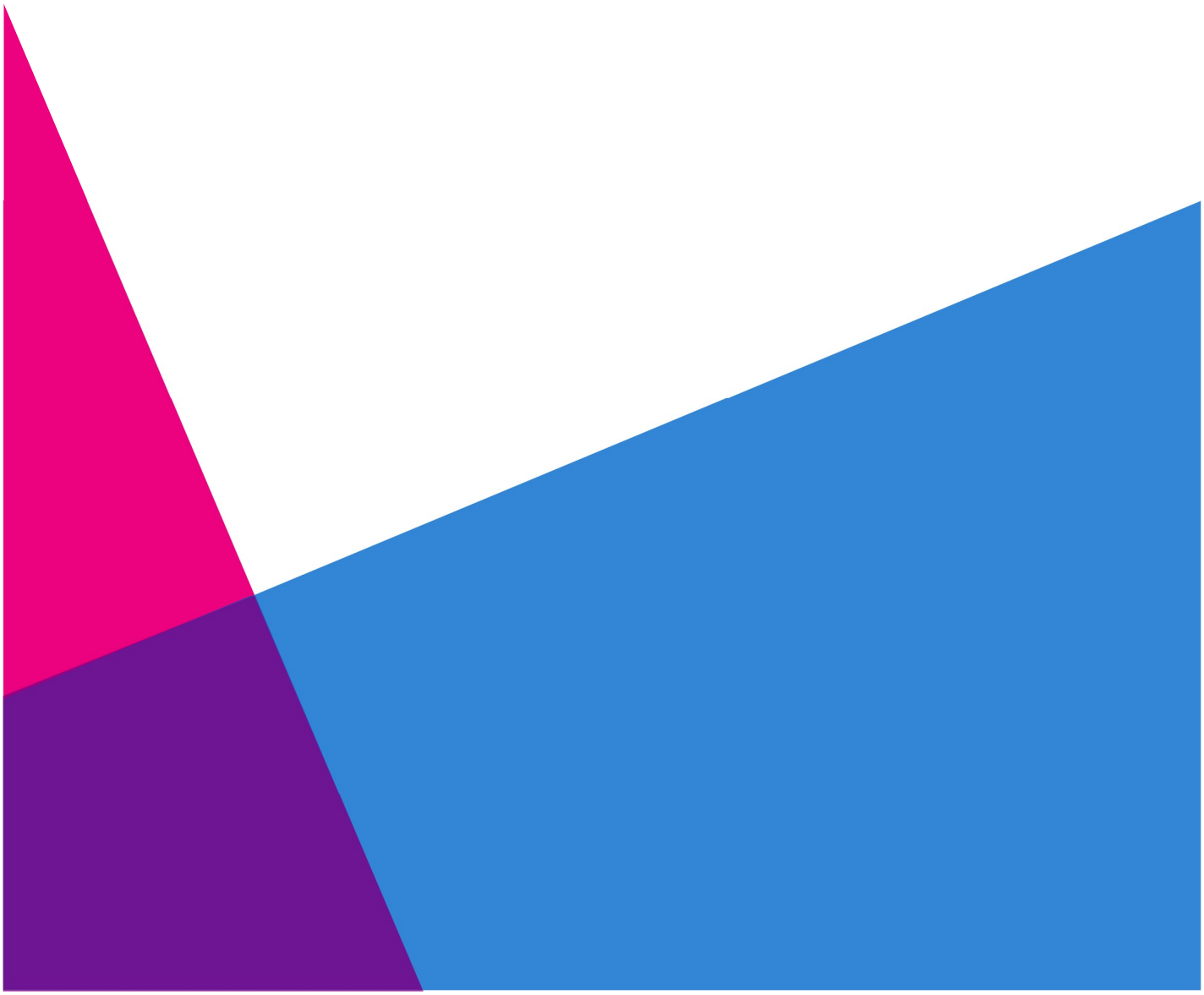
TRAFICOM
Finnish Transport and Communications Agency

.fi DNSSEC Practice Statement (DPS)

Dokumenttyp: Dokumentation
Skapat: 2 augusti 2021
Uppdaterat: -



Innehållsförteckning

1 Inledning

Detta dokument är Traficoms beskrivning av de säkerhetsrutiner och bestämmelser som tillämpas på användningen av DNS-säkerhetstillägg (DNS Security Extensions, DNSSEC) för toppdomänen .fi som administreras av Traficom.

Detta dokument överensstämmer till största delen med RFC 6841: A Framework for DNSSEC Policies and DNSSEC Practice Statements (DPS).

1.1 Översikt

Domain Name System Security Extensions (DNSSEC) är en uppsättning IETF-specifikationer för att lägga till ursprungsautentisering och dataintegritet i domännamnssystemet (DNS). DNSSEC gör det möjligt för programvara att validera att DNS-data inte har manipulerats eller ändrats under överföring. Detta sker genom att digitala signaturer och kryptering av offentliga nycklar införlivas i DNS-hierarkin. Förtroendet följer samma distribution som DNS-trädet, vilket innebär att förtroendekedjan härstammar från rotzonen och delegeras på samma sätt som ansvaret för respektive zon.

1.2 Dokumentets namn och identifiering

Beskrivning av DNSSEC-rutiner (DNSSEC Practice Statement, DPS) för .fi

1.3 Målgrupp och tillämplighet

Följande parter, som detta dokument tillämpas på, har identifierats.

1.3.1 Register

Traficom ansvarar för administrationen och den tekniska driften av .fi-toppdomäner, och därför även för registreringen av domännamn som identifierar underliggande zoner. Detta innebär också att Traficom hanterar ersättningar, ändringar och raderingar av alla data som förknippas med ett domännamn.

Traficom ansvarar för att:

- generera det kryptografiska nyckelmaterial som används i DNSSEC
- skydda sekretessen hos den privata komponenten av nyckelparen
- på ett säkert sätt signera alla officiella DNS-resursposter i den berörda zonen med hjälp av DNSSEC och de utsedda nycklarna.

Slutligen ansvarar Traficom för säker export, registrering och upprätthållande av DS-resursposter i rotzonen, vilket etablerar en förtroendekedja från rotzonen till den tillämpliga zonen och möjliggör validering av DNS-poster med hjälp av rotzonens nyckel.

1.3.2 Registrarer

En registrar är den part som ansvarar för administrationen och hanteringen av ett domännamn för registrantens räkning. Registraren hanterar registreringen, upprätthållandet och hanteringen av registrantens domännamn och är partner till Traficom. Registraren ansvarar för att säkert identifiera en domäns registrant samt för att lägga till, ta bort och uppdatera specifika DS-poster för varje domän på begäran av domänens registrant.

1.3.3 Registrerare

En registrerare är den fysiska eller juridiska person som har registrerat och innehar ett domännamn. Registrerare ansvarar för att generera och skydda sina egna DNSSEC-nycklar, signera relevanta data samt registrera och upprätthålla motsvarande DS-poster genom en registrar.

Registrerarenansvarar också för att ändra nycklar när nycklar misstänks ha äventyrats eller tappats bort.

1.3.4 Förlitande part

Den förlitande parten är den enhet som förlitar sig på DNSSEC-signaturer, såsom validerande resolver-operatörer och parter som tillhandahåller andra motsvarande applikationer. Den förlitande parten ansvarar för konfigurationen och underhållet av lämpliga förtroendeankare.

1.3.5 Tillämplighet

Varje registrerare ansvarar för att fastställa en lämplig säkerhetsnivå för sin domän. Denna DPS gäller endast toppdomänen .fi som förvaltas av Traficom, och beskriver de procedurer, säkerhetskontroller och rutiner som används för hanteringen av DNSSEC i den berörda zonen.

Med hjälp av denna DPS kan den förlitande parten avgöra hur mycket förtroende den kan ge DNSSEC för den berörda zonen, och utifrån detta och andra omständigheter bedöma sin egen risk.

1.4 Administration av specifikationer

Denna DPS uppdateras när det är lämpligt, exempelvis om systemen eller procedurerna ändras i så hög grad att det har en väsentlig inverkan på innehållet i detta dokument.

Traficoms informationssäkerhetsdirektör ansvarar för administrationen av specifikationer för denna DPS. Det yttersta ansvaret för godkännandet och publiceringen ligger hos teamet för Fi-domännamn inom Traficom.

1.4.1 Organisation för administration av specifikationer

Transport- och kommunikationsverket Traficom

1.4.2 Kontaktuppgifter

Transport- och kommunikationsverket Traficom

fi-domain-tech@traficom.fi

1.4.3 Procedurer för ändring av specifikationer

Ändringar i denna DPS görs antingen i form av korrigeringar eller genom publicering av en ny version av dokumentet. Denna DPS och eventuella korrigeringar i den publiceras på:

https://www.traficom.fi/

Endast den senaste versionen av denna DPS gäller. Traficom förbehåller sig rätten att korrigera denna DPS utan att meddela om detta, om korrigeringarna inte anses väsentliga med tanke på säkerheten. Traficom meddelar om eventuella betydande ändringar via ovanstående webbplats.

2 Publicering av nycklar

2.1 Publicering av nyckelsigneringsnycklar (KSK)

Roten .fi använder ett signeringssystem med delade nycklar (se avsnitt 6.1) och publicerar de relevanta nyckelsigneringsnycklarna (key signing key, KSK) för de tillämpliga zonerna enligt följande:

Direkt i rotzonen (endast DS)

Roten .fi använder verktygen för säker elektronisk uppdatering av data i rotzonen.

3 Krav för driften

3.1 Betydelsen av domännamn

Ett domännamn är en unik identifierare, som ofta förknippas med tjänster såsom webbplatser eller e-post. Ansökan om registrering under de tillämpliga toppdomänerna är öppen för alla enskilda individer och juridiska personer som har ett person- eller företagsnummer eller som kan identifieras genom ett register som tillhör en myndighet eller en organisation med en roll som liknar en myndighets. Utländska sökande kan använda andra metoder för unik identifiering.

”Först till kvarn”-principen gäller för registrering av nya domännamn under tillämpliga toppdomäner, vilket innebär att domännamn delas ut i den ordning ansökningarna tas emot av Traficoms registreringstjänster. Villkoren för registrering av domäner för .fi publiceras på:

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

3.2 Identifiering och autentisering av hanterare av barnzon

Registraren ansvarar för att på ett säkert sätt identifiera och autentisera registreraren genom en lämplig mekanism som beskrivs i Traficoms nationella föreskrifter.

3.3 Registrering av delegation signer (DS)-poster

DNSSEC aktiveras genom publicering av minst en DS-post för barnzonen i den tillämpliga toppdomänen. Publicering av DS-poster etablerar en förtroendekedja till de nycklar som barnzonen hänvisar till. Registret antar att alla syntaktiskt korrekta DS-poster är giltiga och gör inga ytterligare kontroller, som att säkerställa att de angivna nycklarna ingår i barnzonens nyckeluppsättning.

Registret godtar DS-poster från registrarer via EPP-gränssnittet, i det format som anges i RFC 5910 Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP). Upp till sex (6) DS-poster per domännamn kan registreras.

3.4 Metod för att bevisa innehav av privat nyckel

Traficom gör inga granskningar för att validera registreraren som innehavare av en viss privat nyckel. Registraren ansvarar för att göra både de kontroller som krävs och de som registraren anser nödvändiga utöver detta.

3.5 Radering av DS-resursposter

En DS-post raderas genom att ett EPP-kommando skickas från registraren till registret eller via registrarens webbgränssnitt. Radering av alla DS-poster inaktiverar DNSSEC-säkerhetsmekanismerna för barnzonen i fråga.

3.5.1 Begäran om radering

Registreraren har rätt att begära att DS-poster raderas. Om registraren tillhandahåller namnservern för registrerarens domännamn, har registraten rätt att radera dessa DS-poster utan att registreraren begärt det. Traficom förbehåller sig rätten att radera DS-poster om Traficom anser att de orsakar eller kan orsaka allvarliga störningar i driften. I fall där namnserveroperatören publicerar den information som krävs för DNSSEC kan Traficom radera DS-posterna för dessa domännamn.

3.5.2 Procedur för begäran om radering

Registreraren eller en representant som utsetts av registreraren instruerar registraren att utföra raderingsuppgiften. En registrar som inte är namnserveroperatör för dessa domäner kan endast göra detta för registrerarens räkning. När ett raderingskommando tas emot av Traficom via EPP eller registratorns webbgränssnitt, görs raderingen genom nästa zongeneration.

Om registraren är namnserveroperatör för registrerarens domän(er), har registraren rätt att lägga till, radera eller ändra DS-poster för dessa domäner utan att registreraren begärt det. Under normala omständigheter uppdateras zonen en gång i timmen. Av denna orsak, när man tar livstiden och distributionstiden i beaktande, kan hela proceduren för distribution av ny delegeringsinformation ta längre innan den är helt genomförd. Registrerare måste beakta denna tidtabell när de beräknar sina signeringssystem och gör ändringar i nycklar.

3.5.3 Begäran om radering i nödsituationer

Om en registrerare befinner sig i en situation där det är omöjligt att genomföra en begäran om radering genom den aktuella registratorn, uppmanar Traficom registreraren att byta registrator och skickar därmed en auktoriseringskod som kan användas för ett sådant byte.

Traficom har rätt att ändra, radera eller neka till att publicera DS-poster om, och endast om, de orsakar eller kan orsaka skador eller störningar i driften av den berörda toppdomän som administreras av Traficom.

4 Administration av lokalerna och administrativa kontroller

4.1 Fysiska kontroller

Utifrån kontinuerliga riskanalyser och nya utvärderingar av hot tillämpas skydd av den fysiska omgivningen, övervakning och kontroll av tillträdet, liksom lämpliga kompenserande kontroller, för att säkerställa att register- och signeringssystemen inte manipuleras, stjäls eller saboteras.

4.1.1 Lokalernas läge och konstruktion

.fi-rotservrarna finns i två fullt funktionsdugliga redundanta och geografiskt utspridda lokaler, mer än 5 kilometer från varandra. Alla DNS-data uppdateras kontinuerligt genom automatisk redundans mellan lokalerna.

Båda lokalerna tillämpar jämförbara fysiska säkerhetskontroller i en struktur i flera nivåer, där den innersta nivån står under strikt kontroll och övervakning.

4.1.2 Fysiskt tillträde

Alla kritiska komponenter är tillgängliga i båda verksamhetslokalerna. Tillträde till lokalerna loggas och de övervakas kontinuerligt.

4.1.3 Strömförsörjning och miljö

Verksamhetslokalerna erbjuder en kontrollerad, reglerad och övervakad verksamhetsmiljö. Varje lokal har reservkraft som överförs under jord från separata transformatorstationer. Lokalerna har även reservkraft från generatorer som kan ge ström till lokalerna i minst 24 timmar.

4.1.4 Exponering för vatten

Lokalerna har mekanismer för att detektera och skydda mot översvämningar.

4.1.5 Förebyggande av och skydd mot eldsvådor

Lokalerna har mekanismer för att detektera brand och automatisk släckning som baserar sig på torra släckmedel. Lokalerna har upphöjt golv och varje rum utgör en separat brandcell.

4.1.6 Hantering av förvaringen av medier

Traficom har infört och upprätthåller ett system för klassificering av information, som definierar de krav som ställs på lagring av känslig information. Lagringsenheter som innehåller sådan information förvaras i utrymmen med fysiska skydd på samma nivå som datorhallar.

4.1.7 Avfallshantering

Kasserade lagringsmedier och annat material som kan innehålla känslig information förstörs på ett säkert sätt, antingen av Traficom eller av en part med vilken man avtalat om detta. Detta gäller även för HSM-moduler, om tillämpligt.

4.1.8 Säkerhetskopiering annanstans än i lokalerna

Vissa kritiska data lagras också säkert utanför lokalerna. Säkerhetskopierade data som förvaras utanför lokalerna lagras i krypterad form, och tillgången till krypteringsnycklarna begränsas till personer med en SA-roll (systemadministratör). Lagringslokalen är geografiskt separat från andra verksamhetslokaler. Lagringslokalen har åtminstone samma nivå av fysiskt skydd som verksamhetslokalerna.

4.2 Procedurkontroller

4.2.1 Betrodda roller

Betrodda roller innehas av individer som är involverade i genereringen och användningen av privat nyckelmaterial samt leveransen och publiceringen av offentligt nyckelmaterial i berörda zoner. De betrodda rollerna är:

1. systemadministratör, SA

2. säkerhetsdirektör, SD

Vid varje given tidpunkt måste det finnas minst två utsedda individer för varje betrodd roll. En individ kan inte inneha fler än en betrodd roll samtidigt.

4.2.2 Antal personer som behövs per uppgift

För kritiska åtgärder tillämpas separation av skyldigheter och roller. Dessa uppgifter kräver att en individ från varje roll deltar i processen.

4.2.3 Identifiering och auktorisering för respektive roll

Endast personer som har undertecknat ett sekretessavtal och ett samtycke till att uppfylla sina skyldigheter gentemot Traficom kan inneha en betrodd roll.

4.2.4 Uppgifter som kräver separation av skyldigheter

Alla kritiska åtgärder med en HSM (Hardware Security Module) måste utföras på plats, i en av verksamhetslokalerna. Skyldigheterna separeras så att säkerhetsdirektören inte har exklusiv fysisk tillgång till verksamhetslokalerna, medan systemadministratören inte ges tillgång till den information som behövs för att aktivera HSM-modulen. Dessutom fördelas ansvaret för export och publicering av de offentliga nyckelkomponenterna för KSK så att endast SD har behörighet att registrera nyckelmaterialet, medan endast SA har behörighet att initiera generering av en nyckel (se avsnitt 5.1.2).

Kritiska åtgärder inkluderar därför aktivering av HSM-modulen, nyckeladministration och -export samt publicering av den offentliga komponenten av KSK-nyckeln.

Åtgärderna får endast utföras i närvaro av auktoriserade personer.

4.3 Procedurer för revisionsloggning

Loggningen är automatisk och involverar kontinuerlig insamling av revisionsinformation gällande aktiviteter i registersystemet. Denna logginformation används i övervakningen av driften, för statistiska ändamål och för analys av den bakomliggande orsaken i händelse av misstänkta dataintrång eller incidenter.

4.3.1 Typer av händelser som registreras

Följande händelser inkluderas i den automatiska loggningen:

- alla typer av händelser som involverar en HSM, såsom generering, aktivering, signering och export av nycklar
- försök till åtkomst på distans, oavsett om de lyckas eller inte
- privilegierade åtgärder
- när någon går in i en lokal.

4.3.2 Processfrekvens för logg

Loggarna analyseras genom automatiska och manuella processer.

4.3.3 Lagringstid för information i revisionsloggar

Logginformation lagras i logginsamlingssystem på nätet i minst fem år.

4.3.4 Skydd av revisionsloggen

Loggsystemen skyddas mot icke-auktoriserad visning, manipulation och förstörelse av loggdata. Revisionsinformation gällande den fysiska tillgången till kontrollsystemet förvaras utanför SA-rollens kontroll.

4.3.5 Procedurer för säkerhetskopiering av revisionsloggen

Loggarna säkerhetskopieras som en del av de normala säkerhetskopieringarna av systemen. Logginsamlingssystemet består av separata enheter där inga säkerhetskopior görs.

4.3.6 Insamlingssystem för revisionsloggen

Elektronisk logginformation överförs till insamlingssystemet i realtid.

4.3.7 Sårbarhetsbedömningar

Alla avvikelser som upptäcks i revisionsloggуppgifterna utreds och analyseras för att upptäcka potentiella sårbarheter.

Traficom är också medlem i flera organisationer och sammanslutningar där säkerhetsrelaterad information samlas in, analyseras och delas i förtroende mellan intressenterna. Denna information utvärderas kontinuerligt för att upptäcka nya hot.

4.4 Äventyrande och katastrofberedskap

4.4.1 Procedurer för hantering av incidenter

Alla faktiska eller uppfattade händelser av säkerhetskritisk karaktär som har lett till eller kunde ha lett till äventyrad säkerhet definieras som incidenter. Alla incidenter hanteras i enlighet med Traficoms procedurer för hantering av incidenter. Procedurerna för hantering av incidenter omfattar en analys av den bakomliggande orsaken samt formell identifiering av händelsens karaktär och effekter, i syfte att identifiera de åtgärder som krävs för att förhindra att händelsen upprepas (eller begränsa dess konsekvenser). Procedurerna inkluderar också metoder för eskalering och rapportering av incidenter till lämpliga ansvariga inom Traficom. En incident som involverar misstanke om att en privat nyckel har äventyrats leder till att nycklarna ändras omedelbart enligt de procedurer som anges i avsnitt 4.5.3.

4.4.2 Skador på datorresurser, programvara och/eller data

Om det upptäcks att datasystem eller resurser har skadats ska procedurerna för hantering av incidenter initieras och lämpliga åtgärder vidtas. Om så krävs ska även procedurerna för katastrofberedskap tillämpas.

4.4.3 Procedurer vid äventyrande av en privat nyckel för en enhet

Om sekretessen för en privat nyckel misstänks ha äventyrats, eller om nyckeln kan ha missbrukats, ska följande åtgärder för ändring av nycklar vidtas:

Om en zonsigneringsnyckel (zone signing key, ZSK) misstänks ha äventyrats slutar Traficom omedelbart använda nyckeln i fråga. Om så krävs genereras en ny ZSK och den gamla nyckeln tas bort från nyckeluppsättningen så snart dess signaturer har gått ut eller på ett säkert sätt tagits bort från resolvern, beroende på vilket som sker först. Om en ZSK misstänks ha äventyrats totalt och avslöjats för icke-auktoriserade parter, meddelas om detta genom en lämplig kanal.

Om en nyckelsigneringsnyckel (KSK) misstänks ha äventyrats genereras en ny nyckel som tas i bruk omedelbart, parallellt med den gamla nyckeln. Den gamla KSK blir kvar och används för att signera nyckeluppsättningen tills det kan anses tillräckligt säkert att ta bort nyckeln, med tanke på risken för störningar i förhållande till den risk som den äventyrade nyckeln utgör. En KSK-ändring utannonseras alltid via lämpliga kanaler.

Om KSK-nycklarna (och eventuellt även ZSK-nycklarna) helt och hållet går förlorade genereras nya nycklar så snart det är praktiskt möjligt och inkluderas i nyckeluppsättningen. Under tiden kan det hända att de relevanta zonerna förblir osignerade tills alla system har återställts och nya DS-poster har publicerats i rotzonen. Under denna tid skjuts alla schemalagda ZSK-ändringar upp.

4.4.4 Krishantering och kontinuitet i affärsverksamheten

Traficom har utarbetat en beredskapsplan som säkerställer att uppdragskritisk verksamhet kan flyttas mellan verksamhetslokalerna inom fyra timmar. Reservdelar för kritisk hårdvara är tillgängliga vid behov. Beredskapsplanen omfattar också en förmåga att återuppta andra uppdragskritiska tjänster och system på någon av de alternativa platserna. Planerna testas regelbundet, och resultaten dokumenteras och utvärderas.

Beredskapsplanen inkluderar:

roller och ansvar vid aktivering av krishanteringsprocedurer

hur och när krishanterarna ska sammankallas

aktivering av reserv-IT-åtgärder

utnämning av en aktivitetshanterare

kriterier och procedurer för att återuppta normal verksamhet.

4.5 Avslutande av DNSSEC

Om Traficom av någon orsak måste avsluta DNSSEC för berörda zoner och gå till en osignerad zon, sker detta på ett ordnat sätt och information om detta offentliggörs.

4.6 Överföring av ansvaret för driften

Om driften av den berörda zonen överförs till en annan part hjälper Traficom till med överföringen för att göra den så smidig som möjligt.

5 Tekniska säkerhetskontroller

5.1 Generering och installation av nyckelpar

5.1.1 Generering av nyckelpar

Alla nycklar som krävs för fortsatt drift av den berörda zonen (under en överskådlig framtid) genereras i förväg genom en formell nyckelceremoni. Genereringen av nyckelmaterialet inkluderar KSK- och ZSK-nycklar samt alla interna nycklar som används för åtkomstkontroll, nyckeldistribution och säkerhetskopiering.

Under den inledande nyckelceremonin genereras HSM-huvudnycklar först. När de på ett säkert sätt har installerats i varje enhet som utsetts för produktionen, genereras applikationsnycklarna (KSK och ZSK) och distribueras på ett säkert sätt med hjälp av huvudnyckeln.

När nya nycklar behöver genereras sker detta genom en schemalagd nyckelceremoni på plats i en av verksamhetslokalerna. Nycklar genereras och säkerhetskopieras till säkerhetskopieringsmodulen (se avsnitt 5.2.4).

Genereringen och distributionen av nycklar kräver att minst en SA och en SD arbetar tillsammans under hela processen.

5.1.2 Leverans av offentliga nycklar

Den offentliga komponenten i en KSK exporteras från signeringssystemet inom ramen för nyckelceremonin. Efter exporten verifieras den av både SD och SA.

5.1.3 Parametrar för offentliga nycklar i generering och kvalitetskontroll

Användningen av validerade hårdvaruenheter, såsom HSM-moduler (se avsnitt 5.2.1), är en rimlig försäkran att genereringen av nycklar sker på ett säkert sätt i fråga om bland annat pseudoslumpmässig generering av tal och kvalitetskontroll av nyckelparametrar, såsom exponentstorlek och primalitetstestning.

5.1.4 Användningssyften för nycklar

Nycklar som genereras av DNSSEC används aldrig för något annat syfte utanför signeringssystemet. Signeringssystemet och HSM-modulerna används inte för några andra syften än DNSSEC.

En signatur som gjorts av en DNSSEC-nyckel har en maximal giltighetstid på 14 dagar för både ZSK och KSK, med en ikraftträdandetid på två timmar från den tidpunkt signaturerna produceras.

5.2 Skydd av privata nycklar och kontroll av byggandet av kryptografiska moduler

Alla kryptografiska åtgärder som involverar KSK- och ZSK-nycklar sker i en HSM-moduls skyddade minne. Inga privata nycklar förvaras någonsin oskyddade utanför HSM-modulerna.

5.2.1 Standarder och kontroller för kryptografiska moduler

Signeringssystemet använder hårdvarusäkerhetsmoduler (Hardware Security Module, HSM) och reservmoduler validerade enligt FIPS 140-2 nivå 3.

5.2.2 Flerpersonkontroll för privata nycklar (m-of-n)

Traficom tillämpar inte flerpersonskontroll för åtgärder med privata nycklar. Se avsnitt 4.2.4 gällande kompenserande kontroller genom separation av skyldigheter i HSM-aktiveringsprocessen.

5.2.3 Deponering av privata nycklar

Privata nycklar för .fi-roten deponeras inte hos tredje part.

5.2.4 Säkerhetskopiering av privata nycklar

Under nyckelceremonin kopieras de förhandsgenererade applikationsnycklarna till en separat reservmodul med liknande egenskaper som själva HSM-modulen. Reservmodulen förvaras separat i ett kassaskåp som är tillgängligt för SD.

5.2.5 Lagring av privat nyckel på kryptografisk modul

När privata nycklar lagras i det permanenta minnet i HSM-modulen lagras de alltid i krypterad form med hjälp av en nyckel som finns i ett manipulationssäkert och i övrigt säkert minnesområde i HSM-modulen.

5.2.6 Arkivering av privata nycklar

Privata nycklar som inte längre används arkiveras.

5.2.7 Överföring av en privat nyckel till eller från en kryptografisk säkerhetsmodul

Under den inledande nyckelceremonin genereras en HSM-huvudnyckel som distribueras till de enheter som utsetts och ställts in för produktionen. Distributionen sker fysiskt med en separat uppsättning hårdvarutokenenheter med de nödvändiga aktiveringsnycklarna. Efter att nyckeldistributionen slutförts förvaras tokenenheterna i ett kassaskåp som endast är tillgängligt för SD.

5.2.8 Metod för aktivering av privat nyckel

För aktivering av HSM-modulen och dess privata nycklar ges en SA SD-tillgång till utrustningen. HSM-modulen och dess privata nycklar aktiveras genom att SD visar att hen innehar aktiveringsdata. Dessa data förvaras av SD.

5.2.9 Metod för inaktivering av privat nyckel

Ingen automatisk procedur för inaktivering tillämpas.

5.2.10 Metod för förstörande av privat nyckel

Inga åtgärder vidtas för att förstöra privata nycklar efter att deras användningsperiod löpt ut och de har blivit ogiltiga.

5.3 Andra aspekter av nyckelhantering

5.3.1 Arkivering av offentliga nycklar

Offentliga nycklar arkiveras inte efter att de gått ut.

Användningstid för nycklar

Efter att användningstiden för en nyckel löpt ut och den har ersatts, övergår nyckeln till utgånget läge och blir ogiltig. Nycklar i utgånget läge återanvänds inte och tas bort som en del av standardrutinerna för upprätthållandet av signeringssystemet.

5.4 Datorsäkerhetskontroll

I system som anknyter till roten .fi används ett rollbaserat system för auktorisering och autentisering, vilket möjliggör diskretionär tillträdeskontroll och rapportering av tilldelade behörigheter. Loggningen sker på en nivå som möjliggör individuellt ansvar för alla (privilegierade) åtgärder i varje undersystem.

Alla uppdragskritiska system övervakas också kontinuerligt för att upptäcka händelser som påverkar systemets stabilitet och säkerhet.

5.5 Nätverkssäkerhetskontroll

Nätverksinfrastruktur som används i rotproduktion för .fi indelas logiskt i olika säkerhetszoner. Brandväggar används för att hantera kommunikationen mellan olika nätverkssegment och för kritiska komponenter i registersystemet. All information som kan vara känslig och som överförs i kommunikationsnätverket skyddas alltid av starka krypteringsmekanismer.

5.6 Tidsstämplar

DNS-systemet för .fi-roten använder officiell finsk tid och andra mycket exakta och lättillgängliga tidskällor.

5.7 Tekniska kontroller under livscykeln

5.7.1 Säkerhetshanteringskontroller

Alla parter som deltar i DNSSEC-administrationen för .fi-roten måste uppfylla de krav som beskrivs i Traficoms informationssäkerhetspolicy.

5.7.2 Säkerhetskontroller för förändringshantering

Traficom använder arbetsmodeller som inkluderar valda delar ur lämpliga standarder såsom ISO/IEC 27001 och delar av moderna arbetsmodeller för kontinuerlig integration och kontinuerlig leverans för att hantera och kontrollera förändringar i IT-miljön.

6 Zonsignering

6.1 Nycklarnas längder, nycklarnas typer och algoritmer

Roten .fi använder ett signeringssystem med delade nycklar vid signering av den tillämpliga zonen. Delningen görs genom nyckelsigneringsnyckeln (key signing key, KSK) och zonsigneringsnyckeln (zone signing key, ZSK). Längderna på och algoritmerna för respektive nyckel ska vara tillräckligt starka för ändamålet och användningsperioden. Endast IETF-standardiserade algoritmer ska användas av den berörda toppdomänen.

För toppdomänen .fi finns även RSA-algoritmen med en modulstorlek (nyckellängd) på 2 048 bitar för både KSK och ZSK.

6.2 Autentiserat nekande av existens

NSEC används för att ge autentiserat nekande av existens enligt RFC 4034.

6.3 Signaturformat

6.3.1 Signaturformat: .fi toppdomän

Signaturer genereras genom kryptering av SHA256-hashar (RSA/SHA256 enligt specifikation i RFC 6594).

6.4 Ändringar i nycklar

ZSK ändras var tredje månad genom en automatisk procedur.

KSK ändras var tolfte månad och kräver även manuella steg.

En av eller båda nycklarna kan också ändras manuellt exempelvis om säkerheten misstänks ha äventyrats.

6.5 Signaturens livstid och återsigneringsfrekvens

Resursposter (RR Sets) signeras med en giltighetsperiod på 14 dagar (randomiseras i ett fönster på 12 timmar). Signaturer som går ut inom 10 dagar uppdateras timme för timme.

6.6 Verifiering av resursposter

För att säkerställa att signaturerna är giltiga och integriteten hos DNSKEY-posten genomförs ett antal kontroller automatiskt vid varje signering. Dessa kontroller omfattar verifiering av signaturer med hjälp av de Delegation Signer (DS)-poster som registrerats hos IANA för rotzonen, liksom verifiering av tiden och datumet. Zoninformation som inte godkänns i de automatiska kontrollerna medför att produktionen av en ny zonfil pausas och informationen flaggas för manuell intervention och felsökning. Produktionen av en ny zonfil pausas tills felsökningen och felhanteringen slutförts. Dessutom verifieras giltigheten hos alla resursposter i enlighet med de aktuella standarderna innan de distribueras.

6.7 Resursposternas livstid

Livstiden för varje DNSSEC-resurspost (RFC 4034) specificeras som följer, i sekunder:

Resursposternas livstid	
Resursposttyp	Livstid
DNSKEY	900
DS	21600
NSEC/NSEC3	som SOA-minimum (86400)
RRSIG	samma som resurspostens livstid (varierar)

Transport- och kommunikationsverket Traficom

PB 320, 00059 TRAFICOM, Finland
Tfn +358 295 345 000

traficom.fi

Finnish Transport and Communications Agency