija da bi se ukazalo ovakvim rezrešiteljima da ne pokušavaju validaciju NSEC3 odgovora.
  - Ovim standardom se definišu dva nova DNSKEY identifikatora algoritma. Algoritam 6, DSA-NSEC3-SHA1 je alias za algoritam 3, DSA. Algoritam 7, RSASHA1-NSEC3-SHA1 je alias za algoritam 5, RSASHA1.
- NSEC3 zapis resursa
  - Kreira listu tipova zapisa koji postoje za originalni (neheširani) naziv na koji se NSEC3 RR odnosi. Ovo obuhvata sledeći heširani naziv u heš redosledu zone. Komplet svih NSEC3 zapisa u zoni pokazuje koji RRset-ovi postoje za originalne nazive i čini lanac heširanih naziva u zoni. Radi zaštite od „*zone enumeration*“ slabosti, nazivi u NSEC3 zapisima predstavljaju heširane originalne nazive dodate kao celovite oznake na naziv zone.
  - Flegovi: Jedini definisani fleg označava da se koristi *Opt-out* mehanizam
  - Iteracije: Funkcija za heširanje se može ponavljati. Ovo povećava vreme potrebno za izračunavanje a time i kriptografsku snagu.
  - *Salt*: Dodatna vrednost koja se koristi za izračunavanje heša. Služi za povećanje kriptografske snage.
  - *Next hashed owner name*: Sledeća stavka u lancu. Svi nazivi domena i hešovi između datog naziva i ove vrednosti ne postoje.
  - *Type bitmap*: Lista tipova podataka za heširani naziv. Tipovi koji nisu navedeni ne postoje.
- NSEC3PARAM zapis resursa
  - Sadrži NSEC3 parametre (heš algoritam, flegovi, iteracije, *salt*) neophodne za izračunavanje neširanih naziva.
- Opt-out
  - Ovaj mehanizam omogućava postojanje nebezbednog delegiranja u okviru potpisane zone bez odgovarajućeg NSEC3 zapisa neširanog naziva.

2.2 Strategije mogućih DNSSEC implementacija

Dokument: „*Choosing a DNSSEC Solution*“[11]

Ovaj dokument kategorizuje moguća DNSSEC rešenja po nivou automatizacije procesa i nivou bezbednosti pri upravljanju ključevima.



Slika 2. Matrica izbora DNSSEC rešenja

2.2.1 Bezbedno upravljanje ključevima

DNSSEC se zasniva na izgradnji i održavanju odnosa baziranih na poverenju. U suštini, ovo se svodi na bezbednost privatnih ključeva. Ovo nije jednostavan problem, naročito ako se koristi dinamički DNS.

Rešenja koja sadrže bilo koji od sledećih atributa se klasifikuju kao rešenja sa **niskim nivoom bezbednosti** pri upravljanju ključevima:

- **Ručno rukovanje ključevima**
  Ljudi su skloni greškama. Ukoliko bi bilo potrebno ručno ukloniti privatni ključ, zatim ga ponovo vratiti, pre ili kasnije neko će pogrešiti. Što se češće ovo radi, veća je šansa da do greške dođe
- **Nekontrolisane dozvole**
  Privatni ključevi moraju uvek imati minimalne dozvole za čitanje, samo onoliko koliko je neophodno za obavljanje postavljenih zadataka. Softver koji generiše ključeve mora automatski da dodeljuje adekvatne nivoe dozvola, tako da privatnom ključu može pristupiti jedino odgovarajuće aplikacije iz DNSSEC rešenja, npr. potpisnik zone. Kod većine sistema root/Administrator ima pristup svemu. Delovi automatizovanih DNSSEC rešenja koji rukuju

privatnim ključevima obično rade na ovim nivoima, stoga zahtevajući da samo root/Administrator imaju dozvole za čitanje na svim privatnim ključevima.

- **Vidljiv potpisnik zone**
  Kod rešenja za automatizaciju DNSSEC-a koja ne mogu da rade u okruženju sa skrivenim masterom (i da mogu da bezbedno prenesu potpisanu zonu do javnih servera) samo je pitanje trenutka kada može doći do katastrofe.

Napomena: DNS sistemi koji samo isporučuju potpisane zone i ne potpisuju ih ne bi nikada trebalo da rade sa privatnim ključevima i stoga nema potrebe za posebnim postupcima nad njima.

Visok nivo bezbednosti pri upravljanju ključevima je jedino moguće ostvariti uz pomoć hardvera, naročito ako se koristi dinamički DNS i neophodno je stalno držati privatne ključeve *online*.

- **Rukovanje ključevima uz pomoć hardvera**
  Ovakva rešenja koriste hardver u vidu kriptografskog modula otpornog na neovlašćeni pokušaj pristupa ili modula gde je nemoguće sakriti dokaze o takvom pristupu. Ovakvi modulu bi trebalo da su sertifikovani sa FIPS 140-2 (nivo 3 ili 4) ili ISO/IEC 19790:2006 (nivo 3 ili 4). Kriptografski moduli postoje u različitim formama kao što su mrežni uređaji, kartice ili kao deo sistema. Generisanje ključeva kao i njihova obrada odvija se unutar ovih modula, i privatni ključevi nikada nisu vidljivi.
- **Bezbedna OS platforma**
  Problem može nastati ukoliko napadač može da instalira zlonamerne programe na serveru i izmeniti DNS podatke pre nego što budu potpisani. Rešenja iz kategorije visoke bezbednosti pri upravljanju ključevima moraju koristiti ojačanu ili bezbednu OS platformu na kojoj rade DNSSEC aplikacije.
- **Skriveni potpisnik zone**
  Problem može nastati ukoliko je sistem javno izložen. Konfiguracija sa skrivenim masterom umanjuje ovakvu izloženost.

U slučaju da je potrebno koristiti rešenje za upravljanje ključevima kod koga se **ne koristi hardver**, postoji nekoliko strategija koje obezbeđuju viši (mada ne visok) nivo bezbednosti.

Deo DNSSEC rešenja za automatizaciju čiji je zadatak generisanje ključeva i potpisivanje bi trebalo da ima iste korisničke/grupne dozvole. Softver koji generiše ključeve bi automatski trebalo da dodeljuje minimalne dozvole koje su neophodne. Softver koji radi sa privatnim ključevima bi trebalo da proverava da li ključevi imaju pravilne (minimalne) dozvole, da ih automatski postavlja ako to nije slučaj i da pošalje obaveštenje o slaboj tački u procesu rukovanja ključevima. Kada bi ključ bio iskorišćen, softver bi trebalo da pošalje obaveštenje o tome i da periodično proverava da li je sporni ključ uklonjen.

Najvažnija stvar u ovom scenariju je pristupačnost fajl sistemu. Na primer, DNS uređaji obezbeđuju različite pogodnosti putem izolacije funkcionalnosti i pružanja rešenja koja su konstruisana po meri zadataka. Međutim, takvi uređaji su obično bazirani na Linux ili BSD varijantama, mnogi sa jedinstvenim rešenjima za ojačanje, ali sa uobičajenim fajl sistemima. Ukoliko legalni korisnici mogu pristupiti tom uređaju, onda to mogu i zlonamerni. Ukoliko uređaj nije pristupačan legalnim korisnicima, velike su šanse (mada nije nemoguće) da neće biti ni zlonamernim stranama.

Razlike između upravljanja ključevima uz pomoć hardvera i ručnog upravljanja ključevima važe bez obzira da li se radi o rešenjima sa zasebnim DNS uređajima ili bez njih.

Napomena: Neki proizvođači koriste otisak prsta ili druge metode za autentifikaciju da bi obezbedile pristup USB uređajima. U nekim slučajevima, ovakvi uređaji mogu biti sertifikovani u skladu sa nižim FIPS 140-2 nivo 1 ili 2 standardima. U najvećem broju slučajeva, odmah posle obavljene autentifikacije, USB fajl sistem je izložen operativnom sistemu. Ovakvi uređaji poseduju karakteristike ručnog upravljanja ključevima.

2.2.2 Automatizacija DNSSEC-a

DNSSEC podrazumeva obavljanje određenog broja procesa koji zahtevaju strogo vremenski definisane okvire, iz čega se može zaključiti da veći nivo automatizacije smanjuje šansu da dođe do greške.

Rešenja koja sadrže sledeće atribute se klasifikuju kao rešenja sa **niskim nivoom automatizacije**:

- **Znatno angažovanje korisnika**
  Mnogi DNSSEC procesi su proceduralni. Periodično ponovno potpisivanje i prelasci između ključeva su takvi procesi. Softver koji pruža nizak nivo automatizacije obično obavlja ove procese na minimalnom nivou. Čak i na tom nivou, takav softver bi trebalo da obaveštava korisnika o tome šta treba uraditi putem elektronske pošte ili nekim drugim putem.
- **Nedostatak granularnosti**
  Neki elementi DNSSEC rešenja za automatizaciju zahtevaju dozvole za pristup ključevima, ali nekim delovima to nije neophodno, tako da bi oni trebalo da rade sa najnižim mogućim dozvolama u okviru sistema. Na taj način, u slučaju da dođe do softverske greške u tim elementima, ne mora da dođe do kompromitacije ključeva.
- **Neophodnost širokog poznavanja DNSSEC-a**
  Rešenja sa niskim nivoom automatizacije obično zahtevaju značajno poznavanje DNSSEC procesa, jer u slučaju da dođe do bilo kakve greške, korisnik mora reagovati što je pre moguće. Takođe, ne treba zanemariti troškove edukacije o DNSSEC.

Rešenja koja sadrže sledeće atribute se klasifikuju kao rešenja sa **visokim nivoom automatizacije**:

- **Malo angažovanje korisnika**
  Visok nivo automatizacije podrazumeva da su implementirani principi najbolje prakse bez potrebe za stalnim konfigurisanjem ili nadgledanjem. Međutim, neki procesi se moraju obavljati ručno, kao što je slanje DS zapisa posle prelaska između ključeva. U tom slučaju, najbolja rešenja obezbeđuju sav neophodni materijal, sa tačnim instrukcijama ili savetima o sledećim koracima u procesu, kao i sistemom kontrole. Na primer, ukoliko je reč o prelasku između KSK ključeva, mora se ažurirati roditeljska zona. Dobra rešenja bi periodično trebalo da proveravaju da li je zadatak obavljen, automatskim pregledom roditeljske zone.
- **Potrebno srednje poznavanje DNSSEC-a**
  Iako bi kvalitetna rešenja za automatizaciju trebalo da zahtevaju vrlo malo intervencija od strane korisnika, potrebno je razumno poznavanje DNSSEC-a i pratećih procesa, za slučaj nepredviđenih okolnosti.
- **Arhitektura sa zaobilaženjem greške („failover“)**
  Uvek postoji mogućnost da dođe do kvara na mreži ili hardveru, što u slučaju dužeg vremenskog perioda može dovesti do isticanja važnosti potpisa i nedostupnosti zona.

Rešenja sa visokim nivoom automatizacije bi trebalo da imaju mogućnost da rezervne kopije potpisnika zone mogu da preuzmu rad u takvim slučajevima.

Po autoru dokumenta, iako je idealno rešenje sa visokim nivoom automatizacije i visokim nivoom bezbednosti pri upravljanju ključevima, moraju se uzeti u obzir i praktični zahtevi, koji mogu biti različiti u zavisnosti od konkretnog scenarija primene. Autorova preporuka je da, u slučaju da je neophodno napraviti kompromis, prioritet treba dati bezbednom upravljanju ključevima, jer su kriptografski ključevi ono na čemu počiva integritet domena obezbeđenog uz pomoć DNSSEC-a.

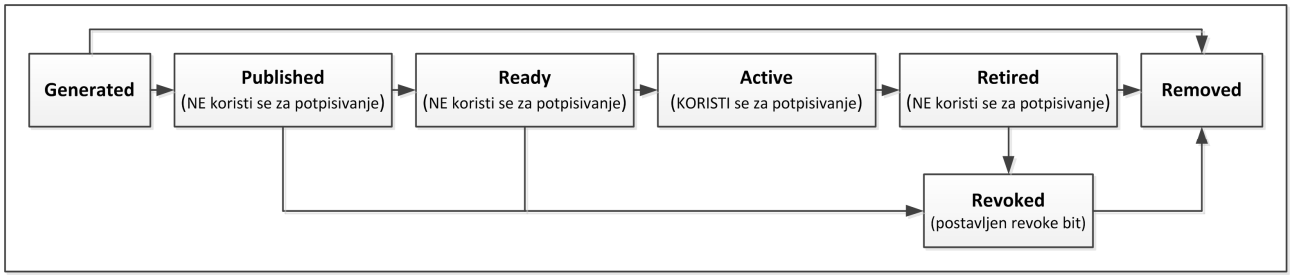
3. Preporuke za implementaciju i bezbednosnu politiku

3.1 Upravljanje ključevima

- Sistem za upravljanje ključevima bi trebalo da podržava zajedničke ključeve za potpisivanje zona i ključeva (CSK). Međutim, sistem za upravljanje ključevima MORA da podržava odvojene ključeve za potpisivanje zona (ZSK) i za potpisivanje ključeva (KSK), kao i prelaske između ključeva u skladu sa preporukama iz RFC 6781[6].
- Sistem za upravljanje ključevima bi trebalo da podržava čuvanje ključeva u odvojenom hardverskom modulu zaštite (HSM). Interfejs između sistema za upravljanje ključevima i HSM-a bi trebalo da bude zasnovan na PKCS#11. Međutim, ukoliko se ne koristi HSM, ključevi MORAJU biti kriptografski zaštićeni tokom čuvanja u trajnoj memoriji sistema.
    - Kada DNSSEC implementacija i HSM podržavaju PKCS#11 interfejs, generisanje ključeva se obavlja direktno unutar HSM-a, umanjujući mogućnost da dođe do kompromitacije ili neovlašćenog pristupa ključevima.
- Sistem za upravljanje ključevima MORA da podržava automatske i planske pralaze između ključeva za potpisivanje zona na *pre-publication* način, u skladu sa preporukama iz RFC 6781[6] i preporukama iz dokumenta “DNSSEC Key Timing Considerations”[12].

3.1.1 Stanja ključeva u DNSSEC-u

Stanja koje ključevi mogu da zauzmu u DNSSEC-u su u skladu sa nacrtom dokumenta „DNSSEC Key Timing Considerations“[12]. Na slici 3. je prikazan dijagram sa stanjima koje ključevi mogu da zauzmu.



Slika 3. Dijagram mogućih stanja ključeva

Generated

Ključevi sa ovim stanjem su kreirani i uskladišteni, ali se još uvek ne koriste.

Published

Ključevi sa ovim stanjem su objavljeni u zoni, ali se još uvek ne smatraju bezbednim za upotrebu (nisu bili u zoni dovoljno dugo da bi se proširili kroz sistem), jer predhodnici ključa mogu i dalje postojati u kešu.

Ready

Ključevi sa ovim stanjem su proveli objavljeni dovoljno dugo da se mogu bezbedno koristiti u sistemu (prethodne verzije DNSKEY zapisa bi trebalo da su istekle iz keša).

Active

Ključevi sa ovim stanjem su oni koji se trenutno koriste za potpisivanje RRset-ova.

Retired

Ključevi sa ovim stanjem su bili u upotrebi ali su zamenjeni. Ostaju objavljeni sve dok potpisi koji su njima kreirani mogu postojati u sistemu.

Dead

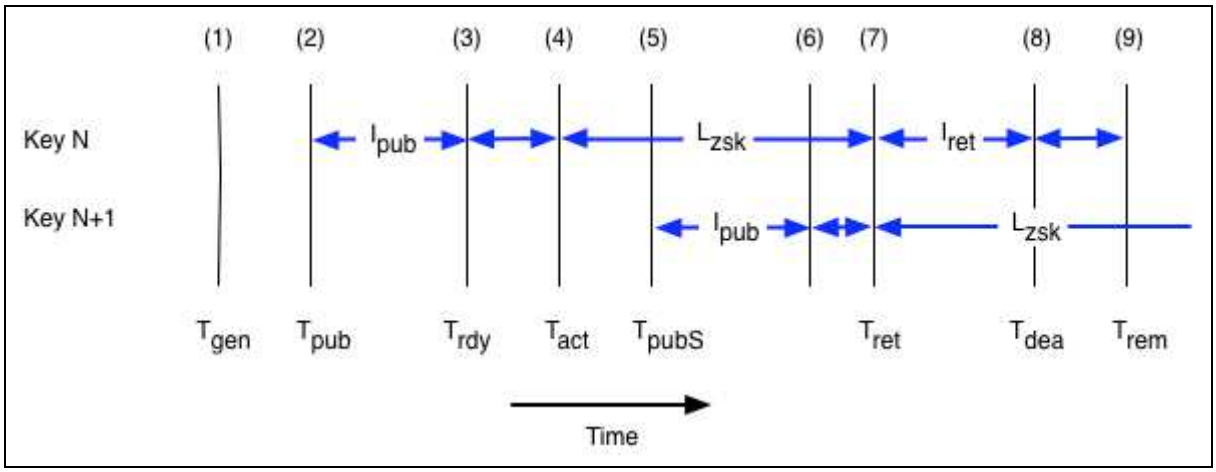
Ključevi sa ovim stanjem su bili u Retired stanju dovoljno dugo da se mogu bezbedno ukloniti iz zone (nigde više nema podataka koji zahtevaju prisustvo ključa).

3.1.2 Pre-publication prelazak između ključeva

Ovaj način prelaska bi trebalo koristiti za ZSK prelaske. Pri korišćenju *pre-publication* mehanizma, novi ključ se uvodi u DNSKEY Rrset, koji biva ponovo potpisan. Ovakvo stanje ostaje sve dok svi keširani RRset-ovi ne budu sadržali oba ključa. U tom trenutku se potpisi kreirani uz pomoć starog ključa mogu zameniti onima kreiranim uz pomoć novog ključa, i stari potpisi ukloniti. Kada u zoni budu postojali samo potpisi kreirani uz pomoć novog ključa, sledi interval u kome RRSIG zapisi generisani uz pomoć starog ključa treba da isteknu iz keša. Nakon toga, nigde više ne bi trebalo da postoje potpisi kreirani starim ključem i on može biti uklonjen iz DNSKEY RRset-a.

Prednosti i mane: Ovaj način prelaska između ključeva ne zahteva dvostruko potpisivanje podataka u zoni. Ali, pošto se pre samog prelaska između ključeva novi ključ objavljuje, to ga čini dostupnim za kriptoanalizu. Takođe, ovaj postupak zahteva četiri faze (inicijalna, novi DNSKEY, novi RRSIG, uklanjanje starog DNSKEY). Ukoliko se koristi za KSK prelaske, stvara dodatni posao na strani roditeljske zone.

- **Prvi ključ**: $I_{pub} = D_{prp} + \min(TTL_{soa}, SOA_{min})$
- **Budući ključevi**: $I_{pub} = D_{prp} + TTL_{key}$
- $T_{pubS} <= T_{act} + L_{zsk} - I_{pub}$
- $I_{ret} = D_{sgn} + D_{prp} + TTL_{sig}$

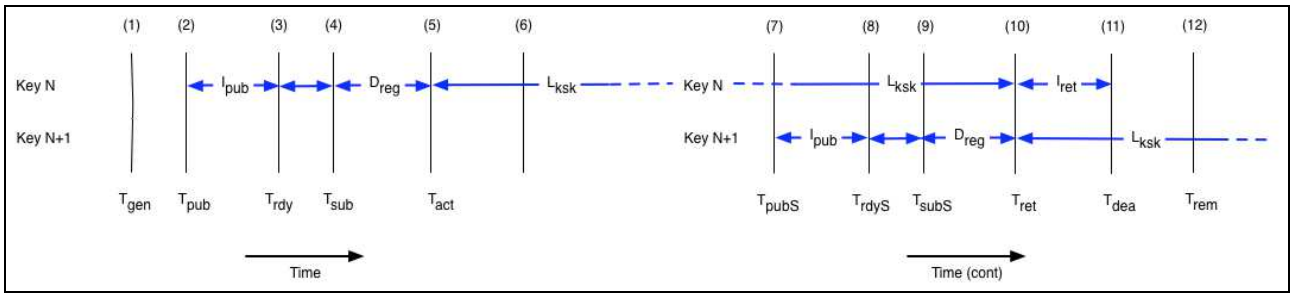


T_{gen} – Vreme generisanja ključa N (**Generated**)
T_{pub} – Vreme objavljivanja ključa N (**Published**)
I_{pub} – Interval u kome ključ mora provesti u **Published** stanju da bi mogao da se koristi
D_{prp} – (Propagation Delay) Vreme potrebno da se promene izvršene na master serveru prošire na sve slave servere
TTL_{soa} – TTL vrednost SOA zapisa
SOA_{min} – Vrednost „minimum“ parametra u SOA
TTL_{key} – Vrednost „Time-to-live“ parametra DNSKEY zapisa
T_{rdy} – Vreme kada je ključ spreman za upotrebu (**Ready**)
T_{act} – Vreme kada ključ počinje da se koristi (**Active**)
T_{pubS} – Vreme objavljivanja ključa naslednika ključu N
L_{zsk} – Životni vek ZSK ključa
T_{ret} – Vreme kada ključ N prelazi u **Retired** stanje
I_{ret} – Interval **Retired** stanja ključa
D_{sgn} – Vreme potrebno da svi postojeći RRset budu ponovo potpisani novim ključem
TTL_{sig} – Maksimalno TTL vreme svih RRsig zapisa kreiranih za ZSK
T_{dea} – Vreme kada svi RRsig zapisi isteknu iz keša razrešitelja
T_{rem} – Vreme kada ključ biva uklonjen (**Removed**)

3.1.3 Double-Signature prelazak između ključeva

Ovaj način prelaska bi trebalo koristiti za KSK prelaske. Pri primeni Double-Signature mehanizma, novi KSK ključ se dodaje u DNSKEY RRset, koji se potom potpisuje starim kao i novim ključem. Nakon isticanja starog RRset iz keša, DS zapis u roditeljskoj zoni se ažurira. Posle određenog vremena, kako bi se i ova promena reflektovala u keš memorijama u sistemu, stari ključ se uklanja iz RRset.

Prednosti i mane: Ova metoda prelaska između ključeva zahteva samo tri faze (inicijalna, novi DNSKEY, uklanjanje starog DNSKEY). Međutim, za vreme prelaska broj potpisa u zoni biva dupliran. Ovo može predstavljati poteškoću kod velikih zona ukoliko se koristi za ZSK prelaze.



- $I_{pub} = D_{prp} + TTL_{key}$
- $T_{pubS} <= T_{act} + L_{ksk} - D_{reg} - I_{pub}$
- $I_{ret} = D_{prpP} + TTL_{ds}$

L_{ksk} – Životni vek KSK ključa
D_{reg} – (Registration Delay) Vreme od trenutka prijema DS zapisa u roditeljskoj zoni do njegovog postavljenja u zonu
D_{prpP} – (Propagation Delay in Parent zone) Vreme potrebno da se novi DS zapis proširi na sve servere koji ga poseduju u kešu
TTL_{ds} – TTL vreme DS zapisa u roditeljskoj zoni

3.2 Sistem potpisivanja

- Sistem potpisivanja MORA podržavati DNSSEC u skladu sa standardima RFC 4033[2], RFC 4034[3] i RFC 4035[4].
- Sistem potpisivanja MORA podržavati potpisivanje uz korišćenje sledećih algoritama: RSA/SHA-1 u skladu sa RFC3110 [28], kao i RSA/SHA-256 i RSA/SHA-512 u skladu sa RFC5702 [29]
- Sistem potpisivanja bi trebalo da podržava potpisivanje uz korišćenje sledećih algoritama: ECDSA P-256/SHA-256 i ECDSA P-384/SHA-384 u skladu sa RFC 6605 [30].
- Sistem potpisivanja MORA podržavati NSEC3 kao što je predviđeno dokumentom RFC 5155[7].
- Sistem potpisivanja MORA podržavati DS zapise objavljene sa SHA-256, kao što je predviđeno dokumentom RFC 4509[31].
- Sistem potpisivanja bi trebalo da podržava simultano potpisivanje sa dva ili više algoritma.
- Sistem za potpisivanje bi trebalo da podržava prelaske između algoritama za potpisivanje, kao i prelaske između NSEC i NSEC3 bez dovođenja zone u nepotpisano stanje.
- Sistem za potpisivanje MORA da podržava promenu NSEC3 parametara bez dovođenja zone u nepotpisano stanje.
- Sistem potpisivanja MORA podržavati konfigurisanje životnog veka potpisa kao i konfigurisanje *refresh* perioda potpisa.

3.3 Distribucija

Svi transferi zone MORAJU biti zaštićeni od modifikacija i skraćivanja. TSIG[33] može predstavljati rešenje za ovaj problem, uz autentifikaciju korišćenjem algoritma iz HMAC-SHA[34] ili GSS-TSIG[35] porodice.

3.4 Validacija

- Sistem za validaciju DNSSEC potpisa MORA podržavati DNSSEC standarde (RFC 4033[2], RFC 4034[3] i RFC 4035[4]).
- Sistem za validaciju mora podržavati algoritme RSA/SHA-1 u skladu sa RFC3110 [28], kao i RSA/SHA-256 i RSA/SHA-512 u skladu sa RFC5702 [29].
- Sistem za validaciju bi trebalo da podržava sledeće algoritme: ECDSA P-256/SHA-256 i ECDSA P-384/SHA-384 u skladu sa RFC 6605 [30].
- Sistem validacije MORA podržavati NSEC3 kao što je predviđeno dokumentom RFC 5155[7].
- Sistem validacije MORA podržavati DS zapise objavljene sa SHA-256, kao što je predviđeno dokumentom RFC 4509[31].
- Sistem validacije bi trebalo da podržava automatsko ažuriranje pouzdanih polazišta u skladu sa RFC 5011[36].
- Sistem validacije bi trebalo da poseduje mogućnost isključenja postupka validacije za deo ili za kompletan imenski prostor.

3.4.1 TTL vrednosti

Jedan od ključnih faktora kada je reč o validaciji predstavlja TTL vrednost koja se dodeljuje zapisima resursa. Kako su ključevi i pripadajući potpisi najveći tipovi koji se šalju kao odgovor na upite, poželjno je TTL vrednosti držati velikom. Međutim, velika TTL vrednost može dovesti do problema prilikom određenih DNSSEC procedura, kao što su prelasci između ključeva. Takođe, povećava se vreme oporavka u slučaju havarije ili isteka ključeva. S druge strane, kraće TTL vrednosti daju agilnost sistemu prilikom prelazaka između ključeva, ali dodatno opterećuju servere i mrežu.

Određivanje preporučene TTL vrednosti je kompleksan zadatak jer podrazumeva pravljenje kompromisa. Videti poglavlje 2.1.5.

U istraživačkom radu[39] koji se bavi otpornošću OpenDNSSEC rešenja na greške, došlo se do rezultata koji su opšte primenjivi na DNSSEC, konkretno na polju optimalne TTL vrednosti. Po pretpostavci da je u pitanju scenario gubitka privatnih ključeva koji se ne može rešiti automatski od strane DNSSEC softvera, potrebno je uvesti nove ključeve u sistem uz postojanje starih ključeva i potpisa u kešu na serverima na Internetu (bez mogućnosti za obavljanje procedure prelaska između ključeva). Da bi se minimizirao uticaj ovakvog scenarija, autor istraživanja preporučuje dodeljivanje TTL vrednosti u odnosu 3:4 za potpise resursa i njihove odgovarajuće javne ključeve. Drugim rečima, TTL vrednost DNS zapisa sa javnim ključem bi trebalo da bude tri četvrtine TTL vrednosti potpisa generisanih tim ključem, kao i obrnuto.

3.4.2 Životni vek potpisa i SOA tajmeri

Vreme isteka (*expiration*) SOA zapisa služi obezbeđivanju stabilnosti zone. Kako zona može biti opsluživana sa više sekundarnih DNS servera, u slučaju da primarni server nije dostupan duži vremenski period, prikladno je da i sekundarni DNS serveri prestanu da odgovaraju na upite. Ovo je jedan od načina da DNS operateri saznaju da postoji mrežni problem ove vrste.

Preporuka RIPE je da SOA *expire* ima vrednost od 1000 časova[48], što iznosi oko 41 dan. Pošto DNSSEC uvodi dodatni parametar koji kontroliše ispravnost zone, životni vek potpisa, važno je uzeti u obzir njihov međusobni odnos. RFC 6781[6] preporučuje da SOA *expire* bude veličine jedne trećine ili jedne četvrtine perioda važenja potpisa. Razlog za ovo je otkrivanje problema sa transferom sa primarnog servera pre nego što dođe do isticanja potpisa. Mnogo je prihvatljivije da DNS operater postane svestan da sekundarni DNS server nije primio ažuriranu zonu, iako postoje ispravni potpisi za postojeći sadržaj.

Preporuka je da bi SOA *expire* vrednost trebalo da bude povezana sa vrednošću životnog veka potpisa. Nedostatak ove veze može dovesti do nedostupnosti, jer se pojavljuje rizik da životni vek ključeva istekne bez upozorenja. Izbor vrednosti životnog veka potpisa i vrednosti SOA *expire*, je izbor između toga koliko brzo DNS operater želi da sazna da postoji problem i toga koliko brzo može da ga reši. Problem jednim delom može biti otkriven praćenjem DNS servera i proveravanjem ispravnosti dobijenih odgovora na upite a drugim delom proveravanjem serijskog broja zone (u okviru SOA zapisa) da bi se utvrdilo da li svi DNS serveri poseduju istu verziju sadržaja zone.

3.4.3 Opterećenje razrešitelja

Dokument: „*Measuring the effects of DNSSEC deployment on query load*“[44]

U ovom dokumentu su predstavljeni rezultati i zaključci merenja uticaja na razrešitelje prilikom slanja upita ka RIPE serverima naziva. Pažnja je usmerena ka upitima sa postavljenim DO bitom u odnosu na one bez njega. Takođe, meren je broj skraćenih (*truncated*) DNS odgovora.

Primećeno je blago povećanje u broju upita, ali ne u broju DO=1 upita u odnosu na one sa DO=0. Zaključak je da nema vidljivog povećanja u ukupnom broju upita.

Što se tiče skraćenih odgovora, odmah po potpisivanju zone, takvi paketi su počeli da se pojavljuju. Osim nekoliko izuzetaka, svi su bili tipa *name error*, i bez izuzetka su posedovali DO bit postavljen na 1, kao i UDP veličinu od 512 bajta. U ovom slučaju, 512 bajta nije dovoljno za smeštanje neophodnih *authority* podataka kao i potpisa za te podatke. U većini pregledanih odgovora su nedostajali potpisi za NSEC podatke.

Analizom pojedinačnih hostova koji su slali upite, došlo se do rezultata da se na njime koristi BIND verzija 9.2.3rc1 - 9.4.0a0. U ovim verzijama BIND-a je podrazumevana EDNS0 veličina bafera 2048 ili 4096, pa se došlo do zaključka da je vrednost od 512 bajta postavljena ručno. Objašnjenje je pronađeno u uputstvu za BIND9, gde se navodi da se ovakve mere primenjuju zbog mogućnosti da pojedini *firewall*-ovi blokiraju fragmentirane pakete i/ili UDP pakete veće od 512 bajta. Zaključak navedene analize je da softver radi ispravno, ali da loša konfiguracija izaziva skraćivanje paketa.

Prikupljeni podaci ne pokazuju znake nelinearnih efekata izazvanih paketima koji su odbačeni između autoritativnih i rekurzivnih servera, usled aktiviranja DNSSEC-a.

3.5 Preporuke o tehničkim parametrima

Dokument: „*Recommendations for DNSSEC deployment at municipal administrations and similar organisations*“[32]

U ovom dokumentu su date preporuke o tehničkim parametrima za implementaciju DNSSEC, na osnovu najbolje prakse i praktičnog iskustva.

3.5.1 Ključevi za potpisivanje

Preporučuje se razdvajanje KSK i ZSK ključeva, na osnovu toga što to predstavlja široko primenjen i uhodan model za upravljanje ključevima. Algoritam za potpisivanje bi trebalo da bude RSA/SHA-256, kako se i koristi za potpisivanje root zone DNS-a. Dužine ključeva za KSK i ZSK bi, u skladu sa trenutnim kriptografskim preporukama da budu 2048 (KSK) i 1024 (ZSK) bita.

3.5.2 Životni vek potpisa

Da bi se omogućio rad i tokom operativnih prekida u slučaju dugih vikenda ili praznika, ovaj dokument preporučuje relativno dugačak životni vek potpisa (32 dana) uz svakodnevno ponovno potpisivanje.

3.5.3 Prelasci između ključeva

Preporučuje se obavljanje prelaska između KSK ključeva jedino u slučaju potrebe, što mora biti praćeno balansiranom analizom rizika. Potreba za obavljanje prelaska se može javiti ako osoblje koje je imalo pristup ključevima napusti organizaciju ili bude premešteno na druge radne dužnosti. Procedure za prelazak između ključeva bi trebalo da budu projektovane u odnosu na to kako se upravlja ključevima za druge sisteme u okviru organizacije. Prelasci između KSK ključeva predstavljaju veći rizik u odnosu na prelaske između ZSK, jer podrazumevaju zadatke koji se obavljaju ručno, kao što je ažuriranje DS zapisa u roditeljskoj zoni.

S druge strane, prelasci između ZSK ključeva se mogu obavljati automatski. Zbog relativno male dužine ključa, preporučuje se obavljanje prelaska svaka tri meseca.

3.5.4 Metoda za autentično poricanje postojanja

Preporučuje se primena NSEC3 (10 iteracija) za sve zone ispod TLD nivoa. Godišnje bi trebalo obavljati izmenu *salt* vrednosti, automatski ili ručno.

- NSEC se ne preporučuje zbog *zone walking* slabosti, tj. mogućnosti da se praćenjem ulančanih naziva mapira kompletna zona. NSEC3 rešava ovaj problem kreiranjem heša svakog naziva u zoni i kreiranja lanca ovakvih heširanih naziva. Upiti usmereni ka ovakvih heširanim nazivima uvek vraćaju NXDOMAIN (naziv ne postoji).
- NSEC3 koristi dva parametra za heširanje, *salt* i iteracije. *Salt* se dodaje nazivu zone pre heširanja. Iteracije predstavljaju korišćenje rezultata heširanja kao ulaznih podataka za kreiranje nove heš vrednosti.

- Primena NSEC3 dodatno opterećuje server usled učitavanja i potpisivanja velike količine podataka, pripreme odgovora na upite kao i zauzeća memorije. Opterećenje može biti do 8 puta veće.
- Primena NSEC3 dodatno povećava neophodan propusni opseg za obavljanja transfera zone. Povećanje može biti do 8 puta veće.
- NSEC3 poseduje mogućnost korišćenja *Opt-Out* mehanizma, koji omogućava lakšu implementaciju, fleksibilnost i skalabilnost. Potpisuju se samo autoritativni podaci u zoni i podaci delegiranih zona koje su samostalno potpisane. Veličina zone raste u skladu sa brojem potpisanih podzona. Međutim, mogućnost dokazivanja postojanja nepostojećih ili nepotpisanih podzona ne postoji. *Opt-Out* se koristi radi bržeg prihvatanja DNSSEC-a, sa mogućnošću uključivanja DNS operatera u DNSSEC u skladu sa njihovim izborom kada to žele da urade.
- Korišćenje *Opt-out* mehanizma može predstavljati bezbednosnu pretnju. Eksperimentalno je pokazano[8] da je moguće iskoristiti upotrebu ovog mehanizma za izvršenje *denial-of-service* napada, *cookie* krađe kao i podmetanje lažnih naziva u keš memoriju razrešitelja. Sa ovog aspekta se ne preporučuje korišćenje *Opt-out* mehanizma, već implementacija NSEC3 za kompletnu zonu.

3.5.5 Zaštita ključeva

Da bi se umanjio rizik od odavanja ključeva, u slučaju da hardver na kome se čuva ključ bude uklonjen, izgubljen ili ukraden, preporučuje se čuvanje materijala u šifrovanoj formi. Ključ ili lozinku za dešifrovanje bi trebalo čuvati van sistema i unositi je u sistem od strane administratora prilikom pokretanja sistema. Ključevi mogu biti čuvani i u nešifrovanoj formi ukoliko je sistem za potpisivanje fizički zaštićen i ukoliko postoje adekvatne procedure za uništenje iskorišćenih medija. Korišćenje HSM-a nije neophodno.

4. DNSSEC implementacija

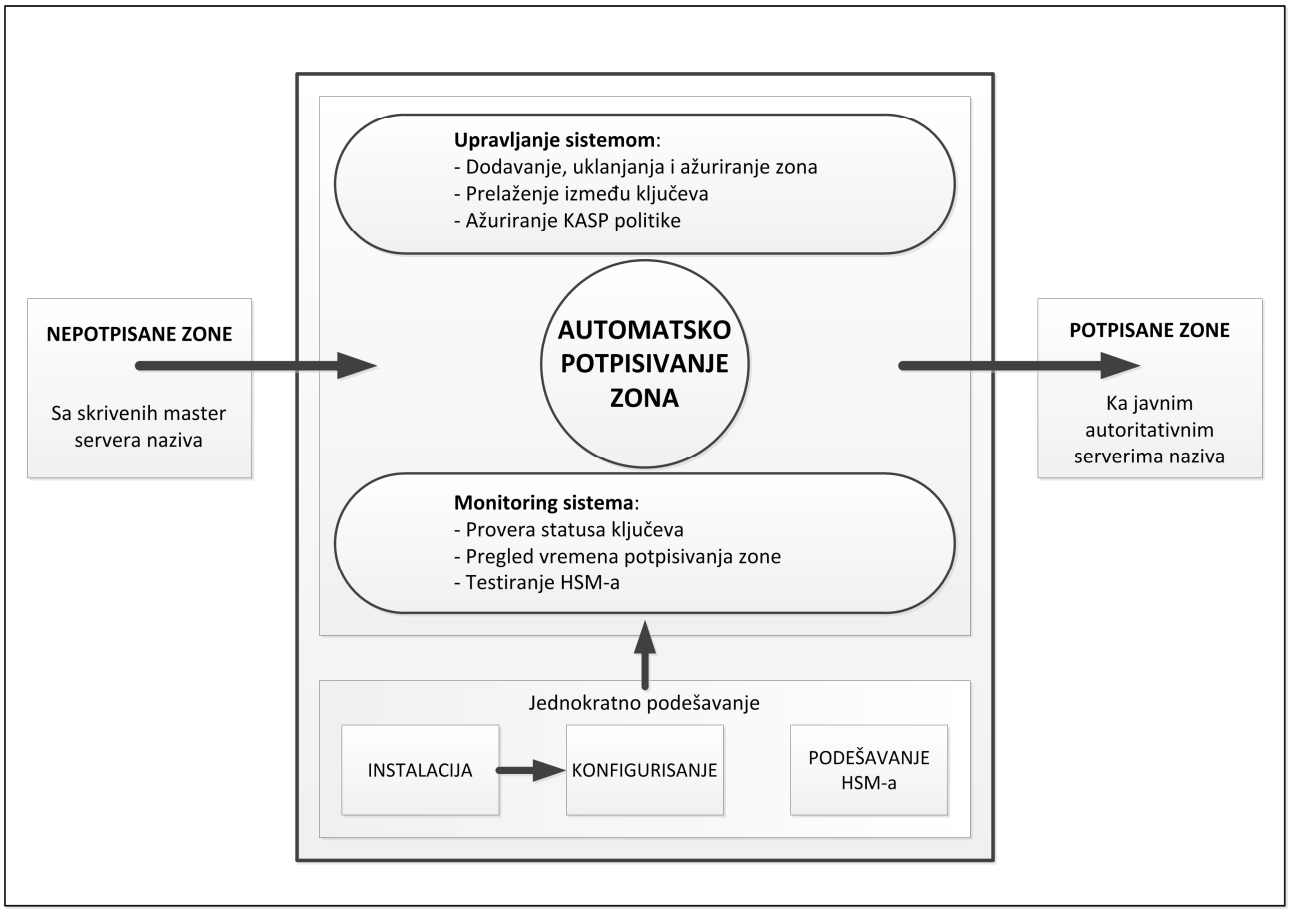
4.1 OpenDNSSEC

OpenDNSSEC predstavlja softver otvorenog koda za potpisivanje DNS zona koji može biti integrisan u praktično bilo koji postojeći sistem, bez potrebe za većim prepravkama ili promenama. Funkcionalno se postavlja između skrivenog master DNS servera koji sadrži jednu ili više nepotpisanih zona koje treba potpisati i eksternih servera koji su javno vidljivi. OpenDNSSEC prihvata nepotpisanu zonu putem AXFR/IXFR transfera zone ili iz zonskih fajlova, vrši potpisivanje i prosleđuje potpisanu zonu autoritativnim serverima. Može da radi potpuno automatski i posle početnog podešavanja nije neophodna intervencija korisnika, ali je u svakom trenutku moguće izvršiti ručni prelazak između ključeva (u slučaju nužde).

OpenDNSSEC je skalabilan, sa mogućnošću potpisivanja zona sa velikim brojem zapisa. Jedna OpenDNSSEC instanca može biti podešena da potpisuje jednu ili više zona, dok se isti ključevi mogu koristiti za više zona, da bi se sačuvao prostor u HSM-u. Moguće je detaljno definisanje politike za potpisivanje zona (dužina ključa, životni vek ključa, interval za potpise, itd.) uz mogućnost postojanja jedne politike za sve zone ili posebne politike za svaku zonu.

Osetljivi kriptografski podaci (privatni ključevi) se čuvaju unutar HSM-a, uz komunikaciju putem PKCS#11 standardnog industrijskog interfejsa. Za potrebe testiranja ili u slučaju da hardverski HSM nije neophodan, moguće je korišćenje softverske emulacije (SoftHSM) bazirane na SQLite. Postoji podrška za RSA/SHA1 i SHA2 potpise, dok je za poricanje postojanja moguće koristiti NSEC ili NSEC3.

OpenDNSSEC predstavlja međunarodni projekat razvijen u saradnji više aktera, među kojima su .SE, NLnet Labs, ICANN, Nominet, SURFnet, CIRA i dr. Podržava sve verzije Unix operativnog sistema. Aktuelna verzija je OpenDNSSEC 1.4.5 (11. april 2014.).



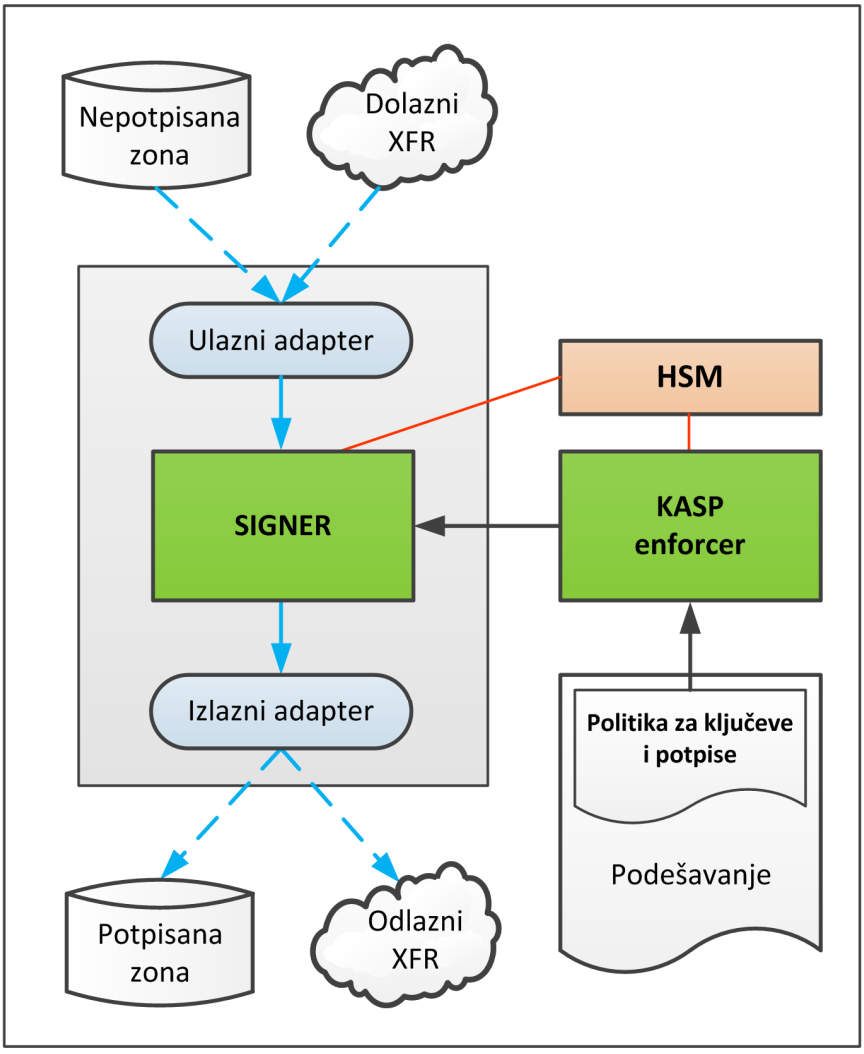
Slika 4. Rad OpenDNSSEC rešenja

4.1.1 Ključne komponente OpenDNSSEC-a

KASP (Politika za ključeve i potpise – *Key And Signing Policy*) podešavanja se beleže u jednom od konfiguracionih fajlova i njime se kontrolišu sledeći aspekti OpenDNSSEC-a: dužina ključa, algoritam ključa, životni vek ključa, životni vek potpisa, izbor između NSEC i NSEC3, itd. Ovde se definiše i broj različitih politika za zone kao i opseg koje te politike obuhvataju.

KASP *enforcer* je zadužen za upravljanje ključevima. Radi u vidu servisa i periodično se aktivira da bi proverio da li je potrebno ažuriranje vezano za stanje ključeva. Poseduje i sopstveni interfejs iz komandne linije (*ods-ksmutil*) za potrebe dobijanja informacija o stanju ključeva i zona. *Enforcer* upravlja:

- Kreiranjem ključeva uz pomoć HSM-a
- Izborom politika koje će biti primenjene na različite zone
- Stanjima i prelazima između stanja ključeva
- Prelascima između ključeva
- Izborom ključeva koji će se koristiti za potpisivanje zone
- Pravljenjem rezervne kopije



Slika 5. Ključne komponente OpenDNSSEC-a

Signer je odgovoran za obavljanje samog potpisivanja zone. Radi u vidu servisa i periodično se aktivira da bi proverio da li je potrebno ažuriranje zona. Poseduje i sopstveni interfejs iz komandne linije (*ods-signer*) koji služi za manuelnu kontrolu potpisivanja zone. On preuzima informacije koje generiše izvršilac zajedno sa nepotpisanim zonama i kreira zone potpisane naznačenim ključevima:

- Može da ponovo koristi potpise koji nisu previše stari
- Može da proširi vreme isteka potpisa („jitter“ – vrednost koja se dodaje ili oduzima od vremena isteka potpisa da bi se obezbedilo da svi potpisi ne isteknu u istom trenutku)
- Održava NSEC/NSEC3 lanac

Adapteri su odgovorni za dobavljanje nepotpisane zone kao i za distribuciju potpisane zone. Trenutno dostupni mehanizmi (za ulaz i za izlaz):

- Fajl: u slučaju da su zonski fajlovi na disku
- AXFR: zonski fajlovi se dobavljaju/distribuiraju putem AXFR
- IXFR: zonski fajlovi se dobavljaju/distribuiraju putem IXFR, ako je podržano

4.1.2 Prelasci između ključeva

OpenDNSSEC podržava *Pre-publication* mehanizam za prelaske između ključeva za potpisivanje zona (ZSK) i *Double signature* mehanizam za prelaske između ključeva za potpisivanje ključeva (KSK).

4.1.3 Alternativni način prelaska između ključeva

NLnet Labs, autori OpenDNSSEC-a, su 2012. predstavili alternativni pristup prelascima između ključeva[49]. Dosadašnji pristup prelasku između ključeva obuhvata kompleksan proces koji je podložan greškama. Postoji više različitih načina za obavljanje prelaska između ključeva i svaki tip prelaska predviđa sopstvene, složene procedure koje su povezane sa vremenskim parametrima. Takođe, administratori zona imaju različite potrebe za načinima prelaska – neke procedure služe za obavljanje prelaska što je pre moguće dok druge brinu o veličini zone i vremenu odziva, što izbor procedure svodi na izbor lokalne politike.

Dodatno ograničenje predstavlja to što se procedure za prelaske sastoje iz strogo definisanih redosleda radnji, od početka do kraja. Kao posledica, nije predviđena strategija konkurentnog prelaska. Ovo obično nije problem, jer se većina prelazaka obavlja po rasporedu i međusobno ne ometa. Ali, u slučaju kompromitacije ključa, potrebno je obaviti prelazak u slučaju nužde, da bi se ključ onesposobio što je pre moguće. Sa trenutnim proceduralnim pristupom, može doći do odlaganja hitnog prelaska dok se prelazak koji je u toku ne okonča.

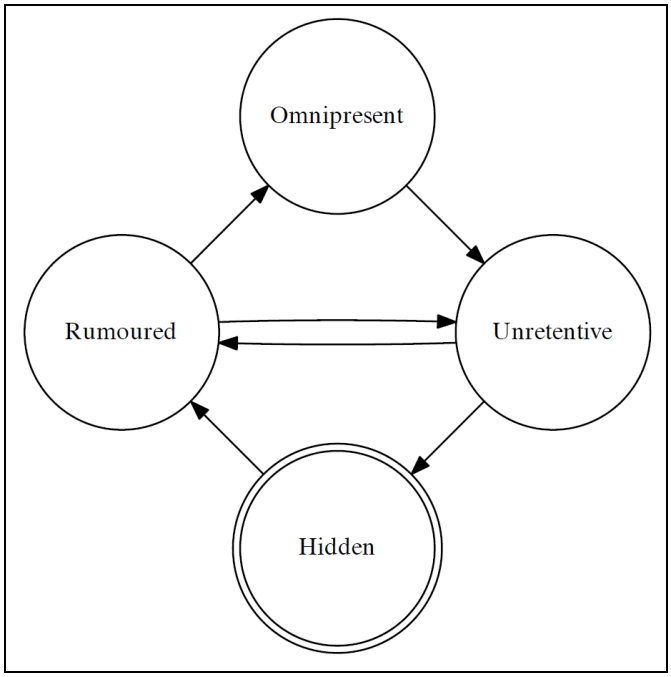
Alternativni i potencijalno svestraniji pristup predviđa dinamičko otkrivanje najbolje moguće strategije prelaska koja se uklapa u postavljenu politiku.

4.1.3.1 Stanja ključeva

Uobičajeni, postojeći pristup se može smatrati kao okrenutim ka prelascima (*rollover centric*) i posmatra prelazak kao proceduralnu specifikaciju više sekvencijalnih koraka sa strogim redosledom i vremenskim zahtevima. Alternativni pristup posmatra podatke iz perspektive svih servera koji ih koriste za validaciju u okviru globalne DNS infrastrukture. Pažnja je okrenuta ka ispravnosti podataka i tome **da li svi serveri mogu da prate lanac poverenja** sa dostupnim informacijama, bez obzira odakle one dolaze. Novi pristup pretvara ovaj princip u formalna pravila, oslobađajući se ograničenja koje nameće sekvencijalni pristup ili broj ključeva.

U trenutnom pristupu prelascima, stanja ključeva određuju napredak prelaska. Umesto jedne komplikovane mašine stanja po svakom ključu, predlaže se održavanje mašine stanja za svaki zapis resursa povezan sa pojedinačnim ključem. Ovo donosi četiri odvojene mašine stanja, koje se odnose na DS, DNSKEY, RRSIG DNSKEY i RRSIG. Poslednji ne predstavlja zapis resursa već se odnosi na sve potpise u zoni (osim za potpis na DNSKEY RRset). Podela između potpisa na DNSKEY RRset i ostalih potpisa je neophodna zbog podele ključeva na KSK i ZSK.

Za svaki ključ posmatra se poseban komplet međuzavisnih mašina stanja, po jedna za svaki zapis povezan sa ključem (Slika 6.).



Slika 6. Dijagram stanja pojedinačnih zapisa

Ove mašine prikazuju vidljivost zapisa resursa kod svih mogućih keš memorija u globalnoj DNS infrastrukturi. Stoga, sve mašine imaju iste komplete stanja. Životni ciklus zapisa resursa počinje i završava se u *Hidden* stanju (nijedan validator ne može da vidi zapis). Suprotno stanje je *Omnipresent*: svi validatori poseduju zapis u kešu ili su u mogućnosti da ga preuzmu po potrebi. Preostala dva stanja predstavljaju nesigurna stanja u modelu. U *Rumoured* stanju, zapis je objavljen u zoni, ali nije prisutan u svim keš memorijama, dok kod *Unretentive* stanja, zapis je uklonjen iz zone ali može biti i dalje keširan. Kod ova dva stanja, nije moguće osloniti se na zapis za formiranje lanca poverenja. Potpuno je bezbedno prelaziti između ova dva stanja, što omogućava prekid prelaska, opovrgavanje prelaska ili obavljanje nekoliko prelazaka istovremeno.

4.1.3.2 Ciljevi ključeva

Ključevi se upotrebljavaju u određene svrhe: Ključ će biti aktiviran da bi se koristio za autentifikaciju ili će biti uklonjen da se ne bi koristio. Prilikom aktiviranja ključa, sve odgovarajuće mašine stanja će pokušati da dostignu *Omnipresent* stanje. Prilikom uklanjanja ključa, cilj je dovesti sve odgovarajuće mašine u *Hidden* stanje. Dakle, **cilj ključa** je ili *Omnipresent* ili *Hidden*.

Cilj ključa ima direktan uticaj na tranziciju koja će se obaviti. Dok je stanje jednako cilju ključa, zapis se smatra stabilnim i neće biti pokušaja da se prevede u neko drugo stanje. U nestabilnoj situaciji, mašine će pokušavati da pređu u stanje korak bliže cilju, tj. željenom stanju.

Tranzicija između različitih stanja su moguća jedino ako novo stanje predstavlja ispravnu DNSSEC situaciju, tj. tranzicija ne prekida lanac poverenja. Da bi se ovo automatski verifikovalo, definisan je komplet formalnih pravila koje proveravaju ispravnost zone. Zahvaljujući ovome, prelaz između ključeva se može definisati kao postavljanje ciljeva za ključeve.

4.1.3.3 Mehanizam i pravila prelaska

Tranzicije između stanja ključeva su ograničene ispravnošću, vremenom i politikom. Algoritam 1 prikazuje promene stanja na svim ključevima u zoni u toku jednog koraka. Prilikom promene stanja bilo kog zapisa, svi ostali zapisi moraju biti provereni zbog međuzavisnosti njihovih stanja.

```
nextRun ← ∞
repeat
   change ← ⊥
   for all key ∈ zone do
      for all record ∈ key do
         nextState ← desiredState(record_state, key_goal)
         if nextState = record_state then
            {This record is in a stable state}
            continue
         end if
         if not policyApproval(keyring, key, record, nextState) then
            {Local policy prevents transition}
            continue
         end if
         if not transitionAllowed(keyring, key, record, nextState)
         then
            {This transition would make the zone invalid}
            continue
         end if
         t ← transitionTime(record, nextState)
         if t > now() then
            {We are not allowed to make the transition at this time}
            nextRun ← minimum(t, nextRun)
            continue
         end if
         record_state ← nextState
         record_lastChange ← now()
         change ← ⊤
      end for
   end for
until not change
return nextRun
```

Algoritam 1. U okviru jednog koraka zapisi dolaze bliže svom cilju. Na kraju se prikazuje sledeće apsolutno vreme kada se može obaviti koristan rad.

Algoritam poseduje četiri funkcije:

- *desiredState*(state, goal)
  Prikazuje „sledeće“ stanje i mašini stanja, s obzirom na cilj i trenutno stanje.
- *policyApproval*(keyring, key, record, nextState)
  Procenjuje da li postoje lokalne politike koji sprečavaju tranziciju zapisa u sledeće stanje. Ova funkcija omogućava postojanje različitih vrsta prelazaka.
- *transitionAllowed*(keyring, key, record, nextState)
  Procenjuje ispravnost tranzicije s obzirom na DNSSEC validnost.
- *transitionTime*(record, nextState)
  S obzirom da zapis i njegovo željeno stanje, izračunava trenutak kada zapis može ući u tranziciju. Ovo zavisi od vremena prethodne tranzicije zapisa, TTL vremena zapisa tog tipa i dodatnih postavljenih kašnjenja.

Za proveru ispravnosti zone sa proizvoljnim kompletom ključeva u proizvoljnim stanjima, neophodno je odrediti pravila za proveru te ispravnosti. Pravila se proveravaju prilikom svakog pokušaja tranzicije zapisa iz jednog stanja u drugo. Ako se ova pravila održe, tranzicija će biti obavljena.

Tranzicija sa *key* na *key'* biva dozvoljena samo ukoliko je sledeća jednačina održiva:

$$(\neg rule1(key) \vee rule1(key')) \quad \wedge \quad (\neg rule2(key) \vee rule2(key')) \quad \wedge \quad (\neg rule3(key) \vee rule3(key'))$$

Pravila su definisana sledećim jednačinama:

$$rule1(x):$$
$$\exists y \in K\ (D_y^{\uparrow +}) \qquad 1a$$

$$rule2(x):$$
$$\exists y \in X\ (D_y^{+} K_y^{+} R_y^{+}) \qquad 2a$$
$$\exists y, z \in X\ (D_y^{\uparrow} K_y^{+} R_y^{+} D_z^{\downarrow} K_z^{+} R_z^{+} \wedge y \overset{D}{\succ} z) \qquad 2b$$
$$\exists y, z \in X\ (D_y^{+} K_y^{\uparrow +} R_y^{\uparrow} D_z^{+} K_z^{\downarrow} R_z^{\downarrow -} \wedge y \overset{K}{\succ} z) \qquad 2c$$
$$\forall y \in X\ (D_y^{-} \vee \exists z \in X\ (K_z^{+} R_z^{+} (D_y = D_z))) \qquad 2d$$

$$rule3(x):$$
$$\exists y \in X\ (K_y^{+} S_y^{+}) \qquad 3a$$
$$\exists y, z \in X\ (K_y^{\uparrow} S_y^{+} K_z^{\downarrow} S_z^{+} \wedge y \overset{K}{\succ} z) \qquad 3b$$
$$\exists y, z \in X\ (K_y^{+} S_y^{\uparrow} K_z^{+} S_z^{\downarrow} \wedge y \overset{S}{\succ} z) \qquad 3c$$
$$\forall y \in X\ (K_y^{-} \vee \exists z \in X\ (S_z^{+} (K_y = K_z))) \qquad 3d$$

x, y, z – ključevi
D – DS
K – DNSKEY
R – RRSIG DNSKEY
S – RRSIG

(+) – *Omnipresent*
(-) – *Hidden*
(↑) – *Rumoured*
(↓) – *Unretentive*

Potpisani simboli (x, y, z) označavaju pripadnost ključevima dok natpisani simboli (+, -, ↑, ↓) označavaju stanje zapisa

Pravilo 1 navodi da u svakom trenutku mora postojati objavljen DS zapis. Ovo služi kao bezbednosna mera koja sprečava prelaz zone u nepotpisano stanje ili prelaz na ključ preko nepotpisanog stanja.

Pravilo 2 se brine o ispravnom stanju DNSKEY set-a. Razmatraju se samo ključevi sa istim algoritmom kao za ključ *x*:

- **2a** predstavlja trivijalan slučaj, gde postoji ključ sa *Omnipresent* DS zapisom i *Omnipresent* DNSKEY zapisom (potpisanim).
- **2b** predviđa da za dva ili više ključeva sa *Omnipresent* DNSKEY zapisima može doći do zamene DS zapisa.
- **2c** predviđa da DNSKEY zapisi mogu biti zamenjeni ako su njihovi DS zapisi u *Omnipresent* stanju.
- **2d** se bavi nepotpisanim stanjem: ključ *x* može biti u bilo kojem stanju sve dok su DS zapisi svih ostalih ključeva *y* u *Hidden* stanju, ili kada njihov DS nije *Hidden*, mora postojati ključ z sa pripadajućim DS u istom stanju i DNSKEY u *Omnipresent* stanju. Drugim rečima, ako je DS zapis za ovaj algoritam i dalje dostupan nekim validatorima, mora postojati lanac poverenja za te validatore.

Pravilo 3 je slično pravilu 2, ali se bavi potpisima. Takođe, razmatraju se samo ključevi sa istim algoritmom kao za ključ *x*:

- **3a** – Postoje DNSKEY i potpisi jednog ključa koji su poznati svim validatorima.
- **3b** – Svi validatori imaju pristup barem jednom od DNSKEY ključeva od *y* do *z*, i svim potpisima. Lanac poverenja može biti uspostavljen u svakom slučaju.
- **3c** – Svi validatori imaju pristup jednom od potpisa ključeva od *y* do *z* i svim DNSKEY zapisima.
- **3d** – Ako nema objavljenih DNSKEY, stanje potpisa je nevažno. U slučaju da je DNSKEY objavljen, mora postojati putanja koja odatle može biti verifikovana.

4.1.3.4 Izazovi i napomene

- Predloženi metod prelaska između ključeva je fleksibilan i podržava CSK kao i prelaske između algoritama, čineći ih ništa drugačijim od ZSK ili KSK prelazaka.
- Mogućnost promene u okviru prelazaka koji su u toku čini hitne prelaske veoma efikasnim.
- Podela pravila omogućava mnogo lakši oporavak iz neispravnog stanja, na primer označavajući da li je u pitanju problem sa DNSKEY ili sa potpisima.
- Model i pravila su razvijeni kao deo OpenDNSSEC projekta, sa planiranim objavljivanjem u 2.0 verziji. Parametri politike kreiranog ključa se čuvaju zajedno sa samim ključem, tako da su pored proizvoljnih prelaza između ključeva, moguće i promene politike i vremenskih parametara bez posebnih mera.
- Ne postoji podrška za opozivanje ključeva (planirano), radi automatskog ažuriranja *trust anchor*-a.
- Ne postoji koncept *standby* ključeva.
- Prilikom primene algoritma na komplet ključeva, stanje zapisa će preći u ciljano onoliko brzo koliko to dozvoljavaju vremenska ograničenja i ograničenja ispravnosti. Međutim, zbog mogućih aspekata politike, najbrži put ne mora uvek biti poželjan. Postoje tri delimično konfliktne strategije:
    - **Minimizirati interakciju sa roditeljskom zonom**
      Uvođenje novog DS zapisa u roditeljsku zonu i uklanjanje starog u isto vreme. Da bi se održao lanac poverenja, DS novog DNSKEY zapisa mora biti u *Omnipresent* stanju.
    - **Minimizirati veličinu DNSKEY**
      Kao i prethodno, ali je u pitanju zamena starog DNSKEY novim. U zavisnosti od tipa ključa, DS zapis i/ili RRSIG zapisi moraju biti u *Omnipresent* stanju.
    - **Minimizirati potpise**
      Potpisivanje svih podataka sa više ključeva značajno povećava mrežni saobraćaj. Potpisi mogu biti zamenjeni atomično, ali DNSKEY zapisi moraju biti u *Omnipresent* stanju.

4.2 BIND

BIND (*Berkeley Internet Name Domain*) je najkorišćeniji DNS server na Internetu. Razvija ga i održava Internet Systems Consortium (ISC). Trenutno aktuelna verzija je 9.10.0-P2 (Jun 2014.). U pitanju je softverski paket otvorenog koda, koji se sastoji od serverske komponente (*named*), koja može raditi kao autoritativni server (*master*, *slave*) ili rekurzivni server naziva ili može obavljati ove funkcije simultano. U paketu je i biblioteka sa interfejsom za razrešavanje kao i različiti alati za administriranje. Kao interfejs sa BIND-om se koristi komandna linija dok se njegova konfiguracija čuva u tekstualnim dokumentima.

4.2.1 BIND i DNSSEC

Dokument: „*A Review of Administrative Tools for DNSSEC – Spring 2010*“[51][1]

- U slučaju da je neophodno, moguće je odabrati različit životni vek za različite zone ali ne i za različite zapise. Moguće je odabrati različit životni vek za ZSK i KSK.
- BIND podržava RFC 5011 (standard za prenos javnog KSK ključa do validatora).
- Pravljanje rezervne kopije je izvan opsega BIND-a. Podrška za PKCS#11 omogućava *offline* čuvanje ključeva.
- Ne postoji automatsko obaveštavanje administratora o potrebi transfera DS zapisa usled automatskog prelaska između ključeva. DS i javni KSK ključ mogu biti manuelno eksportovani. Automatizacija je moguća jedino u slučaju da su roditeljska i zona potomka na istom serveru.
- BIND podržava fajl, AXFR i IXFR dolazne i odlazne metode transfera zone kao i dinamičko ažuriranje (*dynamic updates*).
- Ključevi se podrazumevano čuvaju u clear-text fajlu. Ključevi se mogu čuvati na šifrovanom disku (u kom slučaju nije moguće automatsko potpisivanje) ili u HSM-u.
- Ključevi mogu biti učitani ili eksportovani (fajl format) u BIND private-key formatu v1.3 (format v1.2 je takođe podržan).
- Moguće je, putem skripte, simultano generisati ključeve za više zona. Praćenje automatizovanog potpisivanja se može obaviti putem fajl loga ili *syslog*-a.
- U slučaju *auto-dnssec* potpisivanja, postupak se automatski vremenski raspoređuje, radi smanjenja opterećenja. Parametri se mogu izmeniti u okviru konfiguracionog fajla.
- BIND opciono podržava izmenu SOA serijskog broja. Podržava formate *counter*, *Unix time* i *stay unchanged*.
- Postoji podrška za NSEC3 opt-in i opt-out.
- *Pre-publish* metoda prelaska između ključeva se koristi kako za ZSK tako i za KSK.
- Nije moguće vremenski rasporediti prelaske između ključeva, već se oni odvijaju po rasporedu.

[1] U vreme nastanka navedenog dokumenta, aktuelna verzija BIND-a je bila 9.7

- Putem alata *dnssec-settime* moguće je doći do atributa ključeva, kao što su vreme kreiranja i datum isteka za KSK i ZSK. Da bi se ostvario uvid u atribute potpisa zone, neophodno je pristupiti fajlu zone.
- Postoji više kategorija za logovanje. Logovi mogu biti poslati u fajl ili *syslog*. Međutim, ne postoji podrška za SNMP.

4.3.2 Generisanje DNSSEC ključeva

BIND poseduje alate za dva različita načina generisanja ključeva:

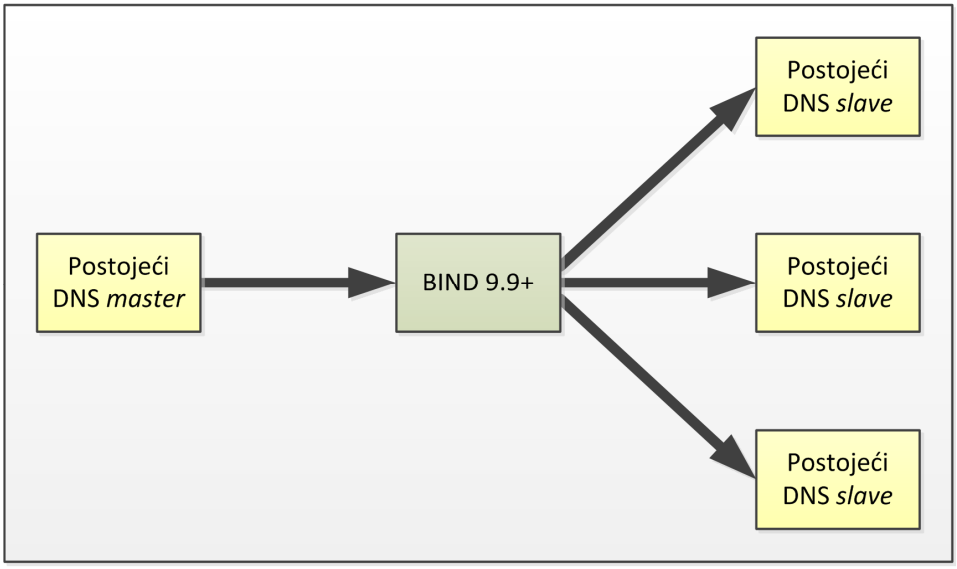
- *dnssec-keygen* (fajl način)
  - Podržani algoritmi za DNSSEC ključeve: RSAMD5, RSASHA1, DSA, NSEC3RSASHA1, NSEC3DSA, RSASHA256, RSASHA512, ECCGOST, ECDSAP256SHA256 or ECDSAP384SHA38.
  - Podržani algoritmi za TSIG/TKEY: DH (Diffie Hellman), HMAC-MD5, HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, or HMAC-SHA512.
  - Za DNSSEC, RSASHA1 (512-4096 bita) je obavezan, dok se preporučuje DSA. Za TSIG, obavezan je HMAC-MD5.
- *dnssec-keyfromlabel* (uz pomoć HSM-a)
  - Obezbeđuje ključeve iz kriptografskog hardvera i kreira fajlove sa ključevima.
  - DNSSEC u BIND-u zavisi od OpenSSL-a, tako da je podrška za HSM/PKCS#11 zasnovana na konfigurisanje HSM-a kao *OpenSSL engine*.

4.3.3 DNSSEC potpisivanje

BIND podržava tri metode za rad sa DNSSEC-om:

- **Manuelno potpisivanje**, koje obavlja administrator servera iz komandne linije.
- **Automatsko potpisivanje**. Od verzije 9.7, postoji podrška za *auto-dnssec*. Nakon početnog podešavanja, serveri koji koriste *auto-dnssec* mogu da automatski potpisuju i ponovno potpisuju zone u odgovarajuće vreme, oslobađajući DNS operatera od manuelnih prelazaka između ključeva i ponovno potpisivanja zonskih podataka za veliki broj zona.
  - Automatsko potpisivanje ovom metodom zahteva konfigurisanje zona kao dinamičke. BIND ne može da vrši izmene nad zonama definisanim kao statičke.
- Od verzije 9.9 moguće je korišćenje „*inline signing*“ metode. ***Inline*** **potpisivanje** funkcioniše na bilo kojoj *master* ili *slave* zoni, tj. ne zahteva konfigurisanje zone kao dinamičke.
  - U slučaju *master* servera, zona se učitava sa diska ali se kreira kopija te zone u kojoj se čuva potpisana verzija. Ne vrše se nikakve izmene na originalnoj zoni. Nakon izmena u fajlu zone i ponovnog učitavanja, BIND prepoznaje inkrementalne izmene i primenjuje ih na potpisanoj verziji, dodajući potpise po potrebi
  - U slučaju *slave* servera, proces funkcioniše vrlo slično, osim što se vrši transfer zone sa master servera i zatim potpisuje. Namenski server za potpisivanje funkcioniše kao posrednik između skrivenog *master* servera (koji obezbeđuje „sirove“ podatke o zoni) i grupe javno dostupnih slave servera (čiji je zadatak da pružaju potpisane podatke).

- Važno je napomenuti da je jedna od posledica *inline* potpisivanja da **serijski brojevi** koji se javno pružaju ne poklapaju sa serijskim brojevima u fajlu zone. Proces potpisivanja povlači i povećanje serijskog broja prilikom promene potpisa, što donosi stalno povećanje serijskog broja potpisane zone čak i bez ikakvih promena u fajlu zone.



Slika 7. *Inline* potpisivanje između master i slave servera

4.3 NSD

NSD predstavlja isključivo autoritativni DNS server. Odlikuju ga memorijska efikasnost i brzina rada. Koristi fajlove zone formatirane u stilu BIND-a, a moguće je i korišćenje BIND-ovih fajlova zone bez izmena, uz konfigurisanje u nsd.conf konfiguracionom fajlu NSD-a. Razvijen je od strane NLnet Labs-a.

NSD se sastoji od dva programa: kompajlera zone (*zonec*) i samog servera (*nsd*). Server radi sa binarnom bazom podataka koju priprema kompajler zone na osnovu fajlova zone. Ovo podrazumeva da je pre rada neophodno izvršiti kompajliranje zona pre nego što NSD može da ih koristi. Ovakva, jednostavna arhitektura omogućava veliku brzinu pokretanja i opsluživanja zone (čak i pod velikim opterećenjem), malo zauzeće memorije i verifikaciju sintakse i označavanje grešaka za vreme faze kompajliranja.

NSD podržava DNSSEC od verzije 2.0, dok je aktuelna verzija 4.0.3. Nisu potrebna posebna podešavanja za rad sa DNSSEC-om, već je moguće odmah preći na fazu generisanja parova ključeva i potpisivanja zone. Ovo se može obaviti uz pomoć alata kao što su *OpenDNSSEC*, *ldns* (takođe razvijen od NLnet Labs-a) ili *Zone Key Tool*.

4.4 Unbound

Unbound je rekurzivni server koji obavlja validaciju i kešira informacije, razvijen od strane NLnet Labs-a. Implementiran je u C jeziku, sa akcentom na što bolje performanse. U poređenju sa BIND-om, efikasnije koristi memoriju i poseduje više mogućnosti za kontrolu keširanja. Poseduje sledeće karakteristike:

- Jednostavnost i lakoća podešavanja
- Visoke performanse
- Podrška za DNSSEC
- Specijalizovanost
- Bezbednost
- Upravljivost
- Portabilnost

Da bi Unbound mogao da obavlja razrešavanje sa DNSSEC-om, neophodno je postaviti početno pouzdano polazište. Alat **unbound-anchor** omogućava dobavljanje početnog *anchor*-a na osnovu ugrađenih podataka, s obzirom da Unbound dolazi sa sertifikatom izdatim od strane ICANN-a. Root ključ se čuva u fajlu /usr/local/etc/unbound/root.key i *unbound-anchor* kreira ovaj fajl ukoliko već ne postoji. Ipak, preporučuje se ručno preuzimanje *trust anchor*-a sa https://data.iana.org/root-anchors/root-anchors.xml. Po preuzimanju, treba koristiti sledeću sintaksu u root.key:

```
. IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A418552...FB5
```

Unbound-anchor bi trebalo da se pokreće zajedno sa sistemom, kao deo Unbound paketa. Po pokretanju se proverava važnost *anchor*-a i ažuriranje po potrebi. Preporučuje se da se pre njegovog pokretanja izvrši sinhronizacija vremena preko NTP servera.

Unbound koristi metode definisane u RFC 5011 za ažuriranje *anchor*-a ukoliko dođe do promene za vreme njegovog rada, ali se koristi *unbound-anchor* alat ako je do promene došlo dok Unbound nije radio.

Konačno, u unbound.conf fajlu, potrebno je definisati lokaciju *root anchor* fajla:

```
server:
     auto-trust-anchor-file: "/usr/local/etc/unbound/root.key"
```

5. Komunikacija sa ovlašćenim registrima i DNS operaterima

5.1 Extensible Provisioning Protocol (EPP)

EPP je stateful XML protokol aplikacionog nivoa koji je namenjen operacijama vezanim za predodređivanje objekata prilikom korišćenja zajedničkog centralnog skladišta objekata. Protokol je izvorno zamišljen kao mehanizam za razmenu podataka o registraciji domena između registara i DNS operatera/ovlašćenih registara na Internetu.

EPP je baziran i zajedno sa proširenjima detaljno opisan u sledećim dokumentima:

- **RFC 5730** – „Extensible Provisioning Protocol (EPP)“[13]
- **RFC 5731** – „Extensible Provisioning Protocol (EPP) Domain Name Mapping“[14]
- **RFC 5732** – „Extensible Provisioning Protocol (EPP) Host Mapping“[15]
- **RFC 5733** – „Extensible Provisioning Protocol (EPP) Contact Mapping“[16]
- **RFC 5734** – „Extensible Provisioning Protocol (EPP) Transport Over TCP“[17]
- **RFC 5910** – „Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)“[18]
- **RFC 3915** – „Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (EPP)“[19]

Takođe, zbog upotrebe XML formata, neophodno je korišćenje sledećih standarda:

- **W3C.REC-xml-20040204** – „Extensible Markup Language (XML) 1.0 (Third Edition)“[20]
- **W3C.REC-xmlschema-1-20041028** – „XML Schema Part 1: Structures Second Edition“[21]
- **W3C.REC-xmlschema-2-20041028** – „XML Schema Part 2: Datatypes Second Edition“[22]

EPP protokol se sastoji iz dva osnovna aspekta: objekti i akcije. **Objekti** predstavljaju entitete koji su uskladišteni u EPP registru, kao što su domeni, kontakti i hostovi (tj. serveri naziva). **Akcije** deluju na promene u registru i objekte koje sadrži (npr. check, create, update, delete...). Komunikacija se obavlja putem poruka u XML formatu, u kome su podaci koji predstavljaju zahteve i odgovore struktuirani u logičke grupe i hijerarhije. Protokol je nezavisan od načina transporta, tj. EPP poruke mogu biti prenošene različitim transportnim protokolima (TCP, TCP+TLS, SMTP...). EPP poseduje i mogućnost lakog proširenja, tako da se mogu definisati dodatne vrste objekata ili akcije kao i dodatni podaci u okviru postojećih poruka.

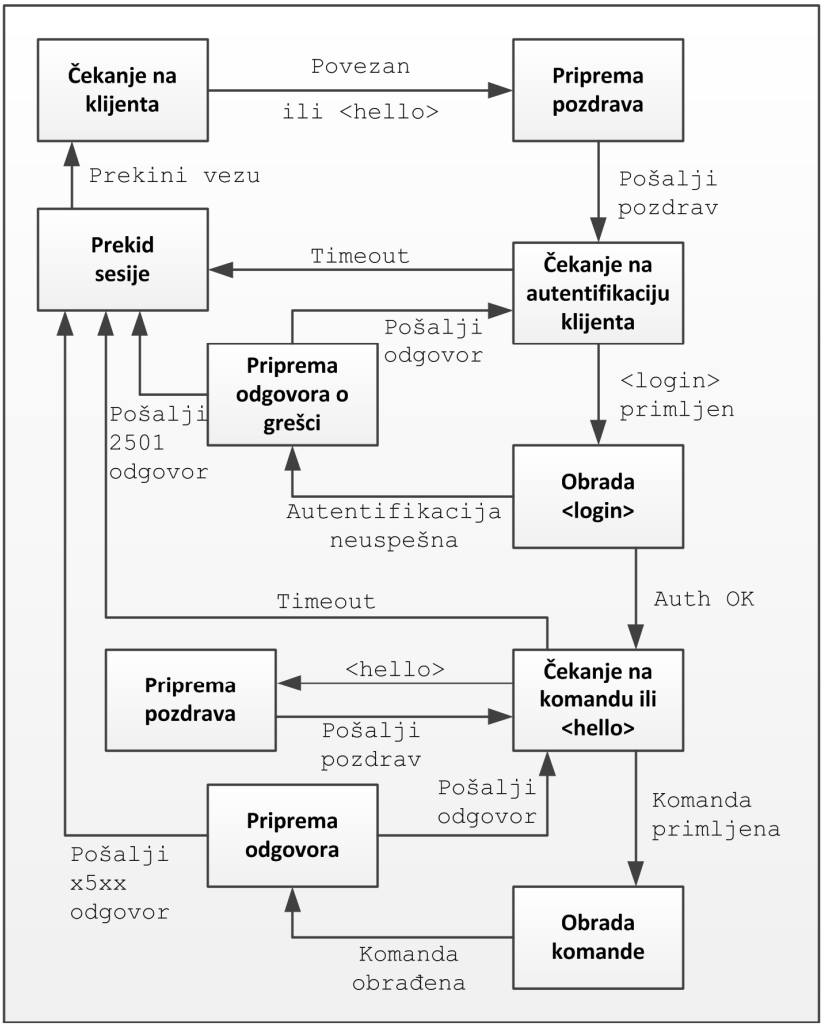
Funkcionalno, EPP se sastoji iz četiri celine:

- Pronalaženje usluge (**Service discovery**)
- Komande (**Commands**)
- Odgovori (**Responses**)
- Okvir za proširenja (**Extension framework**)

Svaki EPP klijent poseduje jedinstveni identifikator na serveru. Takođe, svi objekti moraju da poseduju jedinstvene identifikatore u okviru skladišta (roid), kao i lokalni naziv, koji se koristi kad god se objekat poziva u zahtevu ili odgovoru.

Uz zaštitu protokola nižeg nivoa, klijenti koji koriste EPP šalju identifikacione i autentifikacione podatke nakon kojih je moguće započeti razmenu po principu komanda-odgovor. Sve EPP komande su atomične (nema delimičnog uspeha ili delimičnog neuspeha) i projektovane tako da izvršavanje komande više od jedanput ima isti efekat kao da je izvršena samo jedanput.

Server mora u najkraćem roku da odgovori na svaku EPP komandu, šaljući odgovor u kome se opisuje rezultat obrade komande. Dijagram mašine stanja je prikazan na slici 8.



Slika 8. Mašina stanja EPP servera

Iako se klijentu odmah šalje potvrda o prijemu i obradi komande, EPP protokol poseduje funkciju koja omogućava *offline* pregled komandi za izmenu objekata pre nego što se njima naložena radnja izvrši.

EPP koristi XML prostor imena (*namespace*) za rad proširivog okvira za upravljanje objektima i za definisanje šema (s*chema*) neophodnih za obradu XML podataka. Ovi prostori imena i definicije šema se koriste i za identifikovanje šeme osnovnog protokola kao i šema za objekte kojima se upravlja.

EPP model podataka definiše da svaki objekat mora imati „sponzora“ tj. klijenta koji je autorizovan da upravlja postojećim objektom. Klijent koji kreira novi objekat automatski postaje njegov sponzor. Sponzorstvo nad domenom može biti promenjeno <transfer> komandom, dok sponzorstvo nad objektima tipa kontakt ili host ne može biti promenjeno. Jedino je sponzoru objekta dozvoljeno da obavlja promene na objektu.

EPP komande se mogu svrstati u tri kategorije:

EPP Komande	Opis	Objekti
Komande za upravljanje sesijom	(Session management commands) Uspostavljanje i prekidanje veze sa serverom	
<login>	Prijavljivanje na EPP server	
<logout>	Odjavljivanje sa EPP servera	
Upitne komande	(Querry commands) Operacije čitanja radi dobijanja informacija	
<check>	Provera postojanja objekta	domain, host
<info>	Informacije o objektu	domain, host, contact
<poll>	Dobavljanje poruka sa EPP servera – prijem obaveštenja	
<transfer>	Provera trenutnog statusa zahteva koji su nerešeni ili okončani	domain
Komande za izmenu objekata	(Transform commands) Obavljanje operacija čitanja i pisanja nad objektima	
<create>	Kreiranje novog objekta	domain, host, contact
<delete>	Brisanje objekta	domain, host, contact
<renew>	Produženje vremena važenja objekta	domain
<transfer>	Promene u sponzorstvu objekta	domain
<update>	Promena informacija o objektu	domain, host, contact

EPP objekti (domeni, hostovi, kontakti) poseduju atribute i njima pripadajuće vrednosti koje mogu biti pregledane i promenjene od strane klijenta koji je njihov sponzor ili od strane servera. Detaljni pregled atributa dat je u odgovarajućim dokumentima za domene[14], hostove[15] i kontakte[16]. DNSSEC je u EPP uveden u formi ekstenzije atributa domenskih objekata[18]:

DNSSEC Atribut	Opis	Komande
maxSigLife	Maksimalni životni vek potpisa (RRSIG zapisa) za DS zapis	create, info, update
dsData		create, info, update
keyTag	Oznaka ključa	create, info, update
alg	Oznaka algoritma	create, info, update
	Identifikator algoritma korišćenog za kreiranje sažetka	create, info, update
digestType		
digest	DNSKEY sažetak	create, info, update
keyData		create, info, update
flags	DNSKEY flegovi	create, info, update
	Oznaka protokola	create, info, update
protocol		
alg	Identifikator algoritma	create, info, update
pubKey	Javni ključ	create, info, update
keyData		create, info, update
urgent		update

Uz primenu ekstenzije za DNSSEC, EPP klijent može da kreira, dodaje ili uklanja DS zapis ili informacije koje se odnose na javni ključ. U skladu sa tim, server može podržavati dve vrste

interfejsa. Prvi je „**DS Data Interface**“, u kome klijent kreira DS podatke i odgovoran je za njihovo dodavanje i uklanjanje. Drugi je „**Key Data Interface**“ u kome je klijentu omogućeno da obezbedi podatke o javnom ključu prilikom dodavanja ili uklanjanja. Server mora da podržava samo jedan od interfejsa, osim u prelaznom periodu, tokom kojeg može postojati podrška za oba interfejsa. XML prefiks ove ekstenzije je <secDNS>, dok je oznaka šeme i imenskog prostora *secDNS-1.1*.

Primer korišćenja DS Data interfejsa:

```
<secDNS:dsData>
 <secDNS:keyTag>12345</secDNS:keyTag>
 <secDNS:alg>3</secDNS:alg>
 <secDNS:digestType>1</secDNS:digestType>
 <secDNS:digest>49FD46E6C4B45C55D4AC</secDNS:digest>
</secDNS:dsData>
```

Primer korišćenja DS Data interfejsa sa opcionim podacima o ključu:

```
<secDNS:dsData>
 <secDNS:keyTag>12345</secDNS:keyTag>
 <secDNS:alg>3</secDNS:alg>
 <secDNS:digestType>1</secDNS:digestType>
 <secDNS:digest>49FD46E6C4B45C55D4AC</secDNS:digest>
 <secDNS:keyData>
  <secDNS:flags>257</secDNS:flags>
  <secDNS:protocol>3</secDNS:protocol>
  <secDNS:alg>1</secDNS:alg>
  <secDNS:pubKey>AQPJ////4Q==</secDNS:pubKey>
 </secDNS:keyData>
</secDNS:dsData>
```

Primer korišćenja Key Data interfejsa:

```
<secDNS:keyData>
 <secDNS:flags>257</secDNS:flags>
 <secDNS:protocol>3</secDNS:protocol>
 <secDNS:alg>1</secDNS:alg>
 <secDNS:pubKey>AQPJ////4Q==</secDNS:pubKey>
</secDNS:keyData>
```

5.1.1 Bezbednosne napomene

Kako EPP obezbeđuje samo jednostavnu autentifikaciju klijenta, neophodna je zaštita od uobičajenih napada. Zaštita mora biti realizovana preko transportnog mehanizma ili aplikacionog protokola koji obezbeđuje integritet, poverljivost i autentifikaciju između klijenta i servera. Takođe, istim putem bi trebalo sprečiti i *replay* napade.

Odvraćanje od višestrukih pokušaja prijavljivanja se preporučuje putem ograničenja broja <login> zahteva u toku aktivne veze.

Sve akcije kojima se vrše izmene na objektima moraju biti ograničene na klijente koji su autentifikovani sponzori objekta. Bilo koji pokušaj izvršenja akcije kojom se menja objekat od strane bilo kog klijenta osim klijenta koji je sponzor objekta mora biti odbačen.

Kako provera ispravnosti podataka i kreiranje DS zapisa zahtevaju računarske resurse, sistem može biti preopterećen ukoliko klijent pošalje određen broj zahteva koji prekoračuju procesorske mogućnosti servera. Potrebno je preduzeti korake u cilju upravljanja raspodelom opterećenja i uslovima za obradu komandi, kako bi se sprečio *Denial of Service*.

Maksimalni životni vek potpisa(maxSigLife), kao parametar koji postavljaju klijenti, može biti potpuno isključen.

5.1.2 EPP softver – EPP API – Net::DRI

Net::DRI je Perl biblioteka koja se koristi za komunikaciju sa registrima, uz pomoć API-ja za pristup servisima. Između ostalog, isporučuje se sa:

- Punom RRP implementacijom (RFC 2832 i RFC 3632)
- Punom EPP implementacijom (STD 69, RFC 5730-5734, RFC 3735)
- Mnogim EPP ekstenzijama:
  - GracePeriod (RFC 3915)
  - E164 za ENUM (RFC 4114)
  - Enum validacija (RFC 5076)
  - SecDNS za DNSSEC (RFC 4310)
- Podrškom za UDP/TCP/TLS socket transport
- Podrškom za HTTP/HTTPS transport
- Podrškom za različite vrste SOAP transporta preko HTTP/HTTPS
- Podrškom za SMTP transport

Net::DRI se može preuzeti sa:

http://search.cpan.org/dist/Net-DRI/

5.1.3 Primena EPP – Nacionalni registar Norveške (NORID)

Nacionalni registar Norveške primenjuje EPP u skladu sa dokumentima [13-16]. Ovde će biti predstavljene samo specifičnosti vezane za DNSSEC implementaciju. Detaljna specifikacija EPP implementacije ovog operatera se može naći u dokumentu [23]. Takođe, EPP XML šema koju koristi NORID se može naći na [24].

- Svaki ovlašćeni registar na svom nalogu poseduje „DNSSEC enabled“ fleg, koji određuje da li je ovlašćeni registar voljan i da li može da radi sa DNSSEC podacima. Da bi ovlašćenom registru bilo dozvoljeno da dostavi i održava DNSSEC podatke na svojim domenima, ovaj fleg mora biti postavljen. Ukoliko nije postavljen, ovlašćenom registru će biti dozvoljeno jedino da ukloni DNSSEC podatke sa domena, ukoliko postoje.

- Posebne okolnosti predstavlja prenos domena koji je obezbeđen sa DNSSEC. Ukoliko novi ovlašćeni registar nema dozvolu da radi sa DNSSEC, DNSSEC podaci će biti uklonjeni sa domena.
- Za rad sa DNSSEC, NORID podržava *secDNS-1.1*, što mora biti najavljano prilikom prijave na sistem
- maxSigLife nije dozvoljen i ukoliko se navede, biva odbačen
- DNSSEC podaci se unose preko *DS Data* interfejsa sa opcionim *keyData* i okviru *dsData*.
- *Key Data* interfejs nije podržan
- *urgent* atribut nije dozvoljen i biva odbačen

NORID je obezbedio primere za EPP XML sekvence između EPP klijenta i servera. Primerima, koji obuhvataju i rad sa DNSSEC-om se može pristupiti preko:

http://www.norid.no/registrar/system/dokumentasjon/eksempler/

Takođe, NORID je omogućio preuzimanje izvornog koda njihovog Web EPP klijenta kao i Perl programa za automatsko dohvatanje servisnih poruka i njihovo slanje preko elektronske pošte. Ovaj softver se može preuzeti sa:

http://www.norid.no/registrar/system/epp/div-epp-prog.en.html

5.1.4 Primena EPP – Nacionalni registar Švajcarske (SWITCH)

Nacionalni registar Švajcarske primenjuje EPP u skladu sa dokumentima [13-16]. Ovde će biti predstavljene samo specifičnosti vezane za DNSSEC implementaciju. Detaljna specifikacija EPP implementacije ovog operatera se može naći u dokumentu [25].

- Podržan je jedino *secDNS-1.1*
- Prilikom korišćenja DNSSEC ekstenzija, neophodno je da partner poseduje tu opciju kao aktiviranu. U suprotnom, biće mu poslata poruka o grešci prilikom prijave na sistem.
- Mora biti naznačeno korišćenje DNSSEC-a prilikom prijave na sistem: *urn:ietf:params:xml:ns:secDNS-1.1*
- SWITCH ne proverava delegiranja i ne proverava da li su potpisani domeni dostupni
- *keyData* unosi su opcioni i čuvaju se nakon unosa. Ukoliko se koristi *keyData*, atributi *flags*, *protocol*, *alg* i *pubKey* su obavezni
- Podržan je jedino *DS Data* interfejs

[. . .]

5.2 Prihvatanje DS i DNSKEY podataka

Delegation Signer zapis resursa predstavlja tačku delegiranja autoriteta između roditeljske i zone potomka. Ovaj zapis se kreira putem primene heš funkcije (sažimanja) podataka o ključu iz DNSKEY zapisa. Ovo se može obavljati na strani zone potomka (kao u slučaju **.se** zone), u kom slučaju je neophodno postojanje mehanizma za prihvatanje DS zapisa u roditeljskoj zoni. Ali, ovo

se može obavljati i na strani roditeljske zone (kao u slučaju zona **.nl**, **.cz**, **.eu**, **.de**...), u kom slučaju je neophodno postojanje mehanizma za prihvatanje DNSKEY zapisa.

5.2.1 Prednosti korišćenja DS podataka

- Roditeljska zona ne mora da bude upoznata sa algoritmom za dobijanje heša u DS zapisu, tako da je moguće korišćenje nepodržanih algoritama.
    - Posao registra je da povezuje objekte sa entitetima. Posao registra nije da istražuje, generiše ili ocenjuje.
- Kada se ne obavljaju kalkulacije, nema mogućnosti da dođe do greške. Registar može objaviti DS zapis takav kakav je i primljen.
- DS zapis je kraći i stoga lakši za upravljanje od DNSKEY zapisa.
    - Zahtevati od registra da generiše podatke u ime DNS operatera nije skalabilno. Ovo je naročito važno za registre sa velikim brojem zona, gde ovo može stvoriti dodatni posao (iako generisanje heša traje mnogo kraće od potpisivanja, treba i ovo uzeti u obzir). U DNS-u je delegiranje opterećenja projektovano da bude usmereno na dole, što decentralizovanije.
- Ukoliko je potrebna provera, DNSKEY se uvek može pronaći u DNS-u zone potomka. Ovo nije moguće za DS zapis.
    - Pitanje provere podataka je pitanje razdvajanja autoriteta nad objavljivanjem podataka i autoriteta nad sadržajem tih podataka. Iako roditeljska zona ima autoritet nad DS zapisom, zona potomka je odgovorna za sadržinu.

5.2.2 Prednosti korišćenja DNSKEY podataka

- DNSKEY predstavlja ključ koji je esencijalan podatak za potvrđivanje autentičnosti zone potomka.
- DNSKEY je odmah posle generisanja ključeva dostupan DNS operateru.
- DS zapis je autoritativan za roditeljsku zonu i stoga bi trebalo da potiče od nje.
- Dostavljanjem ključa je moguće direktno proveriti postojanje (i konzistentnost) podataka u zoni potomka.
- Iz DNSKEY zapisa se uvek može izračunati DS zapis, ne i obrnuto.
- Generisanje DS zapisa omogućava roditeljskoj zoni da samostalno određuje snagu heš funkcije.
    - Neki registri žele da imaju potpunu kontrolu nad izborom algoritma koji se koristi (npr. politika nekog registra može biti da ne podržava GOST algoritam, dok politika nekog drugog može biti da podržava samo GOST algoritam).
    - Na primer, registar može doneti odluku o promeni politike i neprihvatanju DS zapisa sa određenim algoritmima. Ukoliko registar poseduje DNSKEY, ovakav prelaz je mnogo lakši od zahtevanja novih DS zapisa od svih zona potomaka.
- Dostavljeni DNSKEY sadrži informaciju o tome da li se radi o SEP-u.
- U slučaju promene DNS operatera, registar mora da prenese DNSKEY podatke od novog operatera do starog. Stoga, registar bi morao da dodatno zahteva DNSKEY podatke od novog operatera. Da bi se interakcija između roditeljske i zone potomka što više smanjila, može se sve vreme koristiti DNSKEY.

5.2.3 Izbor interfejsa

Prihvatanje DS ili DNSKEY zapisa se svodi na izbor politike registra. Strana odgovorna za DS zapis je roditeljska zona, tako da postoji fleksibilnost pri određivanju politike za kreiranje DS zapisa – on može biti dostavljen ili se može kreirati na osnovu DNSKEY zapisa. Kako je opšte pravilo da protokol ne bi trebao da diktira politiku implementacije i kako postoje ispravni razlozi za korišćenje bilo koje od moguće dve, protokol dozvoljava korišćenje obe mogućnosti.

6. Prenosi domena

6.1 DNSSEC i prenosi domena

Dokument: „*DNSSEC and domain transfers*“[9]

Uvođenjem DNSSEC-a, svaki prenos domena (ovlašćenog registra ili DNS operatera) može da stvori probleme prilikom validacije. Ovi problemi mogu dovesti do toga da domeni ne mogu biti razrešeni ili da ne mogu biti bezbedno razrešavani. Potencijalni problemi su slični kao i prilikom prenosa u DNS-u bez DNSSEC-a, gde do okončanja prenosa i stari i novi server naziva moraju paralelno da razrešavaju domen, zbog keširanja u DNS-u.

Kod DNS-a, dovoljno je nastaviti razrešavanje na starom serveru naziva u trajanju (TTL) NS zapisa resursa. Sa DNSSEC-om, promena obuhvata i upravljanje DS zapisom resursa u roditeljskoj zoni kao i svim DNSKEY zapisima u staroj i novoj zoni potomka, da bi DNSSEC lanac poverenja nastavio da funkcioniše za vreme prenosa (uzimajući u obzir TTL za sve zapise resursa).

Registranti očekuju da njihovi domeni budu dostupni i bezbedno razrešavani za vreme prenosa. Iz tog razloga, ovlašćeni registri kao i DNS operateri moraju registrantima da obezbede dokumentaciju i alate za upravljanje DNSSEC aspektima njihovih domena. Postoje tri moguća scenarija prenosa domena:

Scenario 1. Promena ovlašćenog registra (OR) i promena DNS operatera
Scenario 2. Promena DNS operatera
Scenario 3. Promena ovlašćenog registra

U svim scenarijima registrant mora da koordinira prenos, a u slučaju promene DNS operatera, ovo uključuje i rukovanje NS, DS i DNSKEY zapisima između OR. Ovo je čest scenario, jer su većina OR i DNS operateri. Takođe, važno je napomenuti da ni u kom slučaju nema prenosa ključeva. To znači da stari DNS operater ne deli svoj privatni ključ sa novim operaterom, tako da novi DNS operater neće moći da generiše digitalne potpise uz pomoć tog ključa. DNS operateri ne bi nikada trebalo da dele svoj privatni ključ, u skladu sa najboljom bezbednosnom praksom.

Verisign u slučaju **scenarija 1** prenosa domena opisuje preporučeni proces. Stari DNS operater je operater sa koga se vrši prelaz na novog operatera:

1. Proces počinje sa registrantom (vlasnikom DNSSEC domena *primer.rs*) koji kontaktira željenog novog ovlašćenog registra/DNS operatera i obaveštava ga o nameri
2. Novi operater kreira DNSSEC zonu za *primer.rs*, ali ona u ovom stadijumu nije javno dostupna.
3. Novi operater saopštava registrantu sledeće:
    a. DNSKEY zapis u zoni za KSK i ZSK.
    b. DS zapis, koji mora biti postavljen u roditeljskoj zoni (*.rs*), za novi KSK.

4. Registrant kontaktira starog DNS operatera i od njih zahteva sledeće:
    a. Da objave DNSKEY zapise dobijene od strane novog operatera i da ponovo potpišu DNSKEY skup zapisa u zoni koju oni održavaju.
    b. Da dodaju DS zapis za *primer.rs* kreiran od strane novog operatera, putem kontakta sa autoritetnim registrom.
    c. Da umanje TTL vreme DNSKEY i NS zapisa za *primer.rs* koji je u njihovoj zoni, da bi se prelaz na novog DNS operatera obavio što lakše. TTL od 10 minuta (600 sekundi) je dovoljan.
    d. Da registrantu pošalje autorizacione podatke („auth info“) za *primer.rs* koje će registrant proslediti novom operateru, kako bi prenos domena mogao da počne.
5. Registrant verifikuje da je stari DNS operater obavio sve zahtevane radnje i proverava TTL vremena svih DNS zapisa za *primer.rs*. Oni obuhvataju DNSKEY, RRSIG i NS zapise kao i DS zapise u roditeljskom domenu *.rs*).

    a. TTL sa najvećim vremenom određuje koliko registrant mora da čeka pre prebacivanja sa servera naziva starog na DNS servere novog operatera.
6. Nakon što sačeka da pomenuti TTL isteknu, registrant zahteva od starog operatera da kontaktira roditeljsku zonu (*.rs*) da bi:
    a. Uklonio DNS servere starog DNS operatera sa *primer.rs*.
    b. Dodao DNS server novog DNS operatera za *primer.rs*.
7. Registrant treba da sačeka da TTL za NS zapis starog operatera istekne i da potvrdi da DNS serveri novog operatera razrešavaju *primer.rs*.
8. Registrant kontaktira novog operatera i zahteva od njega da otpočne prenos domena.
9. Novi operater kontaktira *.rs* registar i podnosi zahtev za prenos za primer.rs, pružajući na uvid autorizacione podatke. Ovo se obavlja uz pomoć EPP protokola.
10. Stari DNS operater odobrava prenos domena (zahtev za prenos domena će biti automatski odobren ukoliko u roku od 5 dana stari operater ne preduzme nikakve korake).
11. Registrant kontaktira novog operatera i zahteva uklanjanje DS zapisa starog operatera za *primer.rs*.

Ono što je u ovom scenariju problematično je prenos DNS hostinga. U obzir se moraju uzeti DNS serveri na Internetu koji razrešavaju i keširaju i mora se postići da svi oni:

- Imaju DS zapis novog DNS operatera u svom kešu, pre nego što budu usmereni ka DNS serveru novog operatera koji razrešava *primer.rs*.
- Poseduju u svom kešu DNSKEY novog operatera pre pokušaja da se verifikuje bilo koji potpis kreiran uz pomoć tog ključa.

Što se tiče ovlašćenih registara i DNS operatera:

- Stari DNS operater mora da dozvoli registrantu da dostavi „strane“ DNSKEY zapise (novog operatera) u njegovu zonu. To podrazumeva i ponovno potpisivanje DNSKEY RRset-a.
- Stari DNS operater mora da dozvoli registrantu da dostavi DS zapis (novog operatera), koje ovlašćeni registar mora poslati roditeljskom registru.
- U slučaju da ne postoji spremnost za saradnju starog DNS operatera, tj. da isti ne omogući obavljanje prethodnih koraka, jedino rešenje predstavlja privremeni prekid bezbednog razrešavanja (DNS bez DNSSEC-a), uklanjanjem svih DS zapisa iz roditeljske zone. Posle isteka DS TTL vremena (da bi podaci nestali i iz keš memorija) domen može biti prenesen kao nebezbedan pa zatim ponovo obezbeđen DNSSEC-om od strane novog operatera.

U slučaju **scenarija 2**, vrši se promena DNS operatera bez promene OR. Registrant mora da koordinira ovakav prenos, ponovo uključujući rukovanje NS, DS i DNSKEY zapisima između ovlašćenih registara:

1. Registrant kontaktira novog DNS operatera i obaveštava ga o nameri.
2. Novi operater kreira DNSSEC zonu za *primer.rs*, ali ona u ovom stadijumu nije javno dostupna.
3. Novi operater saopštava registrantu sledeće:
    a. DNSKEY zapis u zoni za KSK i ZSK.
    b. DS zapis, koji mora biti postavljen u roditeljskoj zoni (*.rs*), za novi KSK.
4. Registrant kontaktira starog DNS operatera i od njih zahteva sledeće:
    a. Da objave DNSKEY zapise dobijene od strane novog operatera i da ponovo potpišu DNSKEY skup zapisa u zoni koju oni održavaju.
    b. Da umanje TTL vreme DNSKEY i NS zapisa za *primer.rs* koji je u njihovoj zoni, da bi se prelaz na novog DNS operatera obavio što lakše.
5. Registrant kontaktira ovlašćeni registar za svoj domen i zahteva dodavanje DS zapisa novog DNS operatera u registar
6. Registrant verifikuje da je stari DNS operater obavio sve zahtevane radnje i proverava TTL vremena svih DNS zapisa za *primer.rs*, uključujući i TTL za DS zapis u registru.
    a. TTL sa najvećim vremenom određuje koliko registrant mora da čeka pre prebacivanja sa servera naziva starog na DNS servere novog operatera.
    b. Registrant dodaje najduži TTL na trenutno vreme, znajući da će biti bezbedno izvršiti promenu DNS servera kada taj trenutak prođe.
7. Posle isticanja svih ranije pomenutih TTL vremena, registrant kontaktira svoj ovlašćeni registar da bi u saradnji sa registrom:
    a. Uklonio sve DNS servere starog operatera za *primer.rs*.
    b. Dodao DNS servere novog operatera za *primer.rs*.
    c. Uklonio DS zapis starog DNS operatera za *primer.rs*.

U slučaju **scenarija 3** (prenos domena između dva ovlašćena registra, bez promene DNS operatera), Verisign opisuje proces kao vrlo jednostavan, sličan procesu kod DNS-a bez DNSSEC-a, uz dodatnu proveru na kraju:

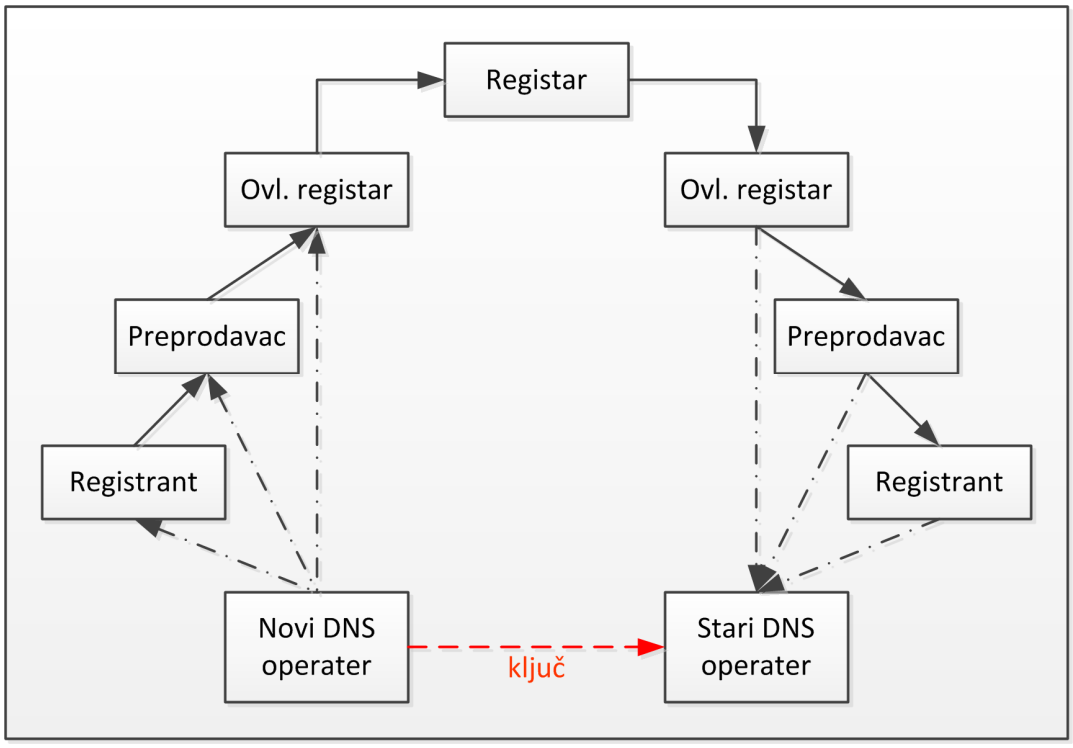
1. Registrant kontaktira stari OR i zahteva svoje autorizacione podatke („auth info“).
2. Registrant kontaktira novi OR i zahteva da u kontaktu sa roditeljskim *.rs* registrom zatraži prenos domena *primer.rs*.
3. Stari OR mora da prihvati zahtev za prenos.
4. Registrant mora da potvrdi ili da zatraži od novog OR da potvrdi, da su svi postojeći DS zapisi i dalje vezani za *primer.rs* kod roditeljskog registra. Dakle, registrant mora da bude siguran da promena OR nije prouzrokovala uklanjanje DS zapisa za *primer.rs* kao neželjenu posledicu prenosa.

6.2 EPP Keyrelay

Trenutno nije definisan standardan način za prenos DNSSEC domena između različitih OR, uz konstantno očuvanje lanca poverenja, koji se može smatrati jednostavnim. Rešenje koje je trenutno u fazi predloga[26] predviđa korišćenje EPP protokola uz uvođenje nove komande, koristeći registar kao posrednika prilikom razmene DNSSEC podataka[27].

Da bi se domen zaštićen DNSSEC-om bezbedno preneo, svaki od dva DNS operatera mora da privremeno uvrsti javni ZSK ključ onog drugog u svoju verziju zone. Novi operater može na bezbedan način da dođe do ZSK starog operatera putem DNS-a. Međutim, ne postoji bezbedan kanal za dostavljanje ZSK novog operatera. Razlog za to je što buduća zona još uvek nije delegirana pa ne postoji ni lanac poverenja kojim bi se izvršila validacija ključa preuzeta iz zone novog operatera. S obzirom na broj DNS operatera u svetu, neizvodljivo je sve njih međusobno bezbedno povezati.

Rešenje koje se predlaže je da DNS operateri razmene ključ putem kanala koji se već koristi za registraciju domena i održavanje registracije: administrativni kanal za komunikaciju sa registrom. Ova interakcija se naziva „*key relay*“: ključ se „prenosi“ slanjem registru. Registar zatim prosleđuje ključe trenutnom ovlašćenom registru za domen, čija je briga da on dođe do starog DNS operatera. Dijagram prenosa je dat na slici 9.

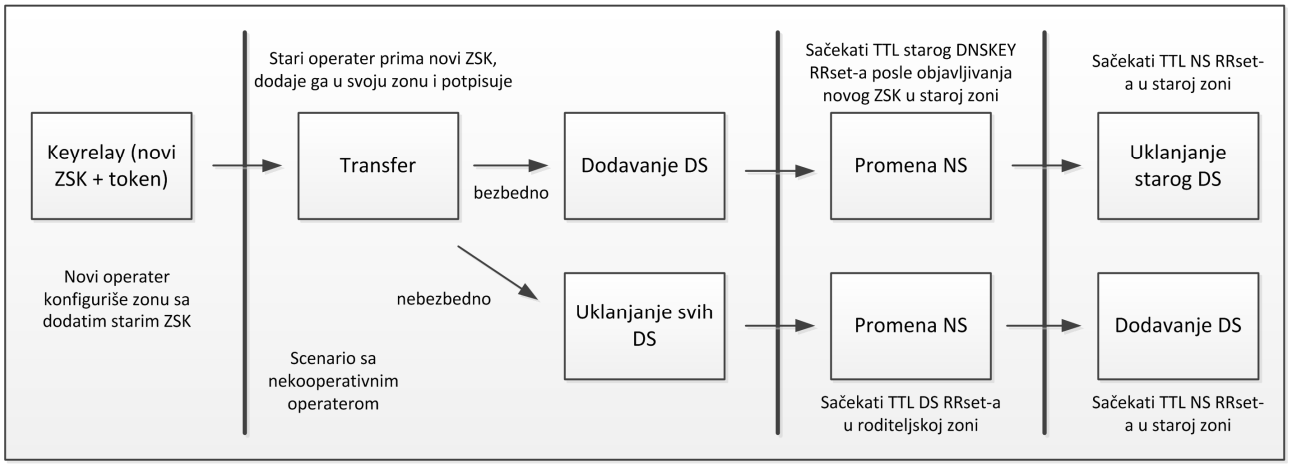


Slika 9. Slanje ZSK starom DNS operateru preko registra

Prednost ovog rešenja je u tome što je u pitanju *stateless* mehanizam, što ga čini skalabilnim, relativno lakim za implementaciju od strane registra i razumljivim za automatizaciju za ovlašćene registre i preprodavce. Takođe, registar ili ovlašćeni registar mogu da verifikuju da li je *key relay* zahtev autorizovan od strane registranta, da bi stari DNS operater automatski mogao da uvrsti ključ u „staru“ zonu. Za ovaj proces nisu važne različite uloge koje mogu ili ne moraju biti prisutne u lancu uloga, tj. ko ima ulogu DNS operatera.

6.2.1 Key relay proces

Na slici 10 je prikazan proces prenosa DNSSEC domena. U procesu nema drugih promena u odnosu na uobičajene korake ovlašćenog registra, osim što ga prethodi prenos ključa sa novog na starog operatera. Novi registar je u stanju da kontroliše kvalitet i brzinu prenosa, kroz podešavanja TTL vremena. Bez obzira da li se administrativna kontrola prenosi sa jednog ovlašćenog registra na drugog, *key relay* se koristi samo kada dođe do promene DNS operatera.



Slika 10. Proces promene DNS operatera

Ukoliko je stari DNS operater kooperativan, prati se bezbedan način prenos. Alternativno, novi registar može uvek da odabere nebezbedan način prenosa i da i dalje zadrži kontrolu nad procesom.

Key relay prenos se sastoji iz dva dela:

1. **Od novog DNS operatera ka registru**
   Dobija se *key relay* zahtev od podređenog aktera (videti sliku 7). Na primer, preprodavac može dobiti key relay zahtev od registranta, koji treba proslediti nadređenom akteru, tj. registru. Svaki akter prati ovaj postupak dok zahtev ne stigne do registra. *Key relay* zahtev mora da prati i autorizacioni token koji obezbeđuje registrant. Putem ovog tokena, registar ili stari DNS operater/ovlašćeni registar mogu da verifikuju da je zahtev odobren od strane registranta.
2. **Od registra ka starom DNS operateru**
   Dobija se *key relay* zahtev od nadređenog aktera, koji se prosleđuje podređenom akteru na strani starog operatera (akter koji je trenutno odgovoran). Svaki akter prati ovaj postupak sve dok zahtev ne stigne do starog DNS operatera, koji dodaje prateći ključ u svoju verziju zone.

Ovaj proces može biti potpuno automatizovan. Komunikacija između ovlašćenih registara i registra se obično obavlja putem EPP poruka, ali ne i kada je reč o ostalim akterima u lancu (DNS operater, preprodavac, registrant). Međutim, što se tiče modela, nije važno koji se protokol koristi za komunikaciju, dok god je najmanje onoliko bezbedan kao onaj koji se koristi za registraciju i održavanje domena. Ovo čini *key relay* koncep široko primenjivim.

Što se tiče registra, proces je vrlo jednostavan. Dobija se key relay zahtev od jednog od ovlašćenih registara. Po prijemu, registar može da verifikuje registrantov autorizacioni token iz *key*

relay zahteva i da pošalje upit u bazu podataka radi pronalaženja trenutnog ovlašćenog registra za traženi domen. *Key relay* zahtev se tada prosleđuje tom ovlašćenom registru. Nema drugih aktivnosti i nema nikakvih izmena u bazi podataka niti ima potrebe za praćenjem nekog stanja ili tajmera. Zadatak registra je samo da olakša komunikaciju između ovlašćenih registara.

6.2.2 EPP key relay komanda

EPP *keyrelay* komanda sadrži sledeće informacije:

- Naziv domena
- Javni ključ koji se prenosi
- Autorizacioni token trenutnog registranta

Opciono sadrži i:

- Koliko dugo bi ključ trebalo da ostane u staroj zoni
- Ovlašćeni registar koji šalje *key relay* zahtev

Registar prenosi nepromenjene informacije smeštajući poruku u *EPP message queue* trenutnog ovlašćenog registra za navedeni domen.

EPP *key relay* je slična *transfer* komandi, ali služi pokretanju promene DNS operatera, ne uvek i ovlašćenog registra. Kao i *transfer* komanda, može biti poslata od strane bilo kog ovlašćenog registra, ali njen rezultat nije izmena bilo kog objekta u bazi podataka. Dolazi do pokretanja postupka, obično za nekog drugog aktera nego što je ovlašćeni registar koji je poslao komandu. Autorizacioni token služi da spreči zloupotrebe ove komande.

EPP *key relay* predstavlja ne samo novu komandu već i novu kategoriju komandi. Pošto se ne može smestiti u postojeće kategorije, najbolje se opisuje kao „komunikaciona komanda“. Takođe, ova komanda sadrži potencijal za korišćenje u drugim procesima u budućnosti u kojima bi se zahtevala razmena ključeva.

7. Propisi i pravila

7.1 DNSSEC Izjave o praksi i politici

Da bi se obezbedio način za zainteresovane strane da provere snagu i bezbednost DNSSEC lanca poverenja, objavljuje se DNSSEC Izjava o praksi (DNSSEC Practice Statements – DPS). Ovaj dokument se sastoji od izjava koje opisuju kritične bezbednosne kontrole i procedure. DPS najčešće sadrži i DNSSEC Politike (DNSSEC Policies – DPs), opisujući na koji način ih ispunjava. Uobičajeno je da se objavljuje jedinstven dokument, „DNSSEC Policy and Practice Statement“. Detaljni opis se može naći u dokumentu[1] RFC 6841.

DP i DPS nisu namenjeni prvenstveno korisnicima koji se oslanjaju na potpisane DNS odgovore već drugim zainteresovanim stranama u DNS infrastrukturi, kao što su regulatorne vlasti.

7.1.1 Skup odredbi

Skup odredbi je skup zahteva DNSSEC Politike ili Izjava o praksi koje koriste pristup opisan u [1]. Predefinisani nacrt sadržine skupa odredbi sastoji se od osam glavnih delova i podkomponenti:

1. UVOD

Ova komponenta identifikuje i uvodi skup odredbi i ukazuje na tipove entiteta i primene za koje je dokument namenjen. Sastoji se od:

- 1.1. Pregled
- 1.2. Naziv dokumenta i identifikator
- 1.3. Zajednica i primenjivost
- 1.4. Administracija nad specifikacijom
  - 1.4.1. Organizacija koja vodi administraciju specifikacije
  - 1.4.2. Kontakt informacije
  - 1.4.3. Procedure za promenu specifikacije

2. OBJAVLJIVANJE I SKLADIŠTA

Ova komponenta opisuje zahteve prema entitetu za objavljivanje informacija vezano za prakse, javne ključeve, trenutni status takvih ključeva zajedno sa detaljima koji se odnose na skladišta u kojima se informacije drže. Sastoji se od:

- 2.1. Skladišta
- 2.2. Objavljivanje javnih ključeva

3. OPERATIVNI ZAHTEVI

Ova komponenta opisuje operativne zahteve za rukovođenje DNSSEC potpisanom zonom. Sastoji se od:

- 3.1. Značenje naziva domena

3.2. Identifikacija i autentifikacija administratora zone potomka
3.3. Upis „Delegation signer“ (DS) zapisa resursa
3.4. Metoda za dokazivanje posedovanja privatnog ključa
3.5. Uklanjanje DS zapisa resursa
  3.5.1. Ko može da zahteva uklanjanje
  3.5.2. Procedura za zahtev za uklanjanje
  3.5.3. Hitan zahtev za uklanjanje

4. POSTROJENJE, UPRAVLJANJE I OPERATIVNE KONTROLE

Ova komponenta opisuje netehničke bezbednosne kontrole (fizičke, proceduralne i vezane za osoblje) koje entitet koristi radi bezbednog izvršavanja DNSSEC funkcija. Ovo obuhvata fizički pristup, upravljanje ključevima, oporavak u slučaju nesreće, revizije i arhiviranje. Ove netehničke kontrole su kritične za poverenje u DNSSEC potpise jer manjak bezbednosti može kompromitovati rad sa DNSSEC-om. Sastoji se od:

4.1. Fizičke kontrole
  4.1.1. Lokacija i konstrukcija
  4.1.2. Fizički pristup
  4.1.3. Napajanje i klimatizacija
  4.1.4. Izloženost vodi
  4.1.5. Zaštita i prevencija od požara
  4.1.6. Skladištenje medija
  4.1.7. Uklanjanje otpada
  4.1.8. Sigurnosna kopija van postrojenja
4.2. Proceduralne kontrole
  4.2.1. Funkcije od poverenja
  4.2.2. Broj osoba neophodnih po zadatku
  4.2.3. Identifikacija i autentifikacija za svaku funkciju
  4.2.4. Zadaci koji zahtevaju podelu dužnosti
4.3. Kontrola osoblja
  4.3.1. Zahtevi po pitanju kvalifikacija, iskustva i podobnosti
  4.3.2. Procedure za proveru prošlosti
  4.3.3. Zahtevi po pitanju obuke
  4.3.4. Učestalost i redosled rotacije poslova
  4.3.5. Sankcije za neautorizovane postupke
  4.3.6. Zahtevi za osoblje po ugovoru
  4.3.7. Dokumentacija koja se obezbeđuje osoblju
4.4. Procedure za beleženje revizija
  4.4.1. Vrste događaja koji se beleže
  4.4.2. Učestalost obrade dnevnika
  4.4.3. Period čuvanja informacija u dnevniku revizija
  4.4.4. Zaštita dnevnika revizija
  4.4.5. Procedure za pravljenje rezervne kopije dnevnika revizija
  4.4.6. Sistem prikupljanja revizija
  4.4.7. Procena ranjivosti
4.5. Oporavak u slučaju kompromitacije i nesreće
  4.5.1. Procedure za postupanje u slučaju incidenta ili kompromitacije
  4.5.2. Oštećenje računarskih resursa, softvera i/ili podataka
  4.5.3. Procedure u slučaju kompromitacije privatnog ključa entiteta
  4.5.4. Kontinuitet poslovanja i mogućnosti IT oporavka

4.6. Okončanje rada entiteta

5. TEHNIČKE BEZBEDNOSNE KONTROLE

Ova komponenta određuje bezbednosne mere preduzete radi zaštite kriptografskih ključeva i podataka za aktiviranje (npr. PIN kodova, lozinki ili podeljenih ključeva) relevantnih za rad DNSSEC-a. Bezbedno upravljanje ključevima je kritično da bi se obezbedilo da svi tajni i privatni ključevi i podaci za aktiviranje budu zaštićeni i korišćeni samo od strane autorizovanog osoblja.

5.1. Generisanje i instaliranje para ključeva
  5.1.1. Generisanje para ključeva
  5.1.2. Isporuka javnog ključa
  5.1.3. Generisanje i provera kvaliteta parametara javnog ključa
  5.1.4. Namene upotrebe ključa
5.2. Zaštita privatnog ključa i tehnička kontrola kriptografskog modula
  5.2.1. Standardi i kontrole kriptografskog modula
  5.2.2. Kontrola nad privatnim ključem od strane više osoba („m of n“)
  5.2.3. Korišćenje treće strane za čuvanje privatnog ključa („key escrow“)
  5.2.4. Rezervna kopija privatnog ključa
  5.2.5. Skladištenje privatnog ključa na kriptografskom modulu
  5.2.6. Arhiviranje privatnog ključa
  5.2.7. Prenos privatnog ključa u i iz kriptografskog modula
  5.2.8. Metoda za aktiviranje privatnog ključa
  5.2.9. Metoda za deaktiviranje privatnog ključa
  5.2.10. Metoda za uništavanje privatnog ključa
5.3. Ostali aspekti upravljanja parom ključeva
5.4. Podaci za aktivaciju
  5.4.1. Generisanje i instalacija podataka o aktivaciji
  5.4.2. Zaštita podataka o aktivaciji
  5.4.3. Ostali aspekti podataka o aktivaciji
5.5. Kontrole računarske bezbednosti
5.6. Kontrole mrežne bezbednosti
5.7. Postavljanje vremenskih žigova
5.8. Tehničke kontrole životnih ciklusa

6. POTPISIVANJE ZONE

Ova komponenta pokriva sve aspekte potpisivanja zone, uključujući kriptografske specifikacije vezane za ključeve za potpisivanje, plan potpisivanja, metodologiju za prelazak između ključeva i samo potpisivanje zone. Zone potomka kao i druge strane mogu zavisiti od podataka navedenih u ovom delu da bi razumeli podatke koji se očekuju u potpisanoj zoni i odredili sopstveno ponašanje. Sastoji se od:

6.1. Dužine ključeva, tipovi ključeva i algoritmi
6.2. Autentifikovano poricanje postojanja
6.3. Format potpisa
6.4. Prelazak između ključeva
6.5. Životni vek potpisa i učestalost ponovnog potpisivanja
6.6. Verifikacija zapisa resursa
6.7. Vreme preživljavanja („time-to-live“) zapisa resursa

7. PROVERA USAGLAŠENOSTI

Da bi se dokazala usaglašenost sa Politikom ili navodima u Izjavi o praksi, provera usaglašenosti može biti sprovedena. Ova komponenta kako provera treba biti sprovedena kod operatera zone kao i kod drugih entiteta koji su uključeni. Sastoji se od:

7.1. Učestalost provere usaglašenosti entiteta
7.2. Identitet / kvalifikacije lica koje vrši proveru
7.3. Povezanost lica koje vrši proveru sa stranom koja se proverava
7.4. Oblasti pokrivene proverom
7.5. Preduzeti postupci kao rezultat nedostatka
7.6. Saopštavanje rezultata

8. PRAVNA PITANJA

Uvođenje DNSSEC-a u zonu može imati pravne implikacije. Stoga, može biti svrsishodno objaviti pravni status veze stvorene u DNSSEC digitalnim potpisima i naglasiti sva ograničenja u odgovornosti koja se ističu od strane rukovodioca registra. Najčešće, DPS Izjava nije ugovor ili deo ugovora; umesto toga, postavljena je tako da se njegovi uslovi primenjuju na strane putem posebnih dokumenata, kao što su dogovori sa ovlašćenim registrima i registrantima. U drugim slučajevima, njena sadržina može biti deo ugovora između strana (direktno ili putem drugih dogovora). U tom slučaju treba koristiti pravnu ekspertizu prilikom sastavljanja delova dokumenata koji mogu imati ugovorne implikacije.

Deo o pravnim pitanjima treba i da ukaže pod kakvom nadležnošću registar radi i da obezbedi reference ka bilo kakvim povezanim dogovorima koji su na snazi. Može biti svrsishodno i ukazati na implikacije koje se odnose na zaštitu privatnih informacija koje mogu biti iskorišćene za otkrivanje identiteta.

7.2 Okvir za proveru DNSSEC infrastrukture

7.2.1 Uvod

Dokument: „*DNSSEC Infrastructure Audit Framework*“[47]

Ovaj dokument opisuje okvir pod kojim bi trebalo sprovesti proveru DNSSEC aspekata registra i rada autoritativnih DNS servera. Provera predstavlja proces strukturalnog pregleda DNSSEC infrastrukture. Svrha ovog procesa je procena nivoa poverenja u sistem. Ovo se postiže pregledom implementacije i rada sistemskih kontrola i da li su u skladu sa odgovarajućim zahtevima politike ili, u odsustvu formalnih politika, trenutno najboljim industrijskim praksama.

Ključni dokument za obavljanje provere je spisak za proveru. On obezbeđuje strukturu zadatka i pruža poverenje da je opseg provere adekvatno pokriven. Ovaj dokument predstavlja generički spisak za proveru za proveru DNSSEC-a i pruža okvir koji pomaže kontrolorima da obave proveru. Međutim, ovde predstavljeni postupci ne spadaju ni u kakve formalne standarde za pregled i namenjeni su za usmeravanje kako bi provera mogla da izgleda.

Dokument ne predstavlja standard niti najbolju praksu i nije pogodan za bilo koji oblik formalne sertifikacije.

7.2.1.1 Metodologija

Dokument je predviđen da bude primenjiv, ali ne ograničen samo na registre domena najvišeg nivoa i rad njihovih servera naziva. Fokus okvira dokumenta je na kontrolama koje služe za očuvanje integriteta i dostupnosti DNSSEC povezanih aspekata DNS infrastruktire. Kao posledica, dokument ne pokriva sve aspekte rada DNS registra, ali se bavi onim aspektima koji utiču na stabilnost ili bezbednost DNSSEC implementacije.

Metodologija je bazirana na ISO/IEC 27008:2011(E) tehničkom izveštaju[45]. Opseg je uglavnom baziran na RFC 6841[1]. Ostale smernice za implementaciju se mogu naći u dokumentu „Secure Domain Name System (DNS) Deployment Guide“ izdatom od strane NIST-a[46].

Za vreme provere, može se utvrditi da kontrole koje bi MORALE (*MUST*) ili TREBALE (*SHOULD*) da budu implementirane, to nisu. Standardno pitanje koje bi se moralo postaviti kao prateće je da li je došlo do odluke uprave, preferirano da bude dokumentovana, kao osnova za odluku da se ne implementira. Neke provere zahtevaju verifikaciju da li su kontrole u skladu sa očekivanom profesionalnom praksom. Šta spada u ova očekivanja je predmet perspektive kontrolora.

7.2.1.2 Priprema

Kontrolori bi trebalo da se pripreme za proveru putem opšteg razumevanja organizacije, njenog rada, arhitekture sistema i kontrola koje treba proveriti.

Sledeće komponente su obično deo infrastrukture registra koji poseduje aktivan DNSSEC:

- Registracioni portal
- Back-end baza podataka
- DNSSEC potpisnik
- DNS serveri
- Interfejs za pregled javnih podataka o registraciji (WHOIS)
- Roditeljski portal (opciono)

Kontrolori bi trebalo da imaju uvid u dokumentaciju visokog nivoa ili u opšti opis implementacije i dostupnosti ovih komponenti pre nego što se započne sa proverom. Takođe, važno je prikupiti preliminarne podatke iz dokumenata koji su već dostupni. Oni obuhvataju:

- Prethodne provere
- DNSSEC izjave o politici i praksi (DPS)
- Druge izjave o politici i praksi
- Interne operativne dokumente

Na kraju, treba identifikovati ključno osoblje:

- *Senior Management* (SM)
- *Security Officer* (SO)
- *Operations Management* (OM)
- *System Administrator* (SA)

7.2.2 Dokumentacija

Javna dokumentacija

DNSSEC izjave o politici i praksi
Zadatak: Steći razumevanje i transparentnost izbora i procedura za sve aktere.
Kontrola: Učiniti DPS dokumentaciju javno dostupnom preko Interneta.

Objavljivanje pouzdanog polazišta
Zadatak: Omogućiti uspostavljanje poverenja *in-band* kao i *out-of-band* način.
Kontrola: Objaviti informacije o javnim ključevima na *out-of-band* način da bi se omogućilo uspostavljanje *trust anchor*-a za zonu.

Interna dokumentacija

Poslovne i tehničke procedure
Zadatak: Omogućiti neprekidnost poslovanja deljenje znanja između zaposlenih.
Kontrola: Učiniti poslovne i tehničke procedure dostupnim DNS operaterima.

Procedure u slučaju nužde
Zadatak: Omogućiti brz oporavak posle otkrivene kompromitacije ili nesreće, na primer posle gubitka privatnog ključa.
Kontrola: Posedovati odredbe koje treba pratiti da bi se izvršio oporavak posle kompromitacije ili nesreće.

Prestanak rada

Onemogućavanje DNSSEC-a
Zadatak: Omogućiti stranama koje se oslanjaju na entitet da reaguju i pronađu moguće alternative i obezbediti nesmetan prelazak na alternativne entitete.
Kontrola: Unapred najaviti događaj prestanka rada sa DNSSEC-om.

7.2.3 Postrojenje i uprava

Fizičke kontrole

Geografska raznovrsnost
Zadatak: Umanjiti uticaj prirodne ili IT nesreće.
Kontrola: Obezbediti da svi DNS serveri ne budu na istoj fizičkoj lokaciji.

Arhitektura postrojenja
Zadatak: Zgrada u kojoj su smešteni registar i DNS serveri bi trebalo da bude adekvatno zaštićena od upada.
Kontrola: Koristiti sisteme za prevenciju i detekciju upada.

Neprekidnost napajanja
Zadatak: Omogućiti kontinuitet rada u slučaju incidenta sa napajanjem.
Kontrola: Obezbediti rezervno napajanje za slučaj nestanka napajanja.

Sprečavanje vatre i drugih nesreća
Zadatak: Omogućiti kontinuitet rada u slučaju incidenta sa požarom.
Kontrola: Posedovati sisteme za zaštitu od požara.

Proceduralne kontrole

Kontrola pristupa
Zadatak: Sprečiti upad u prostor gde su smešteni serveri kritični za rad.
Kontrola: Kontrolisati pristup prostoru gde su smešteni DNS serveri i potpisnici.

Poverljive uloge
Zadatak: Obezbediti ograničen pristup kritičnim operacijama.
Kontrola: Identifikovati više poverljivih uloga za određene operacije.

Razdvajanje dužnosti
Zadatak: Sprečiti neautorizovane, lažne ili neželjene postupke od strane pojedinaca.
Kontrola: Zahtevati prisustvo više od jedne osobe za obavljanje kritičnih operacija.

Personalne kontrole

Zahtevi prema osoblju
Zadatak: Obezbediti da je osoblje osposobljeno za obavljanje poslova za koje je odgovorno kao i njihovu pouzdanost.
Kontrola: Verifikovati kvalifikacije i pouzdanost kandidata.

Sankcije
Zadatak: Obezbediti pouzdanost osoblja i sprečiti štete po imidž entiteta.
Kontrola: Utvrditi sankcije za neovlašćene postupke.

7.2.4 Sistem za registraciju domena

Značenje domena

Zahtevi prema nazivu domena
Zadatak: Sprečiti operativne i pravne probleme koji mogu nastati usled semantičke ili sintaksne sadržine naziva domena.
Kontrola: Odbacivati nazive domena kojima se unose pravni, operativni ili tehnički problemi.

Zahtevi prema delegiranju
Zadatak: Obezbediti pouzdanu i stabilnu konzistentnost DNS-a za entitet i njegove tačke delegiranja, da bi se umanjila krhkost DNS razrešavanja.
Kontrola: Obaviti proveru konzistentnosti nad delegiranjima.

Identifikacija i autentifikacija ovlašćenog registra
Zadatak: Održavati poverenje odgovarajućim delegiranjem i sprečavanjem otimanja.
Kontrola: Autentifikovati podnosioce zahteva za registraciju domena i autorizovati transakcije.

Identifikacija i autentifikacija upravljača zone potomka

Ovi zadaci se smatraju odgovornošću ovlašćenih registara. U slučaju da entitet prihvata registraciju domena direktno od registranata, mogu se koristiti kontrole iz dela "Identifikacija i autentifikacija ovlašćenog registra".

Registracija DS zapisa resursa

Prihvatanje i čuvanje

Zadatak: Održavati konzistentnost i sprečiti izmenu materijala sa javnim ključem zone potomka za vreme trajanja njegovog životnog veka.

Kontrola: Prihvatati DNSSEC zapise na takav način da se može stvoriti ili održati lanac poverenja sa zonom potomka – održavati lanac starateljstva.

Metoda za dokazivanja posedovanja privatnog ključa

Ovi zadaci se smatraju odgovornošću ovlašćenih registara.

Uklanjanje DS zapisa resursa

Procedura za uklanjanje DS RRset-a

Zadatak: Sprečiti degradaciju bezbednosti u delegiranju.

Kontrola: Zahtevati potvrdu za prelazak zone u nebezbedno stanje od registranta ili treće strane ovlašćene od strane registranta.

Uklanjanje ili prenos domena

Procedura za uklanjanje ili prenos domena

Zadatak: Sprečiti neautorizovano ili neželjeno promene u nazivu domena kao i otimanje domena.

Kontrola: Postojanje mehanizama za sprečavanje neautorizovanih ili slučajnih promena u nazivu domena.

7.2.5 DNS serveri

Bezbedne DNS instance

Zadatak: Sprečiti i otkriti neželjeni pristup mašinama koje su kritične za rad entiteta.

Kontrola: Obezbediti sisteme koji su povezani sa DNS-om.

Bezbedan DNS softver

Zadatak: Minimizovati ranjivosti i uticaj iskorišćavanja ranjivosti u DNS softveru.

Kontrola: Održavati modernu i ažurnu implementaciju sa razumljivom konfiguracijom.

Raznovrsnost u sistemima

Zadatak: Umanjiti uticaj softverskih i hardverskih grešaka.

Kontrola: Koristiti raznovrstan hardver i softver za sisteme koji se koriste kao DNS serveri.

DNSSEC obrada
Zadatak: Obezbediti pouzdane DNSSEC odgovore za validatore.
Kontrola: Autoritativni DNS serveri sa omogućenim DNSSEC-om.

Replikacija zone

***In-band* replikacija**
Zadatak: Omogućiti (inkrementalnu) replikaciju zona između DNS servera.
Kontrola: Izvršiti transfer zone entiteta ka različitim serverima koristeći DNS.

***Out-of-band* replikacija**
Zadatak: Omogućiti replikaciju zone u slučaju prekida rada mreže ili u slučaju onemogućenja transfera zone.
Kontrola: Posedovati *out-of-band* metode transfera zone entiteta ka (sekundarnim) DNS serverima.

7.2.6 Upravljanje parovima ključeva

Generisanje i instaliranje para ključeva

Generisanje para ključeva
Zadatak: Generisati bezbedne i pouzdane parove ključeva za obavljanje DNSSEC operacija.
Kontrola: Za generisanje ključeva koristiti sisteme koji pružaju transparentnost i koji su u stanju da generišu kvalitetne slučajne podatke.

Isporuka javnog ključa
Zadatak: Obezbediti da javni ključ koji je isporučen zoni entiteta bude autentičan.
Kontrola: Verifikovati integritet javnog ključa za vreme isporuke iz sistema za generisanje ključeva do zone entiteta.

Svrhe korišćenja ključa
Zadatak: Umanjiti štetu u slučaju kompromitacije ključeva.
Kontrola: Koristiti različite ključeve za različite zadatke.

Zaštita privatnog ključa i tehničke kontrole kriptografskog modula

Čuvanje privatnog ključa
Zadatak: Sprečiti neželjeno otkrivanje i/ili izmenu privatnih ključeva.
Kontrola: Čuvati privatne ključeve na bezbedan način.

Rezervna kopija privatnog ključa
Zadatak: Obezbediti način za oporavak od gubitka privatnog ključa.
Kontrola: Praviti rezervne kopije privatnih ključeva na različitom sistemu.

Aktivacija privatnog ključa
Zadatak: Sprečiti neželjeno korišćenje privatnog ključa.
Kontrola: Koristiti mehanizme za aktiviranje na privatnom ključu.

Deaktiviranje privatnog ključa
Zadatak: Sprečiti neželjeno korišćenje privatnog ključa.
Kontrola: Koristiti mehanizme za deaktiviranje na privatnom ključu.

Podaci za aktivaciju

Generisanje i instalacija podataka za aktivaciju
Zadatak: Generisati bezbedne i pouzdane vrednosti aktivacionih podataka.
Kontrola: Za generisanje aktivacionih podataka koristiti sisteme koji su u stanju da generišu podatke sa nepredvidivim vrednostima.

Zaštita podataka za aktivaciju
Zadatak: Sprečiti neželjeno izlaganje i/ili izmenu privatnih ključeva.
Kontrola: Implementirati m-od-n kontrole.

Upravljanje incidentima sa ključevima

Kompromitacija privatnog ključa
Zadatak: Omogućiti brz oporavak posle otkrivanja kompromitacije ili gubitka ključa
Kontrola: Obaviti prelazak između ključeva u slučaju nužde.

7.2.7 Tehničke bezbednosne kontrole

Mrežna bezbednost

Firewall
Zadatak: Onemogućiti mrežni pristup portovima različitim od onih koji su neophodni za rad DNS-a.
Kontrola: Uspostaviti različita *firewall* pravila za DNS servere.

Inverzno razrešavanje naziva
Zadatak: Odrediti naziv domena koji je povezan sa DNS-om entiteta i drugim uslugama.
Kontrola: Podržavati inverzne DNS upite.

Raznovrsnost u mrežnim lokacijama
Zadatak: Umanjiti rizik od nedostupnosti u slučaju kvara na mreži.
Kontrola: Lociranje DNS servera na različitim, nepovezanim mrežnim segmentima.

Vremenski žigovi
Zadatak: Održavati sinhronizovane kompjuterske časovnike.
Kontrola: Koristiti alate za sinhronizaciju časovnika.

Tehničke kontrole životnog ciklusa

Nema odredbi za potrebe ovog okvira za pregled.

7.2.8 Potpisivanje zone

Dužine ključeva, tipovi ključeva i algoritmi

Šema za potpisivanje

Zadatak: Uspostaviti operativnu fleksibilnost, kontinuitet i transparentnost održavajući poverenje u DNS.

Kontrola: Implementirati šemu za potpisivanje.

Kriptografski parametri

Zadatak: Potpisi mogu biti korišćeni za validaciju integriteta i autentičnosti DNS zapisa resursa.

Kontrola: Koristiti dovoljno jake dužine ključeva i algoritama za njihovu namenu (DNSSEC validacija) i njihov efektivan period.

Autentifikovano poricanje postojanja

NSEC ili NSEC3

Zadatak: Omogućiti validaciju nepostojećih podataka.

Kontrola: Implementirati NSEC ili NSEC3.

Format potpisa

Zadatak: Obezbediti konzistentnost između potpisa i ključeva.

Kontrola: Ovo se implicira preko izabranog algoritma za ključeve i šeme za potpisivanje.

Prelazak između ključeva

Prelazak između KSK

Zadatak: Praktikovati operativnu rutinu da bi se održao lanac poverenja.

Kontrola: Posedovati odredbe za obavljanje prelaska između KSK ključeva.

Prelazak između ZSK

Zadatak: Praktikovati operativnu rutinu da bi se održala autentičnost i integritet RRset-ova.

Kontrola: Posedovati odredbe za obavljanje prelaska između ZSK ključeva.

Prelazak između algoritama

Zadatak: Održavati poverenje u kriptografske parametre korišćene u DNSSEC-u.

Kontrola: Posedovati odredbe za obavljanje prelaska između algoritama.

Implementacija automatizovane procedure

Zadatak: Minimizovati greške prilikom potpisivanja zone.

Kontrola: Automatizovati ili koristiti skripte za obavljanje gore opisanih funkcija prilikom potpisivanja zone.

Životni vek potpisa i učestalost ponovnog potpisivanja

Učestalost ponovnog potpisivanja
Zadatak: Obezbediti sveže digitalne potpise.
Kontrola: Često ponovno potpisivanje.

***Refresh* period**
Zadatak: Obezbediti razumno dug vremenski period za rešavanje operativnih problema bez brige o isteku potpisa.
Kontrola: Osvežiti potpise dovoljno dugo pre nego što isteknu.

Životni vek potpisa
Zadatak: Ograničiti izlaganje u slučaju da ključevi zone potomka budu kompromitovani.
Kontrola: Ograničiti rizik *replay* napada.

Verifikacija zapisa resursa

DNSSEC provera
Zadatak: Proveriti da li su potpisi ispravni, DNSKEY nepromenjen i da sadržaj nepotpisane zone nije menjan.
Kontrola: Pregledati sistem za potpisivanje.

7.2.9 Sadržaj zone

Secure entry point i ključevi za potpisivanje zone

In-band objavljivanje s*ecure entry point*-a
Zadatak: Omogućiti izgradnju lanca poverenja prema određenoj zoni.
Kontrola: Objaviti informacije o javnim ključevima u DNS-u da bi korisnici mogli da izgrade lanac poverenja do zone entiteta.

Standby ključ za secure entry point
Zadatak: Omogućiti kontinuitet rada u slučaju kritičnih problema sa DNSSEC ključevima.
Kontrola: Objaviti javni i čuvati tajni ključ za slučaj nužde da bi se omogućio brz oporavak u slučaju kompromitacije.

Povezanost s*ecure entry point*-a sa potpisima podataka
Zadatak: Omogućiti DNSSEC validaciju za određenu zonu.
Kontrola: Objaviti javni ključ u DNS-u da bi korisnici mogli da validiraju zonu entiteta.

Interoperabilnost DS-a
Zadatak: Omogućiti interoperabilnost sa akterima u lancu poverenja, kao što su razrešitelji koji obavljaju validaciju.
Kontrola: Objaviti najmanje jedan obavezan algoritam za DS sažetak.

TTL zapisa resursa

Minimalno TTL vreme zone

Zadatak: Sprečiti operativne i upravljačke probleme u smislu perioda važenja potpisa.

Kontrola: Koristiti minimalne TTL vrednosti za zonu koje su dovoljno velike za dobavljanje i verifikovanje svi neophodnih zapisa resursa u lancu poverenja.

Maksimalno TTL vreme

Zadatak: Omogućiti razumno brzu propagaciju ažuriranja zone.

Kontrola: Koristiti maksimalne TTL vrednosti za zonu koje omogućavaju razumno vreme tokom kojeg razrešitelj čuva podatke u kešu.

Tajmer isteka SOA

Zadatak: Podesiti DNSSEC server kao neautoritativan pre nego što mogući DNSSEC problemi postanu vidljivi.

Kontrola: Koristiti SOA *expiration* tajmer koji omogućava da problemi sa transferima sa master servera budu primećeni pre nego što potpisi isteknu.

7.2.10 Logovanje

Pregled procedura za logovanje

Tipovi logovanih događaja

Zadatak: Omogućiti otkrivanje ponašanja koje odstupa od uobičajenog i pronalaženje uzroka u slučaju incidenta.

Kontrola: Logovati sve relevantne radnje i pokušaje pristupa.

Zadržavanje logova

Zadatak: Omogućiti pronalaženje uzroka u slučaju incidenta koji nije odmah otkriven.

Kontrola: Arhivirati logove određeni vremenski period.

Zaštita logova

Zadatak: Obezbediti poverljivost, integritet i dostupnost logovanih događaja.

Kontrola: Zaštititi logove od gubitka, manipulacije i neautorizovanog pregleda.

Korišćenje logova

Zadatak: Blagovremeno otkriti incidente i druge vanredne događaje.

Kontrola: Pregled logova.

8. Primena DNSSEC-a – DANE protokol

Autentifikacija imenovanih entiteta na osnovu DNS-a (*DNS-Based Authentication of Named Entities* - DANE) predstavlja protokol[42] kojim se X.509 digitalni sertifikati mogu vezati za DNS imena uz korišćenje DNSSEC-a. U smislu TLS komunikacije, uloga DNSSEC-a bi bila da omogući operaterima domena da klijentima pruže pouzdanu informaciju o tome koje bi sertifikate trebalo prihvatiti kao validne za traženi domen[43].

DANE protokol omogućava operateru domena da postavi određena ograničenja u smislu verifikacije sertifikata za traženi domen. Predviđeno je postoje tri različita scenarija upotrebe tj. slučajeva korišćenja:

1) **Ograničenja CA (*CA Constraints*)**: Klijenti bi trebalo da prihvate sertifikate koje je izdalo tačno određeno CA telo.
2) **Ograničenja sertifikata (*Service Certificate Constraints*)**: Klijenti bi trebalo da prihvate tačno određeni sertifikat.
3) **Navođenje pouzdanog polazišta (*Trust anchor assertion*)**: Klijenti bi trebalo da koriste pouzdano polazište koje obezbeđuje operater domena.

U slučajevima korišćenja **ograničenja CA** i **ograničenja sertifikata**, glavni zadatak je zaštita od zloupotrebe sertifikata, tj. njihovog izdavanja od strane CA strani koja ne predstavlja domen za koji se izdaje. Do ovoga može doći od strane zlonamernih, kompromitovanih ili prevarenih sertifikacionih tela. Zloupotrebu je najčešće teško otkriti, zbog nemogućnosti da se automatski odredi da li određeno CA ima pravo da izdaje sertifikate za traženi domen. Kako operateri domena znaju koje sertifikaciono telo je nadležno da izdaje sertifikate za domene pod njihovom kontrolom kao i tačne sertifikate koji su njima izdati, korišćenjem DANE protokola se ove informacije mogu bezbedno saopštiti klijentskoj strani.

U slučajevima korišćenja **navođenja pouzdanog polazišta**, operaterima domena se omogućava da klijentima pruže informacije o novom pouzdanom polazištu koje bi trebalo koristiti za proveru izdatih sertifikata za te domene. Iako je neuobičajeno da sam domen pruža podatke o pouzdanom polazištu koje treba koristiti za proveru tog istog domena, DANE rešava ovaj problem kroz ograničavanje obima autoriteta koje takvo pouzdano polazište poseduje i proverom tog obima preko DNSSEC-a. Obim se uvek svodi na samo jedan domen, tako da se i u slučaju zloupotrebe putem podmetanja lažnog pouzdanog polazišta, može lažirati samo jedan domen. Uz upotrebu DNSSEC-a, kojim se mora potpisati informacija o pouzdanom polazištu, može se tačno utvrditi da li strana koja pruža informaciju o pouzdanom polazištu zaista predstavlja domen koji se proverava. Kada je reč o pouzdanim polazištima, velika prednost oslanjanja na DNSSEC je i u mogućnosti da se na klijentskoj strani definiše samo jedno – DNS *root*.

8.1 TLSA zapis resursa

DANE protokol uvodi novi zapis resursa, TLSA, u kojem se opisuje koji su sertifikati povezani sa određenim domenom. Sastoji se od četiri polja:

- ***Usage***: Namena zapisa, npr. ograničenje sertifikata.
- ***Selector***: Određuje koji deo sertifikata se proverava, npr. javni ključ.
- ***Matching***: Način na koji se proverava sertifikat, direktnim upoređivanjem ili upoređivanjem sažetaka odabranog sadržaja.
- ***Certificate for Association***: Konkretni podaci na osnovu kojih se proverava sertifikat.

Primer jednog TLSA zapisa, u slučaju korišćenja ograničenja CA (u prefiksu domena su port i transportni protokol koje treba koristiti):

```
_443._tcp.www.example.com. IN TLSA (
0 0 1 d2abde240d7cd3ee6b4b28c54df034b9
      7983a1d16e8a410e4561cb106618e971 )
```

8.2 Izazovi i napomene

- Ograničavajući faktor za DANE protokol predstavlja rasprostranjenost DNSSEC-a na strani klijenata. Veliki broj DNS API-ja koje se koriste u aplikacijama ne pružaju informacije o DNSSEC statusu primljenih odgovora na upite.
- Upotreba DNSSEC-a sa TLS-om može dovesti do kašnjenja u TLS vezi, jer klijent uz TLS *handshake* i proveru sertifikata mora da čeka i na validaciju DNSSEC lanca. Predloženi mehanizam za prevazilaženje ovog kašnjenja je obezbeđivanje DNSSEC zapisa unapred. Njihovom serijalizacijom i slanjem ovih serijalizovanih podataka za vreme TLS *handshake*-a, klijent ne bi morao da čeka na proveru DNSSEC lanca poverenja. Ovo rešenje je trenutno u fazi nacrta[40].
- DNS operateri uz DANE protokol dobijaju ulogu koju danas imaju sertifikaciona tela. Samim tim, DNS operateri nasleđuju mnoge bezbednosne probleme sa kojima se sertifikaciona tela suočavaju.
- U slučaju da DNS operater nije istovremeno i entitet koji je ovlašćen da upravlja sadržinom zone, ne postoje garancije da ono je što je objavljeno u zoni autorizovano od strane vlasnika zone. Ovim DNS operater kao treća strana postaje bezbednosno slaba tačka između klijenta i vlasnika zone. U slučaju da DNS operater počne da pruža lažne DANE podatke usled kompromitacije ili zlonamernih razloga, klijent nema načina da takve podatke razlikuje od ispravnih.
- Različite implikacije korišćenja DANE protokola su opisane u posebnom RFC dokumentu[41].

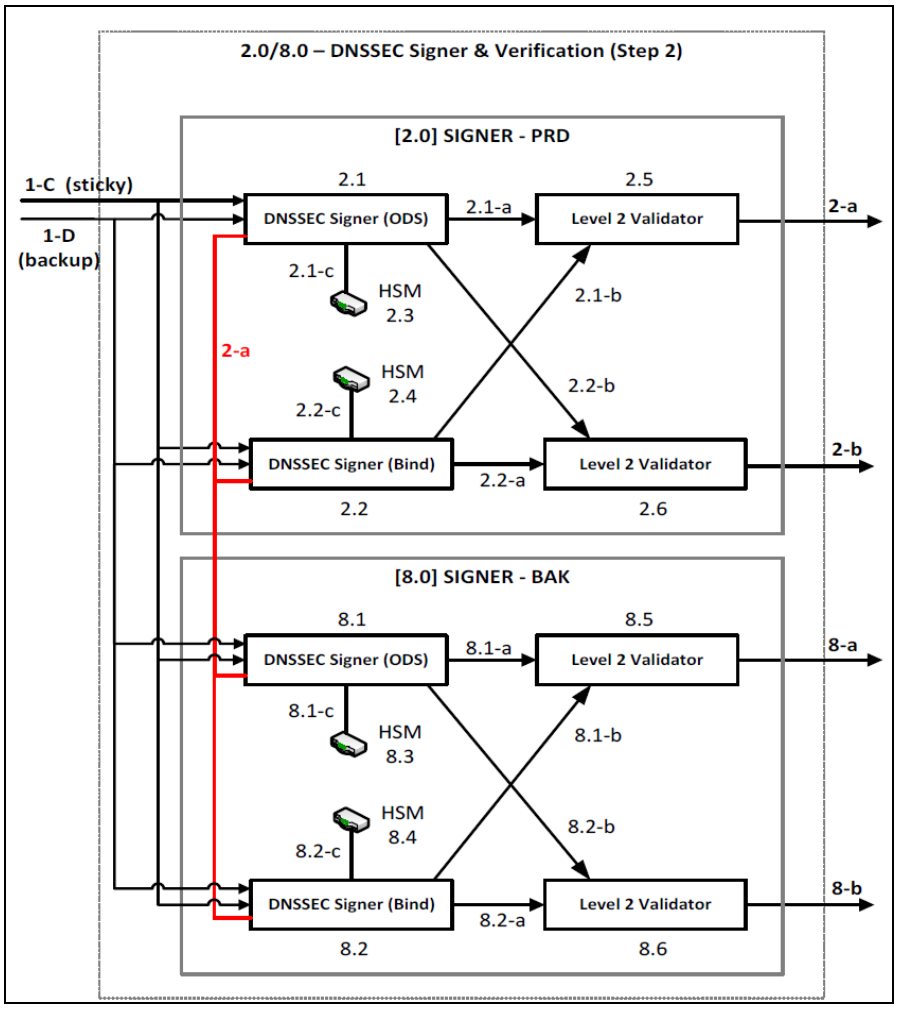
Dodatak A – Iskustva drugih registara po pitanju korišćenja DNSSEC-a

A.1 Implementacija DNSSEC-a u .CA TLD

Kanadski registar nacionalnog internet domena (Canadian Internet Registration Authority - CIRA) je zadatak implementacije DNSSEC-a u .CA TLD podelio u tri faze.

U prvoj fazi, objavljen je DPS dokument, sa namerom da se dobiju komentari i mišljenje javnosti, u kome se opisuje kako CIRA planira da razvije, održava i upravlja DNSSEC-om za .CA. Takođe, održana je i ceremonija potpisivanja ključeva, pri čemu je generisan kriptografski ključ koji je korišćen za obezbeđenje .CA zone. CIRA je već objavio potpisani fajl sopstvene zone i DS zapis za .CA je poslat IANA.

Jedan od ciljeva koji su postavljeni od strane CIRA su visoka dostupnost i otpornost na programske greške. Iz tog razloga, rešenje za potpisivanje podataka je projektovano u vidu dvostrukog „online“ potpisivanja. Podaci se potpisuju uz korišćenje paketa BIND ali i OpenDNSSEC paketa. Rezultati se zatim unakrsno upoređuju, da bi se osiguralo da nema grešaka koji bi potpisane podatke a time i celu zonu učinili neispravnom sa DNSSEC aspekta. Takođe, primarni kao i sekundarni „backup“ sistemi paralelno vrše potpisivanje. Grafički prikaz je dat na slici 11.



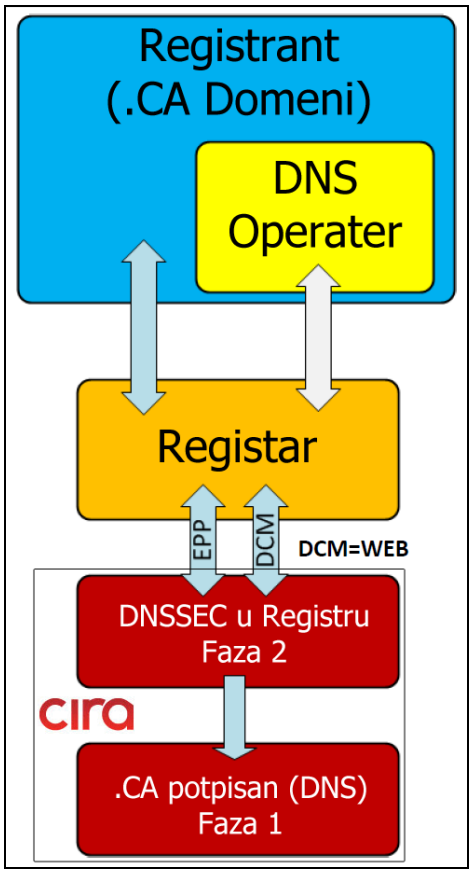
Slika 11. DNSSEC rešenje CIRA sa dvostrukim potpisivanjem

U drugoj fazi, obavljaju se neophodne pripreme na prilagođavanju sistema registra za rad sa DNSSEC potpisanim domenima. Po okončanju ove faze, CIRA će moći da prihvata registraciju .CA domena sa DNSSEC-om.

Još jedan od ciljeva za CIRA je pojednostavljenje i olakšanje rada ovlašćenih registara. DNS operateri, odgovorni za upravljanje svim tehničkim aspektima domena, ukoliko žele da rade sa DNSSEC potpisanim domenima, imaju obavezu da obavljaju sve neophodne kriptografske zadatke koje DNSSEC zahteva (generisanje, upravljanje i prelazak između ključeva, upravljanje DS zapisom...). Do problema dolazi jer funkciju DNS operatera može obavljati:

- Sam registrant, u slučaju da samostalno upravlja svojim DNS-om
- Ovlašćeni registar, kao dodatnu uslugu hostinga
- Specijalizovana kompanija koja pruža DNS usluge, odvojena od registranta i ovlašćenog registra

Hijerarhija odnosa kao i tok komunikacije je prikazan na slici 12. Poteškoće se mogu javiti u slučaju prenosa DNSSEC domena između ovlašćenih registara (što podrazumeva i prenos DNSSEC podataka). Takođe, prelazak između DNSSEC ključeva može biti komplikovan (DNS operater treba da dostavi nove ključeve registrantu, koji ih mora dostaviti ovlašćenom registru). Problem prenosa domena nije specifičan za implementaciju CIRA, već je opšti, poznat problem, o kome ima više reči u poglavlju 6.1. Jedno od rešenja može predstavljati predlog standarda za prenošenje ključeva opisan u poglavlju 6.2.



Slika 12. Hijerarhija odnosa između registranata i OR/registra u .CA

Predviđeno je da se komunikacija između CIRA i ovlašćenih registara obavlja putem interfejsa definisanog u dokumentu RFC 5910, gde OR mogu da uz pomoć EPP proširenja za

DNSSEC dostavljaju sve neophodne podatke. CIRA preko pomenutog interfejsa prihvata kako DS tako i DNSKEY zapise.

Neki od DNSSEC parametara koji se koriste u .CA:

- Mogu se koristiti svi parametri definisani u RFC 5910 – secDNS-1.1.xsd Schema
- Čuva se maksimalno 6 DS i/ili DNSKEY ključeva
- Postoji podrška za svih 11 algoritama koji su predviđeni za potpisivanje zona (DSA, RSA, GOST, ECDSA...)
- Postoji podrška za 4 algoritma prilikom prihvatanja DS zapise (SHA-1/256/384, GOST R 34.11-94)
- Nakon primljenog DNSKEY zapisa, DS zapis se generiše korišćenjem SHA-1 algoritma
- Opcioni <secDNS:maxSigLife> element neće biti podržan
- Whois prikazuje DNSSEC status (potpisan/nepotpisan)

Takođe, CIRA primenjuje sledeća pravila za prijem DNSSEC podataka od strane OR:

- Prihvataće se jedino DS ili DNSKEY zapis, ali ne oboje. Ukoliko oba podatka budu uneta, neće biti prihvaćeni
- U slučaju ažuriranja, biće dozvoljeno dodavanje DS (ili DS i DNSKEY zapisa) ili DNSKEY zapisa čak i ako su prethodno bili uneti suprotni podaci
- Ako se ukloni DNSKEY zapis, svi DS zapisi povezani sa tim ključem će takođe biti uklonjeni
- Ako se ukloni DS zapis za koji postoji povezani DNSKEY zapis – i ako je to poslednji DS zapis koji je povezan sa tim ključem, DNSKEY zapis će takođe biti uklonjen

Ono što se uvek naglašava kada je implementacija DNSSEC u pitanju je da svaka karika u lancu komunikacije mora biti u stanju da obavlja DNSSEC zadatke. CIRA u tom smislu daje neke preporuke prema Internet provajderima, kao karike koja vodi do krajnjeg korisnika:

- DNS softver na rekurzivnim serverima naziva mora podržavati DNSSEC:
  - BIND verzije 9.7 i noviji
  - Unbound verzije 1.4 i noviji
  - Microsoft Windows Server 2012 i noviji
- S obzirom na korišćenje kriptografije i pratećeg opterećenja, infrastruktura oko i na rekurzivnim serverima naziva bi trebalo da bude na adekvatnom nivou, u smislu
  - Hardverske zahtevnosti
  - Propusnog opsega
- Neophodna je podrška za velike UDP pakete (4k) kao i za UDP fragmente
- Neophodna je podrška za prenos DNS paketa preko TCP protokola
- Privremeno omogućiti razrešavanje čak i DNSSEC neispravnih domena

U trećoj fazi je planirana promocija DNSSEC-a u Kanadi, usmerena prema usvajanju kod ovlašćenih registara, Internet provajdera i velikih preduzeća. Neke od predviđenih metoda su dokumentovanje koristi za krajnje korisnike, pronalaženje operativnih uticaja, stvaranje svesti o DNSSEC tehnologiji i edukacija.

A.2 Implementacija DNSSEC-a u .CZ TLD

Dokument: „*DNSSec Operation Manual for the .cz and 0.2.4.e164.arpa Registers*“

A.2.1 Komunikacija

- Podaci o ključevima za pojedinačne domene se unose u registar putem ovlašćenih registara.
- Zahtevi ovlašćenih registara se unose u registar putem standardnog EPP protokola (u skladu sa RFC 3730-3734) sa ekstenzijama i promenama zbog specifičnih potreba registra.
- Komunikacija se odvija putem TCP konekcije obezbeđene SSL-om.
- Osobe za kontakt sa liste kontakata koje su aktivirale email obaveštenja (uključujući i one uklonjene UPDATE zadatkom) se obaveštavaju putem email-a o operacijama (CREATE, UPDATE, TRANSFER i DELETE) nad relevantnimstrukturama podataka (KEYSET, DOMAIN).

A.2.2 Upravljanje DNSSEC ključevima

A.2.2.1 Generisanje ključeva

KSK ključ

Poseban HMS modul sa podrškom za PKCS#11 je posvećen upravljanju KSK. HSM modul i server se koriste samo za generisanje KSK i ZSK ključeva i za potpisivanje vrha zone koji sadrži sve ključeve relevantnih zona potpisanih sa KSK.

U trenutnoj verziji sistema, HSM se ne koristi (nije kompatibilan sa trenutnom verzijom BIND-a). Za upravljanje ključevima se privremeno koristi odvojeni prostori na disku.

Zbog zaštite KSK ključeva od kompromitacije, jedan od KSK se čuva na USB disku uskladištenom *offline* na bezbednom mestu (sef). Ovaj USB disk je namenjen za korišćenje samo u slučaju kompromitacije svih KSK. Ključ koji je na njemu se ne koristi za svakodnevne zadatke. Javni deo ključa je objavljen u ITAR registru i u .cz zoni. Ključ će biti rotiran na standardan način kao i *online* KSK ključevi. Osobe koje imaju pristup sefu se staraju o tome da *offline* ključ bude dostupan po potrebi.

Algoritam ključeva	RSA 2048 bita
Broj ključeva	3 (1 aktivan)
Čuvanje ključeva	Poseban disk na serveru (u budućnosti HSM)

ZSK ključ

Posle generisanja ZSK ključa i potpisivanja vrha zone, ZSK i vrh zone se prenose na server koji se koristi za potpisivanje zone. Proces je automatizovan.

Algoritam ključeva	RSA 1024 bita
Broj ključeva	2 (1 aktivan)
Čuvanje ključeva	Poseban disk na serveru

A.2.2.2 Namenski serveri

Rotacija ključeva – KSK

Za KSK rotaciju se koristi *Double signature* mehanizam. Prelasci se najavljuju pola godine unapred. Posle implementacije mehanizma za rotaciju ključeva opisanog u RFC 5011 u BIND DNS server, rotacija se obavlja na sledeći način:

Validnost ključa	2 godine
Metod rotacije	Ručno

U slučaju kompromitacije ključeva, rotacija treba biti sprovedena kao u slučaju normalnog prelaska između ključeva, da ne bi došlo do prekida u radu .cz zone. Novi KSK će biti generisani i DS zapisi u root zoni, DLV kao i u ITAR registru će biti zamenjeni. U slučaju kompromitacije samo jednog KSK, uklanjanje iz roditeljske zone i generisanje novog ZSK su dovoljni.

Rotacija ključeva – KSK

Validnost aktivnog ZSK je 8 nedelja. Rotacija ZSK se obavlja na svaka dva meseca, korišćenjem *Pre-publishing* mehanizma. Najmanje dva ZSK se objavljuju u zoni. Za vreme rotacije, aktivni ključ se označava kao zastareo dok se novi ključ označava kao aktivan. Po isteku propisanog perioda, zastareli ključ se uklanja iz zone i generiše se novi ZSK ključ.

Validnost ključa	90 dana
Metod rotacije	Automatski (ZKT)

U slučaju kompromitacije ključeva, generiše se novi komplet ZSK, zone na vrhu se potpisuju i ZSK komplet se zamenjuje. Ako je makar jedan ZSK kompromitovan, mora biti uklonjen iz zone. Primer listinga ključeva:

Naziv ključa	Oznaka	Tip	Status	Algoritam	Ispravnost
0.2.4.e164.arpa.	31,333	KSK	aktivan	RSASHA1	12 godina
0.2.4.e164.arpa.	7,834	KSK	aktivan	RSASHA1	2 godine
0.2.4.e164.arpa.	23,092	KSK	rezervni	RSASHA1	2 godine
0.2.4.e164.arpa.	15,590	ZSK	aktivan	RSASHA1	3 meseca
0.2.4.e164.arpa.	42,605	ZSK	objavljen	RSASHA1	3 meseca
cz.	7,978	KSK	aktivan	RSASHA1	12 godina
cz.	1,234	KSK	objavljen	RSASHA1	2 godine
cz.	58,372	KSK	rezervni	RSASHA1	2 godine
cz.	50,820	ZSK	aktivan	RSASHA1	3 meseca
cz.	47,420	ZSK	objavljen	RSASHA1	3 meseca

A.2.2.3 Objavljivanje ključeva

KSK ključevi za zone kojima upravlja registar i za koje postoji potpisana roditeljska zona koja dozvoljava bezbedno delegiranje će biti postavljeni u roditeljskoj zoni. KSK ključevi za zone kojima upravlja registar i za koje ne postoji potpisana roditeljska zona moraju biti objavljeni korisnicima na neki drugi način.

A.2.2.4 Potpisivanje zone

Generisanje potpisa se obavlja na namenskom serveru koji služi i za generisanje zone. Fajl .cz zone se generiše svakih 30 minuta i novi kao i izmenjeni zapisi se potpisuju posle svakog generisanja. Posle generisanja zone, potpisi se izdvajaju iz stare potpisane zone i sjedinjuju sa novim fajlom zone. Sjedinjeni fajl zone se potpisuje uz pomoć *dnssec-signzone* alata iz BIND9 paketa. Na taj način, izmene u potpisima se vrše samo u nezibežnom slučaju.

Vreme ispravnosti potpisa je 1 mesec. Novi potpis se generiše 1 nedelju pre isteka tekućeg potpisa.

A.2.2.5 Odgovorno osoblje

Zadatak	**Obavlja**
Generisanje novog KSK	Uvek dvoje od sledećih: *manager, operations manager, technical manager*
Potpisivanje ZSK	Autorizovani član DNSSEC tima
KSK rotacija	Jedan od sledećih: *manager, operations manager, technical manager*
ZSK rotacija	Automatizovani alat
Rezervna kopija KSK na eksternom skladištu	Jedan od sledećih: *manager, operations manager, technical manager*
Pristup sefu	*Manager, operations manager*

Dodatak B – TTL vrednosti DNSSEC zapisa registara domena najvišeg nivoa

	DNSKEY	DS	RRSIG	NSEC	NSEC3	NSEC3PARAM
.SE	3600 sekundi	3600 sekundi		= minimum polje u SOA zapisu (RFC 5155)		
.NL	7200 sekundi	7200 sekundi	= TTL RRset-a koji pokriva		= minimum polje u SOA zapisu (RFC 5155)	3600 sekundi
.CA	21600 sekundi	86400 sekundi	= TTL RRset-a koji pokriva		3600 sekundi	
.AT	3600 sekundi	10800 sekundi	= TTL RRset-a koji pokriva		3600 sekundi	
.JP	86400 sekundi	86400 sekundi	= TTL RRset-a koji pokriva		900 sekundi	
.NZ	86400 sekundi	86400 sekundi	= TTL RRset-a koji pokriva	3600 sekundi	3600 sekundi	
.PL	3600 sekundi		= TTL RRset-a koji pokriva			
.SI	3600 sekundi	7200 sekundi	= TTL RRset-a koji pokriva		= minimum polje u SOA zapisu (RFC 5155)	3600 sekundi
.COM	86400 sekundi	86400 sekundi	= TTL RRset-a koji pokriva, varira do 48h			
.EDU	86400 sekundi	86400 sekundi	= TTL RRset-a koji pokriva, varira do 48h			
.NET	86400 sekundi	86400 sekundi	= TTL RRset-a koji pokriva, varira		= minimum polje u SOA zapisu (RFC 5155)	

Dodatak C – Spisak poznatih hardverskih modula zaštite (HSM)

Proizvod	Proizvođač	Opis
Keyper	AEP *http://www.ultra-aep.com/*	„Omogućava FIPS-sertifikovanom službeniku i autorizovanom korisniku da generiše, skladišti i koristi ključeve visokog kvaliteta u okviru HSM uređaja sa Ethernet vezom koji reaguje na neovlašćeno rukovanje“
Sapphire Sx20	BT Diamond *http://www.globalservices.bt.com/uk/en/products/diamondip/products*	„Podržava pristup DNSSEC administratora radi podešavanja politika DNSSEC ključeva i potpisivanja, uključujući tipove ključeva, algoritme, dužine i prelaske kao i generisanje i upravljanje životnim vekom ključeva i vremenima isticanja potpisa“
Cryptosec LAN	RealSec *http://www.realsec.com*	„Kriptografski mrežni server koji pruža usluge šifrovanja i digitalnog potpisivanja“
4765 Cryptographic Coprocessor Card	IBM *http://www-03.ibm.com/security/cryptocards/*	„Hardver za obavljanje AES, DES, TDES, RSA, SHA-1, SHA-224 do SHA 51239 kriptografskih procesa, oslobađajući glavni procesor od ovih zadataka
Compact HSM	Kryptus *http://www.kryptus-int.com/#!compacthsm/c9o9*	„Zadaci sa digitalnim potpisima na rešenjima koja koriste PKCS#11... Generisanje i čuvanje sertifikata... Šifrovanje komunikacije“
SCA6000 Crypto Accelerator card	Oracle *http://www.oracle.com/us/products/networking/ethernet/crypto6000-pcie/overview/index.html*	„Ubrzava SSL kriptografske funkcije, oslobađajući glavni procesor ovih zadataka, za bilo koju aplikaciju, uključujući IPSec“
Luna CA4, Luna SA appliance	SafeNet *http://www.safenet-inc.com/products/data-protection/hardware-security-modules/luna-sa/*	CA4 „štiti *root* ključ u PKI i obavlja sve zadatke upravljanja, čuvanja i rada sa ključevima (npr. digitalno potpisivanje) u okviru hardvera“. SA obavlja „potpisivanje sa visokim performansama i ubrzanje SSL kriptografskih funkcija za bilo koju aplikaciju“
nShield Solo i nShield Connect	Thales *https://www.thales-esecurity.com/products-and-services/products-and-services/hardware-security-modules*	„Štiti privatne DNSSEC ključeve i obezbeđuje integritet procesa DNSSEC validacije uz primenu visoko bezbednog, FIPS-sertifikovanog, hardvera otpornog na neovlašćeno baratanje“
CryptoServer HSM	Utimaco *https://hsm.utimaco.com/*	„Kriptografski HSM koji briše ključeve i sertifikate ukoliko se njime neovlašćeno rukuje“
DNSX Secure Signer	Xelerance Corp. *https://www.xelerance.com/product*	Automatizuje zadatke upravljanja DNSSEC-om
DNSX Secure Resolver	Xelerance Corp. *https://www.xelerance.com/product*	Dodaje bezbednosne mere serverima naziva koji razrešavaju i keširaju podatke

Literatura

[1] F. Ljunggren, AM. Eklund Lowinder, T. Okubo, „A Framework for DNSSEC Policies and DNSSEC Practice Statements“, Internet Engineering Task Force, Januar 2013.

[2] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, „DNS Security Introduction and Requirements”, RFC 4033, Internet Engineering Task Force, Mart 2005.

[3] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, „Resource Records for the DNS Security Extensions”, RFC 4034, Internet Engineering Task Force, Mart 2005.

[4] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, „Protocol Modifications for the DNS Security Extensions”, RFC 4035, Internet Engineering Task Force, Mart 2005.

[5] S. Weiler, J. Ihren, „Minimally Covering NSEC Records and DNSSEC On-line Signing“, RFC 4470, Internet Engineering Task Force, April 2006.

[6] O. Kolkman, W. Mekking, R. Gieben, „DNSSEC Operational Practices, Version 2”, RFC 6781, Internet Engineering Task Force, Decembar 2012.

[7] B. Laurie, G. Sisson, R. Arends, D. Blacka, „DNS Security (DNSSEC) Hashed Authenticated Denial of Existence”, RFC 5155, Internet Engineering Task Force, Mart 2008.

[8] J. Bau, J. C. Mitchell, „A Security Evaluation of DNSSEC with NSEC3“

[9] „DNSSEC and domain transfers“, Verisign Inc., 2010.

[10] R. Gieben, M. Groeneweg, R. Ribbers, A.L.J. Verschuren, „Key Relay Mapping for the Extensible Provisioning Protocol“, Internet Engineering Task Force, Jul 2013.

[11] R. Aitchison, „Choosing a DNSSEC Solution“, Maj 2009.

[12] S. Morris, J. Ihren, J. Dickinson, „DNSSEC Key Timing Considerations“, Internet Engineering Task Force, Januar 2013.

[13] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)", RFC 5730, Internet Engineering Task Force, Avgust 2009.

[14] S. Hollenbeck, "Extensible Provisioning Protocol (EPP) Domain Name Mapping", RFC 5731, Internet Engineering Task Force, Avgust 2009.

[15] S. Hollenbeck, "Extensible Provisioning Protocol (EPP) Host Mapping", RFC 5732, Internet Engineering Task Force, Avgust 2009.

[16] S. Hollenbeck, "Extensible Provisioning Protocol (EPP) Contact Mapping", RFC 5733, Internet Engineering Task Force, Avgust 2009.

[17] S. Hollenbeck, "Extensible Provisioning Protocol (EPP) Transport over TCP", RFC 5734, Internet Engineering Task Force, Avgust 2009.

[18] J. Gould, S. Hollenbeck, „Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)“, RFC 5910. Internet Engineering Task Force, Maj 2009.

[19] S. Hollenbeck, „Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (EPP)“, RFC 3915, Internet Engineering Task Force, Septembar 2004.

[20] „Extensible Markup Language (XML) 1.0 (Third Edition)“, http://www.w3.org/TR/2004/REC-xml-20040204/

[21] „XML Schema Part 1: Structures Second Edition“, http://www.w3.org/TR/xmlschema-1/

[22] „XML Schema Part 2: Datatypes Second Edition“, http://www.w3.org/TR/xmlschema-2/

[23] T. Haugen, „UNINETT Norid EPP Interface Specification“, UNINETT Norid AS, Februar 2014. http://www.norid.no/registrar/system/dokumentasjon/EPP_Interface_Specification.5p3.pdf

[24] NORID EPP XML schemas http://www.norid.no/registrar/system/dokumentasjon/epp-grensesnitt.en.html

[25] „EPP Manual“, SWITCH, Novembar 2013. https://www.nic.ch/reg/cm/wcm-resource/download/xform2/EPP-Manual_en.pdf

[26] R. Gieben, M. Groeneweg, R. Ribbers, A.L.J. Verschuren, „Key Relay Mapping for the Extensible Provisioning Protocol“, Internet Engineering Task Force, Jul 2013.

[27] A. Verschuren, „EPP keyrelay: solving the last obstacle for DNSSEC deployment“, SIDN Labs, Jul 2013.

[28] D. Eastlake, „RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)“, Internet Engineering Task Force, Maj 2001.

[29] J. Jansen, „Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC“, Internet Engineering Task Force, Oktobar 2009.

[30] P. Hoffman, W.C.A. Wijngaards, „Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC“, Internet Engineering Task Force, April 2012.

[31] W. Hardaker, „Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)“, Internet Engineering Task Force, Maj 2006.

[32] „Recommendations for DNSSEC deployment at municipal administrations and similar organisations“, Kirei AB, Mart 2014.

[33] P. Vixie, O. Gudmundsson, D. Eastlake 3rd i B. Wellington, „Secret Key Transaction Authentication for DNS (TSIG)“, RFC 2845, Internet Engineering Task Force, Maj 2000.

[34] D. Eastlake 3rd, „HMAC SHA TSIG Algorithm Identifiers“, RFC 4635, Internet Engineering Task Force, Avgust 2006.

[35] S. Kwan, P. Garg, J. Gilroy, L. Esibov, J. Westhead, R. Hall, „Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)“, RFC 3645, Internet Engineering Task Force, Oktobar 2003.

[36] M. StJohns, „Automated Updates of DNS Security (DNSSEC) Trust Anchors“, RFC 5011, Internet Engineering Task Force, Septembar 2007.

[37] D. Eastlake, J. Schiller, S. Crocker, „Randomness Requirements for Security“, RFC 4086, Internet Engineering Task Force, Jun 2005.

[38] E. Barker, J. Kelsey, „Recommendation for Random Number Generation Using Deterministic Random Bit Generators“, NIST 800-90A, National Institute of Standards and Technology, Januar 2012.

[39] A. Kasabov, „Resilient OpenDNSSEC“, University in Amsterdam, System & Network Engineering, Avgust 2012.

[40] A. Langley, „Serializing DNS Records with DNSSEC Authentication“, Internet Engineering Task Force, Jul 2011.

[41] R. Barnes, „Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE)“, RFC 6394, Internet Engineering Task Force, Oktobar 2011.

[42] P. Hoffman, J. Schlyter, “The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA”, RFC 6698, Internet Engineering Task Force, Avgust 2012.

[43] R. L. Barnes, „DANE: Taking TLS Authentication to the Next Level Using DNSSEC“, The IETF Journal, Vol. 7, Issue 2, pp. 1-7, 2011.

[44] J. Jansen, „Measuring the effects of DNSSEC deployment on query load“, NLnet Labs, Maj 2006.

[45] ISO/IEC, 27002:2005(E): Information technology - Security techniques - Code of practice for information security management, 2005.

[46] R. Chandramouli & S. Rose, Secure Domain Name System (DNS) Deployment Guide, Septembar 2013.

[47] O. Kolkman, M. Mekking, „DNSSEC Infrastructure Audit Framework“, NLnet Labs, 2013.

[48] P. Koch, „Recommendations for DNS SOA Values“, RIPE NCC, Jun 1999.

[49] Y. Schaeffer, B. Overeinder, M. Mekking, „Flexible and Robust Key Rollover in DNSSEC“, NLnet Labs, 2012.

[50] R. Gieben, „DNSSEC in NL, final report“, NLnet Labs, Januar 2004.

[51] A. Nilsson, „A Review of Administrative Tools for DNSSEC – Spring 2010“, Certezza AB, Maj 2010.