TRAFICOM
Liikenne- ja viestintävirasto

DNSSEC

Turvallisen internetin puolesta

Reitin turvaa
DNSSEC

Mikä on DNSSEC?

DNSSEC on nimipalvelujärjestelmän (DNS) laajennos, jolla varmistetaan nimipalvelimelta saatavien tietojen alkuperä ja eheys. Teknisillä toimenpiteillä on nyt varmistettu, että kyselyn lähettävä tietokone (esim. verkkoselain) pystyy näkemään, tuleeko internetosoitteeseen nimipalvelun kautta saatu vastaus siltä palvelimelta, joka on rekisteröity luotetuksi palvelimeksi.
DNSSEC varmistaa samalla, etteivät tiedot ole muuttuneet internetin kautta kulkiessaan. Lyhyesti sanottuna DNSSEC on eräänlainen vakuutus, joka takaa, että internetin käyttäjät pääsevät juuri sille verkkosivulle, jolle heillä oli aikomus mennä. Salaustoimenpiteenä toimivat salatut allekirjoitukset, sillä varsinaisia tietoja ei salata. Kaikki tieto on edelleen julkisesti saatavilla, kuten nykyisessä nimipalvelujärjestelmässä.

Mihin DNSSECiä tarvitaan?

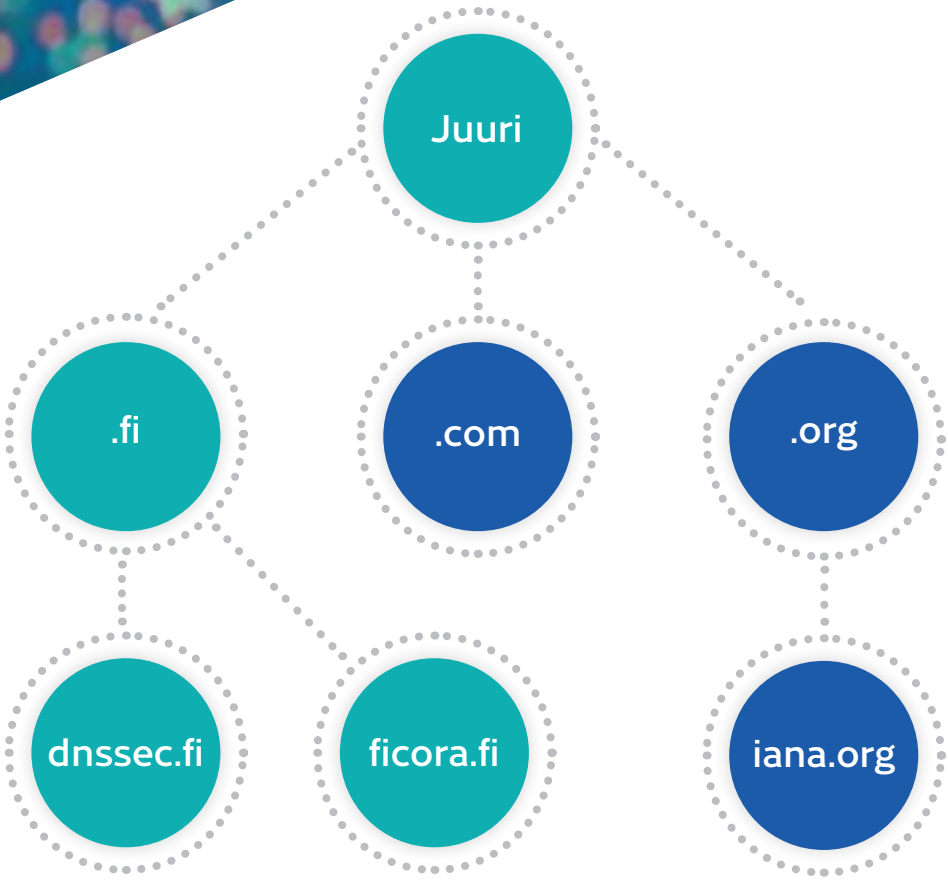
Tarkkaavaiset lukijat ovat jo varmasti huomanneet, että verkkoselaimet käyttävät jo tällä hetkellä tekniikkaa, jonka tarkoituksena on varmistaa, että käyttäjä saapuu oikealle sivustolle. Tämän tyyppiset sivustot on yleensä salattu SSL-tekniikalla (Secure Sockets Layer), mistä selain ilmoittaa avainsymbolilla.

DNSSECin tarkoituksena ei ole korvata SSL-salausta vaan täydentää sitä ja estää tilanteet, joissa käyttäjä joutuu väärälle palvelimelle jo ennen kuin yhteys on turvattu SSL-tekniikalla.

Kuinka nimipalvelujärjestelmä toimii?

Nykyisen internetin perustana on globaali nimipalvelujärjestelmä. Seuraavassa kerrotaan lyhyesti, kuinka se toimii. Nimipalvelua voidaan verrata koko maailman kattavaan puhelinluetteloon, jossa globaalisti ainutlaatuisille verkkotunnuksille (esim. www.dnssec.fi) on annettu omat ainutlaatuiset IP-osoitteensa (esim. 87.239.124.120). Internetosoitteita eli verkkotunnuksia käytetään siksi, että ne on helpompi muistaa. Nimipalvelujärjestelmä on rakenteeltaan hierarkkinen, millä varmistetaan, etteivät kaikki kyselyt päädy samalle palvelimelle. Nimiavaruus on jaettu niin sanottuihin vyöhykkeisiin. Verkkotunnuksessa www.dnssec.fi hierarkian ylätaso (eli juuri) jakautuu Suomen palvelimiin (”fi”) ja edelleen DNSSEC-palvelimiin (”dnssec.fi”). Yksittäisten vyöhykkeiden tehtävät on jaettu eli delegoitu hierarkiassa.

Kun käyttäjä haluaa siirtyä verkkosivustolle www.dnssec.fi, internetyhteyden tarjoajan nimipalvelin käy läpi kaikki hierarkian tasot yksi toisensa jälkeen. Taso, joka ei tiedä vastausta kohdeosoitteelle, lähettää ilmoituksen seuraavalle alemmalle tasolle, kunnes alimman tason palvelin löytää osoitteelle vastauksen.



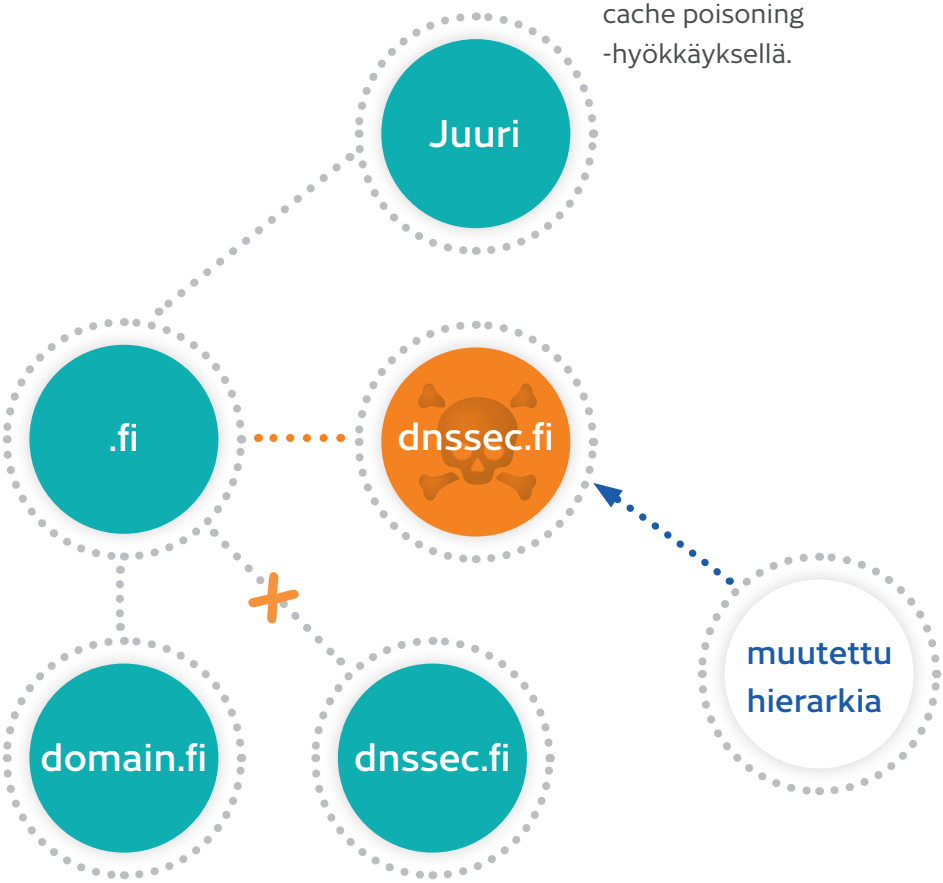
Rakenteeltaan hierarkkisessa nimipalvelujärjestelmässä .fi-verkkotunnuksen nimipalvelimet välittävät pyynnöt .fi-loppuisista verkkotunnuksista (esim. dnssec.fi) automaattisesti oikeaan osoitteeseen.

Mikä on DNSSECin tarkoitus?

Oletetaan, että puhelinluettelon numerotietoja on väärennetty, ja luettelossa ilmoitettu fi-verkkotunnusten asiakaspalvelun numero on väärä. Tällaista luvatonta väärinkäyttöä on lähes mahdotonta havaita. Numerotietojen väärentäminen internetissä voi olla mahdollista, jos hyökkääjä muuttaa edellä kuvatun hierarkian. Jos hyökkääjä onnistuu esimerkiksi saastuttamaan internetyhteyden tarjoajan palvelimen väärillä tiedoilla (cache poisoning), verkkotunnus www.dnssec.fi vie väärälle verkkosivustolle. Seuraukset voivat olla vakavat, jos väärennetty verkkosivusto kuuluu esimerkiksi pankille tai jos yrityksesi uusin strategia päätyy yhteistyökumppanin väärennetylle palvelimelle. Internetiä käytetään nykyisin useisiin eri tarkoituksiin, joten hakkerien hyökkäyksillä voi olla kauaskantoisia seurauksia. DNSSEC tarjoaa tehokkaan suojan verkkotunnusten väärentämistä ja muita hyökkäyksiä vastaan.

DNSSEC ei estä tietojen kalastelua eli phishingiä, mutta se suojaa tehokkaasti nimipalvelujärjestelmään kohdistuvilta hyökkäyksiltä. Juuri tämä on tärkeää, sillä valppaat internetin käyttäjät tunnistavat itse useimmat phishing-yritykset, mutta edes ammattilaiset eivät havaitse nimipalveluun kohdistuvia hyökkäyksiä.

Hierarkiaa voidaan muuttaa ns. cache poisoning -hyökkäyksellä.



DNSSEC pähkinänkuoressa

Kuten edellä mainittiin, DNSSECin perustana ovat salatut allekirjoitukset, joilla nimipalveluhaut allekirjoitetaan. Internetin verkkotunnuksesta vastaava taho voi suojata tietonsa DNSSECillä.Kaikki internetpalveluntarjoajan vastuulla oleva tieto allekirjoitetaan palveluntarjoajan omalla avaimella, ja allekirjoitukset tallennetaan nimipalvelujärjestelmään RRSIG-tietueina.

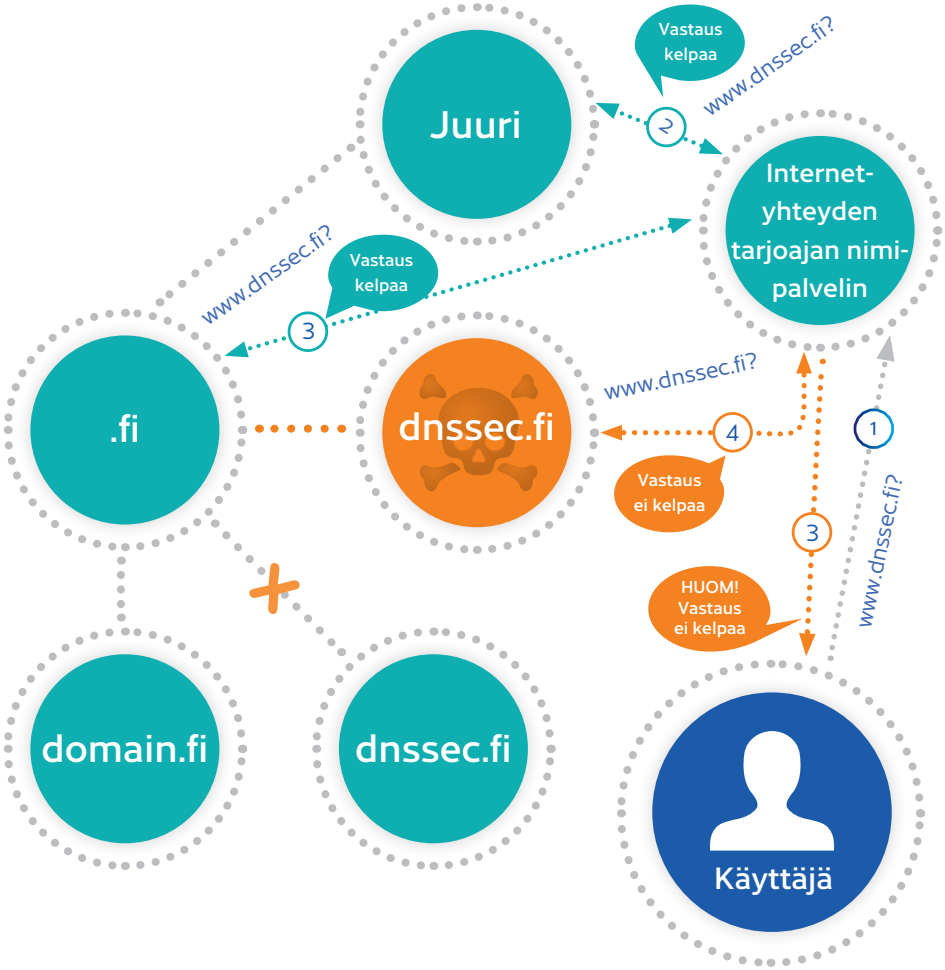
Esimerkki DNSSECin käytöstä:
Internetyhteyden tarjoajan nimipalvelin noudattaa edellä esiteltyä hierarkiaa kyselyyn vastaamiseksi. DNSSECin avulla se voi kuitenkin tarkistaa saatujen allekirjoitusten perusteella, tuleeko vastaus oikeasta lähteestä ja onko se muuttunut matkalla. Nimipalvelin vastaa ainoastaan, jos kaikki vaaditut tiedot ovat oikein.

Kuinka kaikki allekirjoitukset voidaan varmentaa?

Digitaalisen allekirjoituksen luomiseen tarvitaan avainpari, joista toinen on yksityinen ja toinen julkinen (epäsymmetrinen salausjärjestelmä). Kuten nimestä voi päätellä, yksityinen avain on salainen ja on ainoastaan omistajan hallussa. Julkinen avain taas julkaistaan nimipalvelimessa DNSKEY-tietueena. Allekirjoitus voidaan varmentaa yksityistä avainta vastaavalla julkisella avaimella.

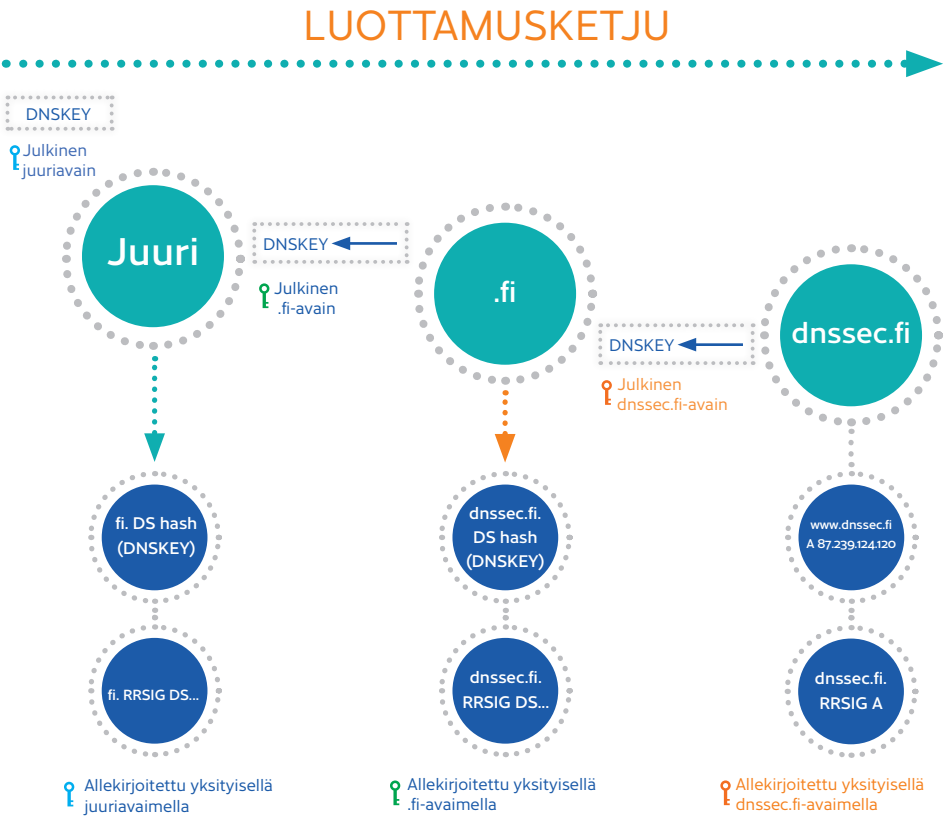
Julkiseen avaimeen on siis voitava luottaa ennen kuin allekirjoitus pystytään varmentamaan. Kaikkiin internetistä löytyviin avaimiin ei voi luottaa, joten apuna käytetään nimipalvelun hierarkian kaltaista avainhierarkiaa (”chain of trust” eli luottamusketju). Toimintatapa vaikuttaa ensi näkemältä monimutkaiselta, mutta sen tarkoituksena on ainoastaan varmistaa, että kaikki allekirjoitukset voidaan varmentaa yhdellä julkisella avaimella.

DNSSECin avulla internetyhteyden tarjoajan nimipalvelin pystyy tunnistamaan hierarkian, jota on muutettu cache poisoning -hyökkäyksellä.



Luottamusketju

Julkinen avain lähetetään aina hierarkiassa seuraavalle ylemmälle tasolle. Ylempi taso tallettaa avaimen vyöhykkeelleen DS-tietueena ja takaa sen oikeellisuuden allekirjoittamalla sen. Sen jälkeen tämän tason julkinen avain lähetetään jälleen seuraavalle ylemmälle tasolle. Luottamusketjussa ylin taso (esim. .fi-tunnuksen nimipalvelin) takaa alemmalta tasolta tulleen tiedon oikeellisuuden.



Mitä tarvitaan DNSSECin käyttöön?

Internetin käyttäjältä ei edellytetä toimenpiteitä. Jos ADSL- tai kaapelimodeemiyhteyden tarjoaja tukee DNSSECiä, kaikki allekirjoitusten varmennukset tapahtuvat tarjoajan nimipalvelimilla.

Verkkotunnuksen haltijan tapauksessa verkko-operaattorin on otettava DNSSEC käyttöön. On todennäköistä, että ennen kuin DNSSECin käyttö yleistyy, sillä suojaavat verkkotunnuksensa alkuvaiheessa lähinnä suojausta tarvitsevat verkkosivujen ylläpitäjät (kuten pankit).

Esitteen teksti pohjautuu the Swiss education and research networkin (www.switch.ch) aineistoon.

Liikenne- ja viestintävirasto Traficom

Asiakaspalvelu
p. 0295 345 656 / Fi-verkkotunnusasiat / arkisin klo 9-15
p. 0295 34 5000 / Traficomin puhelinvaihde / arkisin klo 8-6.15
Postiosoite
Liikenne- ja viestintävirasto Traficom
PL 320
00059 TRAFICOM
Lisätiedot
www.domain.fi / www.traficom.fi

TRAFICOM
Liikenne- ja viestintävirasto