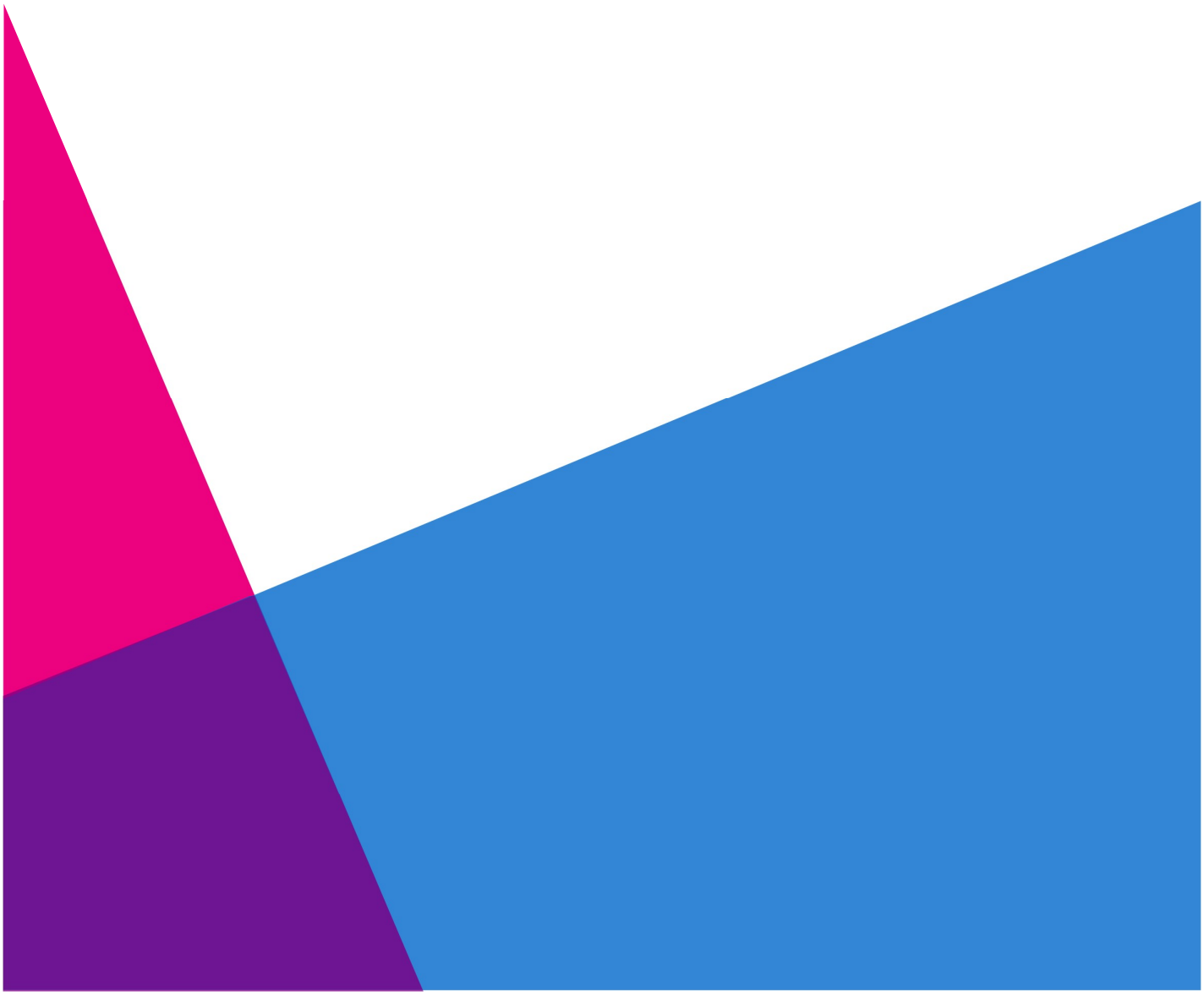
TRAFICOM
Liikenne- ja viestintävirasto

.fi DNSSEC Practice Statement (DPS)

Asiakirjatyyppi: Dokumentaatio
Luontipäivämäärä: 2. elokuuta 2021
Päivitetty: -



Sisältö

1 Johdanto

Tämä asiakirja sisältää Traficomin kuvauksen niistä turvallisuuskäytännöistä ja -järjestelyistä, joita sovelletaan Traficomin hallinnoiman ylätason .fi-verkkotunnuksen nimipalvelun turvallisuuslaajennus DNSSECin (DNS Security Extensions) toimintaan.

Tämä asiakirja noudattaa suurimmalta osin ohjetta RFC 6841: A Framework for DNSSEC Policies and DNSSEC Practice Statements (DPS).

1.1 Yleiskatsaus

Nimipalvelun turvallisuuslaajennus DNSSEC (Domain Name System Security Extensions) koostuu joukosta IETF:n määrittelyjä, joiden avulla nimipalveluun (Domain Name System, DNS) lisätään alkuperän todennus ja tietojen eheyden varmistaminen. DNSSECin avulla ohjelmisto voi tarkistaa, ettei DNS-tietoja ole muokattu tai muutettu matkalla. Tämä on toteutettu sisällyttämällä DNS-hierarkiaan digitaalisia allekirjoituksia ja julkiseen avaimeen perustuva salaus. Luottamuksen jakelu perustuu DNS-puurakenteeseen, mikä tarkoittaa, että luottamusketju alkaa juurivyöhykkeeltä ja se delegoidaan samalla tavalla kuin vastuu vyöhykkeestä.

1.2 Asiakirjan nimi ja tunniste

.fi DNSSEC-käytäntökuvaus (DPS)

1.3 Kohderyhmä ja sovellusala

Seuraavassa on nimetty ne tahot, joihin tätä asiakirjaa sovelletaan.

1.3.1 Rekisteri

Traficom vastaa ylätason .fi-verkkotunnuksen hallinnasta ja teknisestä toiminnasta ja sen seurauksena myös alemman tason vyöhykkeiden tunnistamiseen käytettävien verkkotunnusten rekisteröinnistä. Tämä tarkoittaa myös, että Traficom huolehtii kaikkien verkkotunnukseen liittyvien tietojen täydentämisestä, muuttamisesta ja poistamisesta.

Traficom on vastuussa seuraavista asioista:

- DNSSECissä käytetyn salausavaimen materiaalin generointi
- avainparien yksityisen komponentin salassapidon suojaaminen
- kaikkien autoritääristen DNS-resurssitietueiden turvallinen allekirjoittaminen kohdevyöhykkeellä käyttäen DNSSECiä sille määritettyjen avainten avulla.

Traficom on myös vastuussa DS-resurssitietueiden turvallisesta viennistä, rekisteröimisestä ja ylläpidosta juurivyöhykkeellä, mikä luo luottamusketjun juurivyöhykkeeltä kohdevyöhykkeelle ja mahdollistaa DNS-tietueiden validoinnin juurivyöhykkeen avaimella.

1.3.2 Verkkotunnusvälittäjät

Verkkotunnusvälittäjä on vastuussa verkkotunnuksen hallinnosta ja ylläpidosta Verkkotunnuksen käyttäjän puolesta. Verkkotunnusvälittäjä huolehtii verkkotunnuksen rekisteröinnistä, ylläpidosta ja hoidosta ja toimii Traficomin yhteistyökumppanina. Verkkotunnusvälittäjä on vastuussa verkkotunnuksen käyttäjän turvallisesta tunnistamisesta ja kullekin verkkotunnukselle määritettyjen DS-tietueiden lisäämisestä, poistamisesta tai päivittämisestä verkkotunnuksen käyttäjän pyynnöstä.

1.3.3 Verkkotunnuksen käyttäjä

Verkkotunnuksen käyttäjä on se fyysinen henkilö tai oikeushenkilö, joka on rekisteröinyt verkkotunnuksen ja jonka hallussa tunnus on. Verkkotunnusten käyttäjät ovat vastuussa omien DNSSEC-avaintensa generoinnista ja suojaamisesta, asiaan liittyvien tietojen allekirjoittamisesta ja niitä vastaavien DS-tietueiden rekisteröinnistä ja ylläpidosta verkkotunnusvälittäjän kautta.

Verkkotunnuksen käyttäjä on myös vastuussa avainten korvaamisesta, jos avaimet ovat kadonneet tai jos epäillään, että ne ovat vaarantuneet.

1.3.4 Luottava osapuoli

Luottava osapuoli luottaa DNSSEC-allekirjoituksiin; luottavia osapuolia ovat esimerkiksi validoivien resolvereiden operaattorit ja osapuolet, jotka tarjoavat muita vastaavia sovelluksia. Luottava osapuoli vastaa asianmukaisten luottamusankkurien konfiguroinnista ja ylläpidosta.

1.3.5 Sovellusala

Kukin rekisteröijä on vastuussa asianmukaisen turvallisuustason määrittelemisestä verkkotunnukselleen. Tämä DPS (DNSSEC Practice Statement, DNSSEC-käytäntökuvaus) koskee ainoastaan Traficomin hallinnoimaa ylätason .fi-verkkotunnusta, ja siinä kuvataan kohdevyöhykkeellä DNSSECin hallinnassa käytettävät menettelyt, turvavalvontatoimenpiteet ja käytännöt.

Tämän DPS:n avulla luottava osapuoli voi määritellä DNSSECille haluamansa luottamuksen tason kohdevyöhykkeelle ja arvioida omat riskinsä tämän ja muiden asioiden perusteella.

1.4 Määritysten hallinta

Tätä DPS:ää päivitetään tarvittaessa, kuten esimerkiksi, jos järjestelmiin tai käytäntöihin tehdään merkittäviä muutoksia joilla on merkittävä vaikutus tämän asiakirjan sisältöön.

Traficomin tietoturvasta vastaava johtaja vastaa myös DPS:n määritysten hallinnasta. Vastuu hyväksynnästä ja julkaisemisesta on viime kädessä Traficomin .fi-verkkotunnustiimillä.

1.4.1 Määritysten hallintaorganisaatio.

Liikenne- ja viestintävirasto Traficom

1.4.2 Yhteystiedot

Liikenne- ja viestintävirasto Traficom

fi-domain-tech@traficom.fi

1.4.3 Määritysten muutoskäytännöt

Muutokset DPS:ään tehdään joko korjauksina tai julkaistaessa uusi versio asiakirjasta. Tämä DPS ja sen mahdolliset muutokset julkaistaan kohteessa:

https://www.traficom.fi/

Vain tämän DPS:n viimeisin versio on voimassa. Traficom pidättää oikeuden muuttaa DPS:ää ilmoittamatta erikseen korjauksista, joita ei ole merkitty tärkeiksi turvallisuuden kannalta. Traficom ilmoittaa merkittävistä muutoksista yllä mainitulla sivustolla.

2 Avainten julkaiseminen

2.1 Avainten allekirjoitusavainten (KSK) julkaiseminen

.fi-juuri käyttää jaetun avaimen allekirjoitusmallia (split-key signing, ks. kohta 6.1) ja julkaisee tarvittavat allekirjoitusavaimet (Key Signing Key, KSK) kohdevyöhykkeille seuraavasti:

Suoraan juurivyöhykkeellä (vain DS)

DS-tietueiden päivittämisessä juurivyöhykkeelle käytetään turvallisia menetelmiä.

3 Operatiiviset edellytykset

3.1 Verkkotunnusten merkitys

Verkkotunnus on yksilöllinen tunniste, joka liitetään usein eri palveluihin, kuten verkkosivuihin tai sähköpostiin. Kaikki yksityishenkilöt ja oikeushenkilöt, joilla on henkilötunnus tai y-tunnus, tai jotka voidaan tunnistaa viranomaisen tai viranomaista vastaavan organisaation rekisterin kautta, voivat hakea rekisteröintiä ylätason verkkotunnusten alle. Ulkomaalaiset hakijat voivat käyttää muita tunnistautumiskeinoja.

Verkkotunnukset rekisteröidään ylätason verkkotunnusten alle saapumisjärjestyksessä; verkkotunnukset siis annetaan siinä järjestyksessä, missä Traficomin rekisteripalvelut saavat niitä koskevat hakemukset. .fi-verkkotunnusten rekisteröintiehdot julkaistaan osoitteessa:

- https://www.finlex.fi/fi/laki/ajantasa/2014/20140917
- https://www.finlex.fi/fi/viranomaiset/normi/480001/42590

3.2 Alemman tason vyöhykkeen haltijan tunnistaminen ja todentaminen

Rekisterinpitäjä on vastuussa rekisteröijän turvallisesta tunnistamisesta ja todentamisesta sopivan mekanismin avulla Traficomin kansallisten määräysten mukaisesti.

3.3 Delegoinnin allekirjoittaja (delegation signer, DS) -tietueiden rekisteröinti

DNSSEC aktivoidaan julkaisemalla vähintään yksi DS-tietue ylätason verkkotunnuksen alla olevalle vyöhykkeelle. DS-tietueiden julkaiseminen luo luottamusketjun alemman tason vyöhykkeelle annettuihin avaimiin. Rekisterissä oletetaan, että jos DS-tietueiden syntaksi on oikein, ne ovat myös kelvollisia, eikä ylimääräisiä tarkastuksia suoriteta esimerkiksi sen varmistamiseksi, että määritetyt avaimet kuuluvat alemman tason vyöhykkeen avainsarjaan.

Rekisterissä hyväksytään DS-tietueita rekisterinpitäjiltä EPP-liittymän kautta siinä muodossa, joka on määritelty DNS-järjestelmän turvallisuuslaajennusten kartoittamista EPP-protokollaa varten käsittelevässä asiakirjassa RFC 5910 ”Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)”. Kullekin verkkotunnukselle voi rekisteröidä enintään kuusi (6) DS-tietuetta.

3.4 Yksityisen avaimen hallinnan todistamismenetelmä

Traficom ei suorita mitään tarkastuksia sen varmistamiseksi, että rekisteröijällä on hallussaan tietty yksityinen avain. Rekisterinpitäjä on vastuussa sekä vaadittavien että muiden rekisterinpitäjän tarpeellisina pitämien tarkastusten suorittamisesta.

3.5 DS-resurssitietueiden poistaminen

DS-tietue poistetaan joko lähettämällä EPP-käsky rekisterinpitäjältä rekisteriin tai rekisterinpitäjän verkkoliittymän kautta. Kaikkien DS-tietueiden poistaminen poistaa käytöstä myös kyseisen alemman tason vyöhykkeen DNSSEC-turvallisuusmekanismit.

3.5.1 Poistopyyntö

Rekisteröijällä on oikeus pyytää DS-tietueiden poistamista. Jos rekisterinpitäjä toimii rekisteröijän verkkotunnuksen nimipalvelimen tarjoajana, rekisterinpitäjällä on oikeus poistaa nämä DS-tietueet, vaikka rekisteröijä ei olisi sitä erikseen pyytänyt. Traficom pidättää oikeuden poistaa DS-tietueita, jos ne Traficomin mielestä aiheuttavat tai saattavat aiheuttaa vakavia häiriöitä toiminnalle. Jos nimipalvelimen ylläpitäjä julkaisee DNSSECiä varten tarvittavat tiedot, Traficom voi poistaa kyseisten verkkotunnusten DS-tietueet.

3.5.2 Poistopyyntömenettely

Rekisteröijä tai sen nimeämä edustaja antaa rekisterinpitäjälle tehtäväksi poiston suorittamisen. Jos rekisterinpitäjä ei ole näiden verkkotunnusten nimipalvelimen ylläpitäjä, se voi suorittaa poiston vain toimiessaan rekisteröijän puolesta. Kun Traficom saa poistokehotuksen EPP:n tai rekisterinpitäjän web-käyttöliittymän kautta, poisto suoritetaan seuraavan vyöhykkeen generoinnin yhteydessä.

Jos rekisterinpitäjä on rekisteröijän verkkotunnuksen tai -tunnusten nimipalvelimen ylläpitäjä, sillä on oikeus lisätä, poistaa tai muuttaa näiden verkkotunnusten DS-tietueita, vaikka rekisteröijä ei olisi sitä erikseen pyytänyt. Normaalisti vyöhyke päivitetään kerran tunnissa. Tämän jälkeen elinaika (TTL) ja jakeluaika huomioon ottaen voi kestää kauemmin, ennen kuin uuden delegaatiotiedon jakelu on valmistunut ja se on otettu käyttöön kaikkialla. Rekisteröijien tulee ottaa tämä huomioon laatiessaan allekirjoitusmalliaan ja korvatessaan avaimia.

3.5.3 Hätäpoistopyyntö

Jos rekisteröijä ei voi tehdä poistopyyntöä senhetkisen rekisterinpitäjänsä kautta, Traficom kehottaa rekisteröijää vaihtamaan verkkotunnusvälittäjää ja lähettää viestin mukana välittäjän vaihtoavaimen, jota voi käyttää vaihdon suorittamiseen.

Traficomilla on oikeus muuttaa ja poistaa DS-tietueita tai estää niiden julkaiseminen ainoastaan, jos ne aiheuttavat tai saattavat aiheuttaa vakavaa vahinkoa toiminnalle tai häiriöitä Traficomin hallinnoimassa ylätason verkkotunnuksessa.

4 Tilajohtaminen ja hallinnolliset valvontatoimenpiteet

4.1 Fyysiset valvontatoimenpiteet

Fyysinen alueen rajojen suojaus, valvonta ja kulunvalvonta sekä asianmukaiset korvaavat valvontamenettelyt toteutetaan jatkuvaan riskianalyysiin ja uhkien uudelleenarviointiin perustuen, jotta voitaisiin varmistaa, että rekisteriin ja allekirjoittajajärjestelmiin ei voi kajota eikä niitä voi varastaa tai sabotoida.

4.1.1 Toimipaikan sijainti ja rakenne

.fi-allekirjoitusjärjestelmän palvelimet sijaitsevat kahdessa toiminnallisesti kahdennetussa ja maantieteellisesti erillisessä konesalissa yli 5 kilometrin etäisyydellä toisistaan. Kaikki DNS-tiedot päivitetään konesalista toiseen jatkuvasti automaattisen kahdentamisen avulla.

Molemmissa konesaleissa on toteutettu toisiaan vastaavat fyysiset turvavalvontatoimenpiteet monikerroksisena rakenteena, jonka sisintä tasoa valvotaan ja tarkkaillaan tiukasti.

4.1.2 Fyysinen pääsy

Kaikki kriittiset komponentit ovat käytettävissä kummassakin toimintaan käytettävässä konesalissa. Saapumiset kirjataan lokiin ja aluetta valvotaan jatkuvasti.

4.1.3 Virtalähde ja ympäristö

Laitokset tarjoavat hallitun, säännellyn ja valvotun toimintaympäristön. Kussakin laitoksessa on kahdennettu virransyöttö maan alta erillisiltä muuntoasemilta. Laitokset saavat lisäksi varavoimaa generaattoreista, jotka pystyvät tuottamaan virtaa konesalille ainakin 24 tunnin ajan.

4.1.4 Vesivahingot

Konesaleissa on ilmaisinmekanismeja, ja ne on suojattu tulvaa vastaan.

4.1.5 Palonehkäisy ja -torjunta

Konesaleissa on paloilmoittimet ja automaattiset sammutusmekanismit, jotka perustuvat kuivien sammutteiden käyttöön. Konesalien lattia on korotettu, ja jokainen konesalin huone muodostaa erillisen palo-osaston.

4.1.6 Median tallennustilan hallinta

Traficom on toteuttanut ja pitää yllä tietojen luokittelujärjestelmää, jossa määritellään vaatimukset arkaluontoisen tiedon varastoinnille. Tällaista tietoa sisältävät tallennusvälineet säilytetään paikoissa, joiden fyysinen suojaus on samaa tasoa kuin laitetilojen.

4.1.7 Jätehuolto

Joko Traficom tai sopimuskumppani hävittää turvallisesti poistetut tallennusvälineet ja muut materiaalit, jotka saattavat sisältää arkaluontoista tietoa. Tämä koskee soveltuvin osin myös HSM-moduuleita.

4.1.8 Varmuuskopiot laitoksen ulkopuolella

Tiettyjä kriittisiä tietoja säilytetään myös turvallisesti laitoksen ulkopuolella. Laitoksen ulkopuoliset varmuuskopiot säilytetään salattuina, ja pääsy salausavaimiin on rajoitettu henkilöihin, joilla on järjestelmänvalvojan rooli (system administrator, SA). Varastotilat ovat maantieteellisesti eri paikassa kuin muut toimintaan käytettävät laitokset. Varastotilojen fyysinen suojaus on vähintään saman tasoinen kuin muilla toimintaan käytettävillä laitoksilla.

4.2 Menettelytapoja koskevat valvontatoimenpiteet

4.2.1 Luottamusroolit

Luottamusroolit on annettu henkilöille, jotka osallistuvat yksityisten avainten materiaalin generointiin ja käyttöön sekä kohdevyöhykkeiden julkisten avainten materiaalin toimittamiseen ja julkaisuun. Luottamusroolit ovat:

1. Järjestelmänvalvoja (Systems Administrator, SA)

2. Turvallisuusvalvoja (Security Officer, SO)

Kuhunkin luottamusrooliin tulee aina olla nimitettynä vähintään kaksi henkilöä. Yhdellä henkilöllä ei voi olla enempää kuin yksi luottamusrooli kerrallaan.

4.2.2 Tehtävää kohti vaadittavien henkilöiden määrä

Kriittisten toimintojen velvollisuudet ja roolit on eriytetty. Näissä tehtävissä vaaditaan, että prosessiin osallistuu yksi henkilö kustakin roolista.

4.2.3 Roolien tunnistaminen ja valtuuttaminen

Vain salassapitosopimuksen ja vastuitaan Traficomia kohtaan koskevan sopimuksen allekirjoittaneilla henkilöillä voi olla luottamusrooli.

4.2.4 Velvollisuuksien eriyttämistä vaativat tehtävät

Kaikki kriittiset laitteiston turvallisuusmoduulin eli HSM-moduulin (Hardware Security Module) toiminnot on suoritettava paikan päällä yhdessä laitoksista. Velvollisuudet on eriytetty niin, että turvallisuusvalvoja ei ole ainoa, jolla on fyysinen kulkuoikeus laitoksiin, kun taas järjestelmänvalvojalla ei ole pääsyä HSM-moduulin aktivointiin tarvittaviin tietoihin. Lisäksi vastuu KSK:n julkisen avaimen komponenttien viennistä ja julkaisemisesta on hajautettu niin, että vain turvallisuusvalvojalla on valtuudet rekisteröidä avainmateriaali, kun taas ainoastaan järjestelmänvalvojalla on valtuudet aloittaa avainten generointi (ks. kohta 5.1.2).

Kriittisiin operaatioihin kuuluu siis HSM-moduulin aktivointi, avainten hallinta ja KSK:n julkisen komponentin vienti ja julkaiseminen.

Nämä toiminnot saa suorittaa vain niihin valtuutettujen henkilöiden läsnäollessa.

4.3 Jäljityslokimenettelyt

Lokitus tapahtuu automaattisesti, ja siihen liittyy rekisterijärjestelmän toimintaan liittyvien jäljitystietojen jatkuva kerääminen. Näitä lokitietoja käytetään toiminnan valvontaan, tilastointitarkoituksiin ja perussyyanalyysiin epäillyn turvallisuuden vaarantumisen tai turvallisuuspoikkeaman sattuessa.

4.3.1 Kirjattavat tapahtumatyypit

Seuraavat tapahtumat sisältyvät automaattiseen lokitukseen:

- kaikki HSM-moduuliin liittyvät toiminnot, kuten avainten generointi, avainten aktivointi, allekirjoitus ja avainten vienti
- etäyhteysyritykset, sekä onnistuneet että epäonnistuneet
- etuoikeutetut operaatiot
- saapuminen laitokseen.

4.3.2 Prosessilokin kirjaustiheys

Lokeja analysoidaan automaattisilla ja manuaalisilla prosesseilla.

4.3.3 Jäljityslokin tietojen säilytysaika

Lokitietoja säilytetään verkossa lokien keräysjärjestelmissä vähintään viiden vuoden ajan.

4.3.4 Jäljityslokien suojaus

Lokitusjärjestelmät on suojattu luvattomalta tarkastelulta, muutoksilta ja lokitietojen tuhoamiselta. Fyysiseen kulunvalvontajärjestelmään liittyvät jäljitystiedot säilytetään paikassa, joka ei ole järjestelmänvalvojaroolin hallinnassa.

4.3.5 Jäljityslokien varmuuskopiointiprosessit

Lokeista otetaan varmuuskopiot osana normaalia järjestelmän varmuuskopiointia. Lokien keräysjärjestelmä koostuu erillisistä yksiköistä, joista ei oteta varmuuskopioita.

4.3.6 Jäljityslokien keräysjärjestelmä

Sähköiset lokitiedot siirretään keräysjärjestelmään tosiaikaisesti.

4.3.7 Haavoittuvuusarvioinnit

Kaikki jäljityslokitiedoista löydetyt poikkeamat tutkitaan ja analysoidaan mahdollisten haavoittuvuuksien varalta.

Traficom on myös jäsenenä useissa eri organisaatioissa ja yhteisöissä, joissa kerätään, analysoidaan ja jaetaan luottamuksellisesti turvallisuuteen liittyviä tietoja sidosryhmien jäsenten kanssa. Näitä tietoja arvioidaan jatkuvasti uusien uhkien varalta.

4.4 Toipuminen vaarantumistilanteista ja katastrofeista

4.4.1 Tapahtumien käsittelytavat

Poikkeamiksi on määritelty kaikki todelliset tai koetut turvallisuuden kannalta kriittiset tapahtumat, jotka ovat johtaneet tai olisivat voineet johtaa turvallisuuden vaarantumiseen. Kaikkia poikkeamia hallitaan Traficomin poikkeamanhallintamenettelyn mukaisesti. Poikkeamanhallintamenettelyihin kuuluvat perussyyanalyysin suorittaminen, jotta tapahtuman luonne ja vaikutus voitaisiin tunnistaa muodollisesti ja jotta voitaisiin myös tunnistaa ne toimenpiteet, jotka vaaditaan tapahtuman toistumisen ehkäisyyn (tai sen seurauksien rajoittamiseen). Menettelyt mahdollistavat myös poikkeamien eskaloinnin ja raportoinnin asianmukaiselle viranomaiselle Traficomin sisällä. Jos poikkeamaan liittyy epäily yksityisen avaimen vaarantumisesta, se johtaa avainten korvaamiseen välittömästi kohdan 4.5.3 menettelyjen mukaisesti.

4.4.2 Vioittuneet tietokoneresurssit, ohjelmistot ja/tai tiedot

Jos tietojärjestelmien tai tietovarantojen havaitaan vioittuneen, poikkeamanhallintamenettelyt käynnistetään ja ryhdytään asianmukaisiin toimenpiteisiin. Tarvittaessa käyttöön otetaan myös vakavasta häiriöstä palauttamisen menettelyt.

4.4.3 Menettelyt kohteen yksityisen avaimen vaarantumisen varalta

Jos epäillään, että yksityisen avaimen salassapito on vaarantunut tai jos avainta on mahdollisesti käytetty väärin, käynnistetään seuraavat avainten korvausmenettelyt:

Jos vyöhykkeen allekirjoitusavaimen (zone signing key, ZSK) epäillään vaarantuneen, Traficom lopettaa kyseisen avaimen käytön välittömästi. Tarvittaessa generoidaan uusi ZSK ja vanha avain poistetaan avainsarjasta heti kun sen allekirjoitukset ovat vanhentuneet tai ne on poistettu turvallisesti resolvereilta riippuen siitä, kumpi tapahtuu ensin. Jos epäillään, että ZSK on vaarantunut täysin ja paljastunut luvattomille osapuolille, tästä ilmoitetaan asianmukaisella kanavalla.

Jos avainten allekirjoitusavaimen (key signing key, KSK) epäillään vaarantuneen, uusi avain generoidaan ja otetaan käyttöön välittömästi vanhan avaimen rinnalla. Vanha KSK jää käyttöön avainsarjan allekirjoittamista varten siihen asti, kunnes avaimen poistamista pidetään tarpeeksi turvallisena ottaen huomioon häiriöiden riski suhteessa vaarantuneen avaimen aiheuttamaa riskiin. KSK:n vaihtumisesta ilmoitetaan aina asianmukaisilla kanavilla.

Jos KSK:t (ja mahdollisesti myös ZSK:t) ovat kadonneet täysin, uudet avaimet generoidaan heti kun mahdollista ja lisätään avainsarjaan. Sillä välin kohdevyöhykkeitä ei allekirjoiteta ennen kuin kaikki järjestelmät on palautettu ja juurivyöhykkeelle on julkaistu uudet DS-tietueet. Kaikki tälle ajanjaksolle suunnitellut ZSK-avainten korvaukset siirretään myöhemmäksi.

4.4.4 Kriisinhallinta ja liiketoiminnan jatkuvuus

Traficom on laatinut valmiussuunnitelman, jolla varmistetaan, että toiminnan kannalta oleelliset toiminnot voidaan siirtää yhdestä laitoksesta toiseen neljän tunnin sisällä. Kriittisten laitteiden varaosia on saatavilla tarvittaessa. Valmiussuunnitelmaan kuuluu myös kyky jatkaa muiden toiminnan kannalta oleellisten palvelujen ja järjestelmien käyttöä missä tahansa muista vaihtoehtoisista toimipaikoista. Suunnitelmia testataan säännöllisesti, ja tulokset kirjataan ylös ja arvioidaan jälkeenpäin.

Valmiussuunnitelmaan sisältyvät:

kriisinhallintamenettelyjen käyttöönottoon liittyvät roolit ja vastuut

miten ja missä kriisinhallinta kokoontuu

IT-varatoimintojen käynnistäminen

tehtävävastaavan nimittäminen

kriteerit ja menettelyt normaaliin toimintaan palaamiseksi.

4.5 DNSSECin käytön lopettaminen

Jos Traficomin on jostain syystä lopetettava DNSSECin käyttö kohdevyöhykkeillä ja siirryttävä allekirjoittamattomalle vyöhykkeelle, tämä tapahtuu hallitusti ja siitä ilmoitetaan julkisesti.

4.6 Toimintavastuun siirto

Jos kohdevyöhykkeen toiminnan ylläpito siirretään toiselle taholle, Traficom auttaa siirtymässä niin, että se tapahtuu mahdollisimman sujuvasti.

5 Tekniset turvavalvontatoimenpiteet

5.1 Avainparien generointi ja asennus

5.1.1 Avainparien generointi

Kaikki kohdevyöhykkeen toiminnan jatkumiseen (lähitulevaisuudessa) tarvittavat avaimet generoidaan etukäteen muodollisessa avainseremoniassa. Avainmateriaalin generointiin sisältyvät KSK:t, ZSK:t ja kaikki kulunvalvontaan, avainten jakeluun ja varmuuskopiointiin käytettävät sisäiset avaimet.

Ensimmäisessä avainseremoniassa avainten generointi aloitetaan HSM-moduulien pääavaimista. Kun ne on asennettu turvallisesti kuhunkin tuotantoon käytettävään laitteeseen, sovellusavaimet (KSK:t ja ZSK:t) generoidaan ja jaetaan turvallisesti pääavaimen avulla.

Kun uusien avainten generoiminen on tarpeen, se tapahtuu ennalta sovitussa avainseremoniassa paikan päällä yhdessä toimintaan käytettävistä laitoksista. Avaimet generoidaan ja varmuuskopioidaan varmuuskopiomoduuliin (ks. kohta 5.2.4).

Avainten generointia ja jakelua varten vähintään yhden järjestelmänvalvojan ja yhden turvallisuusvalvojan on työskenneltävä yhdessä koko prosessin ajan.

5.1.2 Julkisten avainten toimittaminen

KSK:n julkinen komponentti viedään allekirjoitusjärjestelmästä osana avainseremoniaa. Viennin jälkeen sekä turvallisuusvalvoja että järjestelmänvalvoja vahvistavat sen.

5.1.3 Julkisen avaimen parametrien generointi ja laadunvalvonta

Validoitujen laitteiden eli HSM-moduulien (ks. kohta 5.2.1) käytöllä voidaan suhteellisen hyvin varmistaa, että avaimet generoidaan turvallisesti ottaen huomioon esim. näennäissatunnaislukugenerointi ja avainparametrien laadunvalvonta, kuten eksponenttien koon tarkastus ja alkulukutestaus.

5.1.4 Avainten käyttötarkoitukset

DNSSECiä varten generoituja avaimia ei koskaan käytetä mihinkään muuhun tarkoitukseen tai allekirjoitusjärjestelmän ulkopuolella. Allekirjoitusjärjestelmää ja HSM-moduuleja ei käytetä mihinkään muuhun tarkoitukseen kuin DNSSECiä varten.

DNSSEC-avaimella luodun allekirjoituksen voimassaoloaika on enintään 14 päivää sekä ZSK:lle että KSK:lle alkaen kaksi tuntia allekirjoitusten luomisesta.

5.2 Yksityisten avainten suojaus ja salausmoduulin tekniset valvontatoimenpiteet

Kaikki salausoperaatiot, joihin liittyy KSK ja ZSK-avaimia, suoritetaan HSM-moduulin suojatussa muistissa. Mitään yksityisiä avaimia ei koskaan säilytetä suojaamatta HSM-moduulien ulkopuolella.

5.2.1 Salausmoduulin standardit ja valvontatoimenpiteet

Allekirjoitusjärjestelmä käyttää HSM-moduuleita (hardware security module, laitteiston turvallisuusmoduuli) ja varamoduuleita, jotka on validoitu FIPS 140-2 tasolla 3.

5.2.2 Yksityisen avaimen (m-of-n) hallinta useamman henkilön toimesta

Traficom ei käytä useamman henkilön hallintaa yksityisiin avaimiin liittyvissä toiminnoissa. Kohdassa 4.2.4 kuvataan korvaavat valvontamenettelyt, joissa HSM-moduulin aktivointiprosessin velvollisuudet on eriytetty.

5.2.3 Yksityisten avainten säilyttäminen kolmannen osapuolen hallussa

.fi-juuren yksityisiä avaimia ei säilytetä kolmannen osapuolen hallussa.

5.2.4 Yksityisten avainten varmuuskopiointi

Avainseremoniassa etukäteen generoidut sovellusavaimet kopioidaan erilliseen varamoduuliin, jonka ominaisuudet ovat samat kuin itse HSM-moduulilla. Varamoduuli säilytetään erillään kassakaapissa, johon turvallisuusvalvojalla on pääsy.

5.2.5 Yksityisten avainten säilytys salausmoduulissa

Kun yksityisiä avaimia säilytetään HSM-moduulin pysyvässä muistissa, niitä säilytetään aina salatussa muodossa käyttäen avainta, joka sijaitsee HSM-moduulin turvallisella ja suojatulla muistialueella.

5.2.6 Yksityisten avainten arkistointi

Kun yksityisiä avaimia ei enää käytetä, ne arkistoidaan.

5.2.7 Yksityisten avainten siirto salattuun turvamoduuliin tai moduulista

Ensimmäisessä avainseremoniassa generoidaan HSM-moduulin pääavain ja se jaetaan tuotantolaitteisiin. Jakaminen tapahtuu fyysisesti erillisillä tunnistevälineillä, joissa on tarvittavat aktivointiavaimet. Kun näiden avainten jakelu on valmis, tunnistevälineitä säilytetään kassakaapissa, jonne vain turvallisuusvalvojalla on pääsy.

5.2.8 Yksityisten avainten aktivointimenetelmä

HSM-moduulin ja sen yksityisten avainten aktivointia varten järjestelmänvalvojalle annetaan turvallisuusvalvojatason pääsy laitteistoon. Turvallisuusvalvoja aktivoi HSM-moduulin ja sen yksityiset avaimet todistamalla, että aktivointitiedot ovat turvallisuusvalvojan hallussa. Turvallisuusvalvoja säilyttää näitä tietoja.

5.2.9 Yksityisten avainten poistaminen käytöstä

Mitään automaattista menettelyä käytöstä poistamista varten ei ole käytössä.

5.2.10 Yksityisten avainten hävittäminen

Yksityisiä avaimia ei hävitetä sen jälkeen, kun niiden toiminta-aika on lakannut eivätkä ne enää ole kelvollisia.

5.3 Muut avaintenhallintaan liittyvät asiat

5.3.1 Julkisten avainten arkistointi

Julkisia avaimia ei arkistoida niiden voimassaolon päättymisen jälkeen.

Avainten käyttöaika

Kun avaimen käyttöaika on lakannut ja avain on korvattu uudella, sen tila on vanhentunut eikä se ole enää voimassa. Vanhentuneita avaimia ei käytetä uudelleen, ja ne poistetaan osana allekirjoitusjärjestelmän normaalia ylläpitoa.

5.4 Tietokoneiden turvavalvontatoimenpiteet

.fi-juureen liittyvissä järjestelmissä käytetään roolipohjaista valtuutus- ja todennusjärjestelmää, joka mahdollistaa harkinnanvaraisen kulunvalvonnan ja annettujen valtuutusten raportoinnin. Lokitus tapahtuu tasolla, joka mahdollistaa yksilöllisen vastuun kaikista (etuoikeutetuista) toiminnoista kussakin alijärjestelmässä.

Kaikkia toiminnan kannalta oleellisia järjestelmiä myös valvotaan jatkuvasti järjestelmän vakauteen ja turvallisuuteen vaikuttavien tapahtumien varalta.

5.5 Verkon turvavalvontatoimenpiteet

.fi-juuren tuotannossa käytetty verkkoinfrastruktuuri on jaettu loogisesti eri turvallisuusvyöhykkeisiin. Palomuureja käytetään viestinnän hallintaan eri verkon osien ja rekisterijärjestelmän kriittisten komponenttien välillä. Kaikki tietoliikenneverkossa siirrettävä mahdollisesti arkaluontoinen tieto on aina suojattu vahvalla salauksella.

5.6 Aikaleimaus

.fi-juuren DNS-järjestelmä käyttää Suomen virallista aikaa ja muita erittäin tarkkoja ja luotettavasti saatavilla olevia aikalähteitä.

5.7 Elinkaaren tekniset valvontatoimenpiteet

5.7.1 Suojauksen hallinnan valvontatoimenpiteet

Kaikkien .fi-juuren DNSSEC-hallintoon osallistuvien tahojen on noudatettava Traficomin tietoturvapolitiikan vaatimuksia.

5.7.2 Muutostenhallinnan turvavalvontatoimenpiteet

Traficom käyttää IT-ympäristön muutosten hallintaan ja valvontaan työmalleja, joihin kuuluu valikoituja osia soveltuvista standardeista, kuten ISO/IEC 27001, ja moderneista jatkuvaa integraatiota ja jatkuvaa toimitusta varten laadituista työmalleista.

6 Vyöhykkeiden allekirjoittaminen

6.1 Avainten pituudet, avaintyypit ja algoritmit

.fi-juuressa käytetään jaetun avaimen allekirjoitusmallia kohdevyöhykkeen allekirjoituksissa. Jako tehdään avainten allekirjoitusavaimen (KSK) ja vyöhykkeen allekirjoitusavaimen (ZSK) avulla. Kunkin avaimen pituuden ja algoritmin tulee olla tarpeeksi vahva niiden käyttötarkoitukseen ja käyttöaikaan nähden. Ylätason verkkotunnuksessa käytetään ainoastaan IETF-standardin mukaisia algoritmeja.

Ylätason .fi-verkkotunnusta varten käytössä on RSA-algoritmi, jonka kertoimen koko (avaimen pituus) on 2 048 bittiä sekä KSK:lle että ZSK:lle.

6.2 Olemattomuuden todentaminen

NSECiä käytetään RFC 4034:n määrittelyn mukaisesti todentamaan se, että kohdetta ei ole olemassa.

6.3 Allekirjoituksen muoto

6.3.1 Allekirjoituksen muoto: ylätason .fi-verkkotunnus

Allekirjoitukset generoidaan salaamalla SHA256-tiivisteitä (RSA/SHA256 ohjeen RFC 6594 määrittelyn mukaisesti).

6.4 Avainten korvaaminen

ZSK-avaimet vaihdetaan uusiin joka kolmas kuukausi automattisella menettelyllä.

KSK-avaimet vaihdetaan uusiin joka 12. kuukausi; siihen vaaditaan myös manuaalisia toimenpiteitä.

Joko toinen tai kummatkin avaimet vodaan myös vaihtaa uuteen esim. epäillyn tietoturvaloukkauksen jälkeen.

6.5 Allekirjoitusten elinikä ja niiden uusimistiheys

Resurssitietueet (Resource Record Sets, RR Sets) allekirjoitetaan niin, että niiden voimassaoloaika on 14 päivää (satunnaistettu 12 tunnin ajanjaksolla). Allekirjoitukset, joiden voimassaolo lakkaa 10 päivän sisällä, päivitetään tunneittain.

6.6 Resurssitietueiden todentaminen

Jotta varmistettaisiin allekirjoitusten voimassaolo ja DNSKEY-tietueen eheys, allekirjoituksen yhteydessä suoritetaan automaattisesti joukko tarkastuksia. Näihin valvontatoimenpiteisiin kuuluvat allekirjoitusten tarkastaminen juurivyöhykettä varten IANA:ssa rekisteröityjen delegoinnin allekirjoittajatietueiden (Delegation Signer, DS) avulla sekä kellonajan ja päivämäärän todentaminen. Jos vyöhyketiedot eivät läpäise automaattisia tarkastuksia, uuden vyöhyketiedoston tuotanto pysäytetään ja se merkitään käsin tehtävää tarkastusta ja vianmääritystä varten. Uuden vyöhyketiedoston tuotanto on pysähdyksissä siihen asti, kunnes vianmääritys ja virheenkäsittely on valmis. Lisäksi kaikkien resurssitietueiden kelpoisuus tarkastetaan nykyisten standardien perusteella ennen jakelua.

6.7 Resurssitietueiden elinaika

Kunkin DNSSEC-resurssitietueen (RFC 4034) elinaika (time-to-live, TTL) on määritelty seuraavasti sekunneissa:

Resurssitietueiden elinaika	
Resurssitietueen tyyppi	TTL
DNSKEY	900
DS	21600
NSEC/NSEC3	SOA-minimi (86400)
RRSIG	sama kuin resurssitietueen TTL (vaihtelee)

Liikenne- ja viestintävirasto Traficom

PL 320 00059 TRAFICOM
Puh. +358 295 345 000

traficom.fi

Liikenne- ja viestintävirasto