



УНИВЕРЗИТЕТ СИНГИДУНУМ
ДЕПАРТМАН ЗА ПОСТДИПЛОМСКЕ СТУДИЈЕ
-Савремене информационе технологије-

Имплементација DNSSEC сервиса

- Мастер рад –

Ментор:

Проф. Др Младен Веиновић

Студент:

Предраг Александров

Бр. индекса: 411098/2014



Београд, 2016

Садржај:

Увод.....	3
Имплементација DNSSEC-а у BIND-у.....	13
Имплементација DNSSEC-а у Windows Server 2012	22
Закључак	34

Увод

Како би се успоставила комуникација са другим рачунаром на Интернету неопходно је унети његову адресу у рачунар која представља име и ли број. Адреса мора бити јединствена на нивоу целог Интернета како би један рачунар пронашао другог. ICANN координише ове јединствене адресе широм света. Без координације неби могао да постоји јединствен Интернет какав познајемо. Када се укуца име у рачунар то име мора бити преведено у број пренего што се успостави комуникација. Овај систем назива се DNS (Domain Name System) и он преводи имена каоо што су www.icann.com у бројеве који се називају Internet Protocol (IP) адресе. ICANN кординише те адресе како би биле јединствене.

У последње време пронађене су рањивости у самом DNS протоколу које омогућавају хакерима да хакују сам процес. Тако на пример нападач може да преузме контролу над сесијом и преусмери корисника на лажни сајт са којим је могуће украсти његову шифру.

Ове рањивости повећале су интерес за за увођењем технологије DNSSEC која уводи сигурносна проширења у сам DNS.

Следећа питања и одговори предстаљају покушај да се објасни DNSSEC и зашто је његова имплементација неопходна.

Шта су root zone?

DNS сервис преводи доменска имена које човек зна да запамти у бројеве које су природније рачунарима нешто слично телефонском именику. Ово се одвија по нивоима. На првом нивоу налазе се top level домени или root зоне. Тако на пример како би рачунар приступио сајту www.google.com рачунар пита top level домене где може да нађе информацију везану за домен .com након тога рачунар пита .com за домен .google.com (други ниво) и на крају пита google.com која је адреса за www.google.com (трећи ниво). Различити субјекти управљају различитим доменима тако на пример google.com се управља од стране Google корпорације, .com домен се управља од стране VeriSign корпорације док се root зона управља од стране ICANN.

Зашто је потребно да потпишемо root зону?

Скоро примећене слабости код DNS сервиса паралелно са напредком технологије омогућавају нападачу могућност да за кратко време овлада DNS lookup процесом а затим преузимањем сесије корисника (тако што ће га преусмерити на свој лажирани сајт) прикупљање поверљивих података као што су лозинке.

Шта је DNSSEC?

DNSSEC је технологија која отклања слабости DNS сервиса тако што дигитално потписује податке на серверу тако да корисник буде сигуран у веродостојност података. Поступак се понавља на свим нивоима у хијерархији од root зоне до на пример домена www.icann.org.

Како унапредити сигурност просечног корисника?

Циљ целокупне имплементације DNSSEC сервиса је да крајњи корисник буде повезан на прави web сајт или други сервис на основу одговарајућег домена. DNSSEC решава сигурносне проблеме у DNS lookup процесу за разлику од SSL-а (https-a) који штити комуникацију између клијента и сервера.

Шта се заправо дешава када се потпише root?

Потписивањем root-а користећи DNSSEC додаје се још записа на сваком top level домену у root зонском фајлу. Оно што се додаје је кључ и потпис који атестира валидност кључа.

DNSSEC омогућава валидациони процес за записе. Он не шифрује нити мења менаџмент података и компатибилан је уназад са текућим DNS-ом и апликацијама. То значи да он не мења постојеће протоколе на којима је адресирање на Интернет-у базирано. Он укључује ланац дигиталних потписа у DNS хијерархији у коме сваки ниво има свој генерисани кључ за потписивање. То значи да на пример домен www.icann.org свака организација мора да потпише кључ дуж ланца за оног испод себе. Тако на пример .org потписује icann.org кључ. Током валидационог процеса DNSSEC следи ланац поверења све до root-а аутоматски валидирајући child кључеве користећи кључеве parent-a.

Пуно увођење DNSSEC-а не подразумева само потписивање root-а (иако је круцијалано) већ подразумева и да сваки домен нижи у хијерархију изврши потписивање са одговарајућим оператером како би употпунио ланац поверења. У последње време TLD оператери убрзавају процес увођења DNSSEC-а у својим зонама (као што су на пример .bg, .se, .cz и т.д.)

Како се управља root зонама?

Управљање root зонама се врши између неколико ентитета:

- ICANN (an International not-for-profit Corporation under contract from United States Department of Commerce) који врши IANA (Internet Assigned Numbers Authority) функцију. ICANN добија и прегледава информације од оператера top level домена (TLD) као што је на пример "com".

- National Telecommunications and Information Administration (NTIA) који представља одељак у United States Department of Commerce – овлашћује промене у root-у.

- VeriSign - америчка профитна компанија која има уговор са владом САД да мења root зоне са информацијама добивеним и овернеиним из ICANN и одобреним од стране

Department of Commerce и дистрибуира root зонске фалјове који садржи информација где се може пронаћи информација за TLD као што је на пример “com”

- Међународна група root сервер оператера који добровољно одржава преко 200 сервера широм света који дистрибуирају root информације из root зонског фајла широм Интернета. То су следећи опеаратери:

- A) VeriSign Global Registry Services;
- B) Information Sciences Institute at USC;
- C) Cogent Communications;
- D) University of Maryland;
- E) NASA Ames Research Center;
- F) Internet Systems Consortium Inc.;
- G) U.S. DOD Network Information Center;
- H) U.S. Army Research Lab;
- I) Autonomica/NORDUnet, Sweden;
- J) VeriSign Global Registry Services;
- K) RIPE NCC, Netherlands;
- L) ICANN;
- M) WIDE Project, Japan.

Зашто је битно за DNSSEC заштиту да једна организација врши прегледање, промену и потписивање?

Снага DNSSEC-а за сваки линк у ланцу поверења лежи у поверењу корисника у организацију која проверава кључеве и остале информације за задати линк. У циљу да се гарантује интегритет информација и сачува поверење подаци се верификују заштићују од грешака случајних или малициозних унутар оквира организација.

У DNSSEC-у шта је KSK and ZSK?

KSK је скраћеница за Key Signing key а ZSK за Zone Signing Key. За одређено време криптографски кључеви могу бити компромитовани. У случају асиметричне криптографије која се користи код DNSSEC-а нападач може коришћењем brute force методе или неке друге приватни део

У случају асиметричне криптографије или криптографије јавних кључева који се користи у DNSSEC-у нападач проналази, користећи методе као што су brute force, тајни део од public-private парова кључева који су кориштени за креирање потписа којима се тестира валидност DNS записа. Ово омогућава нападачу да пробије заштиту коју пружа DNSSEC. DNSSEC се супротставља тим компромитујућим покушајима користећи кључ кратког времена трајања – the zone signing key (ZSK) да би рутински прорачунао потписе за DNS записе и кључ дужег времена трајања – the key signing key (KSK) – да би прорачунао потпис од ZSK како би био валидиран. ZSK се мења често да би како би се отежало нападачу да га погоди док се KSK у дужем периоду (у пракси се показало најбоље годину

дана). Пошто KSK потписује ZSK и ZSK потписује DNS записе, само је KSK неопходан да валидира DNS записе унутар зоне. Он је узорак од KSK и у облику Delegation Signer (DS) записа прослеђен је “parent” зони. “Parent” зона (на пример root) потписује DS записе “child”-а (на пример .org) са својим ZSK који је потписан својим KSK.

То значи да уколико се у потпуности усвоји DNSSEC KSK за root зону постаје део валидационог ланца за свако DNSSEC валидирано име домена.

Ко управља кључевима?

У оквиру овог предлога, ICANN чува инфраструктуру кључева али креденцијале за генерисање KSK носе вањске организације. Ово је битан елемент у прихватању овог процеса. ICANN није предложио ниједно специфично решење који ентитети треба да задрже акредитиве али је верује да су сва ова питања за јавне консултације и за одлуку америчког министарства трговине.

Како DNSSEC ради?

DNSSEC је протокол чији актуелни опис дат у следећим документима: RFC4033, RFC4034 и RFC4035.

Основна идеја DNSSEC-а је начин провере аутентичности записа у зони за задати домен на бази провере електронског потписа извршен над њима. На тај начин се гарантује да записи заиста припадају одговарајућем домену и нису генерисани са циљем да се заваља клијент.

Извршавање и провера електронског потписа у оквирима DNSSEC-а се врши употребом криптографије са јавним кључевима. У моменту алгоритми који се користе за криптографију са јавним кључевима за потребе DNSSEC-а су DSA и RSA. Генерише се пар кључева по један за сваки од наведених алгоритама и уз помоћ тајног кључа администратори домена врше потписивање записа у зони. Електронски потписани записи се смештају у зони исто као и остали записи. Провера потписа се врши уз помоћ јавног кључа. Сам јавни кључ се објављује као запис у зони домена. Када неки клијент хоће да провери аутентичност задатог записа у зони домена најпре затражује запис који проверава а затим и запис који садржи јавни кључ. Подразумева се да онај који врши проверу електронског потписа треба да зна да је јавни кључ аутентичан то се врши методама излазе из теме DNSSEC-а и биће касније објашњени.

С техничке стране провера електронског потписа, извршен употребом криптографских алгоритама са јавним кључевима, представља оптерећење за сам процесор. Ово значи да је повећано оптерећење DNS сервера који врше проверу. Као што домени имају своју хијерархију тако и DNSSEC подлеже хијерархији. То значи да у parent зони

мора постојати податак о аутентичностима кључева у child домену са којима се провера електронски потпис записа у зони. На тај начин parent зона гарантује аутентичност child

зона. Да би се одржало наслеђивање неопходно је да child зона преда оператору parent зоне одговарајуће DS записе које је генерисао.

Да би олакшао валидацију потписа, DNSSEC додаје нове типове DNS записа:

RRSIG- садржи криптографски потпис

DNSKEY- садржи јавни кљич којим се врши потписивање

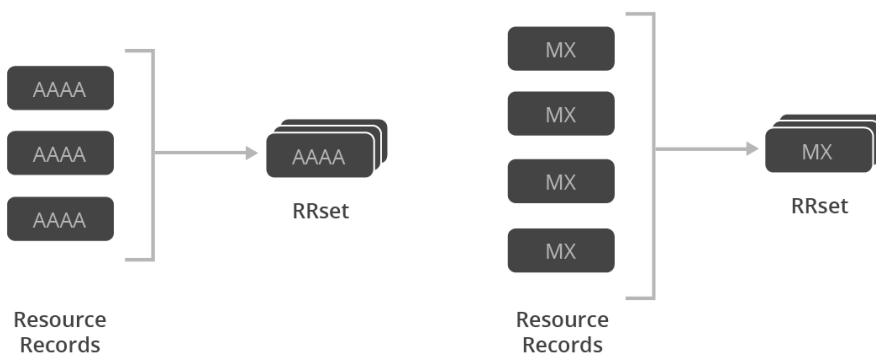
DS- садржи хеш DNSKEY записа

NSEC и **NSEC3**- за експлицитно непостојање записа

CDNSKEY и **CDS**- за child зону захтевана ажурирања за DC записе у parent зони.

RRsets

Први корак у заштити зоне са DNSSEC је груписање свих записа истог типа у т.з. resource record set (RRset). На пример, ако имамо три AAAA записа у зони, биће спаковани у једном AAAA RRset-у. (слика 1).



Слика 1.

Ово је комплетан RRset који је дигитално потписан за разлику од индивидуалних DNS записа. Наравно ово значи морате захтевати и валидирати све AAAA записе уместо валидирања једног од њих.

Zone-Signig Keys

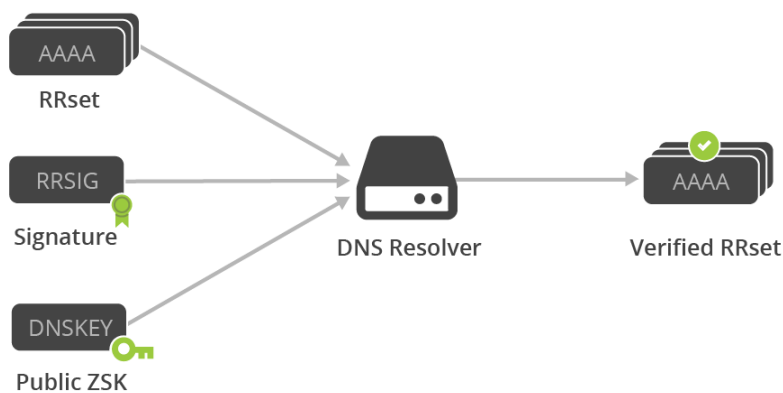
Свака зона у DNSSEC-у има zone-signig пар кључева (ZSK), тајни део кључа дигитално потписује сваки Rrset у зони, док јавни верификује потпис. Да би омогућио DNSSEC оператор зоне креира дигитални потпис за сваки Rrset користећи тајни кљук ZSK-а и складишти их у DNS серверу као Rrsig записе. (слика 2.)



Слика 2.

RRSIG записи су неупотребљиви ако не постоји начин DNS resolver верификује њихов потпис. Оператор зоне мора да омогући да јавни кључ од ZSK буде доступан тако што га додаје у DNS серверу у DNSKEY запису.

Када DNSSEC resolver захтева појединачни тип записа (на пример AAAA) DNS сервер одговара са одговараћим RRSIG-ом. DNS resolver може да смести DNSKEY запис који садржи јавни ZSK од DNS сервера. Заједно RRset, RRSIG, и ZSK могу валидирати одговор.

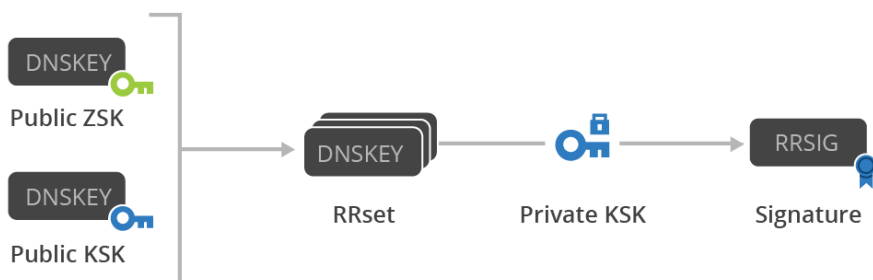


Слика 3

Ако се верује zone-signing кључу (ZSK) у DNSKEY запису тада се може веровати свим записима у зони. Али шта ако је ZSK компромитован? Мора постојати начин да се валидира јавни ZSK.

Key-Signing Keys

Поред ZSK DNSSEC сервери морају имати и Key-Signing Keys (KSK). KSK валидира DNSKEY запис на исти начин као што ZSK штити RRSets. Он потписује јавни ZSK (који је смештен у DNSKEY запису) креирајући RRSIG за DNSKEY. (слика 4)

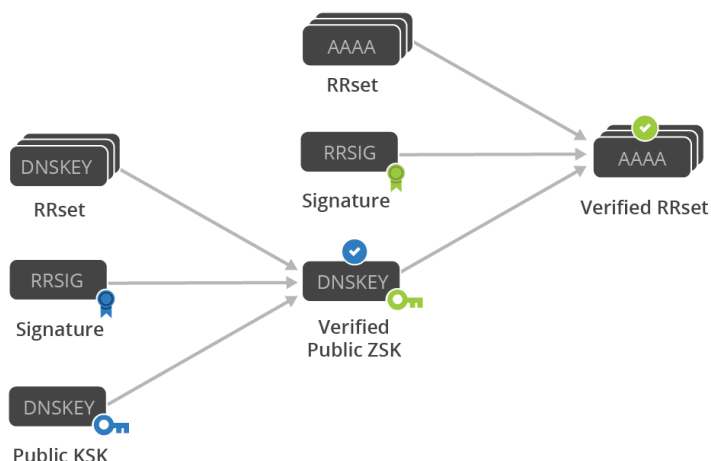


Слика 4.

Као што објављује ZSK DNS сервер објављује и KSK у другом DNSKEY запису чиме се добија DNSKEY RRset који је приказан на слици 4. Оба јавни ZSK и јавни KSK су потписани приватним KSK. DNS resolver може користити јавни KSK да би валидирао јавни ZSK.

Валидациони процес за DNS resolver-е изгледа овако:

- захтева одговарајући RRset, који враћа одговарајући RRSIG запис
- захтева DNSKEY запис који садржи јавни ZSK и јавни KSK који опет враћа RRSIG за DNSKEY RRset
- верификује RRSIG за захтевани RRset са јавним ZSK
- верификује RRSIG од DNSKEY RRset са јавним KSK. (слика 5).



Слика 5.

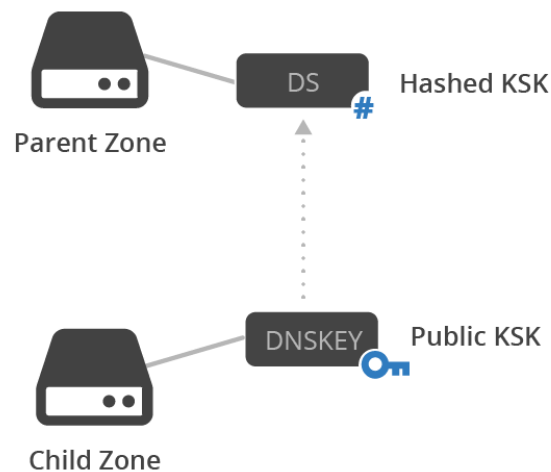
Наравно DNSKEY RRset и одговарајући RRSIG записи могу бити кеширани тако да DNS серверу небуду бомбардовани са непотребним захтевима.

Зашто су издвојени ZSK и KSK кључеви? Тешко је заменити стари или компромитоавни KSK. Променити ZSK-а на другу страну је много лакше извести. Ово омогућава коришћење мањег ZSK без компромитовања заштите сервера минимизацијом количине података који сервер треба послати у сваком одговору.

На тај начин је успостављено поверење са зоном али DNS сервер је хијерархијски систем и зоне функционишу ретко независно. Ствари компликује то што је KSK је потписан самим собом што онемогућује поверење. Мора постојати начин да се успостави поверење између child зоне и parent зоне.

Delegation Signer Records

DNSSEC уводи delegation signer (DS) запис који омогућава трансфер поверења између child зоне и parent зоне. Зонски оператор хешује DNSKEY запис који садржи јавни KSK и предаје га parent зони који га објављује као DS запис. (слика 6).



Слика 6.

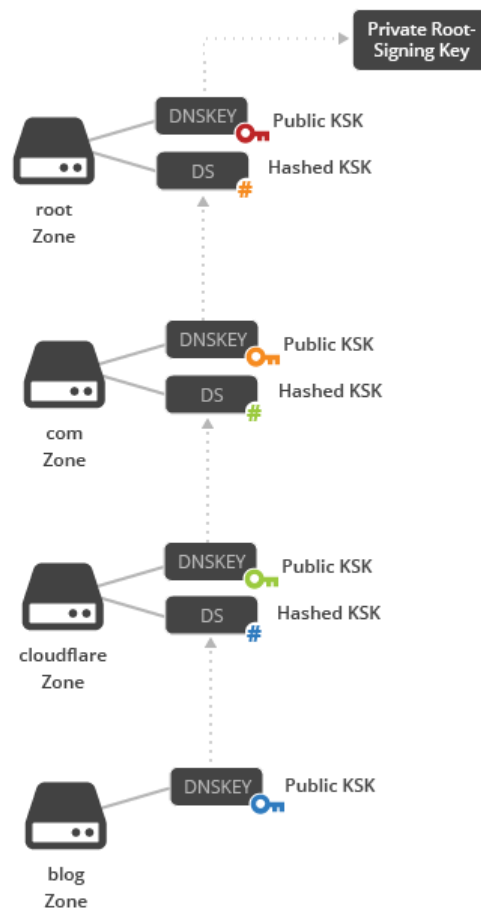
Сваки пут када resolver се референцира на child зону parent зона прослеђује DS запис. Овај DS запис указује на то да child зона има омогућен DNSSEC. Да би се проверила валидност јавног KSK од child зоне resolver хешира га и упоређује са DS записом добијеним од parent зоне. Ако се поклапају resolver је сигуран да јавни KSK није промењен и може да верује свим записима у child зони. Ово је начин како се успоставља ланац поверења у DNSSEC-у.

Свака промена у KSK захтева промену DS записа у parent зони. Промена DS записа је процес који се састоји у више корака који ако се не испоштује разбија зону. Прво parent зона мора да додода нови DS запис а затим је потребно да сачека TTL време да би оригинални DS запис истекао пренего што га избаци. Зато је много лакше заменити ZSK него KSK. Када оператор child домена жели да буде делегиран у оквирима DNSSEC-а он се повезује са оператором parent зоне и по сигурном каналу предаје своје DS записе.

The Chain of Trust

значи да има одговарајући RRSIG у parent зони. Цео процес се понавља све док се не добије parent јавни KSK. Да би се извршила верификација тога узима се DS запис у parent зон

Како би се комплетирао процес поверења морамо обезбедити механизам да верујемо DS записима. DS записи се валидирају као и сваки RRset што и и тако се ствара ланац поверења. (слика 7).



Слика 7.

Када на крају провера дође до root DNS зоне не постоји DS запис у parent зони да би била извршена валидација.

У Root Signing Ceremony неколико одабраних субјеката из целог света долазе и заједно врше потписивање root DNSKEY RRset у веома јавном и високо ревизираном поступку. Церемонија креира RRSIG запис који бива кориштен за верификовање јавних KSK и ZSK кључева код root DNS сервера.

Имплементација DNSSEC-а у BIND-у

Конвенција именовања фајлова за чување кључева

Име фајла који садржи кључеве састоји се од имена и екстензије. Састоји се он низа слова који садржи следеће:

- слово К које означава да фајл садржи кључ;
- име зоне домена за кога су парови кључева предодређени;
- код алгоритма који је коришћен за генерисање кључева типа “.+xyz” где су x, y и z цифре, на пример алгоритми RSASHA1 имају код 005;
- случајни број са горњом границом 2^{16} који је одвојен од кода алгоритма знаком “+” који представља јединствени идентификатор кључа

Екстензија има две вредности "key" или "private" у зависности. Екстензија "key" означава фајл који садржи јавни кључ док "private" означава да фајл садржи приватни кључ.

На пример фајлови који садрже парове кључева генерисани комбинацијом алгоритама RSASHA1 имају следећа имена:

Klocalhost.+005+63675.key – фајл који садржи јавни кључ

Klocalhost.+005+63675.private – фајл који садржи приватни кључ

Радни директоријуми за извршење подписивања

Постојање ових директоријума није обавезно али је израз добре праксе у администрацији. Сваки оператор је дужан да их креира за своје потребе.

На пример путања до радног директоријума може бити смештена у променљиви `${DNSSECDIR}` радни директоријум има следеће поддиректоријуме:

```
${DNSSECDIR}
    KSK/
    ZSK/
    zones/
```

Намена поддиректоријума је следећа

- у поддиректоријуму KSK се налази пар KSK кључева
- у поддиректоријуму ZSK се налази пар ZSK кључева
- у поддиректоријуму zones се налазе шаблони за зоне које треба потписати

Најлакши начин да се сетује променљива `${DNSSECDIR}` је користећи следећу команду:

```
$ export DNSSECDIR=/path/to/dnssec/dir
```

Најудобнији начин да се зада променљива је коришћењем иницијализације променљивих коришћењем команде шела `bash`. У том случају у одговарајућем `home` директоријуму корисника мора бити на располагању фајл `.bashrc`. У том фајлу променљива се најпре декларише а затим јој се сетује вредност.

```
# DNSSEC directory
```

```
export DNSSECDIR=${HOME}/DNS_AS5421/DNSSEC/
```

Како би се избегло излажење из терминалних сесија промене могу бити унешене одмах на следећи начин:

```
$ cd ${HOME}
```

```
$ . .bashrc
```

Доступ до радног директоријума треба да буде рестриктиван и то требају да имају приступ корисници који су оператори зона. Препорука је да приватни кључеви шифрују (на пример коришћењем `GnuP`) или цео директоријум да се налази на криптованом фајл систему.

Алати BIND9-а за генерисање парова кључева и потписивање ресурсних записа у зони

Алати BIND-а за рад са DNSSEC-ом укључује алате **`dnssec-keygen`** и **`dnssec-signzone`**.

Уколико BIND није инсталиран на систему треба се најпре инсталирати. У Red Hat Enterprise Linux провера дали је пакет инсталиран врши се командом

```
$ rpm -q bind
```

Уколико је инсталиран пакет приказаће се информација о пакету. Ако пакет није инсталиран нећемо добити одговор. Да би инсталирали пакет `bind` треба извршити команду:

```
# yum install bind
```

Целокупно упутство за употребу алата `dnssec-keygen` и `dnssec-signzone` можете наћи у одговарајућем `man` и `info` страницама који се инсталирају заједно са осталим фајловима из пакета `bind`.

Генерисање парова кључева за потписивање кључева (KSK)

За генерисање парова кључева користи се алат **dnssec-keygen** из пакета **bind**.

Генерисани парови кључева чувају се у поддиректоријуму **KSK/** у радном директоријуму **\${DNSSECDIR}**. Пре генерисањ кључева треба одабрати алгоритам којим се генерише пар кључева, хеш алгоритам и дужина криптографског кључа.

Препорука је да се користи RSA алгоритма са јавним кључем, хеш алгоритам SHA-1 и дужина криптографског кључа од 4096 бита. Наводимо пример за генерисање таквих кључева:

```
$ if [ -d ${DNSSECDIR}/KSK/ ] ; then cd ${DNSSECDIR}/KSK/ ; \
  else mkdir -p ${DNSSECDIR}/KSK/ && cd ${DNSSECDIR}/KSK/ ; \
  fi
$ /usr/sbin/dnssec-keygen -f KSK -r /dev/urandom -a RSASHA1 -b 4096 \
  -n ZONE localhost
```

Опција “**-f KSK**” при генерисању означава да се генеришу кључеви за KSK.

Употреба генератора случајних бројева (**/dev/urandom**) је неопходни део у процесу генерисања кључева. Не препоручује се генерисање кључева без употребе извора случајних бројева.

Након генерисања кључева оба фајла се чувају у директоријуму **\${DNSSECDIR}/KSK/**.

Генерисање парова кључева за потписивање ресурсних записа ZSK.

За генерисање парова кључева користи се алат **dnssec-keygen** из пакета **bind**.

ZSK/ у радном директоријуму **\${DNSSECDIR}**. Пре него што се генеришу кључеви одабира се алгоритам за генерисање кључева и хеш алгоритам и дужина криптографског кључа.

Препорука је да се користи RSA алгоритма са јавним кључем, хеш алгоритам SHA-1 и дужина криптографског кључа од 1024 бита. Наводимо пример за генерисање таквих кључева:

```
$ if [ -d ${DNSSECDIR}/ZSK/ ] ; then cd ${DNSSECDIR}/ZSK/ ; \
  else mkdir -p ${DNSSECDIR}/ZSK/ && cd ${DNSSECDIR}/ZSK/ ; \
  fi
$ /usr/sbin/dnssec-keygen -r /dev/urandom -a RSASHA1 -b 1024 \
  -n ZONE localhost
```

Израда шаблона за зону која се потписује

Шаблони зона налазе се у поддиректоријуму **zones/** у радном директоријуму **\${DNSSECDIR}**.

Шаблон зоне израђује се из излазног кода зоне који није у DNSSEC формату тако што се употребом директиве `$include` укључују KSK и ZSK јавни кључеви, објављивање се задаје апсолутном или релативном путањом до фајлова који садрже кључеве.

Пример шаблона зоне, који је припремљен за потписивање:

излазни код зоне:

```
$TTL 86400
@ IN SOA localhost. root.localhost. (
    1997022700 ; Serial
    28800      ; Refresh
    14400      ; Retry
    3600000    ; Expire
    86400 )    ; Minimum
IN NS localhost.

1 IN PTR localhost.
```

укључивање KSK и ZSK јавних кључева у шаблону састављен од излазног кода зоне:

```
$TTL 86400
@ IN SOA localhost. root.localhost. (
    1997022700 ; Serial
    28800      ; Refresh
    14400      ; Retry
    3600000    ; Expire
    86400 )    ; Minimum
IN NS localhost.

1 IN PTR localhost.
  $include "${DNSSECDIR}/KSK/Klocalhost.+005+63675.key"; KSK public key
  $include "${DNSSECDIR}/ZSK/Klocalhost.+005+12347.key"; ZSK public key
```

Готов шаблон се записује као фајл у директоријуму **\${DNSSECDIR}/zones/** тако што му се даје име које описује да се ради о шаблону зоне. Добро је да у имену фигурише име зоне као на пример `localhost.unsigned`.

На крају се проверава синтакса шаблона користећи алат `named-checkzone`. Пример такве провере:

```
$ /usr/sbin/named-checkzone localhost localhost.unsigned
```

У овом примеру localhost је име домена чија зона се налази у фајлу localhost.unsigned. Ако провера прође успешно алат ће вратити ОК. Са овим израда шаблона је завршена. Одатле на даље свака промена додавање, брисање записа из зоне се ради директно у шаблону.

Подписивање шаблона зоне

Приликом подписивања зонског шаблона неопходно је задати валидност електронског потписа зоне. Крајњи датум и време електронског потписа се задаје као параметар алата dnssec-signzone .

Да би се потписао шаблон зоне неопходни су KSK и ZSK парови кључева као и име домена који се потписује параметром -o.

```
$ /usr/sbin/dnssec-signzone -r /dev/urandom \  
-o localhost -f ${DNSSECDIR}/zones/localhost.signed \  
-k ${DNSSECDIR}/KSK/Klocalhost.+005+63675.key \  
${DNSSECDIR}/zones/localhost.unsigned \  
${DNSSECDIR}/ZSK/Klocalhost.+005+12347.key
```

Приликом извршење команде у процесу потписивања ради се следеће. Читају се парови кључева KSK и ZSK. Са опцијом -k задаје се путања до фајла који садржи јавни кључ KSK а на крају команде се задаје путања до фајла који садржи јавни кључ ZSK. Иако су кроз команду задане путање до фајлова који садрже јавне кључеве подразумева се да се у истом директоријуму налазе и фајлови који садрже приватне кључеве са екстензијом .private. Након параметра -o у командној линији задаје се име домена у овом случају је localhost. Употребом параметра -f указује се на фајл у коме ће се бити снимљени електронски потписани записи. Додавање екстензије .private није неопходно. Фајл са шаблониме зоне налази се на путањи \${DNSSECDIR}/zones/localhost.unsigned . Путања се додаје на крају као параметар непосредно пре фајла са јавним кључем за KSK.

Потписани ресурсни записи зоне домена наћи ће се у фајлу \${DNSSECDIR}/zones/localhost.signed. Овај фајл се задаје за изчитавање у конфигурацији зоне BIND-а. На пример:

```
zone "localhost" {  
    type master;  
    file "zones/localhost.signed";  
};
```

Подразумевајуће трајање електронског потписа над ресурсним записима траје месец дана. Међутим могуће је задавање кроз параметре алата **dnssec-signzone** трајање електронског потписа, тако на пример `-s` параметар се користи као параметар за почетак важења и `-e` за крајње време трајања. Пример са параметрима за трајање валидности електронског потписа:

```
$ /usr/sbin/dnssec-signzone -r /dev/urandom -s 20160428103959 -e 20160623234540 \
-o localhost -f ${DNSSECDIR}/zones/localhost.signed \
-k ${DNSSECDIR}/KSK/Klocalhost.+005+63675.key \
${DNSSECDIR}/zones/localhost.unsigned \
${DNSSECDIR}/ZSK/Klocalhost.+005+12347.key
```

У овом примеру стартно време валидности електронског потписа домена `localhost` је 20160428103959 28 април 2016 године 10 сати 39 минута и 59 секунди. Рок трајања валидности сертификата ресурсних записа зоне домена `localhost` је 20160623234540 – 23 јуни 2016 23 сати 45 минута и 40 секунди.

Могуће је и релативно задавање времена трајања. На пример `-e +86400` потпис ће бити валидан до сега+86400. Разуме се резултат је опет апсолутно време али не тражи се време почетка само време трајања валидности. Исто тако може да се зада релативно и време почетка трајања електронског потписа на пример `-s +86400` генерисаће потписивање са почетком валидности 86400 секунди након потписивања.

Креирање DS ресурсних записа

У току потписивања ресурсних записа креирају се одговарајући DS записи. Они се налазе у директоријуму у коме је извршено потписивање и налазе се у два фајла које садрже `dsset` у свом имену. Пример извршења потписивања користећи команду линију

```
$ /usr/sbin/dnssec-signzone -r /dev/urandom -s 20070428103959 -e 20070623234540 \
-o localhost -f ${DNSSECDIR}/zones/localhost.signed \
-k ${DNSSECDIR}/KSK/Klocalhost.+005+63675.key \
${DNSSECDIR}/zones/localhost.unsigned \
${DNSSECDIR}/ZSK/Klocalhost.+005+12347.key
```

У директоријуму `${DNSSECDIR}/zones/` креираће се фајл `dsset-localhost`. Он ће садржати одговарајуће DS записе.

Подешавање BIND9 за употребу DNSSEC

Да би се користили потписани ресурси у BIND9 неопходно је да се изврше одговарајућа подешавања у конфигурационом фајлу `named.conf`.

У секцији `options` овог фајла задаје се директива за употребу DNSSEC од стране сервиса `named`:

```
options {  
    ...  
    dnssec-enable yes;  
    ...  
};
```

Ради лагодности праћења могуће је креирати канал за локове догађаја при опслуживању DNSSEC захтева употребом категорија. Пример **`named.conf`** фајла може да буде следећи

```
logging {  
    channel dnssec_log {  
        file "/var/log/named/dnssec.log" versions 16 size 256k;  
        print-time yes;  
        print-category yes;  
        print-severity yes;  
        severity debug 10;  
    };  
    category dnssec { dnssec_log ; };  
};
```

Механизам за промену ZSK парова кључева

Када се употписивању зоне користе два парова кључева, кључеви се деле по намени на - ZSK и KSK, ZSK пар кључева је са мањом дужином приватног кључа, зато се користи за краћи временски период (има кратко време живљења), док KSK пар кључева је са већом дужином приватног кључа, зато што се користи за дужи период времена (карактерисе се дужим периодом живота). Ако се прати упутство о временском трајању кључева онда би требало у границама трајања једног пара кључева KSK да се измењају висе парова кључева за ZSK који треба један друго да замењују. Када један пар кључева ZSK буде изведен ван употребе следи да се не користи за поновно потписивање ресурсних записа зоне (најбоље је да се уништи криптографски кључ да би се онемогућило поновно потписивање корисћењем истог).

Процес периодичне замене парова кључева ZSK назива се "key rollover".

Овако изгледа процес који доводи до замене парова кључева ZSK

1. генерисе се нови пар кључева ZSK;

2. јавни кључ новог пара ZSK уводи се у зони под формом DNSKEY ресурсног записа.
3. Зона се потписује приватним кључем из новог пара ZSK кључева;
4. након неког времена (објасњење је испод), DNSKEY запис за стари пар ZSK кључева се избацује из зоне и врси се предпописивање записа унутар зоне;

Ако се узме у обзир ресурсни запис (RR - Resource Record), на пример А запис, са вредностима параметра TTL једнако 86400 секунди, који је електронски потписан употребом DNSSEC. Када овај запис буде електронски потписан, у зони домена се генерише одговарајући RRSIG запис. По истом принципу за сваки ресурсни запис (RR) у зони домена, постоји одговарајући RRSIG запис, у коме се садржи електронски потпис над RR записом. Време живота сваког RRSIG записа је исто као и време трајања ресурсног записа, за кога је генерисан и у овом примеру време трајања ће бити 86400 секунди. Када један кеширајући сервер имена, који подржава проверу аутентичности ресурсних записа употребом DNSSEC, извуче ресурсни запис и одговарајући RRSIG запис, он складишти оба записа у својој бази. Да би верификовао валидност електронског потписа RRSIG записа, кеширајућем серверу неопходни су DNSKEY записи из зоне домена, из кога су извућени RR и RRSIG записи. Следи извлачење свих DNSKEY записа из зоне. Они се исто складиште у кешу сервера. Након складиштења сваком ресурсном запису у кешу бројач започиње одбројавање времена у секундама и када време достигне време задато параметром TTL сервер брише одговарајући запис.

Ако је TTL кеширање RR и RRSIG записа једнако 86400 секунди, а TTL кеширање DNSKEY записа 3600 секунди, онда је јасно, да време живота RR и RRSIG записа је веће од времена живота DNSKEY записа, који служе за проверу електронског потписа над RR. Ако неко промени DNSKEY записе за ZSK парове у зони, тако што уклони старе и постави нове и потпише записе у зони, појавиће се ситуација при којој DNS сервери широм Интернета имаће кеширане RRSIG записе, чији електронски потпис није могуће верификовати, зато што се они могу верификовати једино користећи стари јавни кључ, који је већ уклоњен са уклањањем старог DNSKEY записа.

Због тога DNSKEY запис, који садржи стари јавни кључ из старог ZSK парова кључева, неопходно је да се чува у зони и након потписивања новим ZSK паром толико да покрије време живота RRSIG записа из зоне са најдужим временом трајања толкова време. Након тога може се уклонити. Ово мора да зна сваки оператор DNSSEC базиране зоне домена.

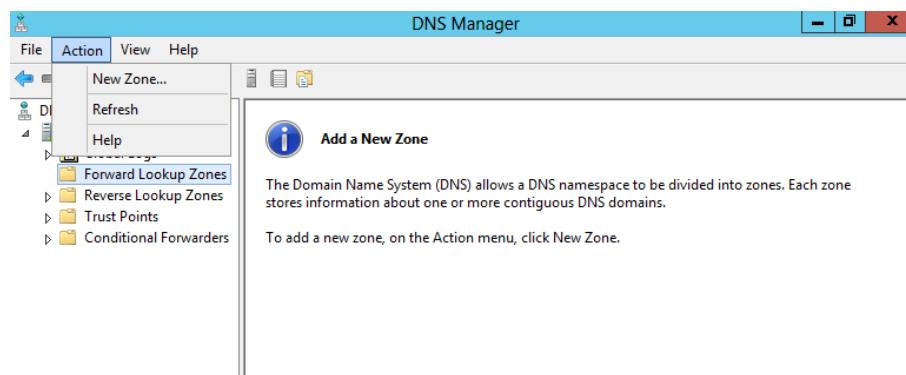
Препорука је да вредност TTL за DNSKEY треба да буде једнака максималној вредности које има ресурсни запис у зони. Ако је време изнад 3600 секунди ово крије опасност. Она

се састоји у следећем. Шта би се десило ако се приватни кључ ZSK парова кључева буде компромитован (ово је вероватно имајући у виду дужину кључа). У том случају неко ће моћи да потписује злонамерно генерисане ресурсне записе и са њима да зарази кеш сервере по целом Интернету. Чак и да администратор зоне сазна да је дошло до компромитовања кључа и да уведе нови ZSK пар кључева на кеш серверима остаје кеширан стари DNSKEY запис који садржи јавни кључ већ компромитованог пара кључева и наставиће да валидира злонамерно генерисане ресурсне записе. Док кеширани DNSKEY запис не достигне крај живота у кешу кеширајућег сервера његови клијенти могу бити на мети хакера.

Због тога вредност TTL-а DNSKEY записа не сме да буде веома висока. Максимална вредност треба да буде 3600 секунди а минимална нула али последње би довело до повећаног саобраћаја DNS сервера и оптерећење за аутентификоване сервере зона.

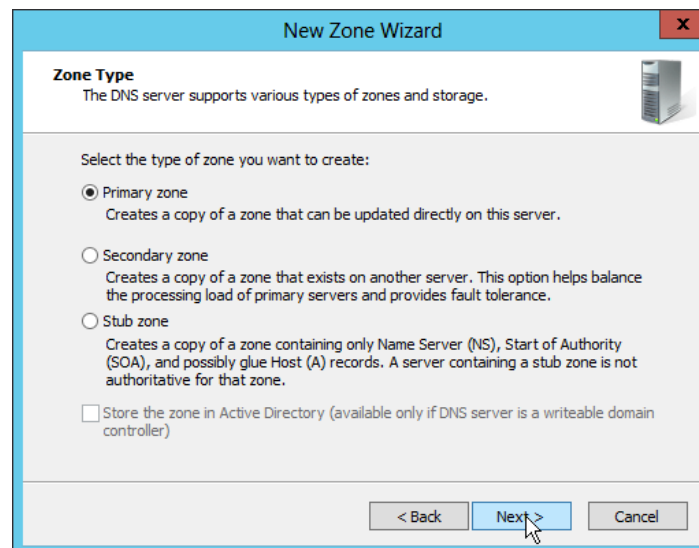
Имплементација DNSSEC-а у Windows Server 2012

Windows Server 2012 подржава DNSSEC и дато је кориснику могућност да га користи уз стандардну DNS ролу. Најпре неопходно инсталирати DNS ролу са подразумевајућим подешавањима. Унутар DNS Manager-а из Action менија треба одабрати New Zone...



Слика 8.

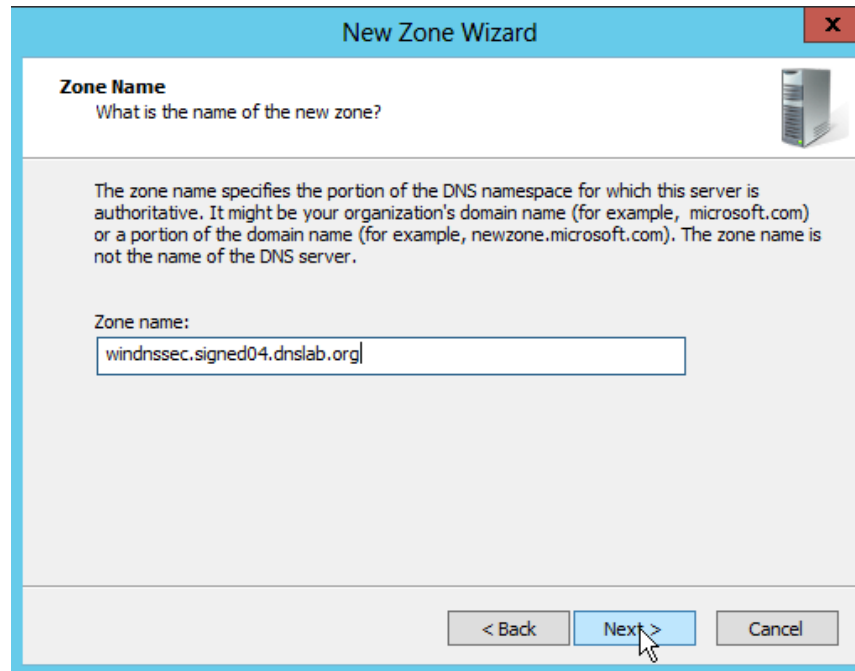
у новом прозору треба одабрати Primary zone и кликнути на Next



Слика 9.

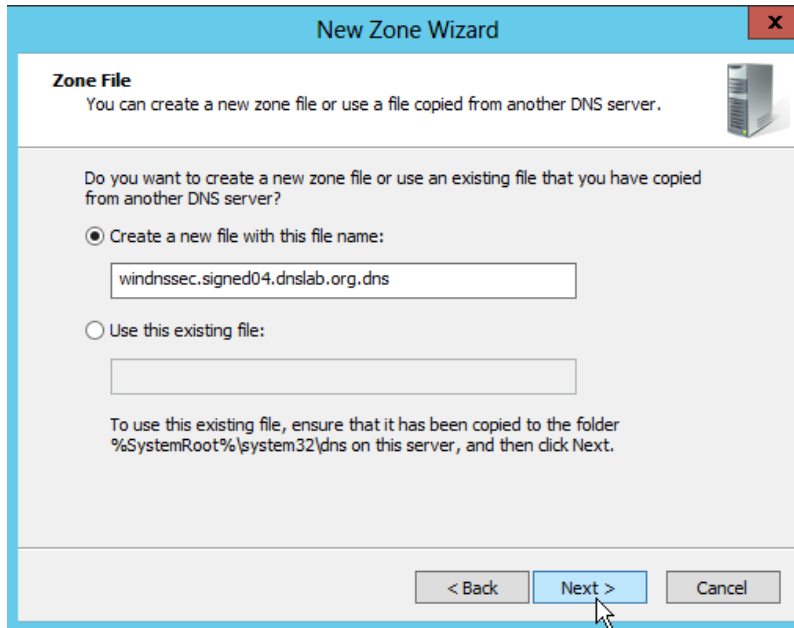
Parent зона се хостује на bind серверу и ради са DNSSEC chain-of-trust to the trust-anchor of the root-zone.

У следећем прозору у пољу Zone Name треба уписати име зоне и наставити wizard кликом на Next.



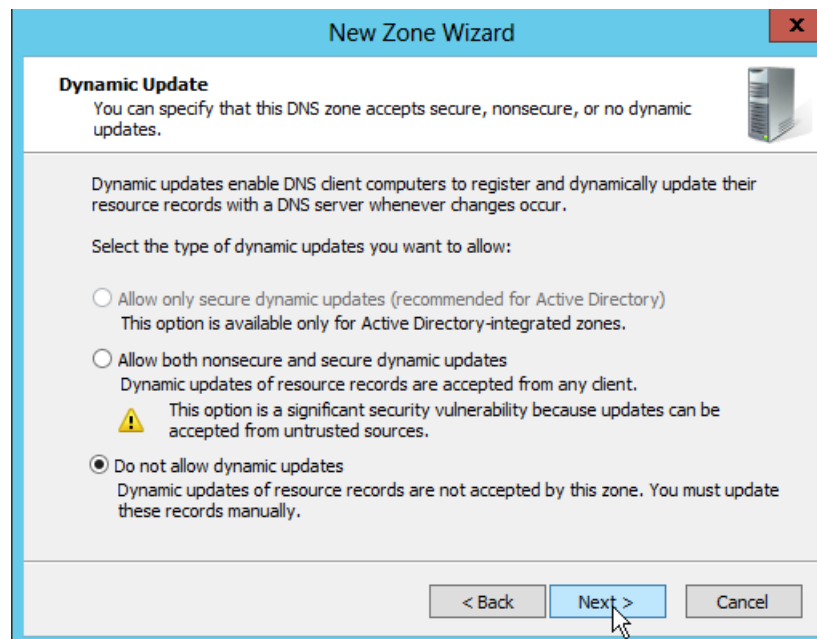
Слика 10.

прихватајући подразумевана **подешавања** кликом на Next, фајл зоне се смешта у директоријуму `"C:\Windows\System32\dns"`



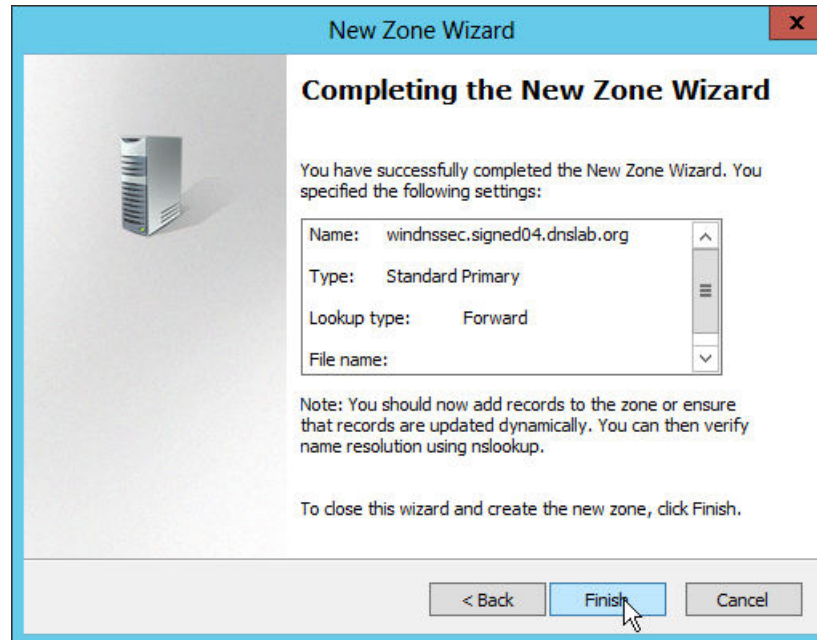
Слика 11.

У следећем кораку треба одабрати “Do not allow dynamic updates” и одабрати Next јер се креира статичка зона



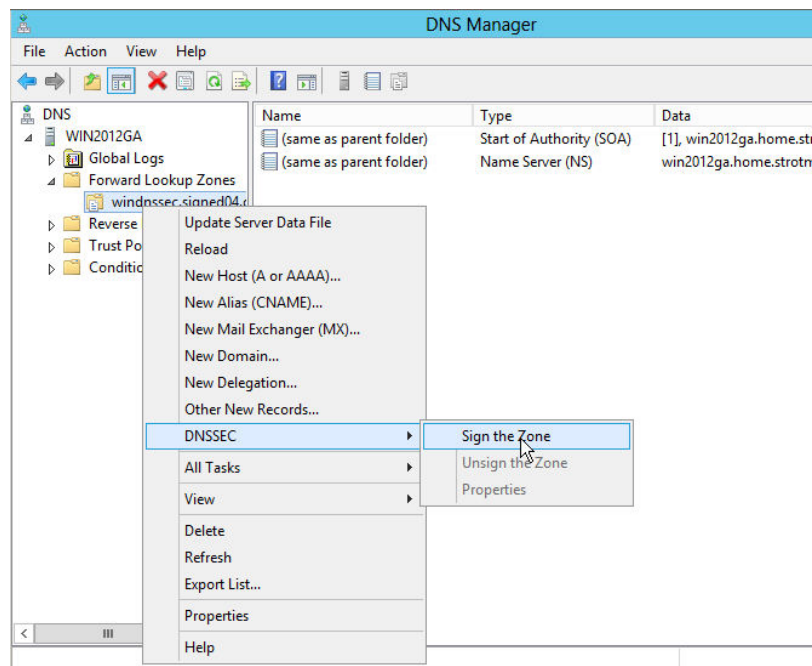
Слика 12.

Кликом на Finish креира се зона која није електронски потписана.



Слика 13.

Потписивање зоне се ради тако што се десним кликом на зону одабере DNSSEC->Sign the zone како би порекунули wizard за потписивање зоне. (Слика...)



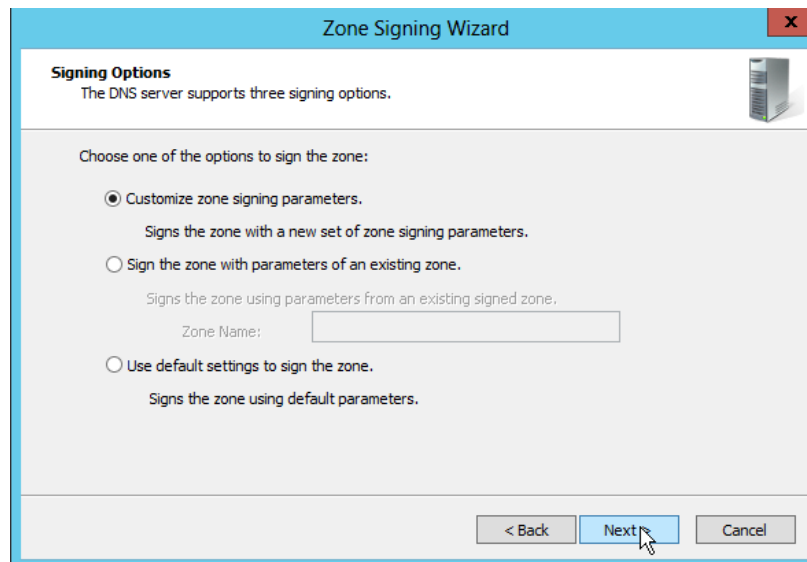
Слика 14.

у следећем прозору одабрати Next



Слика 15.

у наредном прозору Signing Options треба одабрати Customize zone signing parameters и кликнути на Next (Слика 16)



Слика 16.

У следећем кораку кликом на Next у прозору Key Signing Key



Слика 17.

долази се до прозора New Keys Signing Key (Слика 18) где се подешавају параметри за генрисање новог KSK кључа задржавајући подразумевана подешавања осим подешавања за дужину кључа на максималну вредност 4096 бита (подразмевана вредност је 2048). Подразмевани алгоритам је RSASHA256. DNSKEY потпис је валидан седам дана rollover frequency је 755 дана. Могуће је креирати више KSK кључева али за већину случајева потребан је само један Windows Server 2012 DNS сервер ће креирати још један додатни “emergency rollover” KSK кључ аутоматски. Неопходно је потврдити са ОК.

New Key Signing Key (KSK)

Guid: {00000000-0000-0000-0000-000000000000}

Key Generation

☒ Generate new signing keys.
☐ Use pre-generated keys

Use this key as active key:
Use this key as standby key:

Key Properties

Cryptographic algorithm: RSA/SHA-256
Key length (Bits): 4096
Select a key storage provider to generate and store keys: Microsoft Software Key Storage Prov
DNSKEY RRSET signature validity period (hours): 168
☐ Replicate this private key to all DNS servers authoritative for this zone.
(Applicable only to AD integrated zones)

Key Rollover

☒ Enable automatic rollover
Rollover frequency (days): 755
Delay the first rollover by (days): 0

OK Cancel

Слика 18.

У следећем прозору (Слика 19) треба кликнути на Next

Zone Signing Wizard

Key Signing Key (KSK)
Configure one or more KSKs

Configure parameters for at least one KSK. A maximum of three KSKs can be specified for each of the available cryptographic algorithms.

Algorithm	Key length	KSP	Replication	Rollover state	Initial rollover o...
RSA/SHA-256	4096	Microsoft Softw...	Disabled	Enabled	0

Add Edit Remove

< Back Next > Cancel

Слика 19.

Следеће је подешавање ZSK-а подразумевајући параметри су Rollover frequency 90 дана и дужина кључа 1024 бита. Потребно је у прозору Zone Signing Key кликнути на Next (Слика 20).



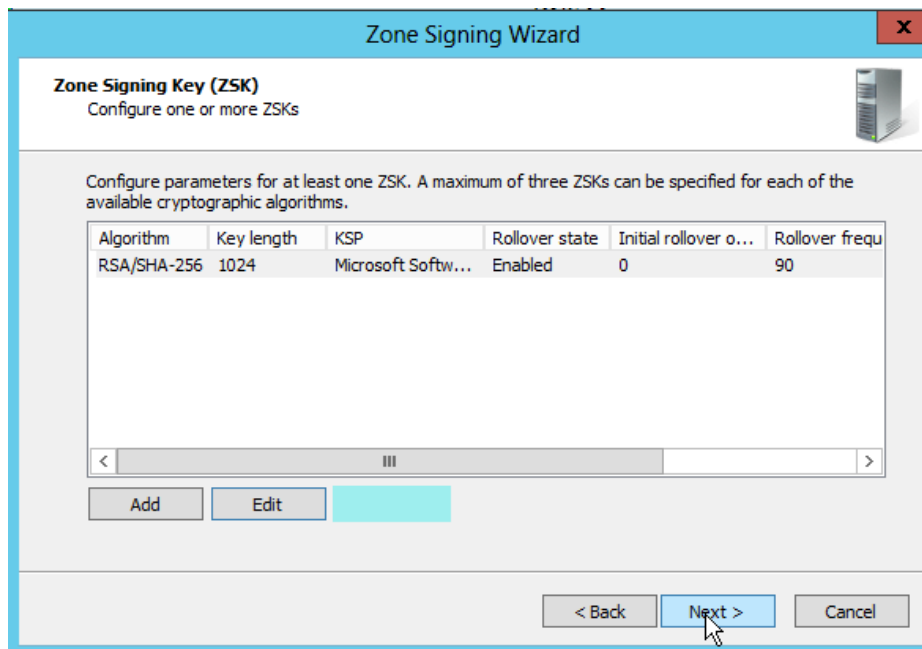
Слика 20.

У прозору New Zone Signing Key треба потврдити са OK. (Слика 21).



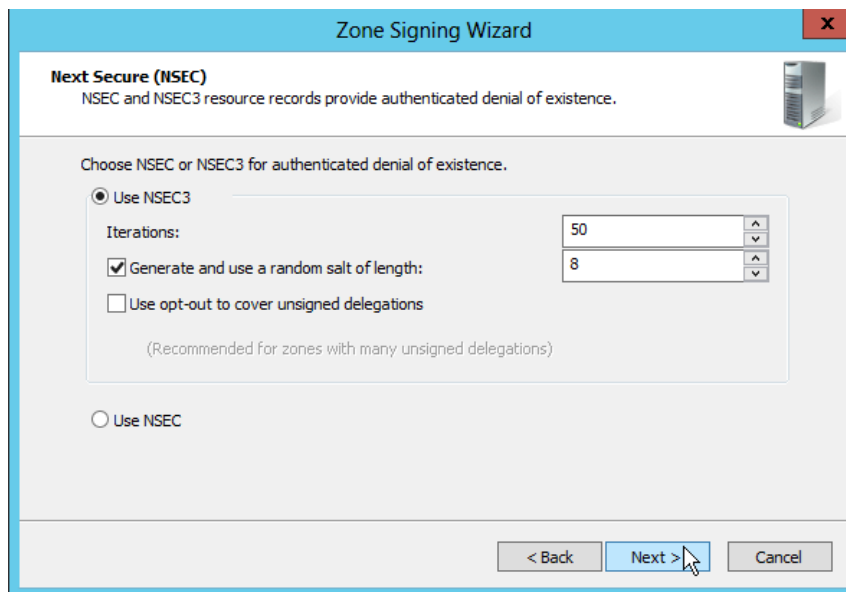
Слика 21.

, у наредном кораку Zone Signing Key треба кликнути на Next (Слика 22)



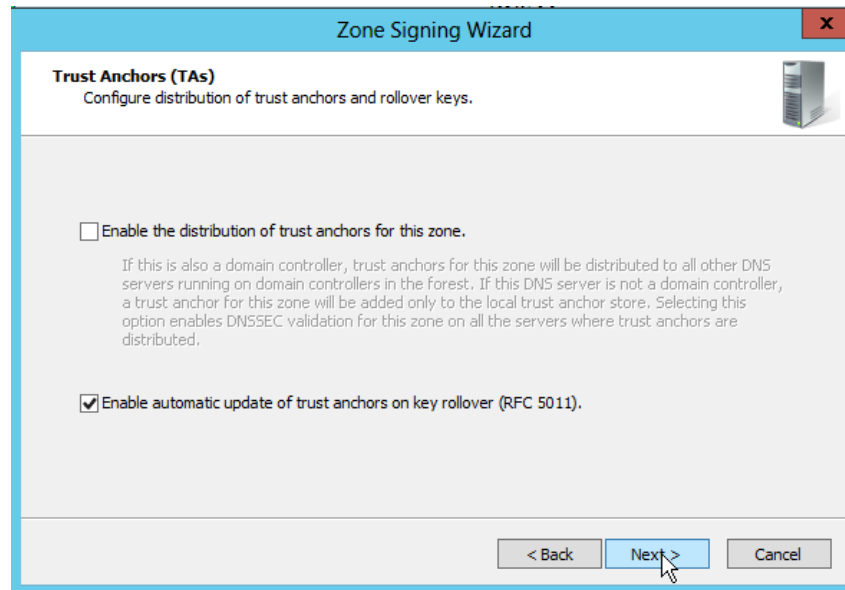
Слика 22.

За authenticated denial of existence узима се NSEC3 који је подразумевани за Windows Server 2012, број итератора је 50, salt је random вредност и величина је 8 бајтова, и не користи се opt-out to cover unsigned delegations.



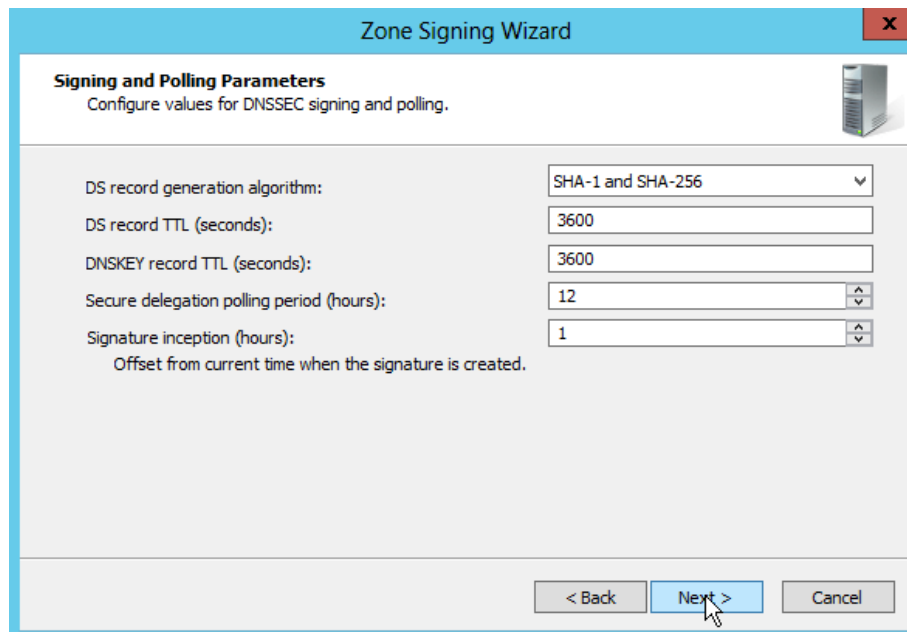
Слика 23.

Треба омогућити automatic update of trust anchors on key rollover који је по стандарду RFC 5011, (Слика 24) и потврдити са Next.



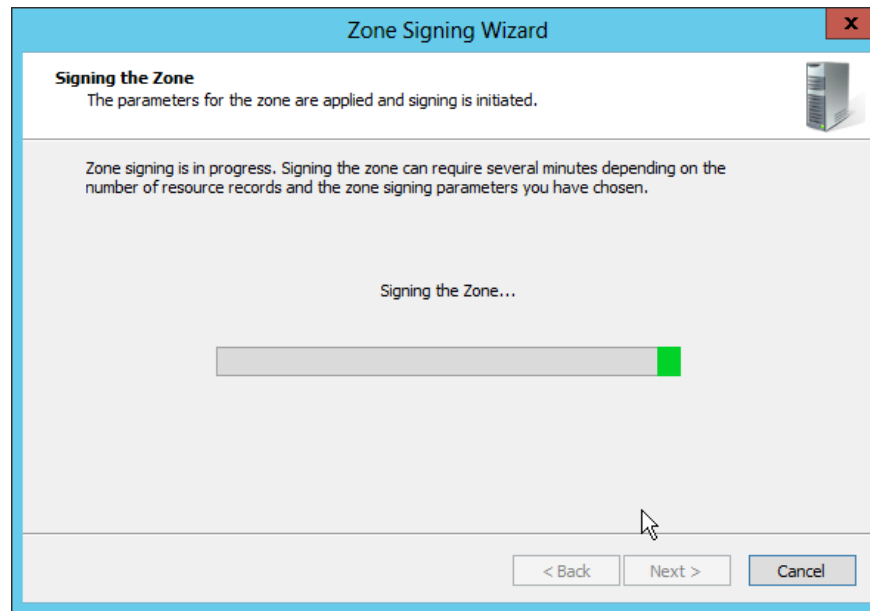
Слика 24.

DS запис се генерише користећи оба SHA-1 и SHA-256, потребно је само кликнути на Next (Слика 25)



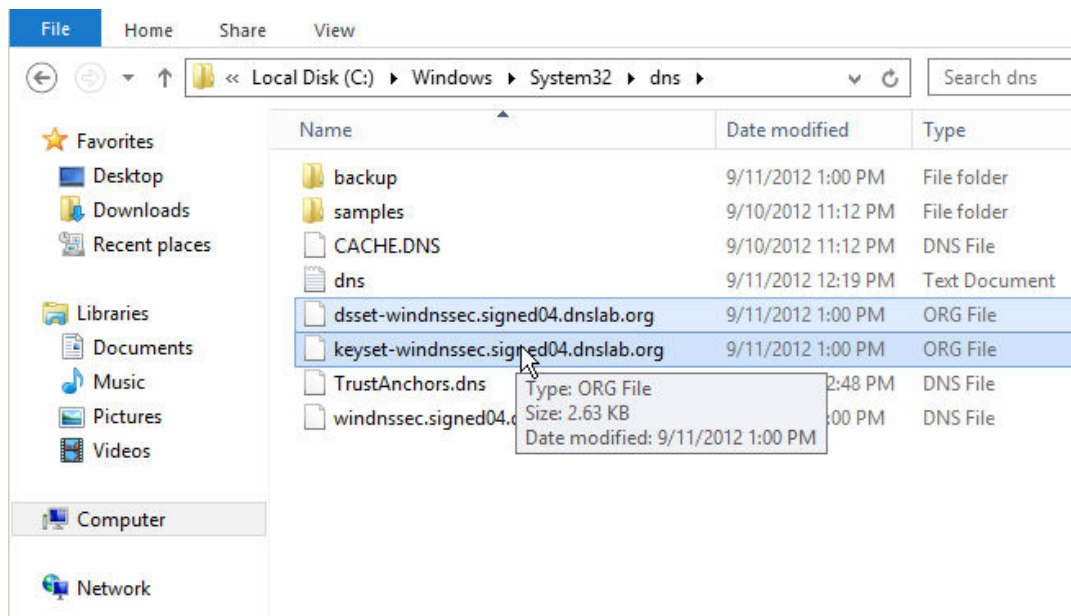
Слика 25.

Након целог wizard зона се потписује (Слика 26) за које је потребно извесно време.



Слика 26.

Када се зона потпише креирају се два фајла унутар DNS фолдера ds-set и key-set у путањи C:\windows\system32\dns (Слика 27).



Слика 27.

Након што се креира А запис он се аутоматски потпише током креирања.

Када се DS и NS запис додају у родитељској зони, нова зона хостована на Windows Server 2012 серверу може да валидира као на слици 28.

```
# dig www.windssec.signed04.dnslab.org a +dnssec +multi

; <>> DiG 9.9.1-P2 <>> www.windssec.signed04.dnslab.org a +dnssec +multi
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 30532
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.windssec.signed04.dnslab.org. IN A

;; ANSWER SECTION:
www.windssec.signed04.dnslab.org. 3600 IN A 192.0.2.10
www.windssec.signed04.dnslab.org. 3600 IN RRSIG A 8 5 3600 (
    20120921134910 20120911124910 20011 windssec.signed04.dnslab.org.
    u24KXaMM+a4ysMlhNvAUvuiuxNrUVyHs6XvAAX0hQmAS
    Jt6cbPhM09QkwRV20WstVukqqVHug00U70GmzGSpfsAi
    3i0cQ4GLK7S6bH091SuutfH1Ezxt2CPEW3pqeyaBbZLZ
    kP53NQ7o/nMuZQmEBv/NqRvBvPuHhpjsx4RV+tc= )

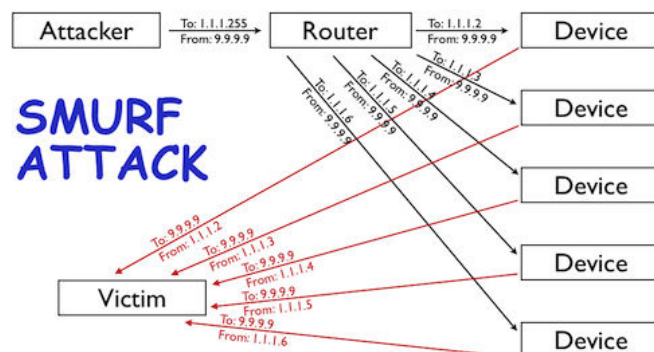
;; Query time: 867 msec
;; SERVER: 192.168.53.251#53(192.168.53.251)
;; WHEN: Tue Sep 11 14:08:00 2012
;; MSG SIZE rcvd: 267
```

Слика 28

Закључак

DNSSEC драстично унапређује сигурност Интернета и система који се ослањају на њега. DNSSEC чини DNS проверљивим, он омогућава да власници домена потписују своје DNS записе и да клијенти могу проверити њихову аутентичност. Заштита домена користећи DNSSEC и применом валидирајућих разрешајућа на клијентској страни елиминише доста DNS spoofing напада и велики опсег MITM напада.

Међутим DNSSEC може да послужи као PKI за друге протоколе као што су HTTPS и TCP. Не постоје други предлози који нуде оно што нуди DNSSEC а то је метода за сигурну делегацију домена. То значи да root authority може декларисати важеће јавне кључеве за домен и за власнике домена декларисати валидна јавна кључева за било који поддомен. Три најчешћа предлога који се наводе као алтернатива DNSSEC-а су DNSCurve, Key pinning и triangulation не нуде основне функције које нуди DNSSEC. Креатори ових алтернативних протокола критикују DNSSEC зато што је он државно контролисани PKI. Постоје сумње да је DNSSEC криптографски слаб, међутим неопходно је доста времена и средстава како би се он компромитовао а такође постоје тежње да се унапреди преласком на савременије алгоритме као што је ECC. Поставља се питање дали DNSSEC производи више проблема него што их решава. Комплексност сигурносног протокола DNSSEC-а је још једна црна тачка против његовог увођења. Ефективност DNS Amplification напада је такође повећана, разлог за то је што је величина одговора код DNSSEC-а доста већа. DNS Amplification напад је случај Amplification напада који се изворно зове Smurf Attack. На слици 28 приказан је случај Smurf напада на коме нападач шаље ICMP захтев са дестинационом бродкаст адресом кроз рутер који је подешен да прослеђује ICMP пакете на другу страну. Изворна адреса је spoof-ана лажном адресом која заправо представља адресу жртве тако да сви уређаји који се налазе са друге стране рутера шаљу одговор жртви.



Слика 28.

Applification напад мора да задовољава два критеријума и то:

- 1) да је изворна адреса spoof-ана лажном адресом заправо адресом жртве и
- 2) да је одговор већи од упита по велићини пакета

Оба критеријума задовољава DNS а поготово DNSSEC на пример упит облика:

dig ANY isc.org @x.x.x.x , даје већи одговор облика:

```
<>> DiG 9.7.3 <>> ANY isc.org @x.x.x.x
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 5147
;; flags: qr rd ra: QUERY: 1, ANSWER: 27, AUTHORITY: 4, ADDITIONAL: 5

;; QUESTION SECTION:
isc.org.                IN          ANY

;; ANSWER SECTION:
isc.org.                4084        IN          SOA         ns-int.isc.org. hostmaster.isc.org. 2012102700 7200 3600 24796800 3600
isc.org.                4084        IN          A           149.20.64.42
isc.org.                4084        IN          MX          10 mx.baol.isc.org.
isc.org.                4084        IN          MX          10 mx.ams1.isc.org.
isc.org.                4084        IN          TXT         "v=spf1 a mx id4:204.152.184.0/21 id4:149.20.0.0/16 id6:2001:04F8::0/32 id6:2001:500:60::65/128"
"all"
isc.org.                4084        IN          TXT         "$Id: isc.org.v 1.1724 2012-10-23 00:36:09 bind Exo $"
isc.org.                4084        IN          AAAA        2001:4f8:0:2::d
isc.org.                4084        IN          NAPTR       20 0 "S" "SIP+D2U" "" sip. udb.isc.org.
isc.org.                484         IN          NSEC        kerberos.isc.org. A NS SOA MX TXT AAAA NAPTR RRSIG NSEC DNSKEY SPF
isc.org.                4084        IN          DNSKEY      256 3 5 BOEAAAAB2F1v2HwzCCE9vNsKfk0K8vd4EBwizNT9K06WYX10oxEL4eOJ
a8W27oO+9oNIP8Jv6zd010uCB/N0fxIvL3371xbednFaoECISFDZa6Hw iUiozveSsw0=
isc.org.                4084        IN          DNSKEY      257 3 5 BEAAAAAchHODBrhObtohaa2wOUaEO5t4DtUHcoMVFu2hWLDmvoOMRX1Gr
u50WIL8ZRI6K7BsYVM/LDx5R1NbPCLv+vT+U8eXEmJ020iISIUlaov3
47cBE1zmmz+4LJ0A0da9ChK3A254T515aNIcWceB6/2+2E63/2ZrOz
KOOedS39Z7SDmsn2eA0FKtOovA6LXsG2w+1xmW3oA81VUoEf/rzeC/bB
vENS070aEFTd
isc.org.                4084        IN          SPF         "v=spf1 a mx id4:204.152.184.0/21 id4:149.20.0.0/16 id6:2001:04F8::0/32 id6:2001:500:60::65/128"
"all"
isc.org.                484         IN          RRSIG       NS 5 2 7200 20121125230752 20121026230752 4442 isc.org.
oFenV69Pn+/JnnltGPUZOnYzo1YGolMhS/SZKnlovMbzt+T2r/2v+X1i
UHDAXMmbok529fIv3MvA/ZwR9PFkXurcfio5fnoEEaavNS0bKxomw48dc
isc.org.                484         IN          RRSIG       SOA 5 2 7200 20121125230752 20121026230752 4442 isc.org.
S+DLHzE/8wObnS170aeMyoKvG1IuKARVlxmscsc+MX6DO/J1xdK9xGac
oCKEvvuiumOP1KCN9OX7ds4siiTirEOGHCaamEoRJoVxoCsoldBjRrR
hKk=
isc.org.                484         IN          RRSIG       MX 5 2 7200 20121125230752 20121026230752 4442 isc.org.
VFOpWRPvulIT8VsIdXKMbMRJTyddaoGoOIKJzKJs/6ZrxmbJtmAxaEu
zNO3XNIdidV6z16ELtCVDr3ISiWdZHyB/CF9oNno1FAP2io1YSwiwsb
isc.org.                484         IN          RRSIG       TXT 5 2 7200 20121125230752 20121026230752 4442 isc.org.
O18hVCZf3iYL9eO8w4Tl9HlWKP3CKXORFed89xeh5TR3KI3tOTKsSeI
k9bbshvbYtXOF8xnv/FCIR5c6NvELmvvu4xeOoSwIoo02zvIEFFP9deR
isc.org.                484         IN          RRSIG       AAAA 5 2 7200 20121125230752 20121026230752 4442 isc.org.
hutAcro0NBmVku/m+21F8sgIvYVWORTu/utIn8KsFIWQwM20MGa5C9
w92eBh1nNdcvT0iF8m1Sldx5/hSgKn8EAscKfo5EM0o5YDFellisTauA
isc.org.                484         IN          RRSIG       NAPTR 5 2 7200 20121125230752 20121026230752 4442 isc.org.
ZD14oEHR7iVXn5uJUn6X9Lvt5Pa7Y7TEW94hNan9Lm3Tlnko11AeZ1OU
XOTaUWHBF2Cs0CvfoRkLVA15AY6P2hb/UU6hV8Go0OFvmmEKJOnxPFw
isc.org.                484         IN          RRSIG       NSEC 5 2 3600 20121125230752 20121026230752 4442 isc.org.
rY1h2oArvM045v3bMY0wJhdhJOCofKXLeRLk20LauImVtvu7uair7ib
P10rsnzC61larXLWNBFlMz02Aza6SSir2OF0bnmK6PLOCdmaVAPrVJOs
isc.org.                484         IN          RRSIG       DNSKEY 5 2 7200 20121125230126 20121026230126 4442 isc.org.
10S2MFovHB3wOhv21PozE/IOABM/eDDCV2D7dJ3AuOwi1A3sbYO29Xud
L2192kx8ZdEhXKiE6om+cFVBHLLMxGKLDVnfflVlG0115YrIvv41iw
isc.org.                484         IN          RRSIG       h0A=
1kKwW+FFW01E222KXo+bitG1rrnG1XoP17b1OT0ZHEladv7F6kEavv1
oAEhmEmezKn901EAOCT0Z4nU50smuYl0xcQKfDbW0ohLdu+/8+d6LIS
YG02i1Jv9sbsbEDHT7C0c05Gg+AlAv5tNN5ao7OHMa0Ve+Ux0nH7JU0Vn
isc.org.                484         IN          RRSIG       SPF 5 2 7200 20121125230752 20121026230752 4442 isc.org.
IB/bo9HP16aZoPFkz7bXbXK7bTbF13HNOloohrouMSBfcMfmJgHxKvD
9Hmbnko7Pe+Lu5AD0s6+E9aav3w0OounBaUkKfSc8B1iIGRkCy8GhC
isc.org.                484         IN          RRSIG       A 5 2 7200 20121125230752 20121026230752 4442 isc.org.
VLS+ao95Di8kZ5kL8vCBRR0L2/M9UwtbVXK18ciolftfMWC9WJza
hWbK7f0S0e4LujZvEoXFEKf16CnVvZCT1TUh2TNDmRasoxrvrOoGePwh
isc.org.                4084        IN          NS          ns.isc.afalias-nst.info.
isc.org.                4084        IN          NS          ams.sns-db.isc.org.
isc.org.                4084        IN          NS          ord.sns-db.isc.org.
isc.org.                4084        IN          NS          sfba.sns-db.isc.org.

;; AUTHORITY SECTION:
isc.org.                4084        IN          NS          ns.isc.afalias-nst.info.
isc.org.                4084        IN          NS          ams.sns-db.isc.org.
isc.org.                4084        IN          NS          ord.sns-db.isc.org.
isc.org.                4084        IN          NS          sfba.sns-db.isc.org.

;; ADDITIONAL SECTION:
mx.ams1.isc.org.        484         IN          A           199.6.1.65
mx.ams1.isc.org.        484         IN          AAAA        2001:500:60::65
mx.baol.isc.org.        484         IN          A           149.20.64.53
mx.baol.isc.org.        484         IN          AAAA        2001:4f8:0:2::2b
sip. udb.isc.org.        4084        IN          SRV         0 1 5060 asterisk.isc.org.

;; Query time: 176 msec
;; SERVER: x.x.x.x#53(x.x.x.x)
;; WHEN: Tue Oct 30 01:14:32 2012
;; MSG SIZE rcvd: 3223
```

Слика 29

У овом примеру велићина упита је 64 бајта а одговор 3223 бајта што представља знатно повећава оптерећење линка жртве. Проблем је у томе што многи администратори остављају подразумевајућу конфигурацију DNS сервиса те он одговара на упите свих клијената не само неке организације или фирме већ и на кориснике који се налазе на

Интернету. Нападач скенирањем Интернета долази до таквих јавних DNS сервера а затим их користи их за своје нападе коришћењем своје бот мреже.

Литература

[1] <https://www.icann.org/resources/pages/dnssec-qa-2014-01-29-en>

- [2] <https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/>
- [3] http://strotmann.de/roller/dnsworkshop/entry/dnssec_signing_a_zone_with
- [4] https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions