Säkerhet

Dokumentation

DNSSEC

Säkerhetsdeklaration (DPS) .se

Stiftelsen för Internetinfrastruktur
Box 92073, 120 07 Stockholm Tel 08-452 35 00 Fax 08-452 35 02 Org.nr. 802405-0190 www.iis.se

1 Inledning

Detta dokument utgör IIS deklaration av säkerhetsåtgärder och rutiner som tillämpas i samband med administrationen av DNS Security Extensions (DNSSEC) i den svenska toppdomänen .se. Dokumentet överensstämmer med RFC 6841: *A Framework for DNSSEC Policies and DNSSEC Practice Statements (DPS)*. Denna DPS är ett av flera dokument relevanta för driften av .se-zonen. Andra relevanta dokument är IIS grundskyddsnivå för IT-säkerhet, IIS informationssäkerhetspolicy och IIS krishanteringsplan, vilka är interna och inte publiceras offentligt.

1.1 Allmänt

Säkerhetstilläggen till DNS (DNSSEC) är en uppsättning IETF-specifikationer som gör det möjligt att autentisera källan i DNS och säkerställa dataintegriteten i domännamnssystemet. DNSSEC erbjuder en möjlighet för programvara att validera att DNS-data inte har förändrats eller förvanskats under överföring via internet. Detta görs genom användning av elektroniska signaturer och asymmetrisk kryptografi i DNS-hierarkin. Tilliten följer samma distribution som DNS-trädet, det vill säga att tilliten utgår från roten och delegeras på samma sätt som ansvaret för en domän.

1.2 Dokumentnamn och -identifiering

Dokumenttitel: Säkerhetsdeklaration (DPS) .se

Version: I

Skapad: 2010-04-19

Uppdaterad: 2018-05-25

1.3 Målgrupp och tillämplighet

Följande roller och ansvarsfördelning identifieras.

1.3.1 Registry

IIS (Stiftelsen för Internetinfrastruktur) utgör registry för internets svenska toppdomän .se och utför som sådant registrering av domännamn som identifierar underliggande zoner i .se-zonen. Detta innebär att IIS hanterar tillägg, ändring och borttagning av all data som är kopplat till ett domännamn i .se.

IIS ansvarar för att:

- generera det kryptografiska nyckelmaterial som används för DNSSEC i .se
- skydda de privata delarna av detta nyckelmaterial samt
- på ett säkert sätt signera samtliga auktoritativa DNS-poster i .se-zonen med användning av DNSSEC och dessa nycklar.

IIS ansvarar slutligen också för att på ett säkert sätt exportera, registrera och underhålla relaterade DS-poster i rotzonen, vilket etablerar den tillitskedja från rotzonen som möjliggör validering av DNS-poster i .se med hjälp av rotnyckeln.

1.3.2 Registrarer

En Registrar är den part som ansvarar för administration och förvaltning av domännamn för en innehavares räkning. Registraren sköter registrering, underhåll och förvaltning av en innehavares domännamn och är en ackrediterad partner till IIS.

Registraren ansvarar för att identifiera innehavare av en domän på ett säkert sätt och för att på Innehavarens begäran lägga till, ta bort eller uppdatera angivna DS-poster för respektive domän.

1.3.3 Innehavare (Registranter)

En innehavare är den fysiska eller juridiska person som har registrerat och förfogar över ett domännamn. Innehavaren ansvarar för att generera och skydda sina egna DNSSEC-nycklar, för signering av relevanta data, samt för att registrera och underhålla motsvarande DS-poster hos en registrar.

Innehavaren ansvarar även för att snarast byta nycklar som misstänks vara röjda eller har förlorats.

1.3.4 Förlitande part

Förlitande part är de som förlitar sig på DNSSEC-signaturer, såsom operatörer av validerande resolvrar och parter med andra motsvarande tillämpningar. Förlitande part har ansvar för att konfigurera och uppdatera nödvändiga tillitsankare (Trust Anchor, TA, enligt RFC 4033). Förlitande part har också ansvar för att hålla sig informerad om relevanta händelser relaterade till DNSSEC i .se-domänen med användning av de källor som anges i avsnitt 2.1.

1.3.5 Tillämplighet

Varje innehavare ansvarar för att avgöra vilken säkerhetsnivå som är relevant för den egna domänen. Aktuell DPS är enbart tillämplig på toppdomänen .se och beskriver de rutiner och säkerhetsåtgärder som tillämpas vid hanteringen av DNSSEC i .se-zonen.

Förlitande part kan med stöd av denna DPS avgöra vilket förtroende denne har för DNSSEC i .se, och mot bakgrund av detta och andra omständigheter bedöma sin egen risk.

1.4 Dokumentförvaltning

Denna DPS uppdateras vid behov, till exempel vid omfattande system- eller rutinförändringar som väsentligt påverkar innehållet i dokumentet. Sådana ändringar meddelas via de källor som anges i avsnitt 2.1.

Ansvarig för dokumentförvaltning av DPS inom IIS är säkerhetschefen. Det yttersta ansvaret för godkännande och publicering åligger PMA-funktionen inom IIS.

1.4.1 Informationsägare

IIS (Stiftelsen för Internetinfrastruktur)

1.4.2 Kontaktuppgifter

DNSSEC PMA (Policy Management Authority):

IIS (Stiftelsen för Internetinfrastruktur)
Box 92073
SE-120 07 Stockholm
SVERIGE

Telefon: +46 8 452 35 00
Fax: + 46 8 452 35 02
Org nr: 802405-0190
https://www.iis.se
dnssec-pma@iis.se

1.4.3 Ändringsförfarande

Ändringar av denna DPS sker antingen i form av rättelse eller tillägg till befintligt dokument eller publicering av en helt ny version av dokumentet. DPS och ändringar av densamma publiceras under adressen:

https://www.iis.se/docs/dnssec-dps-sv.pdf

Endast den senast uppdaterade versionen av DPS är giltig. Alla ändringar godkänns och beslutas av PMA och är giltiga från tiden för publicering.

IIS förbehåller sig rätten att ändra denna DPS utan notifiering för ändringar som inte är att betrakta som väsentliga från säkerhetssynpunkt. Det är IIS PMA som ensidigt avgör om en ändring är att betrakta väsentlig i detta avseende. Sådana ändringar meddelas via de källor som anges i avsnitt 2.1.

2 Publicering och åtkomst till information

2.1 Publiceringsplats

IIS publicerar information av relevans för DNSSEC på IIS webbplats under adressen:

https://www.iis.se/domaner/teknik/dnssec/

Den elektroniska versionen av denna DPS på den särskilda webbplatsen är den som är i kraft. Meddelanden relevanta för DNSSEC i .se distribueras via e-postlistan:

dnssec-announce@lists.nic.se

Information om hur man prenumererar och underhåller sin prenumeration publiceras på http://lists.nic.se/mailman/listinfo/dnssec-announce

2.2 Publicering av nyckelsigneringsnycklar (KSK)

IIS använder sig av ett system med delade nycklar (split key, se avsnitt 6.1) och publicerar relevanta nyckelsigneringsnycklar (KSK) för .se-zonen enligt följande:

- Direkt i rotzonen (endast DS).

IIS använder de verktyg för säker elektronisk uppdatering av uppgifter i rotzonen som IANA från tid till annan tillhandahåller för ändamålet.

3 Operationella krav

3.1 Innebörd av domännamn

Ett domännamn är en unik identifierare, som ofta associeras till tjänster som webbplats eller e-post. Ansökan om registrering under toppdomänen .se står öppen för alla fysiska och juridiska personer som har ett person- eller organisationsnummer eller som kan identifieras genom registerbeteckning i register fört av myndighet, eller av organisation med myndighetsliknande uppgift. För utländsk Innehavare kan i stället annan unik identifieringsuppgift lämnas.

Vid nyregistrering av Domännamn tillämpas principen ”först till kvarn”, det innebär att tilldelning av Domännamn sker i den ordning ansökningar införs i IIS register. Allmänna villkor för registrering av .se-domäner finns under adressen: https://www.iis.se/domaner/registrera/se/villkor/

3.2 Identifiering och autentisering av innehavare för barnzon

Det är Registrarens ansvar att på ett säkert sätt identifiera och autentisera innehavaren via någon för ändamålet lämplig metod, och i enlighet med bestämmelserna i avtalet mellan IIS och Registraren.

3.3 Registrering av Delegation Signer-poster (DS-poster)

DNSSEC aktiveras genom att minst en DS-post för den underliggande domänen publiceras i toppdomänen.se. Publiceringen av DS-poster etablerar en förtroendekedja till den underliggande domänens refererade nycklar. IIS förutsätter att DS-posten är korrekt och kommer inte att genomföra några särskilda kontroller som syftar till att förvissa sig om att refererade nycklar ingår i den underliggande domänens nyckeluppsättning.

Registryt accepterar DS-poster via EPP-gränssnitt från respektive Registrar 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 kan registreras per domännamn.

3.4 Metod för att bevisa innehav av privat nyckel

IIS gör inga kontroller i syfte att föra i bevis att det är rätt innehavare bakom en privat nyckel. Det är Registrarens ansvar att göra de kontroller som krävs, och som man anser vara nödvändiga.

3.5 Avregistrering av DS-poster

En DS-post avregistreras genom en EPP-begäran från Registrar till Registry. Avregistrering av samtliga DS-poster innebär att säkerhetsmekanismerna för DNSSEC avaktiveras för den aktuella underliggande domänen.

3.5.1 Behörighet att begära avregistrering

Endast innehavaren eller innehavarens ombud i form av teknisk kontakt eller administrativ kontakt har behörighet att begära avregistrering av DS-poster.

3.5.2 Rutin för avregistrering

Innehavaren eller innehavarens ombud i form av teknisk kontakt eller administrativ kontakt ger Registraren i uppdrag att genomföra avregistrering. Registraren får endast göra det på innehavarens uppdrag. När en begäran om avregistrering inkommit till IIS

via EPP tar det som längst till nästföljande zongenerering till dess att ändringen införs i zonfilen.

I de fall Registraren är namnserveroperatör för innehavarens domännamn har Registraren rätt att utan begäran från innehavaren lägga till, ta bort eller ändra DS-poster för dessa domännamn.

Under normala förhållanden uppdateras zonfilen varannan timme. Med hänsyn till livslängd (TTL) och distributionstid kan hela processen med att distribuera ny delegeringsinformation ta upp till maximalt fem timmar att fullborda innan ändringarna når fullt genomslag. Innehavaren måste ta med detta i beräkningen när denne beslutar om signeringsfrekvens och eventuella nyckelbyten.

3.5.3 Nödrutin (Reservrutin) för avregistrering

Om en innehavare befinner sig i en situation som innebär att denne inte kan komma i kontakt med sin Registrar för att begära avregistrering av DS-poster, uppmanar IIS innehavaren att byta Registrar och skickar därvid ut en ny auktorisationskod som kan användas för sådant byte. I enlighet med Registry-Registraravtalet förbehåller sig IIS rätten att ändra, ta bort eller avstå från att publicera angivna DS-poster om dessa, enligt IIS bedömning, orsakar eller kan komma att orsaka allvarliga driftstörningar för IIS.

4 Fysisk, administrativ och personalrelaterad säkerhet

4.1 Fysiska kontroller

Baserat på regelbundna riskanalyser upprätthåller IIS fysiskt skalskydd, övervakning och tillträdeskontroll såväl som lämpliga kontroller för att avgöra att registrerings- och signeringssystem inte har manipulerats, stulits eller saboterats.

4.1.1 Anläggningarnas placering och utformning

IIS har etablerat en redundant driftsmiljö separerad i två fysiskt och geografiskt åtskilda anläggningar med minst 5 km avstånd mellan varandra. All information hålls ständigt aktuell genom automatisk replikering mellan driftsanläggningarna.

Båda anläggningarna har likvärdiga säkerhetskontroller i en flerlagerstruktur, där det innersta lagret är strikt kontrollerat och övervakat av IIS.

4.1.2 Fysiskt tillträde

Alla kritiska komponenter finns installerade på båda anläggningarna. Fysiskt tillträde till det innersta lagret är begränsad till endast behörig personal som innehar rollen som systemadministratör, SA (se avsnitt 4.2.1). Inpassering kontrolleras och övervakning av de fysiska lokalerna sker kontinuerligt.

4.1.3 Strömförsörjning och miljö

Anläggningarna erbjuder en kontrollerad, reglerad och övervakad driftsmiljö. Strömförsörjning till driftanläggningarna sker via flera separata matningar med markförlagd överföring från olika transformatorstationer. Utöver detta har anläggningarna reservkraft från generatorer som kan försörja dessa med el under minst 24 timmar.

4.1.4 Vätskeskydd

Anläggningarna har detektorer för och skydd mot utströmmande vätska.

4.1.5 Förebyggande åtgärder och skydd mot brand

Anläggningarna är utrustade med system för branddetektering och automatisk släckanläggning med torrsläckning. Anläggningarna är försedda med brandgolv och varje rum utgör en egen brandcell.

4.1.6 Hantering av informationsbärande media

IIS anvisningar för informationsklassificering definierar de krav som ställs för lagring av skyddsvärd data. Informationsbärare som innehåller sådant data förvaras i utrymmen med fysiskt skydd likvärdigt med driftanläggningarna.

4.1.7 Avfallshantering

Förbrukat lagringsmedia och annat material som kan innehålla känslig information destrueras på ett säkert sätt, antingen av IIS eller av kontrakterad part. Detta gäller i förekommande fall även HSM.

4.1.8 Alternativ lagringsplats

Viss kritisk information finns också förvarad på alternativ lagringsplats i säkert utrymme hos tredje part. Fysisk åtkomst till detta utrymme är begränsad till behörig personal som innehar rollen som säkerhetsansvarig, SO (se avsnitt 4.2.1). Lagringsplatsen är geografiskt och administrativt separerad från IIS övriga anläggningar. Utrymmet har minst samma nivå av fysiskt skydd som det som återfinns i driftanläggningarna.

4.2 Administrativa kontroller

4.2.1 Betrodda roller

Betrodda roller innehas av personer som är involverade i generering eller användning av privat nyckelmaterial, leverans och publicering av publika nycklar eller har möjlighet att påverka innehållet i zonfilen. De betrodda rollerna är:

1. Systemadministratör (Systems Administrator, SA)
2. Säkerhetsansvarig (Security Officer, SO)

Vid varje given tidpunkt måste det finnas minst två individer inom organisationen per betrodd roll. De betrodda roller som beskrivs ovan får inte innehas samtidigt av en och samma person.

4.2.2 Krav på antal personer per uppgift

Separation av uppgifter och roller är tvingande vid kritiska operationer, och kräver att en individ från varje roll deltar i processen.

4.2.3 Identifiering och autentisering av personer i betrodda roller

Endast personer som har tecknat sekretessavtal och ansvarsförbindelse med IIS får inneha en betrodd roll.

4.2.4 Åtgärder som kräver separation av arbetsuppgifter

Alla kritiska HSM-operationer[1] måste ske på därför avsedd plats, i någon av driftanläggningarna. Ansvaret är uppdelat genom att säkerhetsansvarig (SO) inte ensam har fysiskt tillträde till driftsanläggningarna, medan systemadministratör (SA) inte innehar den information som krävs för att aktivera HSM. Vidare är ansvaret för export och publicering av publika komponenter av KSK fördelat på så sätt att endast SO har behörighet att registrera nyckelmaterial, medan endast SA har behörighet att initiera nyckelgenerering (se avsnitt 5.1.2).

Kritiska operationer innefattar därför aktivering av HSM, nyckeladministration och export och publicering av publika komponenter av KSK.

Kritiska operationer får utföras endast i närvaro av behöriga personer.

4.3 Personalrelaterade kontroller

4.3.1 Kvalifikationer, erfarenhet och lämplighetsprövning

Personer som kandiderar till någon av de betrodda rollerna ska ha visat prov på trovärdighet och att denne innehar lämpliga kvalifikationer. Sådan lämplighetsprövning görs av säkerhetschef innan en sådan person tilldelas de behörigheter som följer av respektive roll.

4.3.2 Rutiner för bakgrundskontroll

Utredning av trovärdighet och bakgrundskontroll genomförs av både säkerhets- och HR-funktionerna på IIS. Processen inkluderar verifiering av:

[1] HSM - Hardware security module, validerad hårdvaruenhet

- individens CV,
- tidigare anställningar,
- referenser (öppna och andra), samt
- dokument som styrker relevant och avslutad utbildning.

För att vara kvalificerad för någon av de betrodda rollerna får det i kontrollen inte framkomma några oegentligheter som tyder på olämplighet.

4.3.3 Krav på utbildning

IIS tillhandahåller relevant och nödvändig utbildning om processer, rutiner och teknisk administration av de system som är relevanta för respektive betrodd roll. I utbildningen ingår:

- IIS verksamhet i allmänhet,
- rollens omfattning, ansvarsområde, mandat och befogenheter,
- domännamnsadministration i allmänhet,
- grundläggande tekniska kunskaper i DNS och DNSSEC (för Säkerhetsansvarig – SO),
- fördjupade tekniska kunskaper i DNS och DNSSEC (för Systemadministratör - SA),
- grundläggande kunskaper i informationssäkerhet,
- administration, rutiner och checklistor,
- rutiner för och övningar i incidenthantering,
- rutiner för och övningar i krishantering.

4.3.4 Frekvens och ordning för arbetsrotation

Ansvaret för att genomföra nödvändiga uppgifter enligt 4.2.4 roteras vid varje tillfälle mellan de personer som innehar betrodda roller. I den dagliga driften deltar samtliga utpekade Systemadministratörer (SA), och ansvaret för beredskapstjänstgöring roteras bland dessa enligt ett förutbestämt schema.

4.3.5 Disciplinära påföljder

Påföljd som konsekvens av obehöriga handlingar regleras i ansvarsförbindelser och sekretessavtal. Grov oaktsamhet eller uppsåt kan leda till uppsägning och skadeståndsansvar.

4.3.6 Krav på kontrakterad personal

Under vissa omständigheter kan IIS behöva kontraktera personal som komplement till fast anställd personal. Dessa tecknar samma typ av ansvars- och sekretessförbindelse som fast anställd personal.

Kontrakterad personal som inte varit föremål för bakgrundskontroll och utbildning, och alltså inte kan komma ifråga för en betrodd roll, får inte delta i de aktiviteter som anges i 4.2.4.

4.3.7 Dokumentation till personal

IIS tillhandahåller den dokumentation som krävs för att den enskilda medarbetaren ska kunna utföra sina arbetsuppgifter på ett säkert och fullgott sätt. Detta innefattar systemdokumentation, handledningar, driftrutiner och checklistor för samtliga delar av driftmiljön.

4.4 Rutiner för spårbarhet genom loggning

Loggning sker automatiskt och innebär kontinuerlig insamling av information om de aktiviteter som förekommer i registrysystemet. Denna logginformation används vid driftövervakning, för statistikändamål samt för rotorsaksanalys i händelse av misstänkt säkerhetsbrott eller incident.

Till logginformation som insamlas för internrevision räknas också de journaler, checklistor och andra handlingar på papper som är av betydelse för säkerheten, och som behövs för att följa ett revisionsspår.

4.4.1 Händelser som loggas

Följande händelser inkluderas i den **automatiska** loggningen:

- Alla typer av aktiviteter som involverar HSM, såsom nyckelgenerering, nyckelaktivering, signering och export av nycklar.
- Fjärråtkomst, misslyckad och lyckad.
- Privilegierade bearbetningar.
- Inpassering till driftanläggning.

4.4.2 Frekvens för uppföljning av logginformation

Loggar analyseras kontinuerligt genom automatiserade och manuella kontroller. Särskild granskning sker bland annat vid nyckelgenerering, privilegierade bearbetningar, omstart av systemet och upptäckta avvikelser.

4.4.3 Tid för bevarande av logginformation

Logginformation lagras i loggsystemet i minst 90 dagar. Därefter förs logginformationen över till ett arkiv, och bevaras i minst 10 år.

4.4.4 Skydd av logginformation

All elektronisk logginformation lagras vid båda driftanläggningarna. Systemen för logginsamling har skydd mot obehörig insyn, manipulation och förstörande av logginformationen.

Logginformation rörande fysisk tillgång till anläggningarna lagras utanför SA-rollens kontroll.

4.4.5 Säkerhetskopiering av logginformation

All elektronisk logginformation säkerhetskopieras månadsvis och lagras separat från systemet i ett säkert utrymme. All pappersbaserad logginformation sparas i brandskyddat säkerhetsskåp i anslutning till anläggningarna.

4.4.6 System för insamling av logginformation

Elektronisk logginformation överförs i realtid till insamlingssystemen, ett för varje anläggning. Manuella loggar förs på papper och arkiveras i brandskyddat säkerhetsskåp.

4.4.7 Sårbarhetsanalys

Alla anomalier som upptäcks i logginformationen utreds och analyseras för att upptäcka eventuella sårbarheter.

IIS är också medlem i ett flertal organisationer och sammanhang där säkerhetsrelaterad information samlas, analyseras och delas under konfidentialitet mellan intressenter. Den informationen utvärderas kontinuerligt för att upptäcka nya hot.

4.5 Kontinuitetsplanering

4.5.1 Incidenthantering

Som incident definieras alla verkliga eller uppfattade händelser av säkerhetskritisk karaktär som lett till eller kunnat leda till att säkerheten komprometteras.

Alla incidenter hanteras enligt IIS incidenthanteringsrutin. Incidenthanteringsrutinen innefattar att utföra en rotorsaksanalys för incidenten, vilken påverkan incidenten haft eller kunnat få, samt identifiera vilka åtgärder som krävs för att förhindra att incidenten upprepas (eller för att begränsa dess konsekvenser). Rutinen innefattar även former för eskalering och rapportering till ansvarig person inom IIS.

En incident som innebär misstanke om att en privat nyckel har röjts leder till omedelbart nyckelbyte enligt rutinen som anges i avsnitt 4.5.3.

4.5.2 Skada på utrustning, programvara och/eller information

I händelse av att IIS upptäcker någon form av skada på informationssystem eller resurser ska rutin för incidenthantering initieras och lämpliga åtgärder vidtas. Om nödvändigt ska krisrutiner aktiveras.

4.5.3 Rutin vid misstanke om röjd eller felaktigt använd privat nyckel

Misstanke om att en privat nyckel har röjts eller missbrukats leder till ett kontrollerat nyckelbyte enligt följande:

- Om en zonsigneringsnyckel (ZSK) misstänks ha blivit röjd kommer IIS omedelbart att sluta använda den nyckeln. Om så krävs genereras en ny ZSK och den gamla plockas bort ur nyckeluppsättningen så snart dess signaturer blivit ogiltiga eller med säkerhet kasserats i resolverledet, vilket som inträffar först. Vid misstanke om att ZSK kan ha röjts till obehöriga kommer detta meddelas via de kanaler som angetts i avsnitt 2.1.

- Om en nyckelsigneringsnyckel (KSK) misstänks ha blivit röjd kommer en ny att genereras och börja användas omedelbart, parallellt med den gamla. Den gamla KSK:n kommer att ligga kvar och användas till att signera nyckeluppsättningen till dess att det kan anses tillräckligt säkert att ta bort den med avseende på risken för driftstörningar mot bakgrund av den risk som den röjda nyckeln innebär. En rullning av KSK meddelas alltid via de kanaler som angetts i avsnitt 2.1.

Om KSK (och möjligen också ZSK) förlorats fullständigt kommer nya nycklar att genereras vid tidigast möjliga tillfälle och inkluderas i nyckeluppsättningen. I mellantiden kan det komma att inträffa att .se-zonen befinner sig i osignerat läge, till dess att systemen återställts och nya DS-poster kunnat publiceras i rotzonen. Alla schemalagda byten av ZSK under denna tid kommer att skjutas upp.

4.5.4 Krisberedskap

IIS har utformat en krisberedskapsplan som innebär att verksamhetskritisk produktion kan flyttas mellan de båda driftsanläggningarna. Vanligt förekommande reservdelar och kritiska hårdvarukomponenter lagras på plats i respektive driftanläggning.

Krisberedskapsplanen innefattar även förmågan att återuppta andra verksamhetskritiska tjänster och system på respektive driftanläggning. Planen testas regelbundet och resultatet dokumenteras och utvärderas.

Krisplanen innehåller:

- roller och ansvar för att fatta beslut om aktivering av krisberedskapsplanen,
- hur och var krisledningen samlas,
- aktivering av reservdrift,
- utpekande av uppgiftsansvarig,
- kriterier för och hur beslut fattas om återgång till normalläge.

4.6 Upphörande av verksamhet

Om IIS av någon anledning måste avveckla DNSSEC för .se-zonen och gå till ett osignerat läge sker det på ett organiserat sätt där allmänheten informeras. Om driften för .se-zonen ska flyttas till annan part medverkar IIS till att flytten genomförs så smidigt som möjligt.

5 Tekniska säkerhetskontroller

5.1 Generering och installation av nyckelpar

5.1.1 Generering av nyckelpar

Alla nycklar som krävs för den kontinuerliga driften av .se-zonen (inom en överskådlig framtid) genereras i förväg vid en formell nyckelceremoni. Generering av nyckelmaterial omfattar KSK:er, ZSK:er och alla interna nycklar som krävs för åtkomstkontroll, nyckeldistribution och säkerhetskopiering.

Under den inledande nyckelceremonin genereras först huvudnycklar till HSM. Efter att dessa har installerats säkert i varje enhet avsedd för produktion genereras applikationsnycklar (KSK respektive ZSK) och distribueras säkert med användning av huvudnyckel.

Om nya nycklar behöver genereras kommer detta att äga rum genom planerade nyckelceremonier på plats vid någon av driftanläggningarna. Nycklarna distribueras därefter manuellt med användning av en backupenhet (se avsnitt 5.2.4).

Nyckelgenerering och distribution kräver närvaro av två personer, en från var och en av de betrodda rollerna som arbetar tillsammans genom hela processen.

Hela processen för nyckelgenerering loggas dels maskinellt, dels av SO manuellt på papper som verifieras av SA.

5.1.2 Leverans av publika nycklar

Den publika delen av en KSK exporteras ur signeringssystemet som en del av nyckelceremonin. Efter export verifieras nyckeln av såväl SO som SA. SO ansvarar för att den publika delen av KSK publiceras på ett säkert sätt i enlighet med avsnitt 2.2. SA ansvarar för en andra kontroll av att de nycklar som publiceras är desamma som de som exporterats och schemalagts för produktion, och att de fungerar som förväntat.

5.1.3 Kvalitetskontroll av nyckelparametrar

Användningen av validerade hårdvarumoduler, HSM (se avsnitt 5.2.1) säkerställer med rimlig visshet att nyckelgenereringen utförs på ett säkert sätt med hänsyn tagen till bland annat slumptalsgenerering och kvalitetskontroll av nyckelparametrar såsom exponentstorlek och test av primalitet.

5.1.4 Nycklarnas användningsområde

Nycklar genererade för DNSSEC används aldrig för något annat ändamål eller utanför signeringssystemet. Signeringssystemet och HSM:er används inte för något annat ändamål än DNSSEC.

En signatur skapad av en DNSSEC-nyckel har aldrig en längre giltighetsperiod än 14 dagar för både ZSK och KSK, där denna giltighetsperiod alltid börjar en timme innan tidpunkten då signaturen framställs.

5.2 Skydd av privata nycklar och kryptografiska säkerhetsmoduler

Alla kryptooperationer som involverar KSK:er och ZSK:er utförs i det skyddade minnet på HSM. Inga privata nycklar lagras i oskyddad form eller utanför HSM.

5.2.1 Standarder och kontroller för kryptografiska säkerhetsmoduler

Systemet använder en säkerhetsmodul (HSM) som är validerad mot en säkerhetsnivå motsvarande FIPS 140-2 nivå 3.

5.2.2 Flerpersonskontroll (m-av-n) av privata nycklar

IIS tillämpar ingen flerpersonskontroll för hantering av privata nycklar. Jämför avsnitt 4.2.4 för beskrivning av kompenserande kontroller genom uppdelning av roller och ansvar vid aktivering av HSM.

5.2.3 Deponering av privata nycklar

IIS tillämpar ingen nyckeldeponering av privata nycklar.

5.2.4 Säkerhetskopiering

Under den inledande nyckelceremonin kopieras de förgenererade applikationsnycklarna till en backupmodul med liknande karaktäristika som HSM:en själv. Backupmodulerna förvaras i kassaskåp åtkomliga för rollen SA, medan aktiveringsdata för backupmodulerna lagras i ett säkert utrymme (se avsnitt 4.1.8) som endast SO har tillträde till.

5.2.5 Lagring i kryptografisk säkerhetsmodul

Privata nycklar lagras alltid i krypterad form medan de förvaras på persistent minne i HSM, med en nyckel som finns på en skyddad area på HSM:n.

5.2.6 Arkivering av privata nycklar

Privata nycklar som inte längre används arkiveras inte.

5.2.7 Överföring av privata nycklar till eller från kryptografisk säkerhetsmodul

Under den inledande nyckelceremonin genereras en HSM Master Key som distribueras till samtliga enheter som ska användas för produktion. Distributionen sker fysiskt med användning av en separat uppsättning hårdvarumoduler med erforderliga nycklar. Efter att nyckeldistributionen har genomförts, lagras dessa i hårdvarumoduler i ett kassaskåp som endast SO har åtkomst till. Därefter används HSM Master Key för att skydda applikationsnycklar under nyckeldistribution mellan olika enheter över IIS interna kommunikationsinfrastruktur.

5.2.8 Metod för aktivering av privata nycklar

För aktivering av HSM krävs att SA bereder en SO åtkomst till utrustningen. HSM:n och dess privata nycklar aktiveras av en SO som innehar dess aktiveringsdata. Dessa data ligger lagrade på en säkerhetsmodul som förvaras i ett säkerhetsskåp dit endast SO har tillträde.

5.2.9 Metod för deaktivering av privata nycklar

HSM låses om signeringssystemet stängs av, startas om eller förlorar försörjning av el under mer än två timmar.

5.2.10 Destruktion av privata nycklar

Det sker ingen destruktion av privata nycklar efter det att de blivit ogiltiga. Efter deras användningsperiod tas de bort från signeringssystemet för att undvika återanvändning av misstag, men de kan fortfarande finnas tillgängliga i backupmodulen.

5.3 Andra aspekter på nyckelhantering

5.3.1 Arkivering av publika nycklar

Publika nycklar arkiveras i enlighet med bevarande av annan information relevant för spårbarheten i systemet, som till exempel logginformation.

5.3.2 Nycklars användningsperiod

Efter att den användningsperioden för en nyckel har gått ut och nyckeln blivit utbytt övergår nyckeln till att vara utgången och blir då ogiltig. Utgångna nycklar återanvänds

inte och tas normalt bort som en del av de löpande driftrutiner som används för underhåll av signeringssystemet.

5.4 Aktiveringsdata

Aktiveringsdata lagras på en fysisk säkerhetsmodul som kopplas mot HSM vid aktiveringen.

5.4.1 Generering och installation av aktiveringsdata

Aktiveringsdata skapas maskinellt för att sedan lagras i säkerhetsmodulen som används för att aktivera HSM. Installation av aktiveringsdata sker genom fysisk sammankoppling mellan HSM och säkerhetsmodulen.

5.5 Skydd av aktiveringsdata

Varje SO ansvarar för att skydda säkerhetsmodulen under det att den används, i enlighet med gällande regler. När säkerhetsmodulen inte används förvaras den i säkerhetsskåp endast åtkomlig för SO. Vid misstanke om att aktiveringsdata röjts till obehöriga ska SO omgående se till att det byts ut. Säkerhet i datorsystem

IIS har infört ett centraliserat rollbaserat auktorisations- och autentiseringssystem vilket möjliggör en finmaskig åtkomstkontroll och automatisk och rapportering för uppföljning av tilldelade behörigheter. All åtkomst loggas och loggning sker på en nivå som medger spårbarhet för alla (privilegierade) operationer i varje delsystem på individnivå.

Alla verksamhetskritiska system övervakas kontinuerligt för att upptäcka händelser relevanta för stabiliteten och säkerheten i systemen.

5.6 Nätverkskontroller

IIS har logiskt segmenterade nätverk med indelning i olika säkerhetszoner. Brandväggar används för att styra kommunikation mellan olika nätverkssegment och till kritiska delar av registrysystemet.

Loggning sker av all trafik som går genom brandväggarna.

All information av känslig natur som överförs över kommunikationsnät skyddas alltid av stark kryptering.

5.7 Tidsstämpling

IIS inhämtar tid som är spårbar till tidservrar hos Rise, tidigare SP, Sveriges Tekniska Forskningsinstitut[2]. Tidsstämpling görs i UTC(SP) och är normerande för all loggning samt giltighetstider för DNSSEC-signaturer.

5.8 Tekniska kontroller under systemets livscykel

5.8.1 Kontroller i systemutveckling

Registrysystemet är utvecklat som en del av IIS verksamhet. All källkod lagras och versionshanteras. Källkodsträdet säkerhetskopieras regelbundet och kopior lagras frånkopplat i brandskyddade säkerhetsskåp.

IIS utvecklingsmodell baseras på branschstandarder och innefattar:

- fullständig funktionell specifikation och dokumenterade säkerhetskrav,
- dokumenterad högnivåkonstruktion baserad på en naturlig modularisering av systemet,

[2] https://www.sp.se/sv/index/services/time_sync/ntp/Sidor/default.aspx

- kontinuerlig strävan att minimera komplexitet,
- systematisk och automatiserad testning samt regressionstester,
- utgivning av distinkta programversioner,
- ständig kvalitetsuppföljning av upptäckta fel (i enlighet med ISO 9001:2015).

5.8.2 Säkerhetskontroller

IIS är certifierat enligt SS ISO/IEC 27001:2014.

IIS har etablerat och underhåller en systemsäkerhetsplan för Registryt. Planen uppdateras regelbundet baserat på incidentrapporter, säkerhetsgranskningar (se avsnitt 7) och återkommande hot- och sårbarhetsanalyser. Underhållet av ledningssystemet och systemsäkerhetsplanen följer PDCA-metoden (Plan Do Check Act) som den beskrivs i ISO/IEC 27001, och formar tillsammans med IIS informationssäkerhetspolicy och grundskyddsnivå grunden för hantering av systemsäkerheten.

5.8.3 Säkerhetskontroller i ändringsprocessen

IIS har infört en formell IT Service Management (ITSM) Change Management-process enligt principerna i ISO/IEC 20000 med syfte att styra och kontrollera förändringar i IT-miljön.

6 Zonsignering

6.1 Nyckellängder, nyckeltyper och algoritmer

IIS använder ett signeringsschema med uppdelade nycklar för signering av .se-zonen. Uppdelning görs i nyckelsigneringsnyckel (KSK) och zonsigneringsnyckel (ZSK). Nyckellängder och algoritmer ska ha en styrka som är tillräcklig för ändamålet inom respektive nyckels användningsområde och administrativa livslängd.

Algoritmer ska vara standardiserade av IETF, allmänt tillgängliga och resurseffektiva för alla inblandade parter.

För närvarande används RSA-algoritmen med en nyckelängd av 2048 bitar för både KSK och ZSK.

6.2 Autentiserade negativa svar

IIS tillämpar NSEC för autentiserade negativa svar, enligt RFC 4034.

6.3 Signaturformat

Signaturer genereras över ett kryptografiskt kondensat framställt genom SHA256 (RSA/SHA256, RFC 6594).

6.4 Nyckelrullningar

Byte av zonsigneringsnycklar (ZSK) sker var 84:e dag.

Byte av nyckelsigneringsnycklar (KSK) sker vid behov.

6.5 Signaturlivslängd och frekvens för omsignering

RR-poster (RR Sets) signeras med en slumpmässig giltighetstid på mellan 12 och 14 dagar. Signaturer som går ut inom 10 dagar förnyas varannan timme ojämna klockslag (UTC(SP)).

6.6 Verifiering av RR-poster

För att säkerställa signaturers äkthet och integriteten hos DNSKEY-posten sker ett antal kontroller automatiskt vid varje signeringstillfälle. Dessa kontroller innefattar verifiering av signaturer med användning av Delegation Signer (DS)-posten som har registrerats hos IANA för rotzonen, såväl som verifiering av tid och datum. Zoninformation som inte godkänns vid de automatiska kontrollerna flaggas för manuell hantering. Produktion av ny zonfil stoppas till dess att felsökning och felhantering genomförts.

Vidare verifieras att samtliga poster i zonfilen är giltiga enligt gällande standard innan distribution.

6.7 RR-posters livslängd (Time to live, TTL)

Livslängd (TTL) för varje DNSSEC Resource Record (RFC 4034) specificeras enligt följande, i sekunder:

RR-typ	**TTL**
DNSKEY	3600
DS	3600
NSEC	som SOA minimum (7200)
RRSIG	Samma som TTL för RR (varierar)

7 Revision

För att verifiera att införda kontroller fungerar och är effektiva företar IIS både interna och externa revisioner av registrysystemet.

7.1 Frekvens för revision

Revision utförs både regelbundet och vid behov. Faktorer som ligger till grund för revision innefattar bland annat:

- om mer än 24 månader förflutit sedan senaste revisionen,
- om IIS uppmärksammats på återkommande avvikelser,
- om det sker betydande förändringar på ledningsnivå, i organisationen eller i de processer som stödjer registryverksamheten.

7.2 Revisorns kvalifikationer

Revisorn ska inneha erforderliga färdigheter inom områdena IT-säkerhetsrevision, IT-säkerhet, DNS och DNSSEC.

7.3 Revisorns förhållande till den granskade parten

En extern och oberoende revisor ska utses för att genomföra och leda revisionen. Revisionsledaren kan där så behövs ta in särskild sakkunskap med erfarenhet från IIS verksamhet.

7.4 Revisionens omfattning

Revisioner av registrysystemet sker med användning av befintliga styrdokument.

De dokument som avses är primärt IIS informationssäkerhetspolicy, grundskyddsnivå och systemsäkerhetsplan för registrysystemet samt dokumenterade anvisningar och rutiner för drift.

7.5 Åtgärder vid upptäckt av brist

Revisionsledaren ska omedelbart kommunicera alla avvikelser till IIS ledning. Allvarlighetsgraden för varje avvikelse avgörs i samverkan med revisorn. Lämpliga förbättringsåtgärder utvecklas och införs med den skyndsamhet som krävs.

7.6 Information om resultat från revision

Revisionsledaren ska rapportera funna observationer skriftligt till IIS inom 30 kalenderdagar från revisionstillfället. Rapporten är inte öppen.

8 Rättsliga aspekter

8.1 Avgifter

Eventuella avgifter i samband med DNSSEC regleras i avtal mellan Registry och Registrar. https://www.iis.se/domaner/bli-registrar/avtal/

8.2 Behandling av personuppgifter

Personuppgifter behandlas i enlighet med EU:s dataskyddsförordning samt enligt avtal där skyddet av personuppgifter regleras. IIS hantering av personuppgifter finns beskrivna i IIS integritetspolicy:

https://iis.se/docs/Integritetspolicy_iis.pdf

8.3 Ansvarsbegränsning

Skadeståndsansvaret mellan Registry och Registrar regleras i Registraravtalet:
https://www.iis.se/domaner/bli-registrar/avtal/
IIS skadeståndsansvar gentemot Innehavare regleras i IIS Registreringsvillkor för toppdomänen .se. Dessa finns under adressen:
https://www.iis.se/docs/Registreringsvillkor_sv.pdf

Dokumentkontroll

Dokumentinformation och klassificering

UPPFÖRD AV	FAKTAANSVARIG	DOKUMENTANSVARIG
SÄKERHETSCHEF	SÄKERHETSCHEF	SÄKERHETSCHEF

SÄKERHETSKLASS	FILNAMN
ÖPPEN	DNSSEC SAKERHETSDEKLARATION DPS-SE

Godkänd av

DATUM	NAMN	FUNKTION
2018-05-25	ANNE-MARIE EKLUND LÖWINDER	SÄKERHETSCHEF

Revisioner

DATUM	VERSION	NAMN	BESKRIVNING
2010-04-19	A	AMEL	SLUTVERSION
2010-11-19	A	AMEL	UPPDATERAD, TAGIT BORT HÄNVISNING TILL ITAR
2011-05-20	B	AMEL	UPPDATERAT 6.6. PÅ GRUND AV FÖRÄNDRING AV SIGNATURLIVSLÄNGDER
2011-09-08	C	AMEL	UPPDATERAT 4.4.7 I DEN ENGELSKSPRÅKIGA VERSIONEN P.G.A. FELAKTIG ÖVERSÄTTNING SAMT KORRIGERAT 5.1.4 OM SIGNATURLIVSLÄNGDER.
2012-04-23	C	AMEL	KORRIGERAT EFTER DPS FRAMEWORK DRAFT OCH NY SIGNERINGSLÖSNING.
2012-05-25	PD1	AMEL	ÄNDRAD EFTER KORRIGERINGAR I DEN ENGELSKSPRÅKIGA VERSIONEN

2012-08-17	D	AMEL	SLUTLIG VERSION FÖR PUBLICERING
2013-02-14	E	AMEL	UPPDATERING EFTER ÄNDRING I KEY AND SIGNING POLICY OCH SYNPUNKTER FRÅN IT-DRIFT.
2015-01-07	PF1	AMEL	HARMONISERING MOT DPS FÖR .NU, ÄNDRING AV INFORMATION RÖRANDE NÖDNYCKEL OCH RÄTTELSE AV RFC-NUMMER EFTER PÅPEKANDE FRÅN EXTERN.
2015-01-08	PF2	AMEL	SYNPUNKTER FRÅN PATRIK WALLSTRÖM
2015-01-09	PF3	AMEL	SYNPUNKTER FRÅN ROGER
2015-01-30	F	AMEL	SLUTVERSION
2015-07-07	G	AMEL	UPPDATERAT 3.5.2, NAMNBYTE .SE -> IIS
2017-11-28	PH1	AMEL	UPPDATERAT INFÖR NYCKELRULLNING, ALGORITMRULLNING
2017-12-12	H	AMEL	GODKÄNT AV DNS-GRUPPEN (ULRICH)
2018-05-23	PI1	AMEL	ANPASSNING TILL GDPR
2018-05-25	I	AMEL	NY VERSION PUBLICERAD