OULUN AMMATTIKORKEAKOULU

Henri Siltakoski

Domain Name System Security Extensions järjestelmänvalvojan näkökulmasta

Domain Name System Security Extensions järjestelmänvalvojan näkökulmasta

Henri Siltakoski
Opinnäytetyö
Kevät 2016
Tietojenkäsittely
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittelyn tutkinto-ohjelma, Järjestelmäasiantuntemuksen suuntautumisvaihtoehto

---

Tekijä(t): Henri Siltakoski
Opinnäytetyön nimi: Domain Name System Security Extensions järjestelmänvalvojan näkökulmasta
Työn ohjaaja: Risto Hinkka
Työn valmistumislukukausi- ja vuosi: Kevät 2016 Sivumäärä: 33 + 4

Verkkopalveluiden ylläpitäjät eivät ole välttämättä tietoisia verkkotunnuksiin liittyvästä tietoturvallisuudesta. Tämän opinnäytetyön tarkoituksena on tutkia nimipalvelujärjestelmän tietoturvaominaisuutta nimeltään Domain Name System Security Extensions. Työ on kirjoitettu järjestelmänvalvojan näkökulmasta. Siinä käsitellään miten nimipalvelujärjestelmän tietoturvaominaisuus otetaan käyttöön eri ympäristöissä ja miten se vaikuttaa nimikyselyyn testiympäristössä.

Työssä on käyty läpi vaiheet, joilla on saatu aikaan toimiva Domain Name System Security Extensions ominaisuuden sisältävä nimipalvelujärjestelmä Bind-ohjelmalla Linux-palvelinkäyttöjärjestelmällä. Työssä myös sen tietoturvaominaisuuden käyttöönotto Windows Palvelin 2012 ympäristössä. Lisäksi sen toimivuus on testattu väärennettyjen nimikyselyjen vastauksien ehkäisemisen kannalta.

Opinnäytetyössä on käytetty vain verkkolähteitä. Ensisijaisesti tietopohjana on hyödynnetty Internet Engineering Task Forcen request for comments dokumentteja. Lopputuloksena opinnäytetyössä on tarkasteltu käyttöönotetun järjestelmän tehokkuutta nimipalvelun Cache Poisoning-hyökkäyksen estämisen kannalta. Työn lopussa on pohdittu miten opinnäytetyössä mainitut asiat vaikuttavat internettiin.

Asiasanat: nimipalvelujärjestelmä, DNS, tietoturvallisuus, DNSSEC, palvelin, infrastruktuuri

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Business Information Systems, Computer Systems Expertise

---

Author(s): Henri Siltakoski
Title of thesis: Domain Name System Security Extensions from Administrator's Point of View
Supervisor(s): Risto Hinkka
Term and year when the thesis was submitted: Spring 2016 Number of pages: 33 + 4

The purpose of this thesis is to investigate security extensions of the domain name system. It is written it from system administrator's point of view. It deals with how Domain Name System security extensions are implemented in various systems and how they affect name resolution in the testing environment.

The thesis describes the steps used to implement working security extensions in Domain Name System server Bind in Linux operating system, as well as on Windows Server 2012. Additionally the functionality was tested to prevent false answers to name resolution requests.

The thesis uses online sources. The primary source material used was the Request For Comments documents from the Internet Engineering Task force. The results of the thesis describes how effective the implemented security extensions are in preventing Cache Poisoning attacks on the name service. Reflection on how this feature affects the internet is included at the end of this thesis.

Keywords: domain, name, system, DNS, security, DNSSEC, server, infrastructure

SISÄLLYS

1 JOHDANTO

Tämä opinnäytetyö kertoo nimipalveluista, tietoturvasta ja nimipalveluiden tietoturvaominaisuudesta nimeltään Domain Name System Security Extensions (DNSSEC). Opinnäytetyö on tehty nimipalvelujärjestelmän järjestelmänvalvojan näkökulmasta, eikä siinä syvennytä algoritmeihin tai protokolliin. DNSSEC on kokoelma standardeja ja toimintatapoja ylläpitää turvallista nimipalvelujärjestelmää. Se on vapaaehtoinen järjestelmä verkkotunnuksien omistajille, jonka tarkoitus on antaa nimipalvelun tiedoille alkuperäisyyden todennus ja varmennus väärennettyjen tietojen varalta.

Tämän opinnäytetyön tavoitteena on tutkia ja selvittää miten DNSSEC otetaan käyttöön ja mitä sen käyttöön vaaditaan missäkin ympäristössä. Käytännön toimenpiteet on tehty Linux järjestelmän bind-nimipalvelimella ja Windows Server nimipalvelimella. Työssä tulee myös esille muut toimenpiteet mitä vaaditaan DNSSEC allekirjoitetun verkkotunnuksen ylläpitämiseen. Työn aikana on tehty toimiva nimipalvelujärjestelmä julkiseen internettiin, joka hyödyntää tietoturvaominaisuutta, sekä yksityiseen lähiverkkoon virtuaalinen testiympäristö, jossa on testattu ominaisuuden toimivuus.

Usean verkkopalvelun ylläpitäjänä minulla on ollut tapana tutustua kaikennäköisiin tietoturvaratkaisuihin eri palveluille ja palvelimille, mutta nimipalvelujärjestelmien kannalta en ole tullut tekemisiin tietoturvallisuuden kanssa ennen tämän opinnäytetyön tekemistä. Sain tietää DNSSEC ominaisuudesta vuonna 2014, mutta vasta tämän opinnäytetyön aikana minulla oli tilaisuus tutustua siihen ja ottaa selville mitä sen käyttöön vaaditaan ja miten se otetaan käyttöön.

Opinnäytetyön alussa selvitetään työn taustan kannalta oleelliset asiat kuten nimipalvelut ja niiden toiminta, yleistä tietoturvallisuudesta, sekä DNSSEC ja sen toiminta. Taustatietojen jälkeen selitetään toimivan DNSSEC ympäristön rakentamiseen vaadittavat vaiheet Linux ja Windows-palvelimilla, jonka jälkeen tulokset toimivuuden testauksesta ja pohdinta.

2 DNS NIMIPALVELUJÄRJESTELMÄ

Nimipalvelu on se tekniikka, jonka avulla käännetään internet verkkotunnukset Internet Protocol (IP) osoitteiksi yhteyden muodostamista varten. Domain Name System (DNS) on nimipalvelujärjestelmä, jota käytetään yleisimmin kääntämään verkkotunnus IP-osoitteeksi. IP-osoite on numeerinen osoite, joka osoittaa yhteen tietokoneeseen tai laitteeseen verkossa, jossa käytetään Internet protokollaa keskusteluun. IP-osoitetta käytetään tietokoneiden ja laitteiden väliseen keskusteluun verkossa. IP-osoite tulee käyttöön, kun esimerkiksi nettiselain hakee sivun verkko-osoitteesta. Prosessin taustalla tapahtuu useita asioita, kuten nimiselvitys, jossa niin sanottu DNS-asiakas kysyy nimipalvelimelta verkkotunnuksen IP-osoitteen. Jos DNS-asiakkaan oma nimipalvelin, joka on yleensä hänen operaattorin hallitsema, ei tiedä verkkotunnuksen IP-osoitetta, se hakee sen tiedon toiselta nimipalvelimelta ja välittää vastauksen asiakkaalle. Asiakkaan verkkoselain käyttää sitten hankittua IP-osoitetta yhdistääkseen haluttuun palvelimeen verkkosivun lataamista varten. Tämä kaikki tapahtuu yleensä nopeasti ja internet käyttäjän huomaamatta. Nimipalvelujärjestelmää käytetään myös muunlaisiin kyselyihin, joihin tutustutaan myöhemmin. (Mockapetris 1987, hakupäivä 29.4.2016.)

2.1 Verkkotunnukset

Verkkotunnuksella tarkoitetaan rekisteröityä nimeä, joka päättyy yleensä ”com”, ”org”, ”net” tai ”fi”-päätteeseen. Päätteitä on lukuisia muita ja niitä lisätään uudistuksien mukana kokoajan. Esimerkiksi verkkosivun ”www.esimerkki.net” osista ”net”-pääte on Top Level Domain (TLD) tai ylätason verkkotunnus, ”esimerkki” on verkkotunnus tai vyöhyke ja ”www” on tietue siinä vyöhykkeessä. (Stahl 1987, hakupäivä 14.4.2016.)
Ylätason tunnuksia on usean tyyppisiä. ARPA on infrastruktuurisiin tarkoituksiin käytetty TLD. Kolmen tai useamman merkin ylätunnukset ovat tavallisia tunnuksia (gTLD). Maille ja alueille myönnetyt maatunnukset (cTLD) ovat kahden merkin tunnuksia ISO 3166-standardin mukaisesti. (Stahl 1987, hakupäivä 14.4.2016.)
Verkkotunnuksen hankkimisen yhteydessä käyttöön saadaan yksi vyöhyke, johon voi vapaasti lisätä haluamiansa tietueita. Tunnettu ”www”-tietue on yleistynyt käytettäväksi verkkosivun päätietueena, mutta sitä ei suinkaan tarvitse käyttää, jos ei halua. Myös verkkotunnuksen alkuliitteetön muoto vapaasti käytettävänä tietueena, ja siihen monesti viitataan juurena tai ”@”-tietueena. (Mockapetris 1987, hakupäivä 29.4.2016.)
Oikeus verkkotunnuksien rekisteröimiseen on rekisterinpitäjillä (registrar), joita valvoo Internet Corporation for Assigned Names and Numbers (ICANN) ja muut järjestöt kuten OpenNIC. Heidän tehtävänään on valvoa internetissä käytettäviä nimiä ja numeroita. ICANNin lisäksi jokaista ylätason tunnusta (TLD) valvotaan ja ylläpidetään omilla organisaatioillaan, joita kutsutaan rekistereiksi (registry) tai network information centers (NIC). Rekisteri on vastuussa oman vyöhykkeensä nimien tietokannasta ja sen ylläpidosta. Rekisteröijä (re-

gistrant) on henkilö tai organisaatio, joka on pyytänyt verkkotunnuksen rekisteröimistä. Rekisteri ottaa vastaan rekisteröintitiedot jokaisesta rekisterinpitäjältä heidän omalla ylätason vyöhykkeellään ja julkaisee tiedot WHOIS protokollan mukaisesti. (Stahl 1987, hakupäivä 14.4.2016.)
ICANN julkaisee täyden luettelon TLD:stä, TLD rekistereistä ja verkkotunnuksien rekisterinpitäjistä. Rekisteröijien yhteystietoja ylläpidetään tietokannassa, josta voidaan hakea tietoa WHOIS palvelulla. Esimerkiksi com ja net vyöhykkeille rekisteri pitää vain vähän tietoja WHOIS tietokannassa kuten rekisterinpitäjän nimi ja nimipalvelimet ja rekisterinpitäjä pitää loput tiedot omassa WHOIS tietokannassa kuten rekisteröijän tiedot, nimipalvelimet ja päättymispäivät. Jotkin rekisterit toimivat myös rekisterinpitäjinä loppukäyttäjille. Suurien ylätason vyöhykkeiden kuten com, net, org ja infon tapauksessa on useita rekisterinpitäjiä. Rekisteröijät ovat rekisterinpitäjien asiakkaita ja joissain tapauksessa myös jälleen myyjien asiakkaita. (Stahl 1987, hakupäivä 14.4.2016.)

2.2 Nimipalvelimet

Nimipalvelin on se palvelin, joka vastaa nimikyselyihin. Nimipalvelujärjestelmän nimipalvelimet muodostavat jaetun tietokannan. Jokaisella vyöhykkeellä on vähintään yksi autoritäärinen palvelin. Nimipalvelimet ovat järjestetty niiden tyyppien mukaan. Nimipalvelimen tyyppi määrittelee mihin kyselyihin se vastaa. (Mockapetris 1987, hakupäivä 29.4.2016.)
Kun verkkotunnus rekisteröidään rekisterinpitäjälle, sen asettamiseen ylätason rekisteriin vaaditaan vähintään yksi pääsijainen nimipalvelin ja toissijainen nimipalvelin. Tämän vaatimuksen tarkoitus on taata verkkotunnuksen toiminta myös silloin kun toinen nimipalvelimista on saavuttamattomissa tai toimimattomana. Ensisijainen nimipalvelin määritellään nimipalvelimien järjestyksellä tai rekisterinpitäjälle määritellyllä prioriteetilla. Ensisijainen nimipalvelin on yleensä isäntä-palvelin ja toissijainen orja-palvelin. Yleensä ylemmän tason rekisteriin nimipalvelimeksi tarvitaan vain sen kokonainen verkkotunnus, mutta jos nimipalvelin on samassa vyöhykkeessä, siihen vaaditaan myös IP-osoite. (Mockapetris 1987, hakupäivä 29.4.2016.)

2.2.1 Autoritääriset

Autoritääriset nimipalvelimet vastaavat vain ”omasta” vyöhykkeistään. Sille on asetettu yksi tai useampi vyöhyke, jonka tietueista se on vastuussa ja se vastaa yleensä vain kyselyihin näiden vyöhykkeiden tietueista. Sen tarkoitus on välittää vyöhyketietoa muille nimipalvelimille. Autoritääriseen nimipalvelimeen asetetaan oman vyöhykkeen tietueet. (Mockapetris 1987, hakupäivä 29.4.2016.)
Autoritäärisen palvelimen IP-osoite NS-tietueessa tulee tallettaa ylemmälle tasolle, joka yleensä hoidetaan ilmoittamalla rekisterinpitäjälle. Autoritäärisen palvelimen vyöhyketietoihin pitää myös asettaa oma IP-osoite NS-tietueena, jotta tieto välittyy sitäkin kautta. Autoritäärinen nimipalvelin voi olla ”master”/isäntä- tai

”slave”/orja-palvelin. Isäntä-palvelin säilyttää alkuperäiset tiedot omista vyöhykkeistään. Orja-palvelin käyttää nimipalvelun automaattista päivitysmekanismia, jolla se saa identtiset kopiot isäntä palvelimen vyöhyketiedoista. (Mockapetris 1987, hakupäivä 29.4.2016.)
Autoritäärinen nimipalvelin antaa vastauksensa mukana merkin vastauksen autoritäärisyydestä, asettamalla Authoritative Answer (AA) bitin päälle. Tämän vastauksen merkitys on yleensä näkyvissä DNS järjestelmänvalvonta työkalujen, kuten nslookup ja dig, vastauksessa viestinä, joka ilmoittaa onko tämä vastaus vyöhykkeen autoritääriseltä palvelimelta. (Mockapetris 1987, hakupäivä 29.4.2016.)

2.2.2 Rekursiiviset Resolverit

Teoriassa nimipalvelujärjestelmä toimisi myös pelkästään autoritäärisillä nimipalvelimilla. Mikäli vain autoritääriset nimipalvelimet olisivat käytössä, kaikki nimikyselyt tulisi aloittaa aina internet juuresta ja jokaisella loppukäyttäjällä tulisi olla rekursiivinen ominaisuus käytössä. Jotta nimikyselyt olisivat mahdollisen nopeita ja vältyttäisi liialta nimiselvitys liikenteeltä, nimipalvelujärjestelmä tukee välimuistipalvelimia, jotka tallettavat kyselyiden vastaukset omaan välimuistiinsa ja välittävät tietoja eteenpäin. Näitä kutsutaan rekursiivisiksi resolvereiksi. Ne ovat oleellinen osa nimipalvelujärjestelmän toimivuuden ja nopeuden takaamiseksi. Internet liittymien operaattorit ylläpitävät yleensä rekursiivisia resolvereita asiakkaillensa. On myös olemassa julkisia resolvereita, jotka ovat kaikkien käytettävissä. Monet kotiverkkojen reitittimet sisältävät rekursiivisen resolverin ja välimuistin, jotta kotiverkon tehokkuutta parannettaisiin. (Mockapetris 1987, hakupäivä 29.4.2016.)
Resolverit vastaavat kaikkiin kyselyihin ja niiden tehtävä on hankkia tietoa rekursiivisella tavalla. Ne hakevat autoritäärisien nimipalvelimien osoitteet ylemmältä tasolta ja lähettävät nimikyselyn autoritäärisille palvelimille ja välittävät vastauksen eteenpäin. Resolverit sisältävät myös välimuistin, jossa säilytetään vastauksia, kunnes niiden Time To Live (TTL) loppuu. Joissain tilanteissa verkko-operaattori saattaa asettaa resolverin rikkomaan sääntöjä kuten TTL tai jopa hylätä jonkun vyöhykkeen kyselyt omien sääntöjen mukaan. (Mockapetris 1987, hakupäivä 29.4.2016.)
Kaikissa työpöytäkäyttöjärjestelmissäkin on eräänlainen resolveri, jota käytetään nimikyselyn aloittamiseen. Ne sisältävät myös välimuistin. Käyttöjärjestelmien resolvereita sanotaan yleensä stub resolvereiksi. Stub resolverit eivät yleensä tee varmistusta tai muuta todennusta, joten muiden resolverit tulisi käyttää jotain todennusta. Nettiselaimet ja monet muut loppukäyttäjän ohjelmat sisältävät DNS välimuistin. (Mockapetris 1987, hakupäivä 29.4.2016.)

2.3 Tietueet

Nimipalvelimet säilyttävät tietoja sisäisessä tietokannassa. Tietokannan vyöhykkeet ovat yleensä omissa tiedostoissaan palvelimella. Vyöhykkeen yhtä tietoa sanotaan tietueeksi. Tietueiden tyypit määrittelevät nimipalvelun vastaukset. Erilaisiin kyselyihin käytetään eri tietuetyyppiä. Vyöhykkeessä voi olla monta saman nimisiä tietuetta, kunhan niiden tyyppi ei ole sama.

- A-tietue osoittaa IPv4-osoitteen.
- AAAA-tietue osoittaa IPv6-osoitteen.
- NS-tietue osoittaa verkkotunnuksen nimipalvelimet.
- SOA-tietue osoittaa verkkotunnuksen hallintatiedot.
- CNAME-tietue osoittaa toiseen tietueeseen.
- MX-tietue osoittaa sähköpostipalvelimet.
- TXT-tietue on vapaateksti tietue.

Vaikka nimipalvelujärjestelmää ei ole tarkoitettu käytettävän normaalina tietokantana, sitä voidaan käyttää tallettamaan myös muunlaisia tietoja. (Mockapetris 1987, hakupäivä 29.4.2016.)

3 NIMIPALVELUJÄRJESTELMÄN TIETOTURVALLISUUS

Tietoturvallisuus tarkoittaa yleisesti tiedon, tietokoneen, verkkolaitteen ja tietojärjestelmien puolustamista luvatonta käyttöä, häirintää, tarkkailua, tallettamista tai tuhoamista vastaan. Yksinkertaisesti sanottuna sillä tarkoitetaan tiedon suojaamista väärinkäytöltä. Tietoturvallisuus ei ole vain yhteen laitteeseen tai verkkoon kohdistuva asia, vaan sillä tarkoitetaan myös internetin infrastruktuuriin kohdistuvaa tietoturvaa. Uhkia on useita ja niitä on kaiken muotoisia. Yleisesti tunnettuihin uhkiin lasketaan ohjelmistohyökkäykset, tekijänoikeus varkaus, henkilöllisyys varkaus, laitteisto varkaus ja sabotaasi. Yritykset, organisaatiot ja hallitukset taistelevat kyseisiä uhkia ja monia muita vastaan jatkuvasti.

Mutta mitä tarkoittaa tiedon turvallisuus? Yhdysvaltojen Central Intelligence Agencyn määritelmän mukaan tietoturvallisuus voidaan jakaa kolmeen osaan, jotka ovat confidentiality, integrity ja availability (Perrin 2008, hakupäivä 29.4.2016) eli luottamuksellisuus, eheys ja saatavuus. Luottamuksellisuudella tarkoitetaan, että tieto ei päädy luvattomien ihmisten tai järjestöjen käsiin. Eheydellä tarkoitetaan tiedon ylläpitämistä ja varmentamista niin, että se on oikein ja kokonainen sen käyttöikänsä ajan. Se tarkoittaa sitä, että tietoa ei muokata luvattomasti tai huomaamattomasti. Saatavuudella tarkoitetaan, että tieto on saatavilla kaikille, joilla on lupa käyttää tietoa. Tällä tarkoitetaan myös, että tiedon sisältävät tietokoneet, sitä turvaavat tietoturvaominaisuudet ja sitä siirtävät tietoliikennejärjestelmät toimivat oikein.

Nimipalvelujärjestelmä perustuu luottamukseen ja tietojen oikeellisuuteen. Hakkerit ja muut hyökkääjät voivat käyttää tätä luottamusta hyväkseen huijaamalla resolveria väärennetyillä tietueilla. Resolveri ei voi tietää onko tietue väärennetty vai ei tai edes tietää tuliko vastaus oikeasta paikasta. Resolvereita voi huijata monella tavalla ja koska tietueet jäävät resolverin välimuistiin, väärentäjän ei tarvitse edes pitää hyökkäystä yllä ensimmäisen kyselyn jälkeen. (Arends, Austein, Larson, Massey & Rose 2005a, hakupäivä 30.3.2016.)

Kun internetin käyttäjä kirjoittaa pankin verkkotunnuksen selaimeensa, hän olettaa yhteyden muodostuvan hänen ja pankin välille. Nimipalvelun tietueiden väärentäminen on mahdollista, jos hyökkääjä pääsee saastuttamaan esimerkiksi palvelutarjoajan nimipalvelun. Tässä tapauksessa hyökkääjä voi ohjata pankin asiakkaan omalle palvelimelleen ja käyttää saatuja tietoja pankkitilien varastamiseen.

Jotkin verkko-operaattorit käyttävät nimipalvelujärjestelmää sääntöjen vastausesti omiin tarkoituksiinsa. Monesti tarkoituksena on näyttää mainoksia tai kerätä tilastoja. Nämä tekniikat ovat internetin yhteisen sopimuksien ja standardien vastaiset ja altistavat käyttäjät muille hyökkäyksille. Käytännössä tällaisessa tilanteessa operaattori kaappaa normaalin nimikyselyn vastauksen ja välittää väärän vastauksen asiakkaalleen. Operaattori voi lähettää olemassa olemattoman verkkotunnuksen sijaitsevan heidän omassa IP-osoitteessaan. Operaattori voi siten näyttää IP-osoitteestaan sivua, jolla on mainoksia tai uudelleenohjautuva sivu. Tallainen käytös on ärsyttävää, kun nettiselaimen ei anneta näyttää oikeanlaista virheilmoitusta. Yhteyden luominen tuntemattomaan IP-osoitteeseen saattaa altistaa asiakkaan riskeille, kuten tietämättä herkänlaatuisen tiedon lähettämiselle. (Atkins 2004, hakupäivä 30.3.2016)

4 DNSSEC

DNSSEC on tietoturvaominaisuus, jonka tarkoitus on tarjota todennus DNS tietueille. Se takaa, että nimipalvelukyselyiden vastaukset saadaan allekirjoitettuina takaisin. Digitaalisen allekirjoituksen yksityinen avain pysyy salassa nimipalvelun omistajalla. Julkinen avain julkaistaan nimipalvelun tietueena. Allekirjoituksen oikeellisuus varmennetaan yksityistä avainta vastaavalla julkisella avaimella. Näin varmistetaan vastausten eheys ja todennetaan, että ne tulevat oikeasta lähteestä. DNSSEC:n tarkoitus on estää väärennetyt tai muuten vaan virheelliset vastaukset. (Mockapetris 1999, hakupäivä 30.3.2016.)
Jotta voidaan todeta nimikyselyn vastaus oikeaksi, tarvitaan ainakin yksi avain tai DS-tietue, joka on saatu muusta lähteestä. Näitä aloituskohtia kutsutaan luottamus ankkureiksi (trust anchort) ja ne tulevat yleensä käyttöjärjestelmältä tai muusta luotetusta lähteestä. Luotettavana ankkurina käytetään DNS juurta, jotta siitä alaspäin voidaan varmentaa kaikkien verkkotunnuksien luotettavuus. (Josefsson 2006, hakupäivä 30.3.2016.)

4.1 DNSSEC tietueet

DNSSEC ominaisuuden toimintaan käytetään useita eri tietueita.

- RRISG-tietue tulee jokaisen kyselyn mukana ja sisältää tietueen allekirjoituksen. Resolverit varmistavat allekirjoituksen julkisen avaimen avulla.
- DNSKEY-tietue esittää julkisen avaimen, jolla varmennetaan RRSIG-tietueen allekirjoitukset.
- DS-tietue on Delegation Signer tietue, joka on olemassa Top Level Domainin nimipalvelimissa ja sen tarkoitus on varmentaa DNSKEY.
- NSEC-tietue sisältää linkin seuraavaan tietueen nimeen vyöhykkeellä ja kertoo sen tietueen tyypin. Tätä tietuetta käytetään todistamaan olemattomien tietueiden nimi ja tyyppi. Tämä tietue on tietoturvan kannalta ongelmallinen, koska sitä käyttäen voidaan saada täysi kuva vyöhykkeen tietueista. Menetelmä on nimeltään ”zone walking” tai vyöhyke kävely.
- NSEC3-tietue sisältää saman kun NSEC-tietue, mutta käyttää tietueen nimen sijasta algoritmisesti tiivistettyä kuvausta tietueesta vyöhyke kävelyn estämiseksi.
- NSEC3PARAM-tietue on autoritäärisen nimipalvelimen käyttämä tietue, jolla lasketaan mitä NSEC3-tietuetta käytetään kun vastataan olemattoman tietueen kyselyyn.

Kun DNSSEC on käytössä, jokaiseen kyselyn vastauksen mukaan lähetetään myös RRSIG tieto. RRSIG on digitaalinen allekirjoitus sen vastaavasta tiedosta. Allekirjoitus varmistetaan oikeaksi vertaamalla sitä oikeaan julkiseen avaimeen, joka on DNSKEY-tietueessa. NSEC ja NSEC3 tietueita käytetään vahvistamaan tietueiden olemattomuus, kun niitä ei ole. NSEC ja NSEC3 tietueiden tarkoitus on antaa vahva suoja olemattomien tietueiden väärentämistä vastaan, koska olemattomia tietueita ei voida allekirjoittaa RRSIG-tietueella. DS-tietuetta käytetään vahvistamaan vyöhykkeen DNSKEY. (Arends, Austein, Larson, Massey & Rose 2005b, hakupäivä 30.3.2016; Laurie, Sisson, Arends & Blacka 2008, Hakupäivä 30.3.2016.)

4.2 DNSSEC avaimet

Jotta DNSSEC järjestelmä sallii avaimien korvaamisen, tarvitaan toimiva avainten kierrätysjärjestelmä, jota kutsutaan key rollover järjestelmäksi. Yleensä järjestelmä julkaisee uuden avaimen uudella DNSKEY-tietueella nykyisen avaimen mukana. Uudet avaimet tulevat käyttöön vasta kun voidaan olettaa, että DNS aikarajoitus on ylitetty, jotta vanhaa avainta ei ole enää välimuistissa. Lopuksi vanhentunut DNSKEY voidaan turvallisesti poistaa ja uusi avain tulee käyttöön. Prosessi on huomattavasti monimutkaisempi, kun kyseessä on luottoankkurin, kuten internet juuren avain, jolloin mahdollinen käyttöjärjestelmän päivittäminen tulee pakolliseksi. (Kolkman, Mekking & Gieben 2012, hakupäivä 30.3.2016.)

DNSKEY-tietueen avaimia voidaan käyttää useisiin asioihin ja yleensä eri DNSKEY-tietuetta käytetään eri avaimiin. Ensin DNSKEY-tietueena on key signing keys (KSK), jolla allekirjoitetaan toiset DNSKEY-tietueet. Toiseksi käytetään zone signing keys (ZSK), jolla allekirjoitetaan muut tietueet. Koska ZSK:t ovat vyöhykkeen täydessä hallussa, niitä voidaan vaihtaa useammin ja helpommin. Sen takia ZSK:t ovat myös paljon lyhyempiä kun KSK:t, mutta niiden antama suojaus on sama. (Hardaker 2006, hakupäivä 30.3.2016.)

Kun uusi KSK luodaan, sen DS-tietue pitää siirtää ylemmän tason rekisteriin ja säilyttää siellä. DS-tietueet ovat KSK:n hajautusarvoja (hash), eikä kokonaisia tietueita, jotta niiden koko olisi pienempi. Näin isojen ylätason vyöhykkeiden kuten comin on helpompi hallita DS-tietueita. Tekniikka viedä DS-tietueet ylemmälle tasolle on myös nykyään helpompi, koska ennen vaadittiin, että koko KSK:n DNSKEY-tietue siirrettäisiin ylemmälle vyöhykkeelle. KSK:n hajautusarvon vieminen DS-tietueena ylemmän tason vyöhykkeelle suoritetaan rekisterinpitäjän verkkosivujen kautta. Rekisterinpitäjällä tarkoitetaan sitä tahoa, jolta domain on hankittu ja rekisteröity. (Kolkman, Mekking & Gieben 2012, hakupäivä 30.3.2016.)

DNSSEC allekirjoitukset eivät käytä normaalia DNS TTL arvoa, vaan erillistä allekirjoituksesta alkavaa aikarajaa. DNS TTL aikarajaa käytetään välimuistin toimivuuteen, mutta DNSSEC allekirjoitukset tulee rajoittaa allekirjoitushetkestä lähtien, jotta sitä ei voida käyttää hyökkäyksiin. Tämän aikarajoituksen vuoksi DNS resolvereiden kellonaika tulisi olla kohtuullisen tarkasti synkronisoidut. Se myös tarkoittaa, että vyöhykkeet tulevat uudelleenallekirjoittaa aika ajoin, jotta resolverit eivät hylkää allekirjoitusta. (Eastlake 1999, hakupäivä 30.3.2016.)

5 DNSSEC BIND PALVELIMELLA

Tämän opinnäytetyön aikana tekijä asensi 2 autoritääristä nimipalvelinta siltakoski.com vyöhykkeen nimipalvelimiksi. Tässä luvussa kerrotaan vaiheet joilla saadaan toimiva DNSSEC ympäristö kahdelle autoritäähäriselle nimipalvelimille. Debian Linux palvelimilla käytetiin bind nimistä nimipalvelujärjestelmää. Master nimipalvelin on IP-osoitteessa 51.255.206.224 ja se on nimeltään ns1.siltakoski.com. Slave-nimipalvelin on IP-osoitteessa 51.255.206.231 ja se on nimeltään ns2.siltakoski.com. Molemmissa käytössä Debian 8 käyttöjärjestelmä. Palvelimet on vuokrattu OVH Hosting yrityksen ylläpitämästä virtuaalipalvelin alustasta.
Luvussa 5.1 käydään läpi ensin master palvelimen DNSSEC määritys. Luvussa 5.2 lyhyt slave-palvelimen määritys. Lopuksi järjestelmän toiminnan kannalta oleellinen vaihe, jossa siirretään DS-tietue rekisterinpitäjälle luvussa 5.3. Luvussa 5.4 on kuvattu vapaaehtoinen vaihe järjestelmänvalvojan ylläpitotaakan helpottamiseksi.

5.1 Master palvelimen asetus

Master palvelimella on muokattu /etc/bind/named.conf.options tiedosto seuravan näköiseksi.

```
OPTIONS {
        RECURSION NO;
        ALLOW-TRANSFER { NONE; };
        DNSSEC-ENABLE YES;
        DNSSEC-VALIDATION YES;
        DNSSEC-LOOKASIDE AUTO;
        AUTH-NXDOMAIN NO;    # CONFORM TO RFC1035
        LISTEN-ON-V6 { ANY; };
};
```

Itse tietueet on määritelty vyöhyketiedostoon /etc/bind/zones/db.siltakoski.com seuraavasti.

```
$TTL    604800
@       IN      SOA     NS1.SILTAKOSKI.COM. ADMIN.SILTAKOSKI.COM. (
                              7         ; SERIAL
                         604800         ; REFRESH
                          86400         ; RETRY
                        2419200         ; EXPIRE
                         604800 )       ; NEGATIVE CACHE TTL
;
; NIMIPALVELIMIEN NS TIETUEET
SILTAKOSKI.COM. IN NS NS1.SILTAKOSKI.COM.
SILTAKOSKI.COM. IN NS NS2.SILTAKOSKI.COM.

; NIMIPALVELIMIEN A TIETUEET
NS1 IN A 51.255.206.224
```

NS2 IN A 51.255.206.231

; WWW-PALVELIMEN A TIETUEET
@ IN A 51.255.206.66
WWW IN A 51.255.206.66

Tiedoston kommentit ovat puolipisteellä alkavia rivejä. Vyöhyketiedostossa on ihan ensimmäisenä määritetty TTL aika ensimmäisellä rivillä. Seuraavalla rivillä alkaa SOA tietueen määritys, jonka määritelmät ovat järjestyksessä nimipalvelimen nimi, minipalvelimen ylläpitäjän sähköpostiosoite ilman @-merkkiä, sarjanumero, päivitysaika, uudelleenyrityksen aika, umpeutumisaika ja negatiivinen TTL. Tietueiden määrittelyn jälkeen Zone Signing Key (ZSK) luodaan dnssec-keygen komennolla.

ROOT@NS1:~# CD /ETC/BIND/ZONES
ROOT@NS1:/ETC/BIND/ZONES# DNSSEC-KEYGEN -A NSEC3RSASHA1 -B 2048 -N ZONE SILTAKOSKI.COM
GENERATING KEY PAIR.....+++ .....+++
KSILTAKOSKI.COM.+007+54050

Seuraavaksi luodaan Key Signing Key (KSK) myöskin dnssec-keygen komennolla.

ROOT@NS1:/ETC/BIND/ZONES# DNSSEC-KEYGEN -F KSK -A NSEC3RSASHA1 -B 4096 -N ZONE SILTAKOSKI.COM
GENERATING KEY PAIR.....++
.....
.....++
KSILTAKOSKI.COM.+007+15441

Hakemistossa on nyt 4 avaintiedostoa. Julkiset ja salaiset avaimet ZSK:lle ja KSK:lle. Julkiset avaimet listataan DNS tietue tiedostoon /etc/bind/zones/db.siltakoski.com seuraavasti.

$INCLUDE KSILTAKOSKI.COM.+007+15441.KEY
$INCLUDE KSILTAKOSKI.COM.+007+54050.KEY

Vyöhykkeen allekirjoittamista varten luodaan suolatiedoksi satunnaista dataa.

HEAD -C 1000 /DEV/RANDOM | SHA1SUM | CUT -B 1-16
F7ACBF9C95CCA737

Vyöhyke allekirjoitetaan seuraavaksi käyttäen suolatietoa ja tietuetiedostoa.

ROOT@NS1:/ETC/BIND/ZONES# DNSSEC-SIGNZONE -A -3 F7ACBF9C95CCA737 -N INCREMENT -O SILTAKOSKI.COM -T DB.SILTAKOSKI.COM
VERIFYING THE ZONE USING THE FOLLOWING ALGORITHMS: NSEC3RSASHA1.
ZONE FULLY SIGNED:
ALGORITHM: NSEC3RSASHA1: KSKS: 1 ACTIVE, 0 STAND-BY, 0 REVOKED
ZSKS: 1 ACTIVE, 0 STAND-BY, 0 REVOKED
DB.SILTAKOSKI.COM.SIGNED
SIGNATURES GENERATED: 17
SIGNATURES RETAINED: 0
SIGNATURES DROPPED: 0

```
SIGNATURES SUCCESSFULLY VERIFIED:          0
SIGNATURES UNSUCCESSFULLY VERIFIED:        0
SIGNING TIME IN SECONDS:                   0.042
SIGNATURES PER SECOND:                     399.079
RUNTIME IN SECONDS:                        0.051
```

Hakemistoon on nyt tullut tiedosto db.siltakoski.com.signed, jossa on RRSIG tietueet kaikille tietueille. Seuraavaksi muokataan BIND palvelimen /etc/bind/named.conf.local tiedostoa käyttämään signed-loppuista tietuetiedostoa.

```
ZONE "SILTAKOSKI.COM" {
   TYPE MASTER;
   FILE "/ETC/BIND/ZONES/DB.SILTAKOSKI.COM.SIGNED";
   ALLOW-TRANSFER { 51.255.206.231; };
};
```

Seuraavaksi voidaan tarkistaa vyöhyketietojen toimivuus named-checkzone komennolla.

```
ROOT@NS1:/ETC/BIND/ZONES# NAMED-CHECKZONE SILTAKOSKI.COM
/ETC/BIND/ZONES/DB.SILTAKOSKI.COM
ZONE SILTAKOSKI.COM/IN: LOADED SERIAL 10
OK
ROOT@NS1:/ETC/BIND/ZONES# NAMED-CHECKZONE SILTAKOSKI.COM
/ETC/BIND/ZONES/DB.SILTAKOSKI.COM.SIGNED
ZONE SILTAKOSKI.COM/IN: LOADED SERIAL 11 (DNSSEC SIGNED)
OK
```

Jotta vyöhyke tulee voimaan, BIND palvelin käynnistetään uudelleen service komennolla.

```
ROOT@NS1:/ETC/BIND/ZONES# SERVICE BIND9 RELOAD
```

Seuraavaksi voidaan kokeilla antaako palvelin DNSSEC tietueita. Katso esimerkki liitteestä 1. (Internet Systems Consertium, Inc 2014, hakupäivä 25.3.2016.)

5.2 Slave-palvelimen asetus

Seuraavaksi voidaan asettaa slave-nimipalvelin käyttämään DNSSEC tietueita. Se onnistuu helposti vaihtamalla /etc/bind/named.conf.options tiedostoon options sulkeisiin.

```
DNSSEC-ENABLE YES;
DNSSEC-VALIDATION YES;
DNSSEC-LOOKASIDE AUTO;
```

Ja slave-palvelimen /etc/bind/named.conf.local tiedostoon laitetaan myös signed-loppuinen tiedosto.

```
ZONE "SILTAKOSKI.COM" {
   TYPE SLAVE;
   FILE "/ETC/BIND/ZONES/DB.SILTAKOSKI.COM.SIGNED";
```

MASTERS { 51.255.206.224; };
};

Ja käynnistetään BIND uudelleen service komennolla

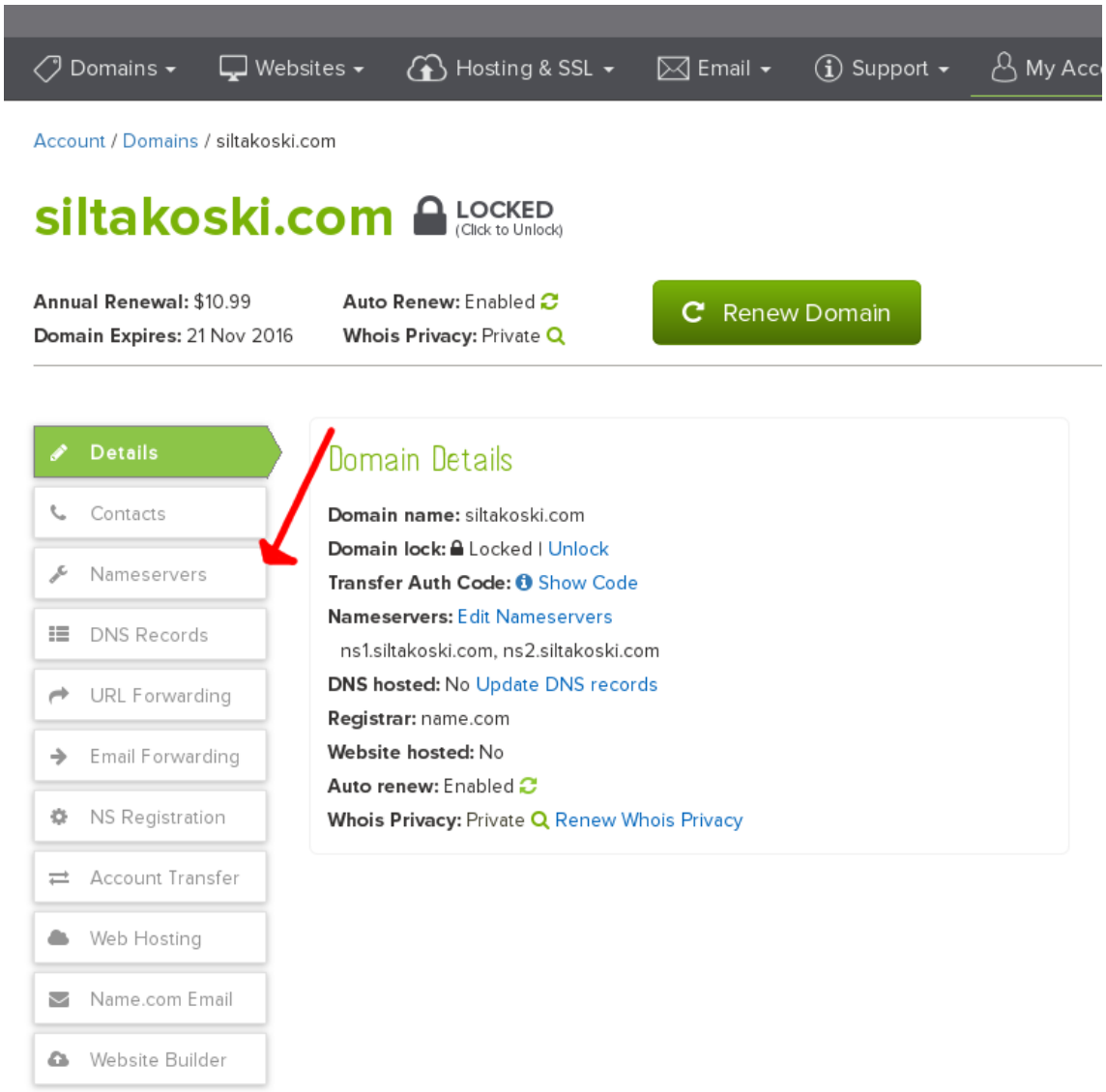
ROOT@NS2# SERVICE BIND9 RESTART

Jos vyöhyketieto siirtyi onnistuneesti, slave-palvelimen hakemistoon /var/cache/bind pitäisi ilmestyä db.siltakoski.com.signed vyöhyketiedosto. Nimipalvelimen lokitiedostossa on yleensä hyödyllistä tietoa vyöhyketietojen päivityksestä ja sarjanumero, jolla voidaan todeta onko uusin vyöhyketieto käytössä. Jos prosessin aikana tuli virheitä, ne ovat myös siellä. (Internet Systems Consertium, Inc 2014, hakupäivä 25.3.2016.)

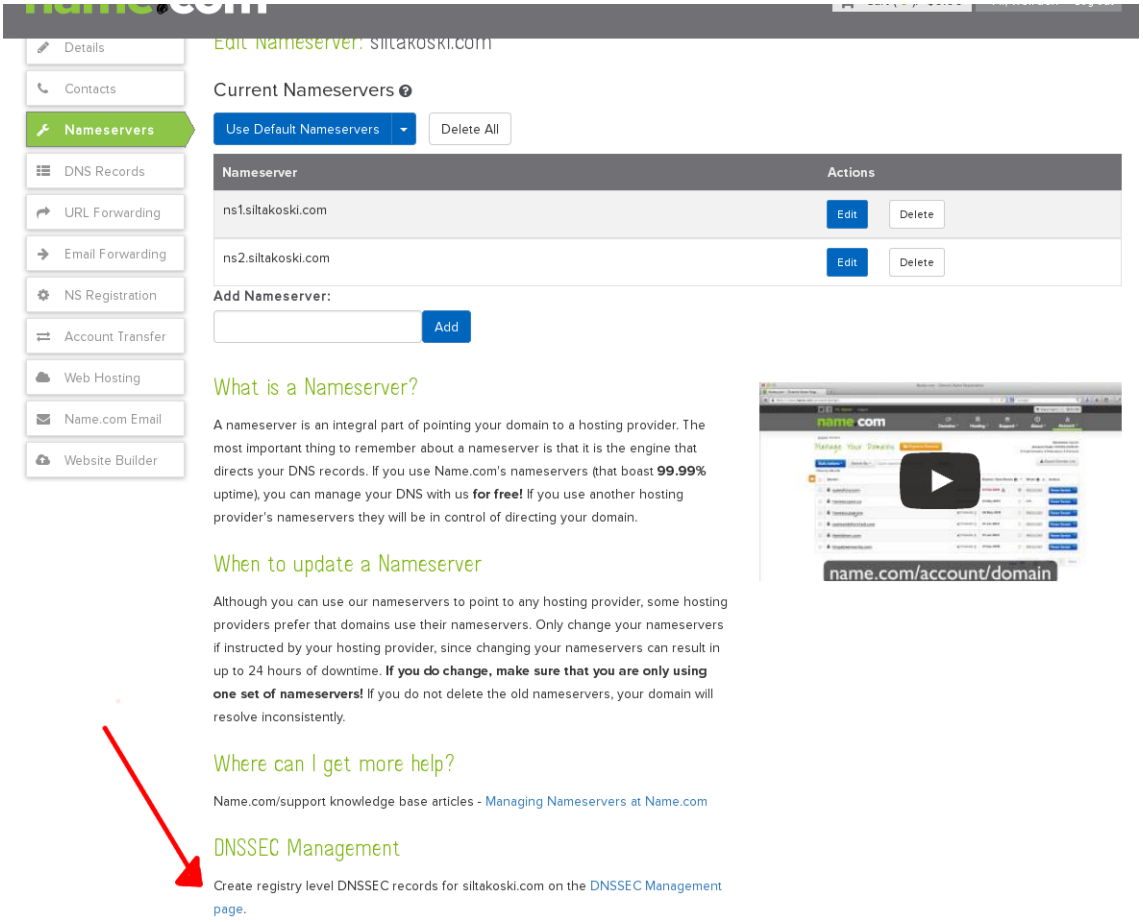
5.3 DS-tietueiden vienti rekisterinpitäjälle

Kun dnssec-signzone komento suoritettiin master palvelimella, hakemistoon tuli myös tiedosto dsset.siltakoski.com., jonka avulla voidaan siirtää DS-tiedot rekisterinpitäjälle. Rekisterinpitäjä on tälle vyöhykkeelle name.com, koska domain on alun perin tilattu heiltä.

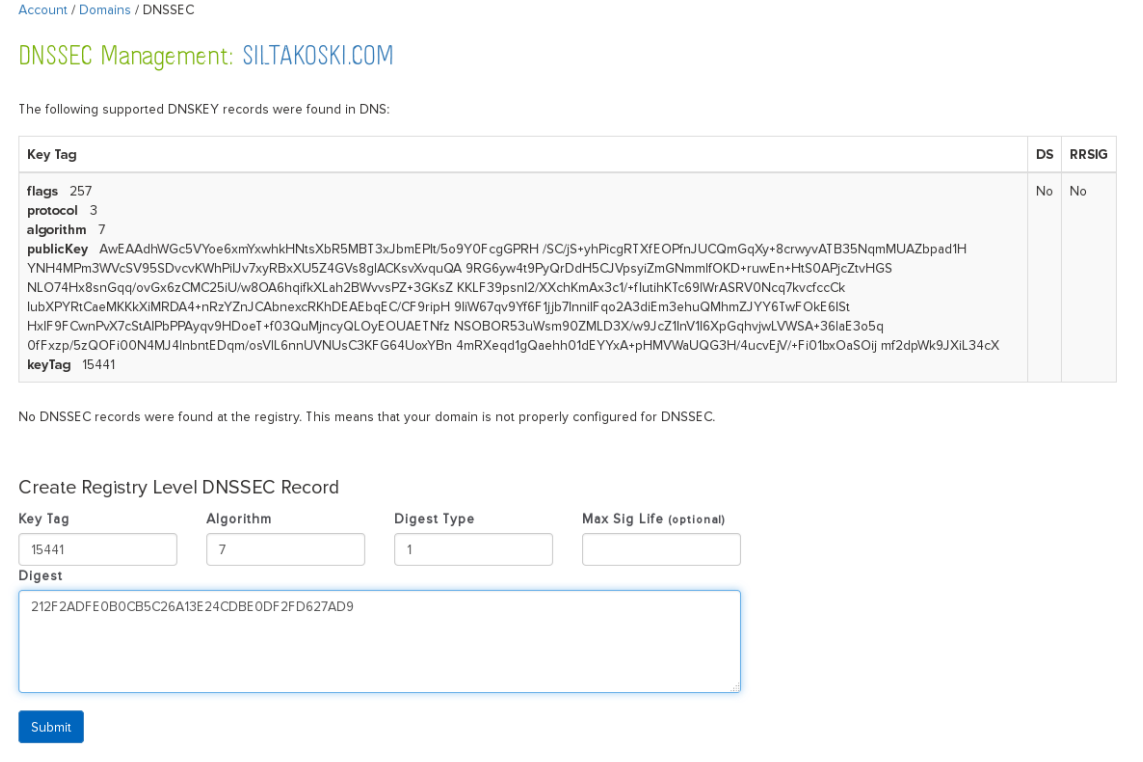
ROOT@NS1:/ETC/BIND/ZONES# CAT DSSET-SILTAKOSKI.COM.
SILTAKOSKI.COM. IN DS 15441 7 1
212F2ADFE0B0CB5C26A13E24CDBE0DF2FD627AD9
SILTAKOSKI.COM. IN DS 15441 7 2
B1A5EB048413562F44F685CA4A108A64AAE713ABE2DF98D1F4DE2C9B AAF30916

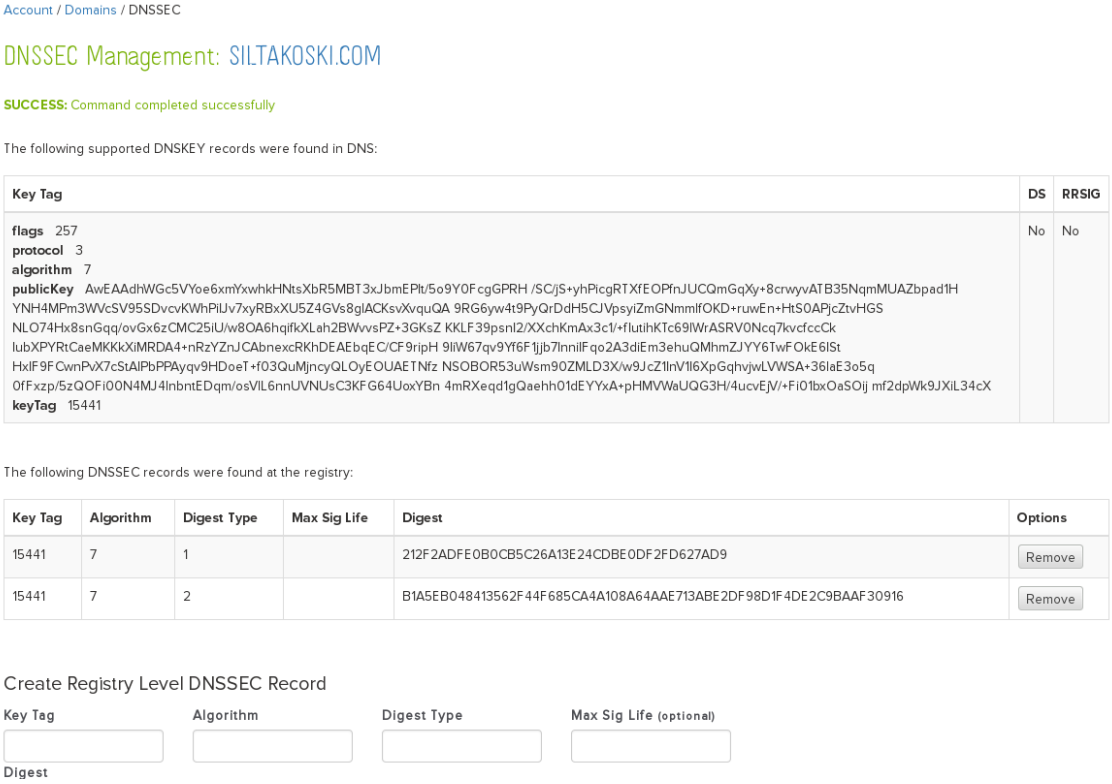


Name.com vyöhykkeen asetuksista valitaan ”Nameservers”-painike.



Sivun alareunassa ”DNSSEC Management”-kohdan alla on linkki ”DNSSEC Management page”-sivulle.




Account / Domains / DNSSEC

DNSSEC Management: SILTAKOSKI.COM

SUCCESS: Command completed successfully

The following supported DNSKEY records were found in DNS:

Key Tag	DS	RRSIG
flags 257 **protocol** 3 **algorithm** 7 **publicKey** AwEAAdhWGc5VYoe6xmYxwhkHNtsXbR5MBT3xJbmEPlt/5o9Y0FcgGPRH /SC/jS+yhPicgRTXfEOPfnJUCQmGqXy+8crwyvATB35NqmMUAZbpad1H YNH4MPm3WVcSV95SDvcvKWhPiUv7xyRBxXU5Z4GVs8gIACKsvXvquQA 9RG6yw4t9PyQrDdH5CJVpsyiZmGNmmlfOKD+ruwEn+HtS0APjcZtvHGS NLO74Hx8snGqq/ovGx6zCMC25iU/w8OA6hqifkXLah2BWvvsPZ+3GKsZ KKLF39psnI2/XXchKmAx3c1/+flutihKTc69IWrASRV0Ncq7kvcfccCk lubXPYRtCaeMKKkXiMRDA4+nRzYZnJCAbnexcRKhDEAEbqEC/CF9ripH 9liW67qv9Yf6F1jjb7InnilFqo2A3diEm3ehuQMhmZJYY6TwFOkE6ISt HxIF9FCwnPvX7cStAlPbPPAyqv9HDoeT+f03QuMjncyQLOyEOUAETNfz NSOBOR53uWsm90ZMLD3X/w9JcZ1lnV1l6XpGqhvjwLVWSA+36IaE3o5q 0fFxzp/5zQOFi00N4MJ4InbntEDqm/osVIL6nnUVNUsC3KFG64UoxYBn 4mRXeqd1gQaehh01dEYYxA+pHMVWaUQG3H/4ucvEjV/+Fi01bxOaSOij mf2dpWk9JXiL34cX **keyTag** 15441	No	No

The following DNSSEC records were found at the registry:

Key Tag	Algorithm	Digest Type	Max Sig Life	Digest	Options
15441	7	1		212F2ADFE0B0CB5C26A13E24CDBE0DF2FD627AD9	Remove
15441	7	2		B1A5EB048413562F44F685CA4A108A64AAE713ABE2DF98D1F4DE2C9BAAF30916	Remove

Create Registry Level DNSSEC Record

Key Tag | Algorithm | Digest Type | Max Sig Life (optional)

Digest

Dsset tiedostosta otetaan tarvittavat tiedot ja kopioidaan ne name.com DNSSEC Management sivun vastaaviin laatikkoihin.

Molemmat DS-tietueet on asetettu rekisterinpitäjän sivulle ja niiden pitäisi tulla voimaan heti. Sitten voidaan tarkistaa näkyykö DS-tietueita, kun kysellään julkiselta DNS resolverilta (8.8.8.8).

```
ROOT@NS1:/ETC/BIND/ZONES# DIG +TRACE +NOADDITIONAL DS SILTAKOSKI.COM. @8.8.8.8 | GREP DS
; <<>> DIG 9.9.5-9+DEB8U6-DEBIAN <<>> +TRACE +NOADDITIONAL DS SILTAKOSKI.COM. @8.8.8.8
COM.                    86400   IN      DS      30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CF C41A5766
COM.                    86400   IN      RRSIG   DS 8 1 86400 20160404050000 20160325040000 54549 . F82KPMK8GICG3XCSQUB3SXYYFZIHGRK8N4Z9T2J2SW5NDT0GERGGVUXA 1J0OD/HKH/CUZG9L55NGXSO2BMHDCQUH49QGUTVHKWQRC9I5XMCRS1/F 4TJRH93IAY0VOVLOBLVURH0WKWCQYJPFURTGD0PHPVHDLFI/39VPJJRN SYG=
SILTAKOSKI.COM.         86400   IN      DS      15441 7 2 B1A5EB048413562F44F685CA4A108A64AAE713ABE2DF98D1F4DE2C9B AAF30916
SILTAKOSKI.COM.         86400   IN      DS      15441 7 1 212F2ADFE0B0CB5C26A13E24CDBE0DF2FD627AD9
SILTAKOSKI.COM.         86400   IN      RRSIG   DS 8 2 86400 20160401181814 20160325170814 28259 COM. MBNWXKBERHH8SWWSH0OUT-MOM1FTABDNHBUYQJTCW9HFYOX6VJBQ1ILV7 V7NSLJXHQ1AHTTDF2FQMN5BNLTJN06ANX59KEGAVCMR1KOV7CGWGQPGZ /AM3WISYCTMMUFMHLCCS1LCDD/OM0XZGJ9EB4XAP3UXOUXTCPTNYHJWV 8VM=
```

DNSSEC toimivuutta voidaan myös testata verkosta löytyvillä työkaluilla. Liitteissä 2 ja 3 on esimerkit testaustyökalujen ilmoittavan onnistuneesta vyöhykkeen määrittelystä.

5.4 Vapaaehtoinen vaihe

Vyöhykkeen allekirjoittamiseen vastausuudessa pitää käyttää samoja komentoja, jotka ovat hankalia ja monelle liian pitkiä muistettavaksi. Vyöhykkeen allekirjoittamista voidaan helpottaa yksinkertaisella skriptalla.
/usr/sbin/allekirjoittaja.sh:

```
#!/BIN/SH
PDIR=`PWD`
ZONEDIR="/ETC/BIND/ZONES/" #ZONE HAKEMISTON SIJAINTI
ZONE=$1
ZONEFILE=$2
DNSSERVICE="BIND9"
CD $ZONEDIR
/USR/SBIN/DNSSEC-SIGNZONE -A -3 $(HEAD -C 1000 /DEV/RANDOM | SHA1SUM |
CUT -B 1-16) -N INCREMENT -O $1 -T $2
SERVICE $DNSSERVICE RELOAD
CD $PDIR
```

Annetaan allekirjoittaja skriptalle suoritusoikeus chmod komennolla.

```
ROOT@NS1:~# CHMOD +X /USR/SBIN/ALLEKIRJOITTAJA.SH
```

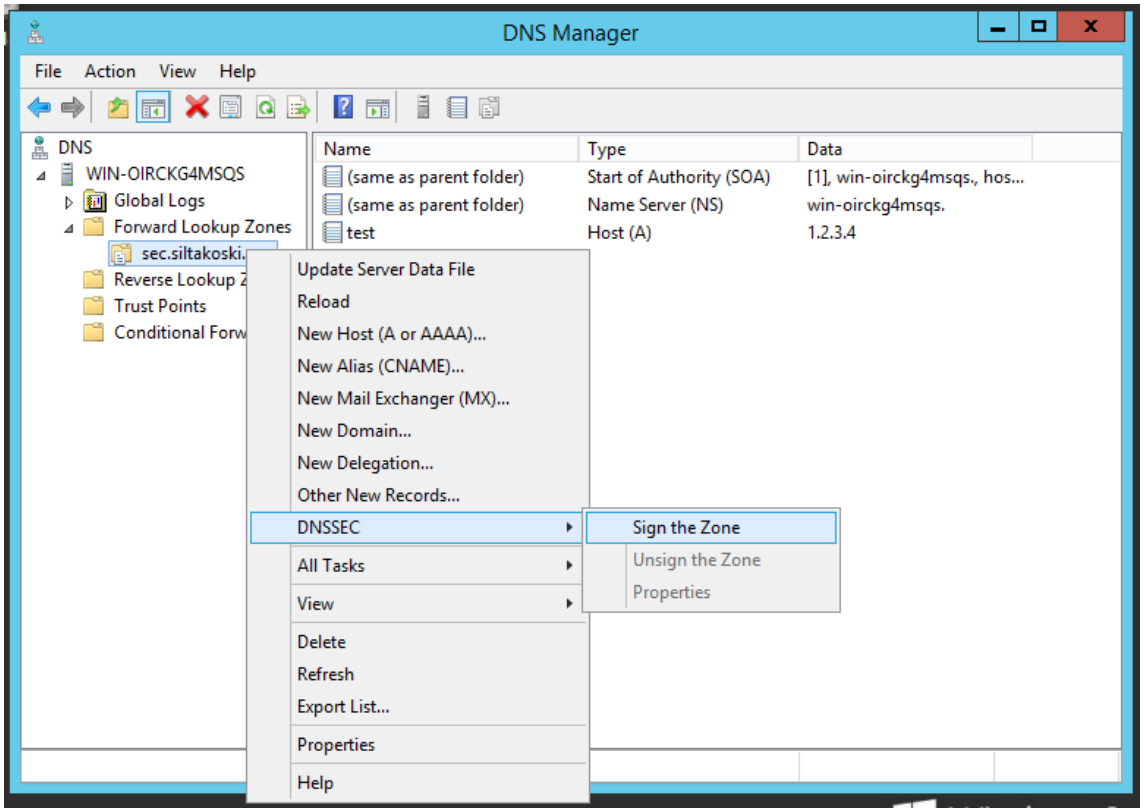
Pitkiä komentoja ei tarvitse muistaa itse, jos käyttää allekirjoittaja skriptiä ja näin helpotetaan vyöhyketietojen päivittämistä ja kevennetään järjestelmänvalvojan taakkaa. Kun tietueita muokataan, ne laitetaan /etc/bind/zones/db.siltakoski.com tiedostoon eikä signed päätteiseen tiedostoon. Vyöhykettä muokatessa tarvitsee vain muistaa aina korottaa serial eli sarjanumero kohtaa, jotta nimipalvelimet tietävät tietojen päivittyneen. Kun zonesigner skriptalla päivitetään vyöhykettä, se antaa-signed päätteiselle tiedostolle isomman sarjanumeron, jotta nimipalvelin tietää käyttää vain allekirjoitettuja tietueita.
Skriptalle annetaan ensimmäiseksi vyöhyke ja toiseksi vyöhyketiedoston nimi.

```
ROOT@NS1:~# ALLEKIRJOITTAJA.SH SILTAKOSKI.COM DB.SILTAKOSKI.COM
VERIFYING THE ZONE USING THE FOLLOWING ALGORITHMS: NSEC3RSASHA1.
ZONE FULLY SIGNED:
ALGORITHM: NSEC3RSASHA1: KSKS: 1 ACTIVE, 0 STAND-BY, 0 REVOKED
                         ZSKS: 1 ACTIVE, 0 STAND-BY, 0 REVOKED
DB.SILTAKOSKI.COM.SIGNED
SIGNATURES GENERATED:                    19
SIGNATURES RETAINED:                     0
SIGNATURES DROPPED:                      0
SIGNATURES SUCCESSFULLY VERIFIED:        0
SIGNATURES UNSUCCESSFULLY VERIFIED:      0
SIGNING TIME IN SECONDS:                 0.043
SIGNATURES PER SECOND:                   438.961
RUNTIME IN SECONDS:                      0.052
```

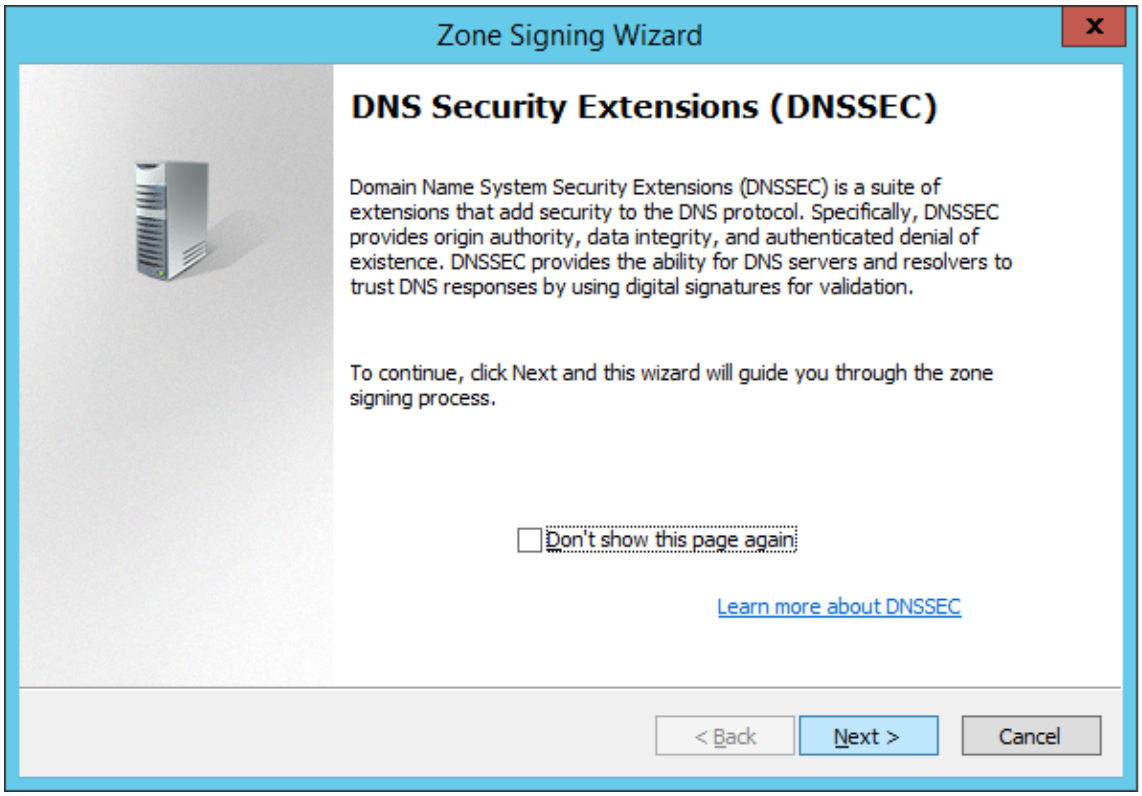
Komento ilmoittaa kuinka monta allekirjoitusta on tehty ja kauanko se kesti. Aina vyöhykkeen muokkaamisen jälkeen autoritäärinen nimipalvelin pitää käynnistää tai ladata uudelleen. (Internet Systems Consertium, Inc 2014, hakupäivä 25.3.2016.)

6 DNSSEC WINDOWS SERVER PALVELIMELLA

DNSSEC on saatavilla Windows Server 2008 ja uudemmilla palvelimilla. Windows palvelimia käytetään yleisimmin pienissä ja keskikokoisissa yrityksissä, eikä yleensä operaattorien minipalveluina. Tässä luvussa on kuvattu DNSSEC määritysvaiheet Windows 2012 palvelimella opinnäytetyön aiheen kokonaisuuden vuoksi. Windows palvelimien määrittelyyn suositaan graafisen käyttöliittymän käyttöä, mutta nämä vaiheet voitaisiin tehdä myös PowerShell komentorivijärjestelmällä. Yleisimmin Windows palvelimella DNS-palvelu tulee käyttöön Active Directory palvelun yhteydessä, mutta DNS-palvelun voi ottaa käyttöön myös ilman Active Directorya.

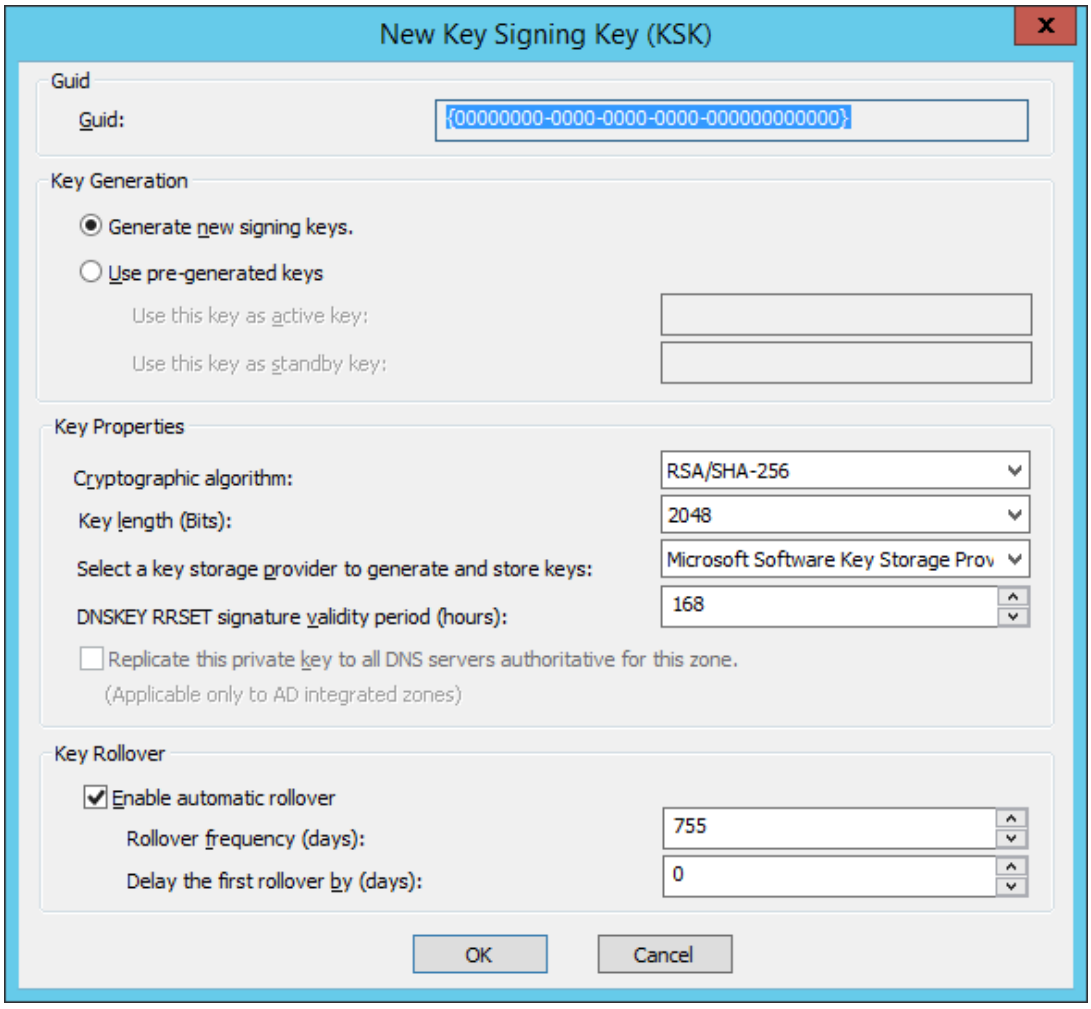


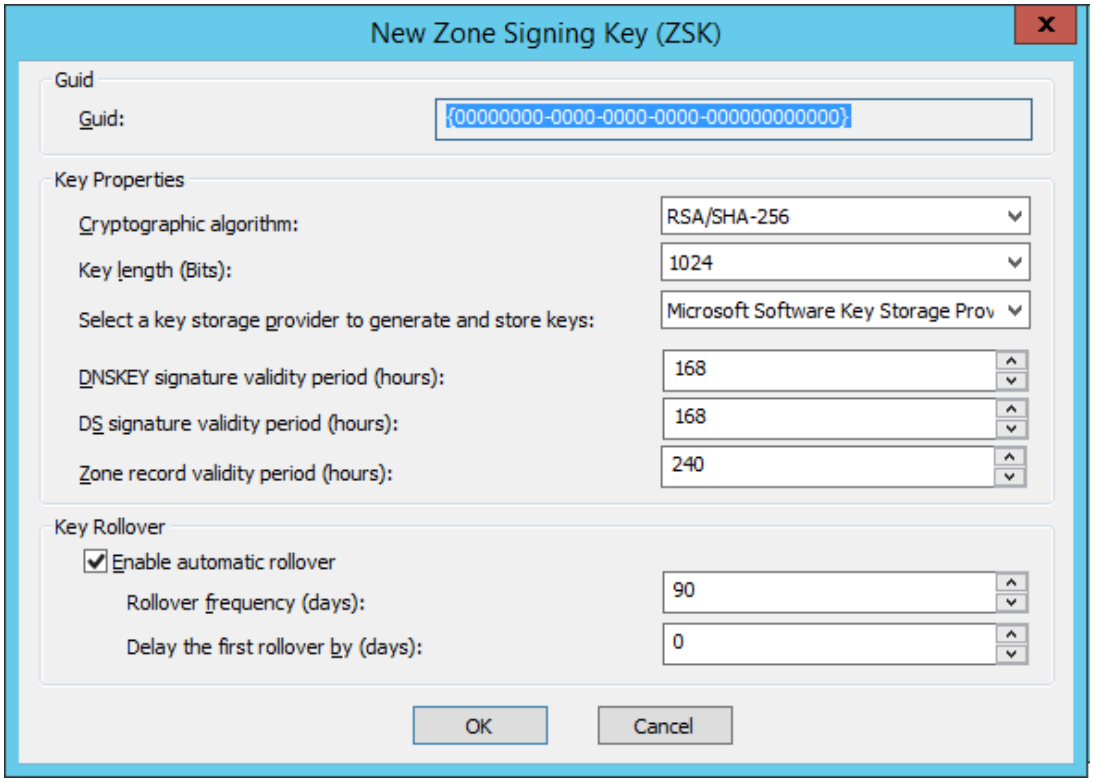
Oletetaan, että DNS-palvelimelle on määritelty jo vyöhyke, joten DNSSEC määritys aloitetaan DNS managerin vyöhykkeen vaihtoehdosta ”Sign the Zone”.



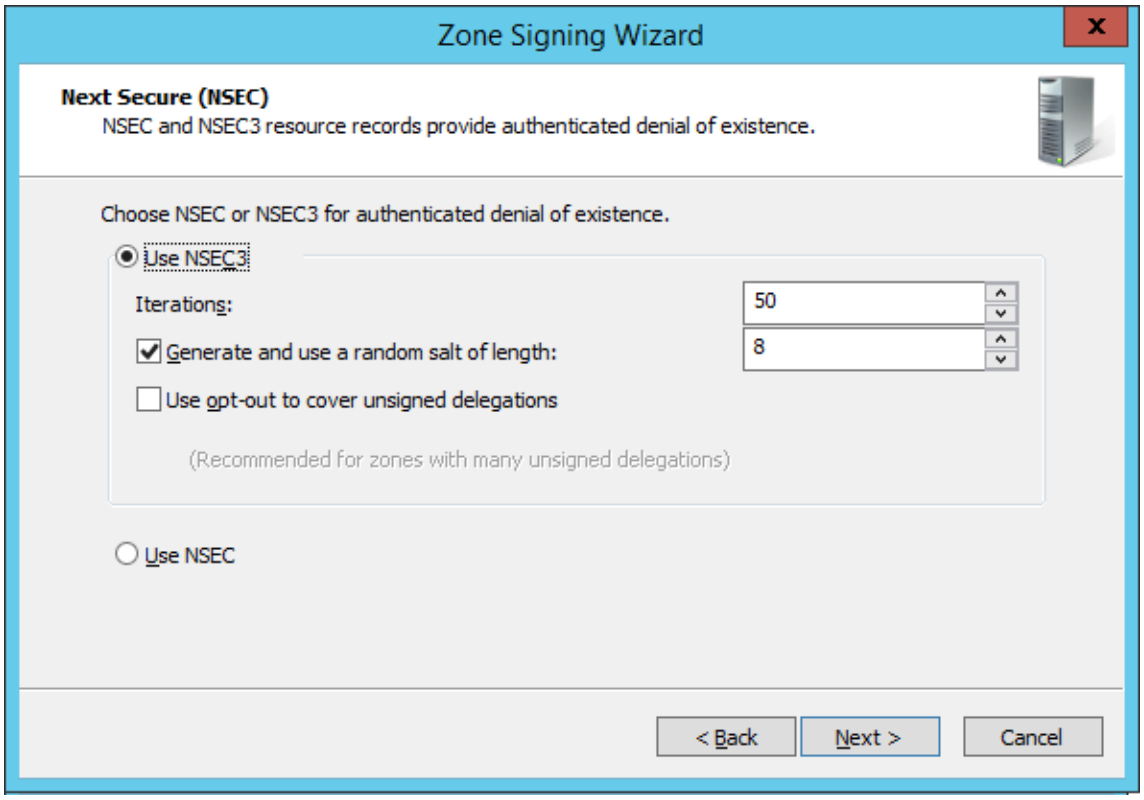
Vyöhykkeen allekirjoittamiseen käytettävä velho ohjaa tuttuun tapaan ja antaa lisätietoa prosessista.

Velhon alussa voidaan valita määritelläänkö vyöhykkeen asetukset itse vai otetaanko ne olemassa olevasta vyöhykkeestä vai käytetäänkö vakioasetuksia.

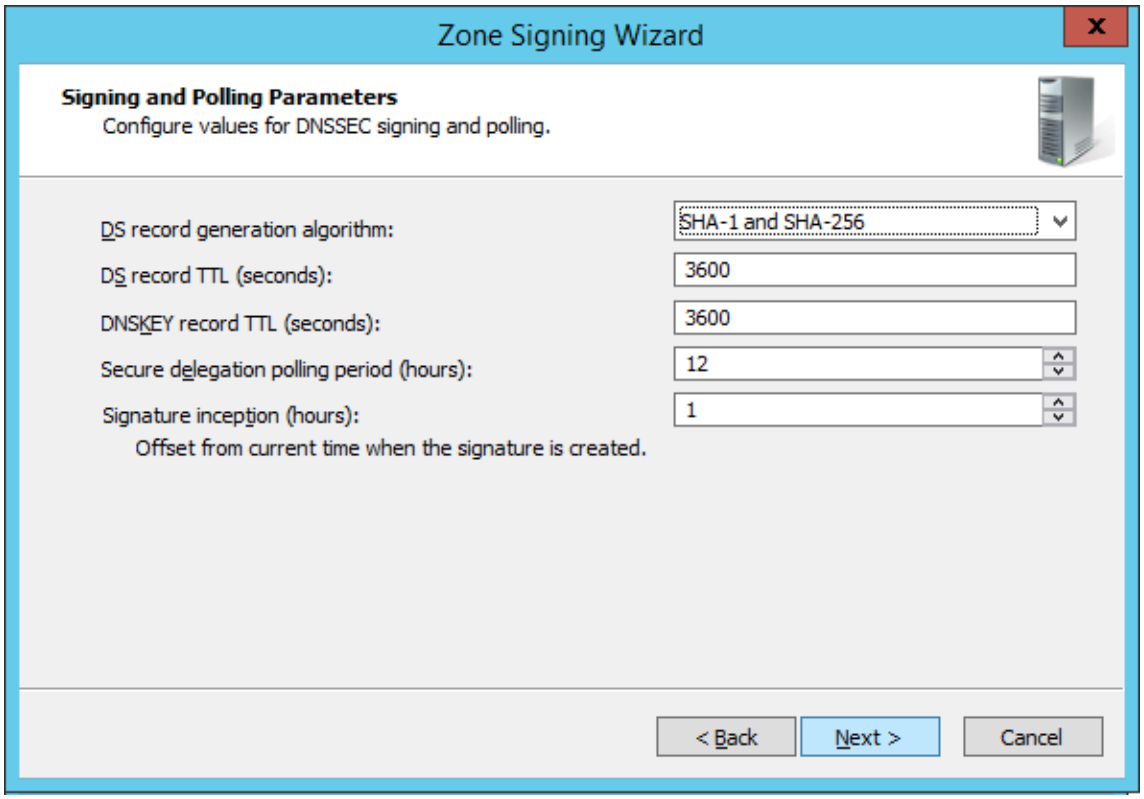

New Key Signing Key (KSK)
Guid
Guid:
{00000000-0000-0000-0000-000000000000}
Key Generation
Generate new signing keys.
Use pre-generated keys
Use this key as active key:
Use this key as standby key:
Key Properties
Cryptographic algorithm:
RSA/SHA-256
Key length (Bits):
2048
Select a key storage provider 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


New Zone Signing Key (ZSK)
Guid
Guid:
{00000000-0000-0000-0000-000000000000}
Key Properties
Cryptographic algorithm:
RSA/SHA-256
Key length (Bits):
1024
Select a key storage provider to generate and store keys:
Microsoft Software Key Storage Prov
DNSKEY signature validity period (hours):
168
DS signature validity period (hours):
168
Zone record validity period (hours):
240
Key Rollover
Enable automatic rollover
Rollover frequency (days):
90
Delay the first rollover by (days):
0
OK
Cancel

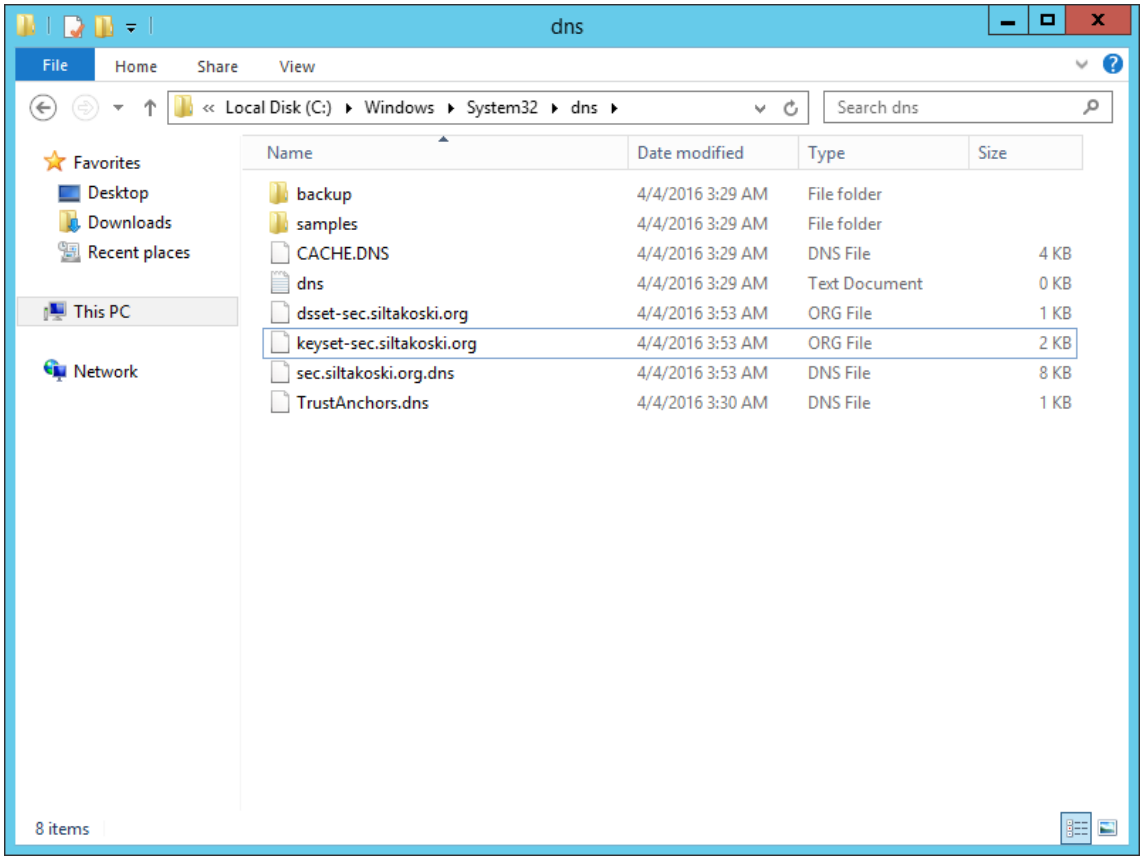
Kun valitaan vyöhykkeen asetuksien muokkaaminen, saadaan paljon vaihtoehtoja KSK ja ZSK asetuksiin. Avaimien algoritmeja ja pituutta voidaan vaihtaa, sekä voidaan valita luodaanko avaimet uudelleen automaattisesti. Tässä automaattisessa uudelleenallekirjoituksella helpotetaan järjestelmänvalvojan toimenpiteitä, jotta niitä ei tarvitse aina manuaalisesti uudelleenallekirjoittaa.



Velho antaa myös mahdollisuuden käyttää joko NSEC3-menetelmää tai NSEC-menetelmää.



DS-tietueen algoritminkin voi valita ja tietueiden aikarajoja muuttaa haluamakseen.



Kun DNSSEC on otettu onnistuneesti käyttöön vyöhykkeellä, avaimia voidaan tarkastella selaamalla resurssinhallinnalla ”C:\Windows\System32\dns”-hakemistoon. (Microsoft TechNet 2014b, hakupäivä 30.3.2016.) Windowsin PowerShellillä voidaan kokeilla DNSSEC toimivuutta resolve-dnsname komennolla. Esimerkiksi.

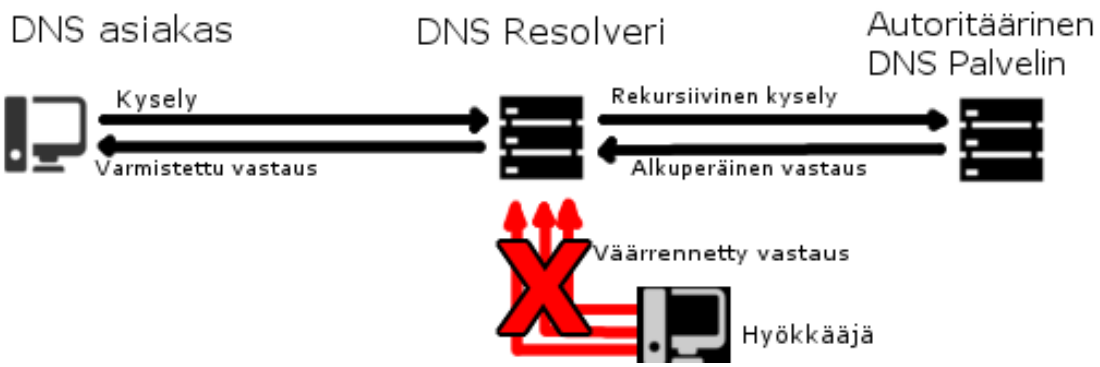
PS C:\> RESOLVE-DNSNAME TEST.SILTAKOSKI.ORG –SERVER DNS1 –DNSSECOK

Komento tuottaa vastauksen, jossa on A-tietueen vastaus, mutta sen perässä myös tietoa sen RRSIG-allekirjoituksesta. Windows palvelimien DNSSEC varmennusta ohjataan Group Policyn avulla. Siitä lisää seuraavan luvun lopussa.

7 DNS CACHE POISONING HYÖKKÄYKSEN ESTÄMINEN

Tämän opinnäytetyön aikana tekijä otti käyttöön useita virtuaalisia koneita, joilla testattiin DNSSEC toimivuutta hyökkäyksen estämisen kannalta. Ympäristönä hyökkäyksien demonstrointiin käytettiin virtuaalisien koneiden yhteistä lähiverkkoa. Verkossa on Debian Linux DNS rekursiivinen resolver, joka esittää ISP:n nimipalvelua. Hyökkäävä Debian Linux DNS palvelin, jolta suoritettiin DNS cache poisoning hyökkäykset. Debian Linux työpöytäkäyttöjärjestelmäinen DNS asiakaskone, sekä Windows 10 asiakaskone.

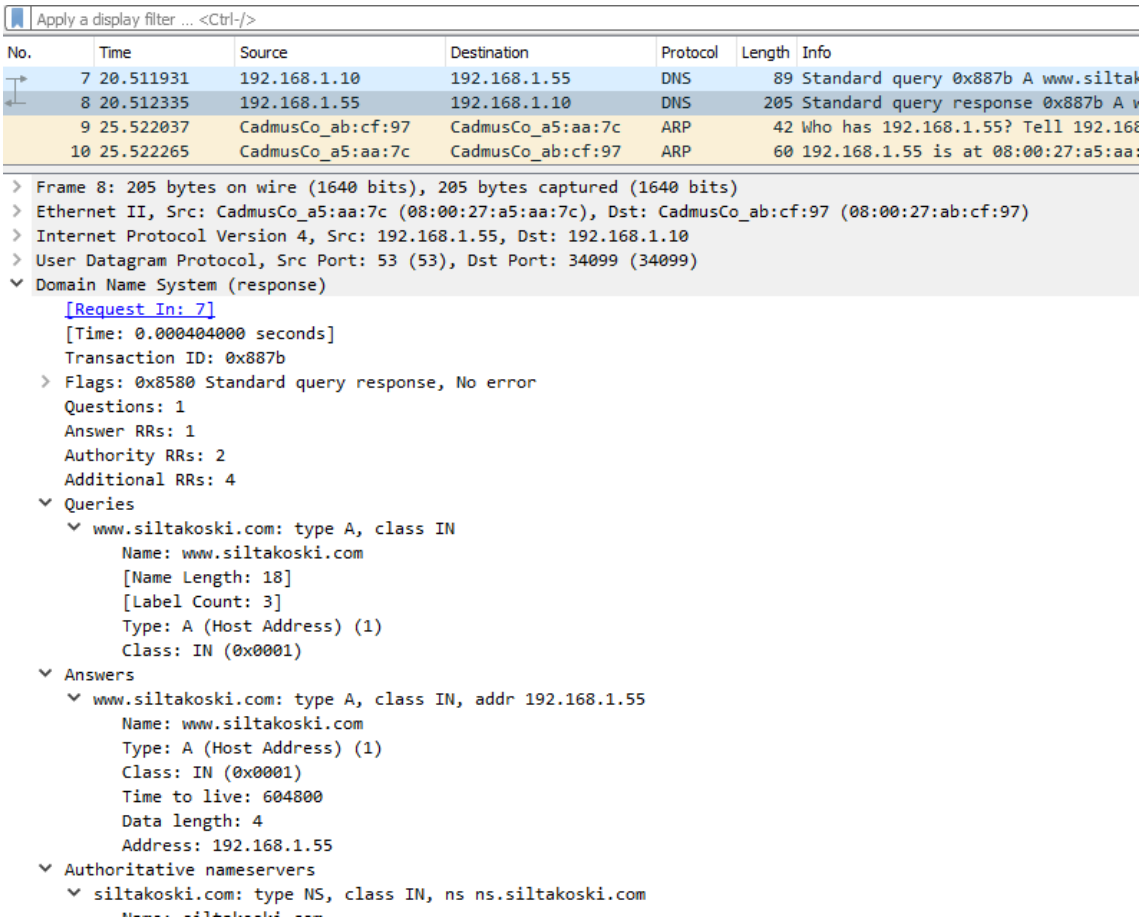
7.1 Hyökkäys resolveriin



DNS resolveriin hyökkäämällä saadaan mahdollisesti saastutettua isolta alueelta useita vyöhykkeitä tai tietueita. Kokeilussa DNS asiakas on osoitteessa 192.168.1.20 DNS resolveri osoitteessa 192.168.1.10 ja hyökkäävä kone 192.168.1.55.

Hyökkäävä kone voi asettaa huijaavan DNS palvelimen, joka esittää olevansa täysin normaali autoritäärinen DNS palvelin (AA flag). Hyökkääjä määrittelee DNS palvelimen vyöhyketietoihin väärennetyt tietueet, jotka hän haluaa syöttää DNS resolverille ja aloittaa sitten hyökkäyksen. Hyökkäyksen simuloimiseksi käytettiin DNS resolveria osoitteesa 192.168.1.10, joka asetettiin lähettämään rekursiiviset kyselyt osoitteessa 192.168.1.55.

Hyökkäys on aloittanut ja resolverin puolella kysytään siltakoski.com osoitteen A-tietuetta.



Vastaus kyselyyn.

Vastauksesta nähdään että hyökkääjä yrittää tarjota A-tietueelle vastauksena IP-osoitetta 192.168.1.55, joka on hyökkääjän IP-osoite. Hyökkääjän koneella on myös web-palvelin käynnissä, josta tarjotaan siltakoski.com esittävää sivua.

APR 14 21:00:45 DNSRESOLVER NAMED[775]: ERROR (NO VALID RRSIG) RESOLVING 'COM/DS/IN': 192.168.1.55#53
APR 14 21:00:45 DNSRESOLVER NAMED[775]: ERROR (NO VALID DS) RESOLVING 'SILTAKOSKI.COM/A/IN': 192.168.1.55#53
APR 14 21:02:24 DNSRESOLVER NAMED[775]: VALIDATING @0X7FB970633C10: SILTAKOSKI.COM A: BAD CACHE HIT (COM/DS)
APR 14 21:02:24 DNSRESOLVER NAMED[775]: ERROR (BROKEN TRUST CHAIN) RESOLVING 'SILTAKOSKI.COM/A/IN': 192.168.1.55#53

DNS-resolverin loki tiedostossa näkyy heti, että hyökkäys estettiin. Ensimmäisenä palvelin tarkistaa com vyöhykkeen RRSIG allekirjoituksen, joka puuttuu. Palvelin ilmoittaa myös siltakoski.com vyöhykkeen DS-tietueen puuttuvan ja näin palvelin tietää, että tämä vastaus ei voi olla aito. Kysely siis epäonnistui ja DNS resolveri antaa vastaukseksi virhekoodin.

; <<>> DIG 9.9.5-9+DEB8U6-DEBIAN <<>> A @127.0.0.1 WWW.SILTAKOSKI.COM
; (1 SERVER FOUND)
;; GLOBAL OPTIONS: +CMD
;; GOT ANSWER:
;; ->>HEADER<<- OPCODE: QUERY, STATUS: SERVFAIL, ID: 45968

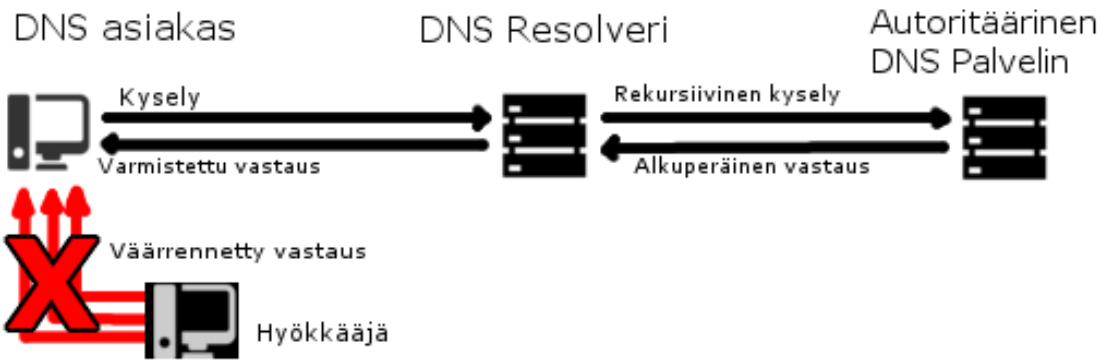
;; FLAGS: QR RD RA; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: VERSION: 0, FLAGS:; UDP: 4096
;; QUESTION SECTION:
;WWW.SILTAKOSKI.COM. IN A

;; QUERY TIME: 1 MSEC
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: THU APR 14 21:03:45 EEST 2016
;; MSG SIZE RCVD: 47

Huomaa kohta “status: SERVFAIL”. Vastauksessa ei ole vastausosaa eikä IP-osoitetta, vaan pelkästään tieto, että kyselyn aikana tapahtui virhe. Virhe näkyy useimmissa ohjelmissa vain normaalina virheenä, eikä vaikuta muuhun toimintaan mitenkään.

7.2 Hyökkäys Linux asiakaskoneeseen

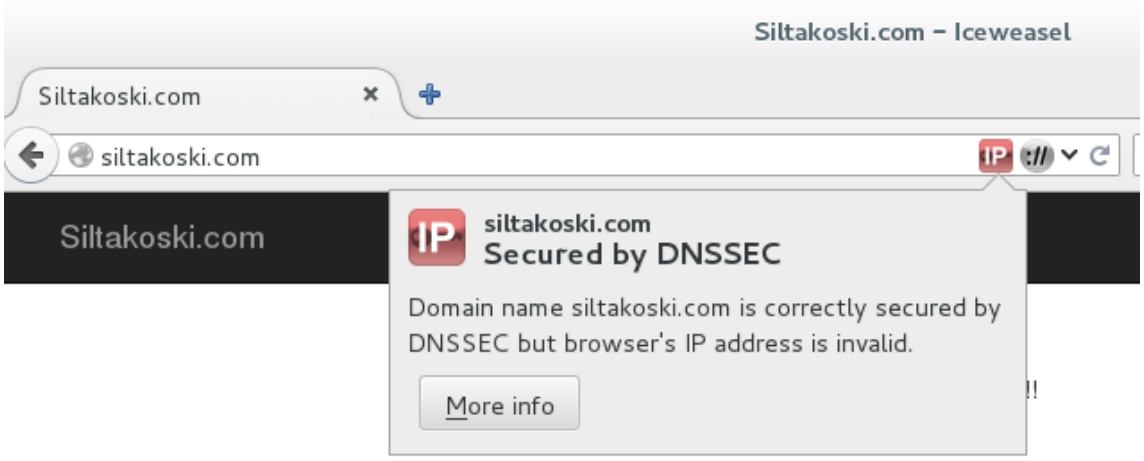


Hyökkäys asiakaskoneeseen. DNS asiakkaan tapauksessa koneessa ei ole muuta kuin stub resolveri, joka ei ole hyödynnä DNSSEC turvaominaisuutta.

Hyökkäys onnistuu vakioasetuksin varustellulla Debian jakelulla. Debian Linux jakelulla on saatavilla dns-sec-trigger paketti, joka asentaa kevyen nimipalvelun vakio resolvin tilalle ja käyttää DNSSEC tietoturva-ominaisuutta. (Debian Wiki 2014, hakupäivä 14.4.2016.)

DNSSEC trigger paketin asentamisen jälkeen siltakoski.com vyöhyke näkyy taas normaalina asiakaskoneessa. Firefox selaimelle saatavilla oleva DNSSEC-validator lisäosa helpottaa tietoturvaominaisuuden toimivuuden varmistamista.

Jos asiakaskoneella ei ole DNSSEC varmennusta, DNSSEC-validator voi varoittaa väärennetystä osoitteesta.



Vyöhyke on onnistuneesti asetettu käyttämään DNSSEC-ominaisuutta, mutta selain on saanut väärän IP-osoitteen hyökkääjältä.

7.3 Hyökkäys Windows asiakaskoneeseen

Windows puolella Windows 7 ja uudemmissa käyttöjärjestelmissä on ”tietoturva tietoinen” resolveri. Se tarkoittaa, että resolveri osaa arvioida onko vastaanotettu DNS vastaus varmistettu vai ei. DNS resolveri itsessään ei tee validointia, vaan se luottaa DNS palvelimen tarjoamaan DNSSEC varmistukseen. Asiakas resolveri voi vaatia validointia palvelimelta, jos Name Resolution Policy Table (NRPT) tauluun on määritelty varmistus Group Policyn avulla. (Microsoft TechNet 2014a, hakupäivä 30.3.2016.)

Ennen DNS kyselyn alkamista käyttöjärjestelmä tarkistaa NRPT ja vertaa kysely nimeä taulusta löytyviin sääntöihin ja käyttää säännön mukaista asetusta kyselyn aikana. Kyselyt, jotka eivät vastaa yhtään sääntöä suoritetaan normaalisti. NRPT taulusta voidaan asettaa DNSSEC varmennus määritellyssä vyöhykkeessä, kaikissa vyöhykkeissä tai vyöhykkeen etu- tai takaliitteellä. (Microsoft TechNet 2014b, hakupäivä 30.3.2016.)

Windows käyttöjärjestelmille on myös saatavilla DNSSEC-trigger ohjelma, joka korvaa Windowsin sisäisen DNS-resolverin DNSSEC ominaisuuden sisältävän nimipalvelimella. Luonnollisesti Firefox selaimen lisäosa DNSSEC-validator toimii myös Windows käyttöjärjestelmällä.

8 POHDINTA

Opinnäytetyön aikana nimipalvelujärjestelmä tuli minulle paremmin tutuksi. Tarkoituksena oli ottaa selville mikä on nimipalvelujärjestelmän tietoturvaomaisuus ja miten sitä käytetään. Autoritäärisien nimipalvelimien määritys ei ole minulle mitään uutta, mutta tietoturvaominaisuuden lisääminen siihen tuo tietynlaista mielenrauhaa. Varsinkin kun kyseinen ominaisuus ei ole vielä laajassa käytössä tai edes isojen organisaatioidenkaan näköpiirissä. Omistan useita verkkotunnuksia, joita käytän moniin tarkoituksiin, mutta siltakoski.com tunnukseni on ollut vähäisessä käytössä, vaikka olen omistanut sen vuodesta 2011 lähtien. Ajattelin että tämä vyöhykkeen nimi on tarpeeksi neutraali, jotta voin käyttää sitä tässä opinnäytetyössä.

DNSSEC ominaisuuden käyttöönotto on huomattavasti helpompaa Windows-palvelin käyttöjärjestelmällä, mutta suurin osa internetin infrastruktuurista varmasti käyttää jotain Linux, UNIX tai BSD pohjaista ratkaisua. Tämän opinnäytetyön kannalta minä näin tärkeäksi tutustua Linux ja Windows määritystoimenpiteisiin.

Mielestäni DNSSEC ei ole täydellinen, mutta se osoittaa oikeaan suuntaan kohti turvallisempaan nimipalvelujärjestelmään. Siinä on huonojakin puolia kuten vastauksien mukana tulevat allekirjoitukset johtavat isompaan datansiirtoon ja tietenkin niiden varmistamiseen käytetään enemmän prosessointivoimaa. Mutta nämä haittapuolet eivät ole iso hinta maksaa siitä, että järjestelmä on luotettavampi, turvallisempi ja eheämpi. Luottamuksellisuus ja eheys ovat tärkeitä asioita internetin turvallisen toiminnan takaamisessa. Tietenkään täysin turvalliseksi mitään järjestelmää ei voi sanoa, mutta tämä on tärkeä askel ottaa. Kuten mikä tahansa standardi, DNSSEC-järjestelmä tulee todennäköisesti muuttumaan tulevaisuudessa ja toivon ihmisten ja organisaatioiden alkavan huomaamaan sen ja lähtemään mukaan.

DNSSEC-järjestelmä on käytössä jo myös fi-tasolla, joten suomalaisilla firmoilla ja organisaatioillakaan ei ole syytä olla hyödyntämättä sitä. Tämän opinnäytetyön alkaessa tarkistin käyttävätkö mitkään pankit tai valtion sivut vielä DNSSEC-järjestelmää. Kokeilemistani verkkotunnuksista seuraavat eivät ole DNSSEC allekirjoitettuja suomi.fi, tunnistus.fi, valtiolle.fi, op.fi, s-pankki.fi, nordea.fi ja suomenpankki.fi. Ainut DNSSEC allekirjoitettu suomen verkkotunnus jonka löysin oli domain.fi, joka on Viestintäviraston verkkosivu. Eikä tilanne näytä kovin lohduttavalta muualla maailmallakaan. Ehkä tietoisuus tästä tekniikasta ei ole vielä levinnyt tarpeeksi pitkälle, vaikka tekniikka on ollut nykyisessä muodossaan käytettävissä useita vuosia. Ehkä yritykset ja organisaatiot luottavat enemmän Transport Layer Security tietoliikenteen salausprotokollaan eivätkä usko tarvitsevansa toista varmennustekniikkaa. Toki DNS-tietoturvaominaisuuden käyttämisen lisäksi voidaan käyttää myös salausprotokollaa, jotta saadaan täydellisempi turva sivustolle. Mielestäni molemmat kannattaisi ottaa käyttöön varsinkin jos verkkosivu on pankki tai valtion virallinen verkkosivu.

LÄHTEET

Arends, R. Austein, R. Larson, M. Massey, D. & Rose, S. 2005a. DNS Security Introduction and Requirements. Hakupäivä 30.3.2016, https://tools.ietf.org/html/rfc4033.

Arends, R. Austein, R. Larson, M. Massey, D. & Rose, S. 2005b. Resource Records for the DNS Security Extensions. Hakupäivä 30.3.2016, https://tools.ietf.org/html/rfc4034.

Atkins, D. 2004. Threat Analysis of the Domain Name System (DNS). Hakupäivä 30.3.2016, https://tools.ietf.org/html/rfc3833.

Debian Wiki. 2014. DNSSEC. Hakupäivä 14.4.2016, https://wiki.debian.org/DNSSEC.

Eastlake, D. 1999. Domain Name System Security Extensions. Hakupäivä 30.3.2016, https://tools.ietf.org/html/rfc2535.

Hardaker, W. 2006. Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs). Hakupäivä 30.3.2016, https://tools.ietf.org/html/rfc4509.

Internet Systems Consertium, Inc. 2014. BIND DNSSEC Guide. Hakupäivä 25.3.2016, http://users.isc.org/~jreed/dnssec-guide/dnssec-guide.html.

Josefsson, S. 2006. Storing Certificates in the Domain Name System (DNS). Hakupäivä 30.3.2016, https://tools.ietf.org/html/rfc4398.

Kolkman, O. Mekking, W. & Gieben, R.. 2012. DNSSEC Operational Practices, Version 2. Hakupäivä 30.3.2016, https://tools.ietf.org/html/rfc6781.

Laurie, B. Sisson, G. Arends, R. & Blacka, D. 2008. DNS Security (DNSSEC) Hashed Authenticated Denial of Existence. Hakupäivä 30.3.2016, https://tools.ietf.org/html/rfc5155.

Microsoft TechNet. 2014a. DNS Clients. Hakupäivä 30.3.2016, https://technet.microsoft.com/en-us/library/dn593685.aspx.

Microsoft TechNet. 2014b. The NRPT. Hakupäivä 30.3.2016, https://technet.microsoft.com/en-us/library/dn593632.aspx.

Mockapetris, P. 1987. DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION. Hakupäivä 29.4.2016, https://tools.ietf.org/html/rfc1035.auto

Perrin, C. 2008. The CIA Triad – TechRepublic. Hakupäivä 29.4.2016, http://www.techrepublic.com/blog/it-security/the-cia-triad/.

Stahl, M. 1987. Domain Administrators Guide. Hakupäivä 14.4.2016, https://tools.ietf.org/html/rfc1032.

```
root@ns1:/etc/bind/zones# dig DNSKEY siltakoski.com. @localhost +multiline
; <<>> DiG 9.9.5-9+deb8u6-Debian <<>> DNSKEY siltakoski.com. @localhost +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34441
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;siltakoski.com.                IN DNSKEY

;; ANSWER SECTION:
siltakoski.com.                604800 IN DNSKEY 256 3 7 (
                               AwEAAaxWli63TP6gBBAXu3HsRjtQsvPLuMj0uZYVuKhc
                               gYHqWBscTV2NBKIMSDeu11z6Zsz2W9WrmGWOtpXt8N+1
                               6HChN8at/Rx3UfVG7sBv+KY0x0LaHq8l/IMSKV0Rn6kS
                               4/UciPOaDkAC8uhw7h9kHH/0kq1r+dy8RUJRGNOFyJ2j
                               b5L3mT/87cXceI703j2KrooxAayl90p7tQBVR/7vQgY6
                               qYOEMNK5eDR9NqeSwnm3fT4hYmTlpLcLN1ZiZta1lsxm
                               2OZi3f7Aj+BV8aiW5Y1wpVqQodYI3EV5dbQFtuWgJvl1
                               wwhzhWzOoS/ld5XB82lldH0kK1e4FsAhLZocyvk=
                               ) ; ZSK; alg = NSEC3RSASHA1; key id = 54050
siltakoski.com.                604800 IN DNSKEY 257 3 7 (
                               AwEAAdhWGc5VYoe6xmYxwhkHNtsXbR5MBT3xJbmEPlt/
                               5o9Y0FcgGPRH/SC/jS+yhPicgRTXfEOPfnJUCQmGqXy+
                               8crwyvATB35NqmMUAZbpad1HYNH4MPm3WVcSV95SDvcv
                               KWhPiIJv7xyRBxXU5Z4GVs8glACKsvXvquQA9RG6yw4t
                               9PyQrDdH5CJVpsyiZmGNmmlfOKD+ruwEn+HtS0APjcZt
                               vHGSNLO74Hx8snGqq/ovGx6zCMC25iU/w8OA6hqifkXL
                               ah2BWvvsPZ+3GKsZKKLF39psnI2/XXchKmAx3c1/+flu
                               tihKTc69lWrASRV0Ncq7kvcfccCkIubXPYRtCaeMKKkX
                               iMRDA4+nRzYZnJCAbnexcRKhDEAEbqEC/CF9ripH9IiW
                               67qv9Yf6F1jjb7InnilFqo2A3diEm3ehuQMhmZJYY6Tw
                               FOkE6IStHxIF9FCwnPvX7cStAIPbPPAyqv9HDoeT+f03
                               QuMjncyQLOyEOUAETNfzNSOBOR53uWsm90ZMLD3X/w9J
                               cZ1InV1I6XpGqhvjwLVWSA+36laE3o5q0fFxzp/5zQOF
                               i00N4MJ4lnbntEDqm/osVlL6nnUVNUsC3KFG64UoxYBn
                               4mRXeqd1gQaehh01dEYYxA+pHMVWaUQG3H/4ucvEjV/+
                               Fi01bxOaSOijmf2dpWk9JXiL34cX
                               ) ; KSK; alg = NSEC3RSASHA1; key id = 15441

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Mar 25 19:09:34 CET 2016
;; MSG SIZE  rcvd: 851

root@ns1:/etc/bind/zones# dig A siltakoski.com. @localhost +noadditional +dnssec +multiline
; <<>> DiG 9.9.5-9+deb8u6-Debian <<>> A siltakoski.com. @localhost +noadditional +dnssec
+multiline
;; global options: +cmd
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28549
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;siltakoski.com.                IN A

;; ANSWER SECTION:
siltakoski.com.                604800 IN A 51.255.206.66
siltakoski.com.                604800 IN RRSIG          A 7 2 604800 (
                               20160424165540 20160325165540 54050 siltakoski.com.
                               C0F6ifPGd0MUatdPWgxYBLn/7Bc3Q6zhYKSq3ptZmjSE
                               IC+hLYBVixO5aG5uCEuQUixeJTlJ9YRWQtTlxR1tRHVR
                               PPTg51URMqXWGcL7uOUScYP4v4IBjC75SJDwTZFJ1yvk
                               N5SLq97LjUhQi0MCe/IQTfdrIH1qV3segqKyUz16BgTr
                               eqi2oAuyFbHDxAc1Oajx26EYL71aWjpNHjtCUEHghpLD
                               zMHaSbcdPqMxz3R5I9IKn/2m0C2kSnlRS4AlaHdK16IU
                               Qm7RJc4IXCOxMRHXlosKvu8xHqpVpXrYulk30Pwr8cn/
                               QGNWRADkLStZBrvgDrtifaoBGslhvpeecw== )

;; AUTHORITY SECTION:
siltakoski.com.                604800 IN NS ns1.siltakoski.com.
siltakoski.com.                604800 IN NS ns2.siltakoski.com.
siltakoski.com.                604800 IN RRSIG          NS 7 2 604800 (
                               20160424165540 20160325165540 54050 siltakoski.com.
                               ZSy/O7BXyh2AVY5jrENt8J9SsSi6589HvMtOjgEwlatN
                               Nv17QUbJSG6Xxs5hLs3Sr9Vyz9xpbXmEiRUAp0r2AlWJ
                               3d+r9MFbD5sVjGYaFt3L4XWq/mFCTqfAny8G3DO6+JSR
                               SjqyiwPtS4tykeTv1crlzvMXG53YBDNUliZuKh0MOyf5
                               zpKDzOv6lcqfUvY77f0JRS3o1GaxfEZSLeEcKexrL1B/
                               kH9wXoDm+8bJ1UVrR4lFFDb8Taebt80194xXssJiei/c
                               WMPgIQGtEXcm50DT2+vt1DvonIEgCKh9ntsWLiD3pR7Y
                               F31NZurMU3MCc/D9hnAw679Hol8SuKZZzA== )

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Mar 25 19:10:15 CET 2016
;; MSG SIZE  rcvd: 1335
```

Domain Name: siltakoski.com

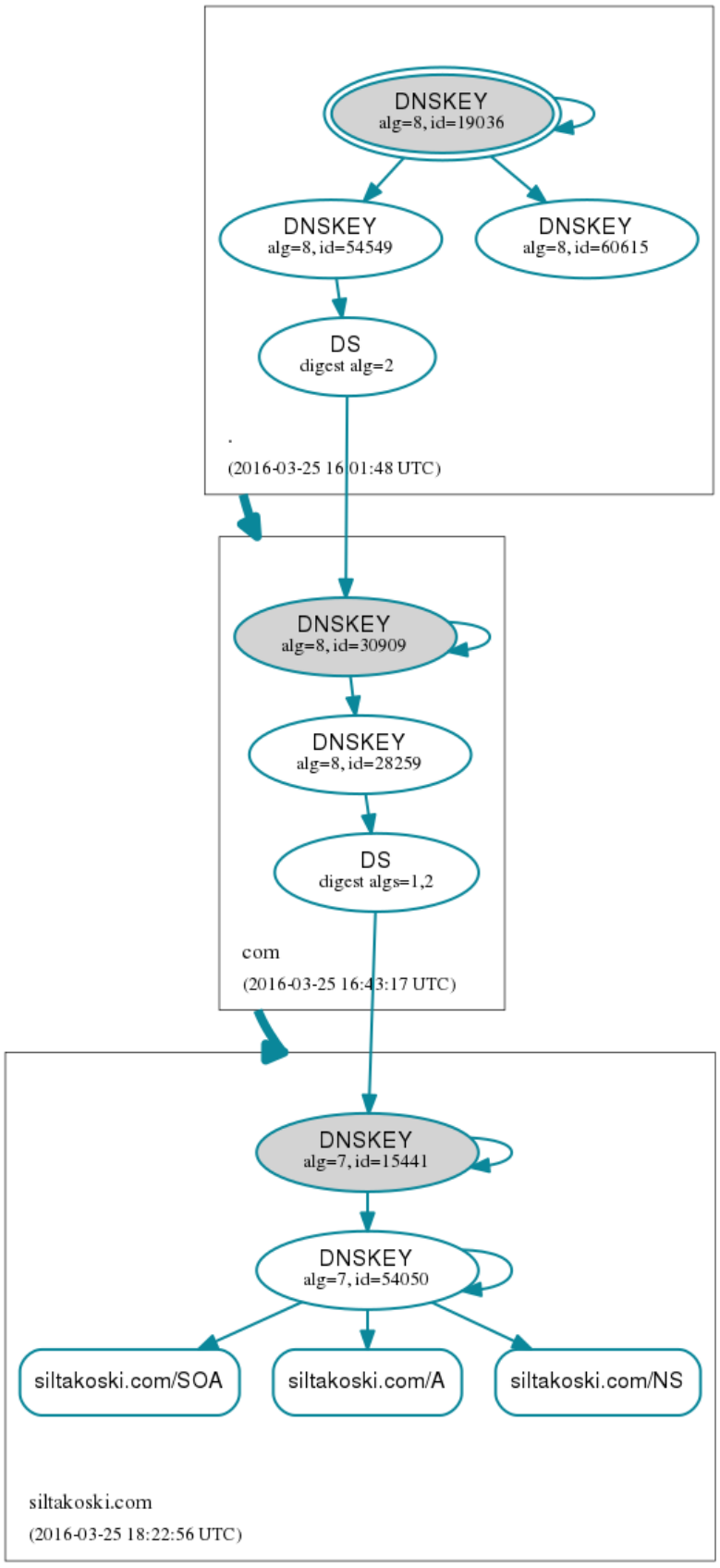
Analyzing DNSSEC problems for siltakoski.com

.	Found 3 DNSKEY records for . DS-19036/SHA-1 verifies DNSKEY-19036/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG-19036 and DNSKEY-19036/SEP verifies the DNSKEY RRset
com	Found 1 DS records for com in the . zone Found 1 RRSIGs over DS RRset RRSIG-54549 and DNSKEY-54549 verifies the DS RRset Found 2 DNSKEY records for com DS-30909/SHA-256 verifies DNSKEY-30909/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG-30909 and DNSKEY-30909/SEP verifies the DNSKEY RRset
siltakoski.com	Found 2 DS records for siltakoski.com in the com zone Found 1 RRSIGs over DS RRset RRSIG-28259 and DNSKEY-28259 verifies the DS RRset Found 2 DNSKEY records for siltakoski.com DS-15441/SHA-256 verifies DNSKEY-15441/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG-15441 and DNSKEY-15441/SEP verifies the DNSKEY RRset siltakoski.com A RR has value 51.255.206.66 Found 1 RRSIGs over A RRset RRSIG-54050 and DNSKEY-54050 verifies the A RRset

Move your mouse over any ⊗ or ⚠ symbols for remediation hints.

Want a second opinion? Test siltakoski.com at dnsviz.net.

http://dnssec-debugger.verisignlabs.com



http://dnsviz.net/