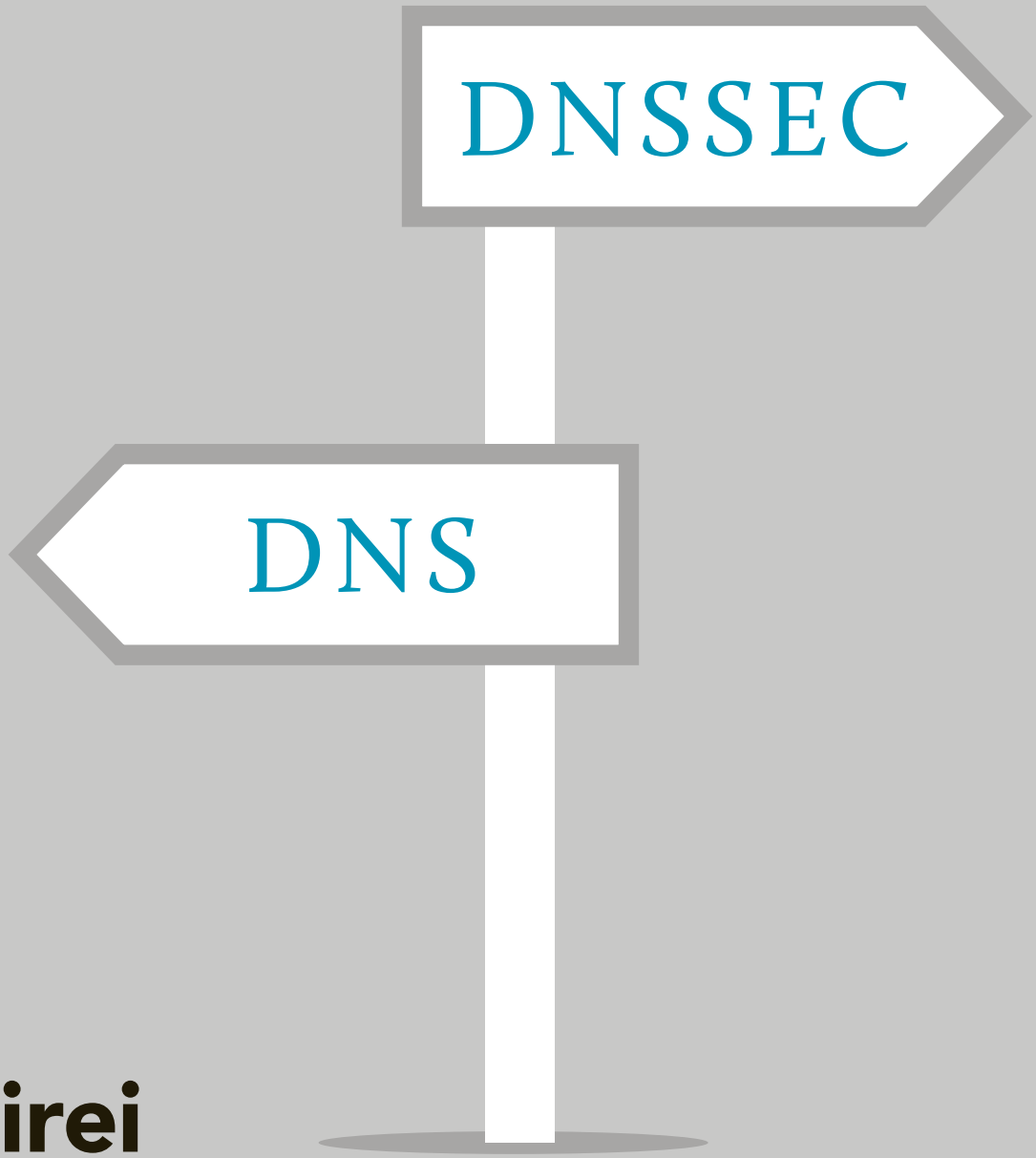
.se

Rekommendationer för införande av DNSSEC i kommuner och motsvarande verksamheter



kirei

Rekommendationer för införande av DNSSEC i kommuner och motsvarande verksamheter

Innehåll

1 Introduktion

1.1 Bakgrund

Regionförbundet i Kalmar län bedrev 2012 ett projekt med syfte att införa DNSSEC i regionens kommuner. Projektet genomfördes med stöd av länsstyrelsen i Kalmar län i samarbete med MSB (Myndigheten för samhällsskydd och beredskap) och resulterade i att samtliga kommuner inom Kalmar län är säkrades med DNSSEC.

Under arbetets gång dokumenterade regionförbundet i Kalmar erfarenheter och tillvägagångssätt i en vägledning som stöd till kommunerna i deras arbete.

Denna vägledning bygger på den som regionförbundet i Kalmar utarbetade, men är till vissa delar omarbetad för att passa en bredare målgrupp.

Manuskriptet till vägledningen har skrivits av Fredrik Ljunggren och Jakob Schlyter, Kirei AB, samt bearbetats av Anne-Marie Eklund Löwinder, .SE. Synpunkter på innehållet har inhämtats från MSB, PTS (Post- och telestyrelsen), SKL (Sveriges Kommuner och Landsting) samt från .SE:s DNS-referensgrupp. Bearbetning och publicering av vägledningen har finansierats av .SE.

1.2 Syfte

I princip alla Internetbaserade tjänster är beroende av att domännamnssystemet (DNS) fungerar. Konsekvensen av att göra fel kan bli omfattande. Detta gäller i än högre grad vid införandet av DNSSEC som är ett sätt för att skydda informationen som kommuniceras mellan servrarna i DNS från manipulation. DNSSEC ställer högre krav på teknisk kompetens för drift än traditionell DNS.

Denna vägledning är framtagen för att kunna tjäna som ett hjälpmedel och verktyg för kommuner har för avsikt att införa DNSSEC. Ambitionen är att den också ska utgöra ett stöd i det löpande arbetet med DNSSEC. Den fungerar givetvis också i andra typer av verksamheter inom både offentlig förvaltning och näringsliv.

1.3 Finansiering

Tillsammans med .SE, SKL samt PTS har MSB gjort det möjligt för Sveriges kommuner att via länsstyrelserna kunna ansöka om finansiellt stöd för införandet av DNSSEC.

MSB har varje år möjlighet att bevilja medel ur det så kallade 2:4-anslaget, Krisberedskap, som kan sökas av utpekade statliga myndigheter. Med början 2012 prioriterade MSB området robusthetshöjande åtgärder med inriktning mot att säkerställa adressuppslagningar

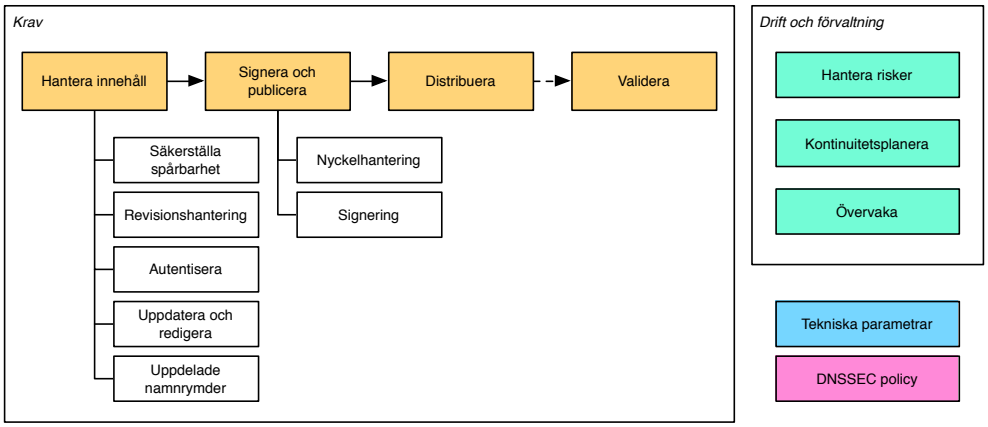
på internet, det som sker via domännamnssystemet, DNS. Myndigheten har bland annat tryckt på att det är mycket angeläget att domäner för offentliga webbplatser signeras med DNSSEC. Samma budskap förs även fram av den högsta politiska ledningen, IT-minister Anna-Karin Hatt, i den digitala agendan för Sverige.

1.4 Struktur

Vägledningen är uppdelad i tre kapitel och två bilagor (se figur 1.1):

- Kapitlet *Krav* är tänkt att användas som rekommendationer för kravställning vid upphandling och systemkonstruktion. Rekommendationerna är uppdelade i ett antal kategorier beroende på vilka delar av en DNS-implementation som avses.
- Kapitlet *Rekommendationer för tekniska parametrar* är tänkt att användas som grund för konfiguration av ett färdigt system.
- Kapitlet *Drift och förvaltning* redovisar ett antal områden som påverkas vid införande av DNSSEC.
- *Bilaga A* formulerar ett styrdokument för DNSSEC baserat på de rekommendationer som redogörs för i denna vägledning.
- *Bilaga B* utgör exempel på tekniska kontroller för uppfyllande av vägledningens rekommendationer.

Notationen *Kx*, där K innebär krav, används för att redogöra för krav som bör beaktas vid DNSSEC-införande.



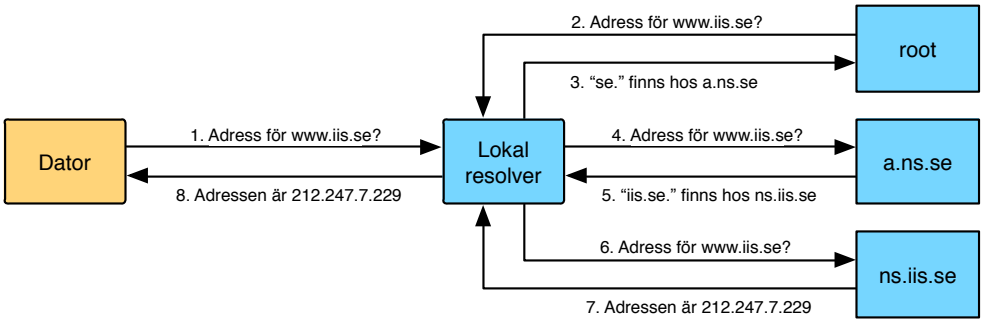
Figur 1.1 – Dokumentstruktur

1.5 Mer information om DNS och DNSSEC

Ett domännamn är adressen till en server på internet i en form som människor kan minnas, till exempel www.regeringen.se. Bakom varje domännamn döljer sig en unik IP-adress. Man kan

säga att domännamnet är ett alias för de IP-adresser som maskinerna kommunicerar med, till exempel http://194.14.70.181/ som är samma sak som www.regeringen.se. Samma sak gäller för e-posthantering. Du behöver inte kunna några krångliga sifferkoder för att få ditt e-brev att landa hos mottagaren, bara en adress med formen mottagare@exempel.se.

Bakom den översättningen ligger en katalogfunktion som kallas domännamnssystemet (DNS) och som alltså kopplar samman domännamnet med den aktuella IP-adressen för just det namnet.



Figur 1.2 – Delegering

När DNS skapades på 1980-talet var huvudtanken att minimera den centrala administrationen av nätverket och göra det lätt att koppla upp nya datorer till internet. Däremot fästes inte särskilt stor vikt vid säkerheten. Bristerna på detta område har öppnat för olika typer av missbruk och attacker där svaren på DNS-uppslagningar förfalskas. På så vis kan internetanvändare ledas fel, exempelvis i syfte att lura av folk känslig information som lösenord och kreditkortsnummer.

Även om man gör sitt allra bästa för att täppa till säkerhetshål i de program som används vid DNS-uppslagningar ligger grundproblemet i hur DNS fungerar. Därför har man utvecklat säkerhetstillägg till DNS som fått beteckningen DNSSEC (DNS Security Extensions). Med DNSSEC säkras domännamnssystemet från missbruk genom att svaren på DNS-uppslagningar signeras kryptografiskt. Då säkerställs att svaren verkligen kommer från rätt källa och inte ändrats under överföringen. Att så är fallet kontrolleras genom validering av signaturens riktighet.

.SE har tagit fram en internetguide om domännamnssystemet och hur DNS fungerar. Guiden heter *DNS – Internets vägvisare* och finns att hämta på:
`https://www.iis.se/lar-dig-mer/guider/dns-internets-vagvisare/`.

.SE har också tagit fram en kort beskrivning över DNSSEC och vad DNSSEC skyddar mot. Beskrivningen finns att hämta på:
`https://www.iis.se/domaner/teknik/dnssec/`.

2 Krav

Detta kapitel innehåller kravrekommendationer för kommuner och motsvarande organisationer som inför DNSSEC. Rekommendationerna baseras på gällande praxis för drift av DNSSEC i domäner på nivån under toppdomänen, men dessa kan självfallet kräva anpassning för att bättre möta den egna verksamhetens behov och förutsättningar.

En rad faktorer bör beaktas vid tillämpning av dessa rekommendationer, innefattande:

- allmän riskbedömning,
- verksamhetens tekniska plattform, samt
- driftpersonalens kompetens.

2.1 Hantera innehåll

Med *innehållshantering* avser vi hur den data som publiceras via DNS underhålls och uppdateras. Detta kan ske genom manuell hantering (till exempel via ett användargränssnitt eller via direkt redigering av en textfil) eller automatiskt baserat på händelser i andra system (till exempel DHCP eller katalogtjänst). Exempel på hur dessa krav kan mötas beskrivs vidare i stycke B.1.

2.1.1 Säkerställa spårbarhet

För att i efterhand kunna spåra ändringar i information, och vilken information som har förändrats och när, bör krav på spårbarhet ställas. För att underlätta uppföljning bör det även finnas möjlighet att följa ett revisionsspår av dessa förändringar i befintligt ärendehanteringssystem, och där kunna utröna transaktionens ursprung och orsak.

[K1] All förändring av konfiguration och/eller data SKALL loggas med information om tid för ändringen, vilken administratör som utfört ändringen samt information som gör det möjligt att i efterhand utreda vad som ändrats.

[K2] Det BÖR vara möjligt att till varje förändring bifoga information, till exempel en kommentar eller ett ärendenummer.

2.1.2 Revisionshantering

Förutom att veta vem som har vidtagit vilken åtgärd och när, så finns det i många fall behov av att kunna gå tillbaka och jämföra vilken information som funnits i systemet vid olika tidpunkter.

[K3] Information i DNS SKALL revisionshanteras.

[K4] Det SKALL finnas möjlighet att återställa data från en tidigare revision.

[K5] Det BÖR finnas möjlighet att visa skillnaden mellan två olika revisioner.

2.1.3 Autentisera

Samtliga användare av systemet ska autentiseras och använda unika och personliga systemidentiter. För att inte behöva administrera flera uppsättningar systemidentiteter, bör dessa kunna verifieras mot externt behörighetskontrollsystem.

[K6] Samtliga användare SKALL autentiseras vid användning av systemet.

[K7] Personliga användaridentiteter SKALL alltid användas.

[K8] Användarkonton BÖR kunna hämtas från externa system, till exempel LDAP eller RADIUS.

[K9] Autentisering BÖR kunna ske mot externa system, till exempel LDAP, Kerberos eller RADIUS.

2.1.4 Uppdatera och redigera

Ändring av information som publiceras via DNS bör ske på ett sätt som förutom att det uppfyller kraven på spårbarhet och åtkomstkontroll, också minimerar risken för att felaktig information publiceras. Detta kan uppfyllas genom kontroller vid inmatning eller genom att informationen kontrolleras ytterligare en gång innan publicering.

[K10] Det system som används för uppdatering av DNS SKALL innehålla kontroller för att säkerställa att felaktigt formaterat data inte kan publiceras.

[K11] System för uppdatering BÖR kunna hantera olika användarbehörigheter, till exempel styra vilka användare som får redigera viss information.

2.1.5 Uppdelade namnrymder

Namnrymd (*namespace*) är en omgivning eller kontext i vilken alla namn är unika. Den vanligaste och största namnrymden i DNS är den som gäller för hela världen och alltså är den som alla internetanslutna noder kan använda. En del organisationer har interna namnrymder som endast är åtkomliga inom den egna organisationen.

Ibland finns det anledning att ge olika DNS-svar beroende på varifrån frågan ställs. Detta kan exempelvis behövas om viss information inte skall publiceras gentemot externa nätverk eller om privata IP-adresser används för resurser inom en del av ett nät, samtidigt som samma resurser ska vara nåbara via publika IP-adresser inom en annan del. Samtidigt bör den information som publiceras i alla namnrymder hanteras på ett och samma ställe.

Införandet av DNSSEC ställer särskilda krav på hur uppdelade namnrymder hanteras, särskilt vad gäller nyckelhantering. I vissa fall är det lämpligt att använda samma nyckelmaterial för flera namnrymder, medan det i andra fall är mer lämpligt att strikt separera namnrymderna eller kanske avstå från att signera delar av namnrymden.

[K12] Uppdelade namnrymder (*split DNS*) BÖR stödjas av systemet.

[K13] DNSSEC för uppdelade namnrymder BÖR kunna konfigureras att använda antingen gemensamt eller separat nyckelmaterial för olika namnrymder. Detta BÖR vara valbart per zon.

För att förenkla administrationen av DNS är det ofta önskvärt att om möjligt undvika uppdelade namnrymder. Alternativa metoder för att separara information är till exempel att placera namn som endast ska användas internt i en underdomän.

- I moderna nätarkitekturer är begrepp som "insida" och "utsida" ofta inte tillämpliga. Datorer och annan utrustning flyttas ofta runt och används därmed på både interna och externa nät, och når i många fall samma resurser. Att använda olika adresser på tjänster beroende på varifrån de används kan vara en komplicerande faktor.

2.2 Signera och publicera

Kraven på system för DNSSEC delas upp i två delar – system för nyckelhantering och system för signering. Många programvaror skiljer inte på dessa två funktioner, men eftersom uppgifterna kan hanteras helt separat presenteras kraven åtskilda. Exempel på hur dessa krav kan mötas beskrivs vidare i stycke B.2.

2.2.1 Krav på system för nyckelhantering

Följande krav specificerar en miniminivå på system för nyckelhantering.

[K14] Nyckelhanteringssystemet SKALL stödja separation av nycklar för nyckelsignering (KSK, *Key Signing Key*) och zonsignering (ZSK, *Zone Signing Key*).

[K15] Nyckelhanteringssystemet BÖR stödja gemensamma nycklar för nyckelsignering och zonsignering (CSK, *Combined Signing Key*).

[K16] Nyckelhanteringssystemet SKALL stödja byte av nycklar (nyckelrullning) enligt RFC6781 [20].

[K17] Nyckelhanteringssystemet SKALL stödja automatiska schemalagda byten av ZSK med förpublicering (*Pre-Publish Zone Signing Key Rollover*) enligt RFC6781 [20].

[K18] Nyckelhanteringssystemet BÖR stödja lagring av nycklar i en separat säkerhetsmodul (HSM, *Hardware Security Module*).

[K19] Om separat säkerhetsmodul inte används SKALL lagrade nycklar skyddas mot insyn och förändring.

[K20] Gränssnittet mellan nyckelhanteringssystemet och eventuell säkerhetsmodul (HSM) BÖR vara baserat på PKCS#11 [23].

2.2.2 Krav på system för signering

Följande krav specificerar en miniminivå på system för signering.

[K21] Signeringssystemet SKALL stödja DNSSEC enligt RFC4033 [13], RFC4034 [15] och RFC4035 [14].

[K22] Signeringssystemet SKALL stödja signering med följande algoritmer: RSA/SHA-1 enligt RFC3110 [11] samt RSA/SHA-256 och RSA/SHA-512 enligt RFC5702 [19].

[K23] Signeringssystemet BÖR stödja signering med följande algoritmer: ECDSA P-256/SHA-256 och ECDSA P-384/SHA-384 enligt RFC6605 [18].

[K24] Signeringssystemet SKALL stödja NSEC3 enligt RFC5155 [21].

[K25] Signeringssystemet SKALL stödja DS-poster publicerade med SHA-256 enligt RFC4509 [17].

[K26] Signeringssystemet BÖR stödja signering med två eller fler algoritmer samtidigt.

[K27] Signeringssystemet BÖR stödja byte av signeringsalgoritmer utan att zonen återgår till att vara osignerad.

[K28] Signeringssystemet BÖR stödja byte mellan NSEC och NSEC3 utan att zonen återgår till att vara osignerad.

[K29] Signeringssystemet SKALL stödja byte av NSEC3-parametrar utan att zonen återgår till att vara osignerad.

[K30] Signeringssystemet SKALL stödja konfiguration av signaturernas livslängd (*signature lifetime*).

[K31] Signeringssystemet SKALL stödja konfiguration av återsigneringstid (*signature refresh period*).

2.3 Distribuera

Följande krav specificerar en miniminivå på system för distribution av DNSSEC-signerade zoner. Exempel på hur dessa krav kan mötas beskrivs vidare i stycke B.3.

[K32] All zonöverföring SKALL vara skyddad mot förändring och avkortning (trunkering).

[K33] Zonöverföring BÖR skyddas mot förändring och avkortning genom TSIG [25].

[K34] Zonöverföring BÖR autentiseras genom någon av algoritmerna i familjen HMAC-SHA [12] eller GSS-TSIG [25].

2.4 Validera

Följande krav specificerar en miniminivå på system för validering av DNSSEC-signaturer. Dessa system implementeras ofta som en del av en rekursiv namnserver (*Validating Recursive Resolver*). Exempel på hur dessa krav kan mötas beskrivs vidare i stycke B.4.

[K35] Validering SKALL ske enligt RFC4033 [13], RFC4034 [15] och RFC4035 [14].

[K36] Validering SKALL stödja följande algoritmer: RSA/SHA-1 enligt RFC3110 [11] samt RSA/SHA-256 och RSA/SHA-512 enligt RFC5702 [19].

[K37] Validering BÖR stödja följande algoritmer: ECDSA P-256/SHA-256 och ECDSA P-384/SHA-384 enligt RFC6605 [18].

[K38] Validering SKALL stödja NSEC3 enligt RFC5155 [21].

[K39] Validering SKALL stödja DS-poster publicerade med SHA-256 enligt RFC4509 [17].

[K40] Validering SKALL stödja DNSSEC Opt-In enligt RFC5155 [21].

[K41] Validering BÖR stödja automatisk uppdatering av tillitsankare enligt RFC5011 [24].

[K42] Validering BÖR kunna stängas av för hela eller delar av namnrymden.

2.5 Övervaka

Följande krav specificerar en miniminivå på system för övervakning av nyckelhantering, signering och distribution. Exempel på hur dessa krav kan mötas beskrivs vidare i stycke B.5.

[K43] Övervakningssystemet SKALL kontrollera att signaturer uppdateras enligt gällande konfiguration.

[K44] Övervakningssystemet SKALL kontrollera att samtliga namnservrar svarar med korrekta autentiserade positiva svar för zonens SOA-, NS- samt DNSKEY-poster.

[K45] Övervakningssystemet SKALL kontrollera att samtliga namnservrar svarar med korrekta autentiserade negativa svar.

[K46] Övervakningssystemet SKALL kontrollera att samtliga namnservrar är uppdaterade med aktuell data.

[K47] Övervakningssystemet BÖR kontrollera att samtliga namnservrar har korrekt tid genom att via NTP regelbundet hämta tid från de publika tidsservrarna i Sverige [5][6] för att få tillgång till svensk spårbar tid.

3 Rekommendationer för tekniska parametrar

I det här kapitlet ges rekommendationer för tekniska parametrar vid införande av DNSSEC hos större organisationer och företag. Parametrarna är valda baserat på gällande branschpraxis och praktiska erfarenheter från införande av DNSSEC.

Signeringsnycklar

Denna vägledning rekommenderar en separation av nycklar mellan nyckelsigneringsnyckel (KSK) och zonsigneringsnyckel (ZSK), av den anledningen att det i dagsläget är den vanligast förekommande och mest beprövade modellen för nyckelhantering. Signeringsalgoritmen som används bör vara RSA/SHA-256, då detta är den algoritm som idag används av roten för domännamnssystemet (DNS). Nyckellängderna för KSK/ZSK bör, baserat på i skrivande stund gällande kryptografiska rekommendationer, sättas till 2048 respektive 1024 bitar.

- KSK: 2048-bit RSA/SHA-256
- ZSK: 1024-bit RSA/SHA-256

Livslängd på signaturer

För att med god marginal kunna hantera driftstörningar under bland annat långhelger och semestertider, rekommenderar denna vägledning att man sätter en förhållandevis lång livslängd på signaturer. Detta bör kombineras med en daglig omsignering.

- Livslängd på signaturer: 32 dagar
- Omsignering dagligen.

Nyckelrullning

Det rekommenderas att nyckelmaterial för nyckelsigneringsnycklar (KSK) endast bytes vid behov, och att byte sker baserat på en väl avvägd riskanalys. En anledning till byte kan till exempel vara att personal som haft åtkomst till nyckelmaterial slutat eller fått andra arbetsuppgifter. Rutiner för nyckelbyte bör utformas i relation till hur nyckelmaterial för andra system (till exempel webbservrar, katalogtjänst och terminalinloggning) hanteras. Att byta KSK innebär en större risk (jämfört med byte av ZSK) då ett byte normalt medför manuella rutiner för uppdatering av DS-poster i överliggande zon.

Byte av nyckelmaterial för ZSK kan av de flesta system hanteras helt automatiskt. Baserat på den relativt korta nyckellängden rekommenderas att byte sker var tredje månad.

- Byte av KSK vid behov.
- Byte av ZSK var tredje månad (med automatik).

Metod för autentiserade negativa svar

NSEC3 används i normalfallet endast då man önskar försvåra för utomstående att genom uttömmande sökning samla in samtliga i zonen ingående poster. Det är en rekommendation att använda NSEC3 för samtliga zoner på nivån under toppdomänen.

- Negativa svar autentiseras enligt NSEC3 med 10 iterationer.
- Byte av NSEC3-salt årligen – manuellt eller automatiskt.

Nyckelskydd

För att minska risken för att nyckelmaterial röjs vid exempelvis utbyte eller stöld av maskinvara, rekommenderas att allt nyckelmaterial lagras på krypterat lagringsmedia, även om detta inte ger ett skydd mot exponering när system är i produktion. Nyckelmaterial eller lösenord för att dekryptera nyckelmaterial bör lagras utanför systemet och matas in av administratör när systemet aktiveras.

- Samtliga signeringsnycklar (KSK/ZSK) bör om möjligt lagras på krypterat lagringsmedia, men kan lagras okrypterat om signeringsutrustningen skyddas fysiskt samt att adekvata rutiner för att förstöra förbrukat lagringsmedia finns etablerade.
- Användning av säkerhetsmodul (HSM) krävs inte.

4 Drift och förvaltning

I det här kapitlet beskrivs tre viktiga moment i arbetet med att införa DNSSEC. Dessa bör hanteras inom ramen för organisationens ordinarie processer och rutiner för drift och förvaltning.

4.1 Hantera risker

Organisationer bör ha en förmåga och beredskap för att kunna hantera eventuella risker och incidenter som kan uppstå. En sådan förmåga kan byggas upp med hjälp av utbildning och kompetensförsörjning samt dokumenterade processer och rutiner. Dokumenterade rutiner bör finnas för exempelvis manuell omsignering, nyckelbyte samt återgång till osignerad zon i händelse av att en allvarlig incident inträffar.

De huvudsakliga riskerna som introduceras genom ett införande av DNSSEC relaterar till zonens tillgänglighet för de validerande rekursiva namnservrarna. Om signaturer, nycklar och överordnade DS-poster inte hålls aktuella finns risk att zondatat inte kan valideras, varvid de resurser som publiceras i zonen blir otillgängliga.

För att hantera och minimera dessa risker bör en rad samverkande åtgärder övervägas. Det krävs bland annat att kompetensförsörjningen kring DNSSEC är säkerställd, samt att signaturlivslängder och nyckelbytesintervall anpassas till de tillgänglighetskrav som råder för system och personal inom organisationen.

4.2 Övervaka

För att säkerställa zonens tillgänglighet och tidigt kunna upptäcka och agera på fel, krävs även ingående övervakning av zondata, nycklar och signaturers tillstånd. Betingelser som bör övervakas och jämföras sinsemellan innefattar:

- signeringsfunktionens uppfattning om aktuell tid,
- signaturernas aktualitet på samtliga utpekade namnservrar,
- DS- och NS-posters aktualitet i överliggande zon,
- nyckelpostens aktualitet.

Övervakning bör verifiera hela valideringskedjan från DS-post till enskild DNS-post.

4.3 Kontinuitetsplanera

De flesta verksamheter har idag behov av en kontinuitetsplan (business continuity plan, BCP). Syftet är både att ha beredskap och förmåga att hantera oönskade händelser som påverkar tillgängligheten till information och informationsresurser, och att snabbt och systematiskt kunna hantera en krissituation som involverar alla berörda delar av verksamheten. Det innebär att ha beredskap och förmåga att hantera oönskade händelser som exempelvis dödsfall, skandal, brand, avbrott i produktion, avbrott i logistik med mera. Kontinuitetsplanering skall även säkerställa att verksamheten vid avbrott i IT-stödet kan bedrivas i begränsad omfattning men under kontrollerade förhållanden. Kontinuitetsplanering innefattar även att vidta åtgärder för att förebygga eller minimera effekten av en oönskad händelse.

Vid den händelse att fel ändå skulle inträffa i hanteringen av nyckelmaterial, program och utrustning som används för DNSSEC, krävs beredskap för att avhjälpa felet och återgå till normal drift. Kontinuitetsplanering innefattar rutiner för att hantera och ersätta röjt eller otillgängligt nyckelmaterial, samt metoder för att återstarta eller byta till en helt ny valideringskedja.

A Säkerhetsbestämmelser för DNSSEC

A.1 Inledning

A.1.1 Allmänt

Denna bilaga formulerar ett förslag till säkerhetsbestämmelser för DNSSEC, en så kallad *DNSSEC Policy (DP)*. En DP formulerar således kravbilden och talar om *vad* som ska göras, till skillnad från en DPS (*DNSSEC Practice Statement*) som talar om *hur* implementationen är gjord. En DPS kan alltså vara en redogörelse för hur kravuppfyllnad av en DP uppnås, men kan även vara ett självpåtaget initiativ för att erbjuda transparens och visa vilken nivå av tillit som kan fästas vid DNSSEC hos den aktuella parten.

Bilagan är anpassad för kravställning av införande vid kommunala och regionala förvaltningar. Den speglar de säkerhetsrelaterade krav som redogjorts för i denna vägledning, samt övriga tillkommande aspekter på säkerhet som följer av en generell riskanalys och som också ligger till grund för existerande branchpraxis på området.

Bilagan följer standarden RFC 6841 [22], som ger stöd för hur en DP kan uttryckas. Genom att följa denna struktur underlättas jämförelser mellan olika DP, deras bestämmelser och deras avgränsningar. Standarden ger även ett stöd för vilka områden som bör innefattas i en DP, även om vissa områden kan lämnas utan några formulerade bestämmelser.

A.1.2 Dokumentnamn och -identifiering

Dokumentnamn: Kirei 2013:08/A1/sv

A.1.3 Dokumentförvaltning

Detta dokument uppdateras inte, då det endast utgör ett förslag till en grundplåt för en DP. Dokumentet förväntas också förfinas och förankras, innan det används som styrande vid införande av DNSSEC.

A.2 Publicering och åtkomst till information

A.2.1 Publiceringsplats

Ingen särskild publiceringsplats krävs för information som relaterar till DNSSEC i den aktuella zonen, med undantag för vad som anges i A.2.2.

A.2.2 Publicering av publika nyckel

Publika nycklar som är i bruk, eller avses att tas i bruk inom kort, publiceras endast i överliggande zon som DS-poster.

A.3 Operationella krav

Inga bestämmelser.

A.4 Fysisk, administrativ och personorienterad säkerhet

A.4.1 Fysiska kontroller

Utrustning och lagringsmedia som innehåller nyckelmaterial som tagits i bruk, eller som kan komma att tas i bruk, ska förvaras i skyddade utrymmen dit endast behörig personal har åtkomst.

A.4.2 Administrativa kontroller

Endast personer vars arbetsuppgifter motiverar det, och som genomgått erforderlig utbildning, ska ges åtkomst till signeringssystemet. Tilldelade behörigheter ska regelbundet granskas.

En särskild ansvarsförbindelse ska tecknas med de som har tillgång till signeringssystemet.

A.4.3 Personalorienterad säkerhet

Minst två personer inom organisationen ska ges det utpekade ansvaret för systemet, samt ha erhållit nödvändig utbildning för att på egen hand och på ett betryggande sätt kunna administrera systemet och utföra felavhjälpning inom den tid som krävs för att upprätthålla zondatas tillgänglighet.

A.4.4 Spårbarhet

Alla åtgärder som vidtas inom systemet ska kunna härledas på individnivå, och registreras i en säkerhetslogg som innefattar tid för åtgärden, åtgärdens ursprung och åtgärdens art. Säkerhetsloggen ska skyddas mot manipulation och obehörig insyn.

A.4.5 Kontinuitetsplanering

Kontinuitetsplan ska upprättas som innefattar rutiner för att hantera och ersätta röjt eller otillgängligt nyckelmaterial, samt metoder för att återstarta eller byta till en helt ny valideringskedja.

Kontinuitetsplanen och metoderna för återstart ska övas regelbundet.

A.4.6 Upphörande av verksamhet

Vid upphörande av verksamhet och om signeringen skall upphöra ska nyckelmaterial och eventuell HSM destrueras på ett kontrollerat sätt enligt A.5.8, livscykelhantering.

A.5 Tekniska säkerhetskontroller

A.5.1 Framställning och installation av nyckelpar

Nycklar ska framställas med omsorg i en skyddad omgivning, enligt tillförlitliga metoder och med tillförlitlig källa till slumptal. Den privata komponenten av nyckeln ska aldrig lagras på beständigt lagringsmedia i oskyddad form.

Överföring, distribution och installation av nyckelmaterial i annan omgivning än där nyckelmaterialet genererades, ska göras så att nyckelmaterialets konfidentialitet och integritet skyddas på ett tillbörligt sätt med hänsyn till dess känslighetsgrad.

Nyckelmaterial som framställs för användning med DNSSEC ska aldrig användas för några andra ändamål.

A.5.2 Skydd av privata nycklar

De privata komponenterna av nycklar som används för DNSSEC ska aldrig lagras på beständigt lagringsmedia i oskyddad form.

A.5.3 Övriga aspekter på nyckelhantering

Publika nyckelsigneringsnycklar (KSK) kan arkiveras under en bestämd tidsperiod av spårbarhetsskäl.

A.5.4 Aktiveringsdata

Aktiveringsdatat som krävs för användning av privata nycklar ska förvaltas av de för systemet utpekade ansvariga systemadministratörerna.

Aktiveringsdatat ska bytas om någon av de utpekade systemadministratörerna lämnar sin anställning eller får andra arbetsuppgifter. Ansvaret för att detta utförs vilar hos närmaste chef.

A.5.5 Säkerhet i datorsystem

Inga bestämmelser.

A.5.6 Nätverkssäkerhet

Signeringssystemet ska logiskt separeras från övriga system och nätverk, och kommunikation mellan dessa logiska sektioner ska styras så att endast nödvändig trafik kan flöda till och från systemet.

A.5.7 Tidsstämpling

Signeringssystemets klocka ska kontinuerligt synkroniseras mot minst tre olika tillförlitliga källor till standardtid spårbar till UTC(SP). Synkroniseringen ska övervakas.

A.5.8 Livscykelhantering

Ny utrustning ska testas under tillräckligt lång tid för att säkerställa dess funktion under en nyckels hela livscykel, innan utrustningen tas i fullt bruk. Uttjänt utrustning som lagrat aktivt okrypterat nyckelmaterial ska förstöras innan deponering för återvinning.

A.6 Zonsignering

A.6.1 Nyckellängder, nyckeltyper och algoritmer

Algoritmer och nyckellängder ska väljas så att dess styrka står i proportion till nycklarnas användningsperiod och signaturernas giltighetstid. För nycklar som ska användas under längre tid än ett år, eller vars signaturer ska vara giltiga under längre tid än ett år, ska RSA med ett modulus av längden 2048 bitar användas.

Nycklar som publicerats i ovanliggande zon ska kunna användas under en längre tid än ett år, varför nyckelsigneringsnyckel (KSK) eller kombinerad signeringsnyckel (CSK) alltid ska ha modulus av längden 2048 bitar.

För nycklar som endast ska kunna användas under en kortare tid än ett år (och vars signaturer således även är giltiga under en kortare tid än ett år), får RSA med ett modulus av längden 1024 bitar användas.

A.6.2 Autentiserade negativa svar

Negativa svar ska autentiseras enligt NSEC3 med 10 iterationer, om inte omständigheterna tydligt talar för något annat.

A.6.3 Signaturformat

Funktionen för framställande av kryptografiskt kondensat som används vid signeringen, ska väljas så att styrkan står i proportion till styrkan hos signeringsnycklarna.

Algoritmen för framställande av kryptografiskt kondensat ska vara SHA-256.

A.6.4 Nyckelbyte

Nycklar som refereras till i ovanliggande zon bytes endast vid misstankar om att nyckeln blivit röjd, om nyckeln förlorats eller om omständigheterna i övrigt föranleder byte av nyckellängd eller algoritm.

Zonsigneringsnycklar som inte refereras till i ovanliggande zon bytes var tredje månad genom automatiskt förfarande.

A.6.5 Signaturlivslängd och frekvens för omsignering

Signaturers livslängd och frekvens för omsignering ska väljas så att den kvarvarande kortaste giltighetstiden alltid överstiger tiden det tar för organisationen att återupprätta driften i enlighet med kontinuitetsplanen.

Det rekommenderas att signaturlivslängderna bestäms till 32 dagar, och att omsignering sker dagligen.

A.6.6 Verifiering av DNS-poster

I de fall zondatat administreras utanför signeringssystemet, så ska överföringen av zondatat autentiseras genom stark kryptografisk metod, till exempel TSIG med HMAC-SHA.

A.6.7 DNS-posters livslängd

Indikeringen för zondatats maximala giltighetstid (*SOA Expire*) ska harmoniseras så att zondata i sekundära namnservrar som inte uppdateras blir ogiltigt innan signaturernas livslängd går ut. Det rekommenderas att *SOA Expire* sätts till 30 dagar (2 592 000 sekunder).

Signaturposternas livslängd (TTL) ska sättas till samma livslängd som den post signaturen täcker, men bör aldrig överstiga 1 timme.

Livslängden för nyckelposter för DNSSEC (DNSKEY) ska sättas till maximalt 1 timme.

Livslängden för autentiserade negativa svar (NSEC3) ska sättas till samma värde som angetts för *SOA Minimum*, men aldrig överstiga 1 timme.

A.7 Revision

A.7.1 Revisionsintervall

Säkerheten kring signeringssystemet bör granskas minst vartannat år, utförd av oberoende intern kontrollfunktion. Revisionens omfattning och avgränsning bör vara de kontroller som föreskrivs i denna DNSSEC-policy. Internrevisionen ska ledas av en revisionsledare med god erfarenhet av IT-revisioner. Denne kan ta teknisk expertis till sin hjälp för att verifiera kontrollernas effektivitet och verkan.

Upptäckta brister och deras allvarlighetsgrad ska rapporteras till ansvarig chef, och en åtgärdsplan ska upprättas. I den mån bristerna är av en sådan karaktär att de utgör en påtagligt förhöjd risk ska dessa avhjälpas skyndsamt. Avhjälpning av övriga typer av brister planeras, införs och följs upp i samråd med inblandade parter.

A.8 Legala frågor

Inga bestämmelser.

B Exempel på tekniska kontroller

Detta kapitel innehåller exempel på tekniska kontroller som kan implementeras för att uppfylla de krav som ställs i kapitel 2.

Det bör noteras att många av de standardprodukter för IP-adresshantering och DNS/DHCP (IPAM/DDI) som finns på marknaden idag kan användas för möta dessa krav.

B.1 Hantera innehåll

- Genom att lagra allt innehåll i ett revisionshanteringssystem (till exempel Subversion [8] eller GIT [2]) uppfylls kraven på spårbarhet och revisionshantering – K1, K2, K3, K4 och K5.
- En central säkerhetslogg (till exempel *syslog [16]*) kan användas för att ytterligare säkra spårbarhet – K1.
- Personlig inloggning med koppling mot central katalog (till exempel *Active Directory*) uppfyller kraven på autentisering – K6, K7, K8 och K9.
- Automatisk indatakontroll vid incheckning av ny/modifierad data skyddar mot publicering av felaktigt formaterat data – K10.
- Revisionshanteringssystemets behörighetskontroller kan användas för att uppfylla kravet på differentierade användarbehörigheter – K11.

B.2 Signera och publicera

- ZKT [10] och OpenDNSSEC [7] stödjer samtliga SKALL-krav vad gäller nyckelhantering – K14, K16 och K17.
- Lagring av nyckelmaterial på krypterat filsystem (till exempel *TrueCrypt*, *Linux LVM*, *Microsoft Bitlocker*) skyddar mot insyn och förändring när systemet inte är drift – K19.
- OpenDNSSEC [7] stödjer kraven på lagring av nycklar i separat säkerhetsmodul – K18 och K20.
- ZKT [10] och OpenDNSSEC [7] stödjer samtliga SKALL-krav vad gäller signering – K21, K22, K24, K25, K29, K30 och K31.
- BIND [1] har grundläggande stöd för kombinerade signeringsnycklar (CSK) – K15.
- OpenDNSSEC [7] och BIND [1] stödjer flera samtidiga signeringsalgoritmer – K26.

B.3 Distribuera

- BIND [1] och NSD [4] stödjer skydd av zonöverföringar med hjälp av TSIG/HMAC-SHA256 – K32, K33 och K34.
- Åtkomstkontroll för zonöverföring behöver inte ske baserat på IP-adress – det skydd som TSIG ger är tillräckligt och eliminerar dessutom behovet av att distributionssystemet behöver känna till vilka IP-adresser som skall ges åtkomst till zondata.

B.4 Validera

- BIND [1] och Unbound [9] stödjer samtliga krav på validering – K35, K36, K37, K38, K39, K40, K41 och K42.

B.5 Övervaka

- Lämpliga insticksmoduler till till exempel NAGIOS [3] kan användas för att möta kraven på övervakning – K43, K44, K45, K46 och K47.

Referenser

[1] BIND. URL: https://www.isc.org/software/bind/.

[2] GIT. URL: http://git-scm.com.

[3] NAGIOS. URL: http://www.nagios.org.

[4] NSD. URL: http://www.nlnetlabs.nl/projects/nsd/.

[5] NTP via Netnod. URL: http://www.netnod.se/other/valueadd/ntp.

[6] NTP via SP. URL: http://www.sp.se/en/index/services/time_sync/ntp/sidor/default.aspx.

[7] OpenDNSSEC. URL: http://www.opendnssec.org/.

[8] Subversion. URL: http://subversion.tigris.org.

[9] Unbound. URL: http://www.unbound.net/.

[10] ZKT. URL: http://www.hznet.de/dns/zkt/.

[11] D. Eastlake 3rd. RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS). RFC 3110 (Proposed Standard), May 2001. URL: http://www.ietf.org/rfc/rfc3110.txt.

[12] D. Eastlake 3rd. HMAC SHA (Hashed Message Authentication Code, Secure Hash Algorithm) TSIG Algorithm Identifiers. RFC 4635 (Proposed Standard), August 2006. URL: http://www.ietf.org/rfc/rfc4635.txt.

[13] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. DNS Security Introduction and Requirements. RFC 4033 (Proposed Standard), March 2005. Updated by RFC 6014. URL: http://www.ietf.org/rfc/rfc4033.txt.

[14] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. Protocol Modifications for the DNS Security Extensions. RFC 4035 (Proposed Standard), March 2005. Updated by RFCs 4470, 6014. URL: http://www.ietf.org/rfc/rfc4035.txt.

[15] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. Resource Records for the DNS Security Extensions. RFC 4034 (Proposed Standard), March 2005. Updated by RFCs 4470, 6014. URL: http://www.ietf.org/rfc/rfc4034.txt.

[16] R. Gerhards. The Syslog Protocol. RFC 5424 (Proposed Standard), March 2009. URL: http://www.ietf.org/rfc/rfc5424.txt.

[17] W. Hardaker. Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs). RFC 4509 (Proposed Standard), May 2006. URL: http://www.ietf.org/rfc/rfc4509.txt.

[18] P. Hoffman and W.C.A. Wijngaards. Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC. RFC 6605 (Proposed Standard), April 2012. URL: http://www.ietf.org/rfc/rfc6605.txt.

[19] J. Jansen. Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC. RFC 5702 (Proposed Standard), October 2009. URL: http://www.ietf.org/rfc/rfc5702.txt.

[20] O. Kolkman, W. Mekking, and R. Gieben. DNSSEC Operational Practices, Version 2. RFC 6781 (Informational), December 2012. URL: http://www.ietf.org/rfc/rfc6781.txt.

[21] B. Laurie, G. Sisson, R. Arends, and D. Blacka. DNS Security (DNSSEC) Hashed Authenticated Denial of Existence. RFC 5155 (Proposed Standard), March 2008. URL: http://www.ietf.org/rfc/rfc5155.txt.

[22] F. Ljunggren, AM. Eklund Lowinder, and T. Okubo. A Framework for DNSSEC Policies and DNSSEC Practice Statements. RFC 6841 (Informational), January 2013. URL: http://www.ietf.org/rfc/rfc6841.txt.

[23] RSA Security, Inc. *PKCS #11: Cryptographic Token Interface Standard*, June 2009. Version 2.30.

[24] M. StJohns. Automated Updates of DNS Security (DNSSEC) Trust Anchors. RFC 5011 (INTERNET STANDARD), September 2007. URL: http://www.ietf.org/rfc/rfc5011.txt.

[25] P. Vixie, O. Gudmundsson, D. Eastlake 3rd, and B. Wellington. Secret Key Transaction Authentication for DNS (TSIG). RFC 2845 (Proposed Standard), May 2000. Updated by RFCs 3645, 4635. URL: http://www.ietf.org/rfc/rfc2845.txt.