DNS OCH DNSSEC UTAN FACKSNACK

När du skriver en adress som www.sunet.se i webbläsarens URL-ruta är den fullständigt obegriplig för läsaren. Webbläsaren har ingen aning om vad den ska göra av den, så den behöver hjälp utifrån. Den ber en namnserver på Internet att reda ut eländet. Namnservern är snäll (eller elak) och lämnar tillbaka en IP-adress (eller en falsk piratadress) som webbläsaren förstår och kan använda att navigera på Internet med. Då kan webbläsaren hämta just den sida som du vill ha (eller någon annan lurat den att visa). Här får du reda på hur det går till och hur du kan skydda dig mot piraterna.

Internet är en helt platt organisation. Alla servrar och tjänster är lika nåbara oavsett var i världen man ansluter till Internet. Men för att veta vart man ska, behövs en adressbok. Den finns och kallas DNS, som betyder Domain Name System. Adressboken bygger på frivillighet. Man behöver inte lägga in sin adress i DNS men det är lämpligt att man gör det, om man vill bli hittad.

DNS är det hierarkiska och redundanta system av servrar som förser all världens kommunikationsprogram med adresser till de internetbaserade tjänster de är ute efter, såsom webbservrar, mailservrar osv. Alla som vill kunna navigera på Internet måste använda DNS.

Eftersom DNS kan störas av cyberbrottslingar och tvinga dina applikationer till fel ställen, finns ett tillägg till DNS som heter DNSSEC (Domain Name System Security Extensions). Det är ett system som utökar DNS med förbättrad säkerhet. DNS finns ändå kvar. Det har bara blivit bättre.

Internet är demokratiskt och det finns inget tvång att använda DNSSEC. Metoden är robust och omöjlig att lura och alla borde utnyttja den, särskilt samhällsviktiga funktioner, men tyvärr är uppslutningen ännu katastrofalt låg.

ADRESSERA MIG HIT OCH ADRESSERA MIG DIT

Alla fysiska adresser på Internet är konstruerade enligt modellerna IPv4 eller IPv6. Adresserna består av långa sifferserier som det är omöjligt att memorera. Människan gillar å andra sidan att sätta namn på saker, som Aftonbladet, Google eller Sunet och gärna i någon form av hierarki.

Det är lätt för oss att minnas namn och därför har man skapat DNS-tjänsten som omvandlar namn till fysiska IP-adresser. Samtidigt kan tjänstägarna få för sig att byta adresser och hitta på nya. Sådant sker stup i ett och skulle man försöka att själv hålla en lista på fysiska adresser vore den omodern ganska snart. Då är det bättre att lita på DNS-tjänsten.

Frågar du till exempel DNS efter **www.sunet.se** eller **www.rubidium.se** får du adresserna 192.36.171.231 respektive 176.10.207.183 om du använder IPv4 (sk A-record) eller 2001:6b0:8:2::232 respektive 2001:470:28:759::12 om du använder IPv6 (sk AAAA-record). Låt helst bli att försöka minnas dem.

Eftersom Internet har blivit som en andra värld som många i praktiken ”lever i” förstår man hur viktig DNS är för oss i vardagen. Då förstår man också hur viktigt det är att DNS inte ska kunna störas eller förfalskas.

ORGANISATIONEN BAKOM

Man får inte hitta på namn och adresser på Internet hur som helst, utan namngivningen måste standardiseras och regleras hårt. Internet Corporation for Assigned Names and Numbers (ICANN) är den organisation som håller i det övergripande ansvaret för namn och nummer på Internet och ser till att systemet är rimligt. Detta inkluderar de sk rotservrarna (root servers), vilka toppdomäner som finns och vilka dessa är utdelade till.

TOPPDOMÄNERNA

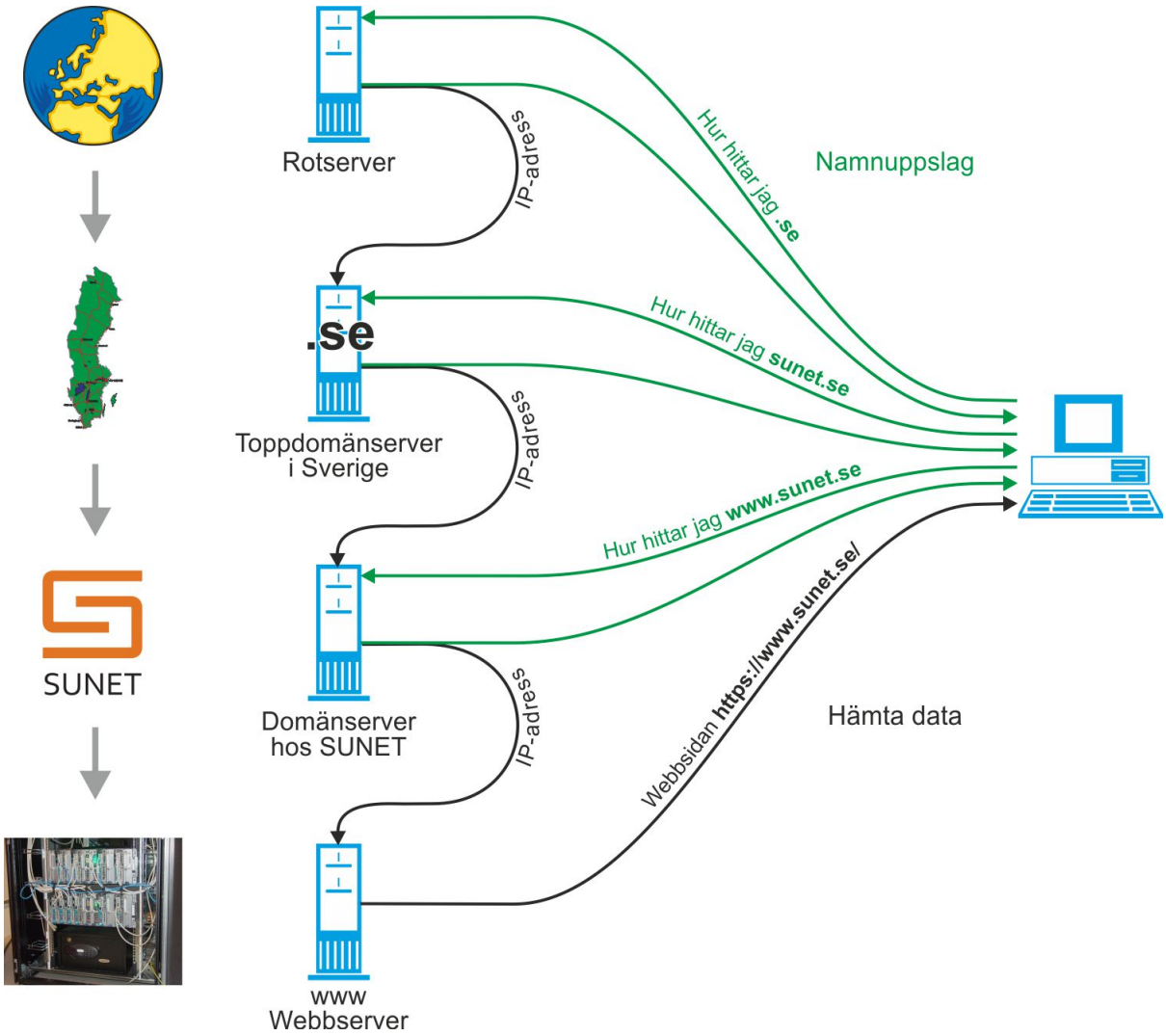
Toppdomänerna är namn på länder eller vissa övergripande klasser av organisationer. På engelska kallas detta för TLD: Top Level Domain. Typiska sådana är **.se**, **.au** och **.be**, men också **.gov**, **.org** och **.edu**, samt **.museum**, **.info** och **.travel** och intressant nog även vissa kommersiella varumärken och **.stockholm**. ICANN bestämmer exakt vilka toppdomäner som ska få finnas genom rimlighetskontroll enligt sitt regelverk och exakt vem som har rätt att peka ut adresserna till servrarna med information om dessa.

Listan med toppdomäner lagras i en mängd redundanta rotservrar världen över i en form av distribuerad molntjänst. Alla rotservrar är exakt likadana, håller exakt samma information och kan ersätta varandra. Det finns många av dem för att det inte ska spela någon roll om några går sönder, och för att man ska kunna sprida lasten över dem.

Det är bara ICANN som får lägga in information i rotservrarna och ICANN garanterar att informationen är riktig.

DNS I KORTHET

En namnfråga till DNS kallas för ett **namnuppslag**. Alla namnuppslag går till på samma sätt. Antag att du ska ha tag i servern **www.sunet.se**. Grovt förenklat fungerar det så här. Ett uppslag börjar alltid i trädets rot.



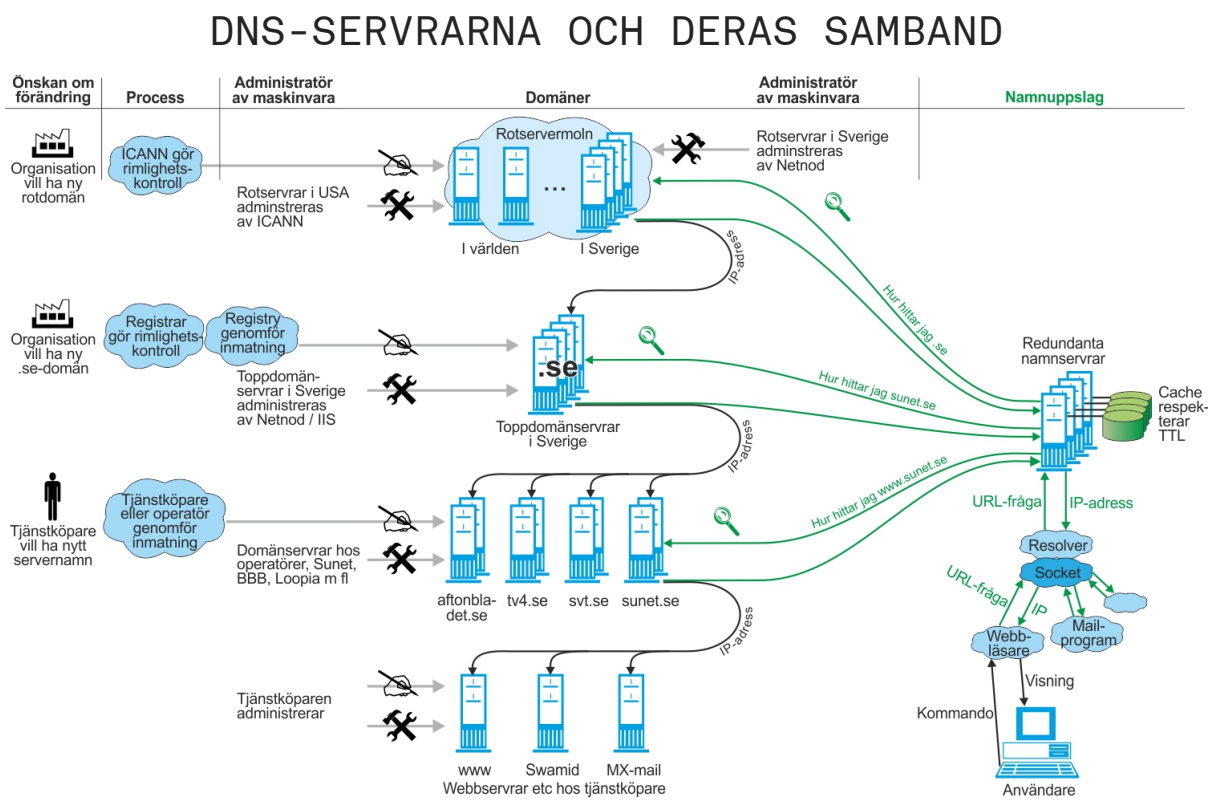
1. Datorn börjar med att fråga servern på världsnivå (roten) var **.se** kan finnas. Världsservern pekar ut Sverige.
2. Datorn frågar servern på landsnivå (toppdomänen) var **sunet.se** kan finnas. Sverigeservern pekar ut SUNETs server.
3. Datorn frågar SUNETs server (domänen) var webbservern med namnet ”**www**” kan finnas. SUNETs server ger dig slutligen IP-adressen till **www.sunet.se**.

Dessa tre steg genomlöps alltid, men det går så fort att du inte märker det. Ett namnuppslag tar mellan 0,1 och 0,25 sekunder beroende på vilken operatör man är ansluten till och vilken plats man befinner sig på.

Men du är inte ensam i landet om att vilja komma åt **www.sunet.se** så din bästa kompis på Internet, namnservern har redan gjort det där namnuppslaget tidigare, och har lagrat svaret åt dig i sin cache.

1. Sanningen är att din dator helst frågar operatörens namnserver om namnuppslaget och får tillbaka IP-adressen mycket fortare än om din egen dator skulle ha behövt fråga sig igenom hela trädstrukturen av servrar.
2. Skulle namnservern inte ha lagrat namnuppslaget i sin cache, är det namnservern som går ut och frågar sig igenom trädstrukturen, så du slipper.

Det är dessutom en massa extra krångligheter med att fråga sig igenom DNS-trädet. Det är vad den här artikeln ska handla om.



Servrarnas namn och innehåll och processerna vid namnuppslag

Det finns många rotservrar världen över, alla med kända adresser. En av de 12 organisationer som jobbar med rotservrar råkar finnas i Sverige, nämligen Netnod och deras servrar har alla IP-adressen 192.36.148.17 (IPv4) eller 2001:7fe::53 (IPv6). Alla rotservrars IP-adresser finns i en publikt tillgänglig lista som alla namnservrar redan har. Naturligtvis har inte alla fysiska maskiner enbart samma IP-adress, för det skulle inte fungera, utan man använder sig av metoden ”anycast” för att representera flera fysiska maskiner med geografisk spridning med en enda adress.

Rotservrarna pekar ut land – toppdomäner

Rotservrarna innehåller en lista med alla toppdomäner och uppgifter om vilka servrar som svarar för alla toppdomäner. Det är bara ICANN som får lägga in information i rotservrarna.

Namnservern väljer en toppdomänserver. Det finns flera sådana, som alla är lika och svarar samma sak på en fråga.

Toppdomänservrarna pekar ut organisationer – domäner

Toppdomänservrarna pekar ut enskilda svenska operatörers domänservrar, varav SUNET är en, KTH, SU, Chalmers, Telia, Tele2, Bredbandsbolaget, Bahnhof, IP-Only med flera, är andra.

Informationen i en toppdomänserver får bara ändras av en sk registrar, som är en organisation som säljer domännamn på kommersiell basis. Toppdomänservrarna i Sverige sköts av Netnod åt IIS (Internetstiftelsen).

Vill man köpa rätten till en .se-domän går man till en sådan registrar. Denne skickar frågan vidare till ett sk registry, en funktion som undersöker om domännamnet är ledigt och uppfyller vissa andra krav. Detta är idag en helt automatiserad process som bara tar ett par minuter.

Domänservrarna pekar ut faktiska tjänster

Varje operatör, högskola, internetleverantör osv har domänservrar som övervakas, uppdateras och hanteras av operatörerna själva. Det finns tusen och åter tusen domänservrar. Det är regel att dessa servrar är dubblerade för att få robusthet.

Domänservrarna pekar ut alla tjänster i operatörens nät, som webbservrar, mailservrar, servrar för strömmande video, identiteter osv.

Dessutom finns fristående leverantörer som specialiserat sig på att agera domänserver, att leverera domäntjänster. Det kan vara både bra och dåligt, särskilt om man bara använder sig av en enda leverantör och leverantören befinner sig långt bort och blir störd. Genom att köpa flera domäntjänster kan man öka sin redundans som organisation, men genom att bara ha en enda kan man råka minska sin redundans på ett farligt sätt.

Det är operatörerna som har allt ansvar för sina egna domänservrar och får lägga till och ändra informationen efter behag.

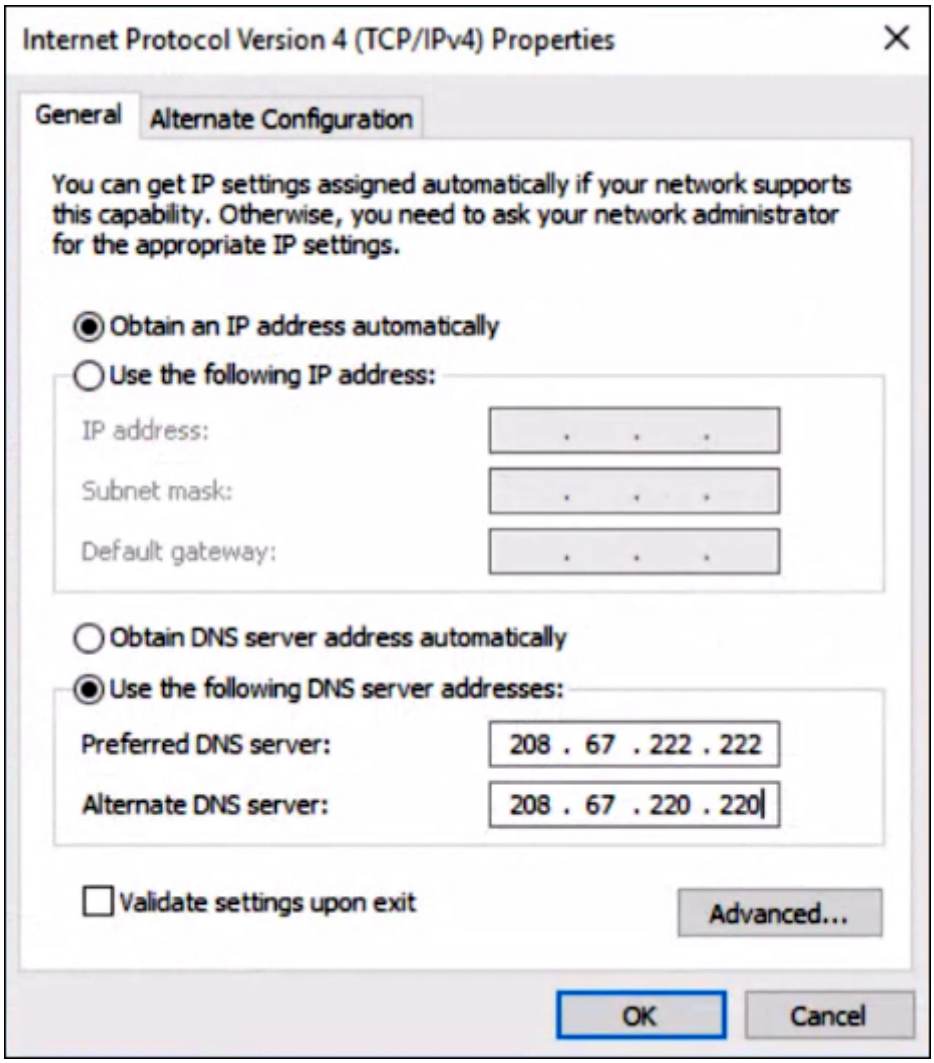
INTE WEBBLÄSARENS SAK

Webbläsaren är bara en av många funktioner i en dator som behöver göra namnuppslag. Andra kan vara olika kommunikationsprogram, telnet, e-posthanterare etc. Alla dessa frågar en gemensam funktion i operativsystemet, ett gränssnitt som kallas för **socket**, som samlar ihop sådana förfrågningar och skickar dem till en **resolver** (en upplösare). Det är resolvern som vet var den kan hitta första bästa namnserver och skickar namnuppslaget dit. När uppslaget resulterat i en slutlig IP-adress, får webbläsaren eller vem det nu kan vara som frågade, tillbaka den slutliga, upplösta IP-adressen från socket.

Uppgiften om adressen till namnservern får resolvern när datorn startas, i samma förfrågan som görs till operatören för att få IP-adressen till datorn, DHCP-uppslaget.

Så här ser det ut i Windows 10 (före Creators Update) när man gör följande steg:

1. Högerklicka på **Startmenyn**.
2. Välj **Nätverksanslutningar**.
3. Högerklicka på den nätverksanslutning du använder (ex. **Ethernet**).
4. Välj **Egenskaper**.
5. Välj **Internet Protocol Version 4 (TCP/IPv4)**.
6. Välj **Egenskaper**.



Normalt ska båda inställningarna stå på ”automaically”, men för förklaringens skull visas en manuellt angiven adress. Överst anges att datorn ska skaffa sig en IP-adress automatiskt från internetleverantören eftersom det är standardläget, såvida du inte erhållit en fast IP-adress.

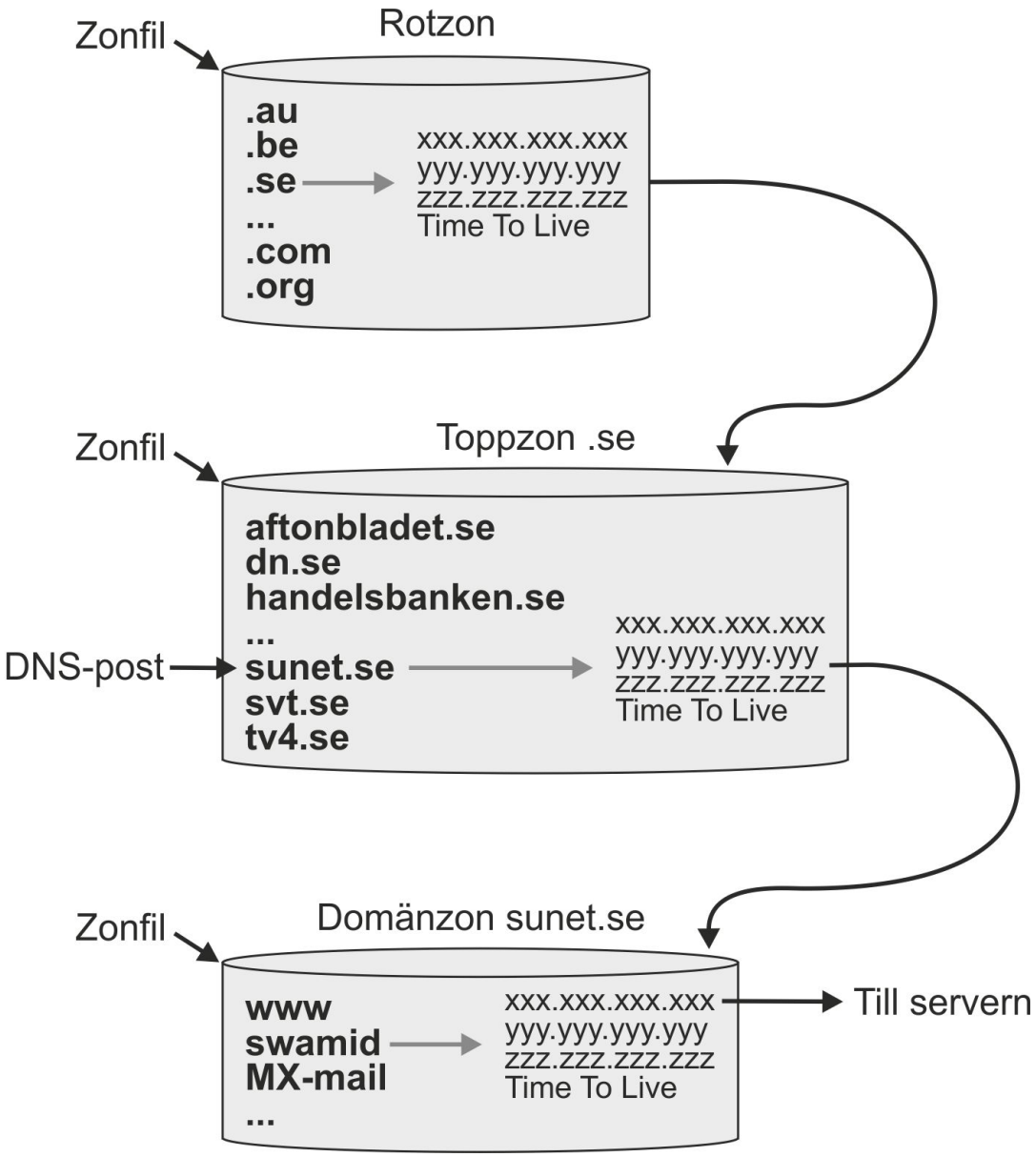
Längst ned har två öppet tillgängliga DNS-servrar angivits. Egentligen är terminologin fel. Man väljer inte en DNS-server utan en namnserver, men namnservrarna finns ofta i anslutning till DNS-servrarna. Adresserna hänvisar till två servrar i det globala nätet OpenDNS. Din internetleverantör kan ge dig andra adresser eller rekommendera helautomatiskt läge. Andra, som Google, har servrar som de uttalat erbjuder vem som helst att använda. Detta är ett exempel.

VAR FINNS NAMNSERVERN?

Namnservrarna kan finnas jämte DNS-servrarna, men kan också finnas på andra ställen, till exempel hos internetleverantörerna, större företag osv. Googles publika namnserver har adressen (8.8.8.8). Detta för att få spridning och redundans.

Den enskilde skulle också kunna ha sin egen namnserver, men det blir väldigt ineffektivt för då måste man fråga alla DNS-servrar för varje sökning man gör. Det kan emellertid vara lämpligt att ha sin egen namnserver i olika högsäkerhetssammanhang, för att hålla koll på förgiftningar, manipulation mm. Det finns öppen källkodsprogram för detta.

HUR GÅR DET TILL ATT SLÅ UPP EN ADRESS?



När namnservern ska ha tag i en adress i **.se** frågar den en av rotservrarna om IP-adressen till en server med information om toppdomänservern för **.se**. Svaret finns i rotserverns zonfil, som sägs omfatta **rotzonen**. Svaret är en post i zonfilen, en uppsättning med IP-adresser och ett livslängdsvärde för uppgifterna i listan, ett Time To Live (TTL). **Zonen** är bara ett annat namn på alla poster i zonfilen, listan som innehåller alla DNS-poster i domänservern.

Man väljer en adress i listan, likgiltigt vilken eftersom alla toppdomänservarna har identiskt innehåll, och uppsöker denna. Samtidigt lagras adressen i namnserverns cache och får bli kvar där så länge som livslängdsvärdet TTL anger.

Kommen till toppdomänservern frågar man efter IP-adressen till en server med information om domänen **sunet.se** och får åter en lista med IP-adresser att välja bland, samt en TTL.

Kommen till domänservern hos SUNET frågar man efter IP-adressen till **www.sunet.se** och får IP-adressen till webbservern **www** och får en IP-adress och en TTL.

Alla dessa adresser hamnar i cachen hos namnserven som har frågat och sparas så länge TTL gäller.

Denna sista IP-adress till www.sunet.se lämnas ut till resolvern i den dator som gjorde förfrågan, som lämnar den vidare till webbläsaren.

Men varför måste man börja fråga från rotservern hela tiden? Vi vet ju att vi är i Sverige. Man skulle kunna börja fråga toppdomänen och spara tid, men datorn eller namnservern vet inte var i världen den är och måste använda sig av en överenskommen metod att fråga. Visst skulle man kunna hålla en tabell med uppgifter om exakt var varje dator befinner sig, men då måste man underhålla den tabellen. Genom att alltid börja med att fråga rotservern slipper man underhålla en extra tabell.

TIME TO LIVE

TTL är ett bäst-före-datum som alltid följer med ett namnuppslag för att signalera för cachen som IP-adressen hamnat i, hur länge adressen får vara kvar där innan den blivit ogiltig. Har uppgiften legat kvar längre än TTL duger den inte som uppgift åt en som frågar, utan namnservern måste fråga domänservern igen.

Servrars IP-adresser ändras hela tiden, för operatörer kommer och går, får nya adresser, byter servrar osv. Men om IP-adressen inte hade en minsta liggetid i cachen vore det ingen cache. Genom att sätta en lagom kort TTL kommer en adressändring att slå igenom när liggetiden tagit slut. Väljer man en för lång TTL blir det trögt att införa nya uppgifter i domänservrarna. Väljer man en för kort liggetid görs cachen snabbt obrukbar och antalet förfrågningar mot domänservrarna börjar öka. Därför brukar man dra ned TTL på domänen inför en planerad förändring och får acceptera den ökade mängden förfrågningar.

Typisk TTL är en timme, 3600 sekunder. Mängden förfrågningar till .se-domänen kan trots detta räknas i flera tiotusental per sekund.

MÅSTE ALLA ORGANISATIONER HA SIN EGEN DOMÄNSERVER?

Alla organisationer behöver inte ha en egen domänserver. Det är en tjänst man kan köpa från andra. Det finns företag som enbart jobbar med DNS som registrar och tillhandahåller DNS-servrar för sina kunder. Bland dessa kan man nämna **dyn.com** och **frobbit.se**. Det finns de som har detta som en del av ett större erbjudande, t ex webbhotell som **loopia.se**.

Beroende på behov bör man välja DNS-leverantör med mer eller mindre omsorg. Är man väldigt mån om robusthet för sin tjänst bör man lägga mer tid på sitt val av DNS-tjänstleverantör så att det finns robusthet och redundans, något som blivit uppmärksammat som problem under senaste året, men knappast varit ett okänt problem innan dess.

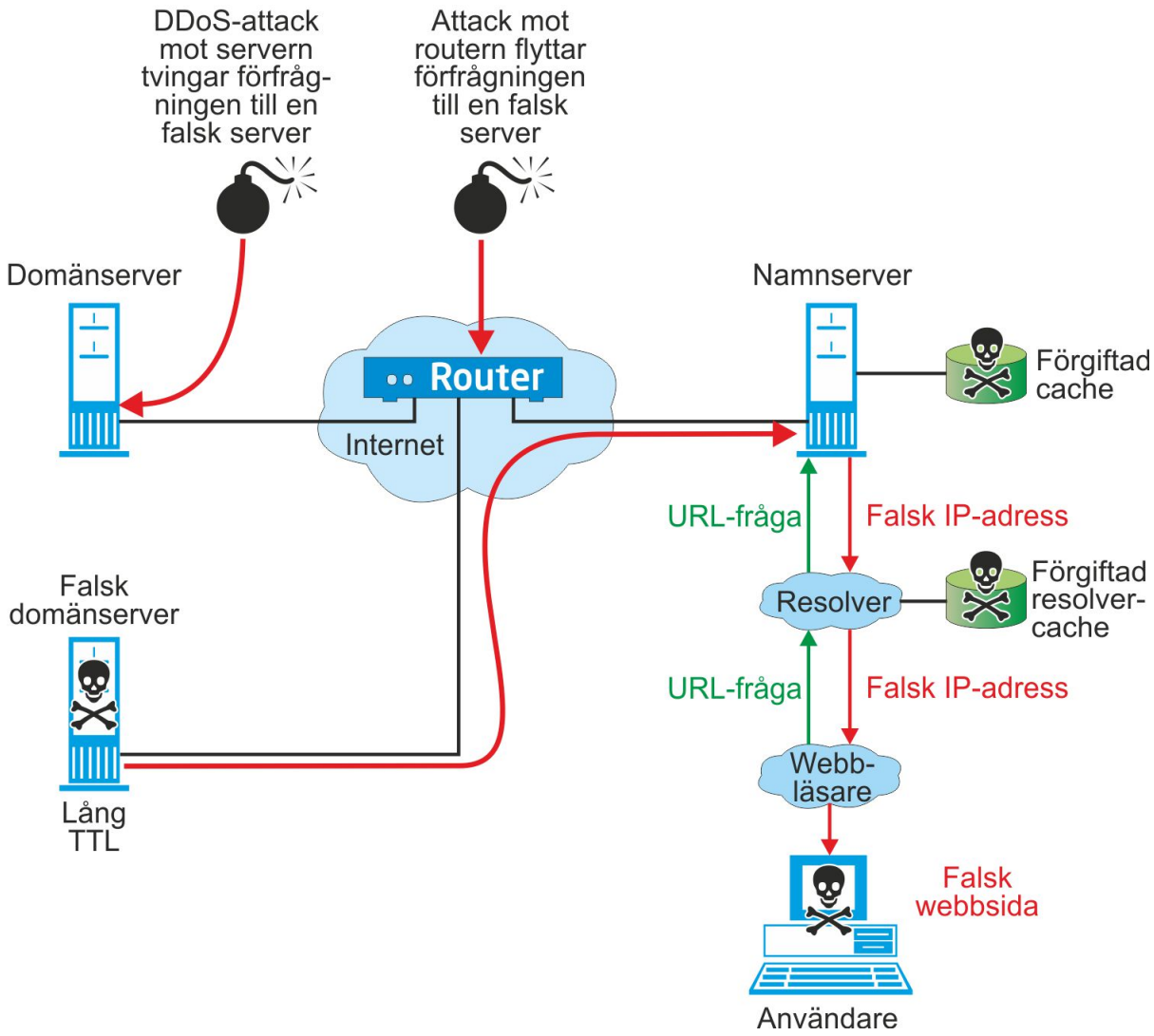
HAR SUNET EN?

SUNET har två egna DNS-servrar, och dessutom två andra hos KTH och NORDUnet. Detta är ett gott exempel på hur man sprider riskerna genom att ha flera servrar som kan leverera samma svar. Vid uppdatering så informerar huvudservern (master) de andra servarna (sekundärer) om uppdatering och dessa hämtar den uppdaterade zonfilen som innehåller den kompletta uppsättningen med svar för hela domänen.

HUR KAN MAN STÖRA DNS

DNS är en väldigt enkel tjänst i sin grund. Man skickar förfrågan till en server och får ett svar, sen tror man på det svaret och frågar nästa server och tror på svaret från denna, hela kedjan ned. Vi känner alltså ett förtroende för att vi får korrekta svar från de korrekta servrarna i en kedja. Detta blir ett kedjeberoende av förtroende, **chain of trust**.

Så som dagens Internet är utformat medger det för många spelare att sabotera på ett eller annat sätt. Det inkluderar allt från script-kiddes, cracker-communities som t ex Anonymous, utpressarligor som agerar för ekonomisk vinning och stater som testar sina muskler mot en annan stats infrastruktur och dess förmåga att motstå det.



Trots DNS viktiga roll inom användandet av IP-nätverk finns ett par sårbarheter. Detta beror främst på DNS öppna, distribuerade konstruktion och användningen av det osäkra UDP-protokollet.

Eftersom alla förfrågningar på Internet går genom routrar kan man attackera en router och få den att koppla DNS-frågor till en falsk domänserver.

Alternativt kan man överbelasta en domänserver eller attackera den på andra sätt, så att den avvisar ytterligare förfrågningar och på så sätt tvingar frågorna till en falsk server.

Den falska servern levererar DNS-information som hamnar i namnserverns cache. **Cachen har blivit förgiftad**. När en resolver frågar namnservern om information, hamnar den falska informationen i resolverns cache. **Resolvern har också blivit förgiftad**.

Förfalskaren sätter gärna väldigt lång TTL på sin information för att den ska stanna i den förgiftade cachen länge, och bli kvar där även om själva angreppet upptäcks och avbryts.

Den falska sidan som till sist hämtas, kan exempelvis leverera falska nyheter eller bara lagra användarens inloggningsdata för att kunna använda det senare.

Det förtroende man har haft är då brutet, men det finns inget sätt att verifiera om man har korrekt information, utan man tror fortfarande blint på den information som lämnats.

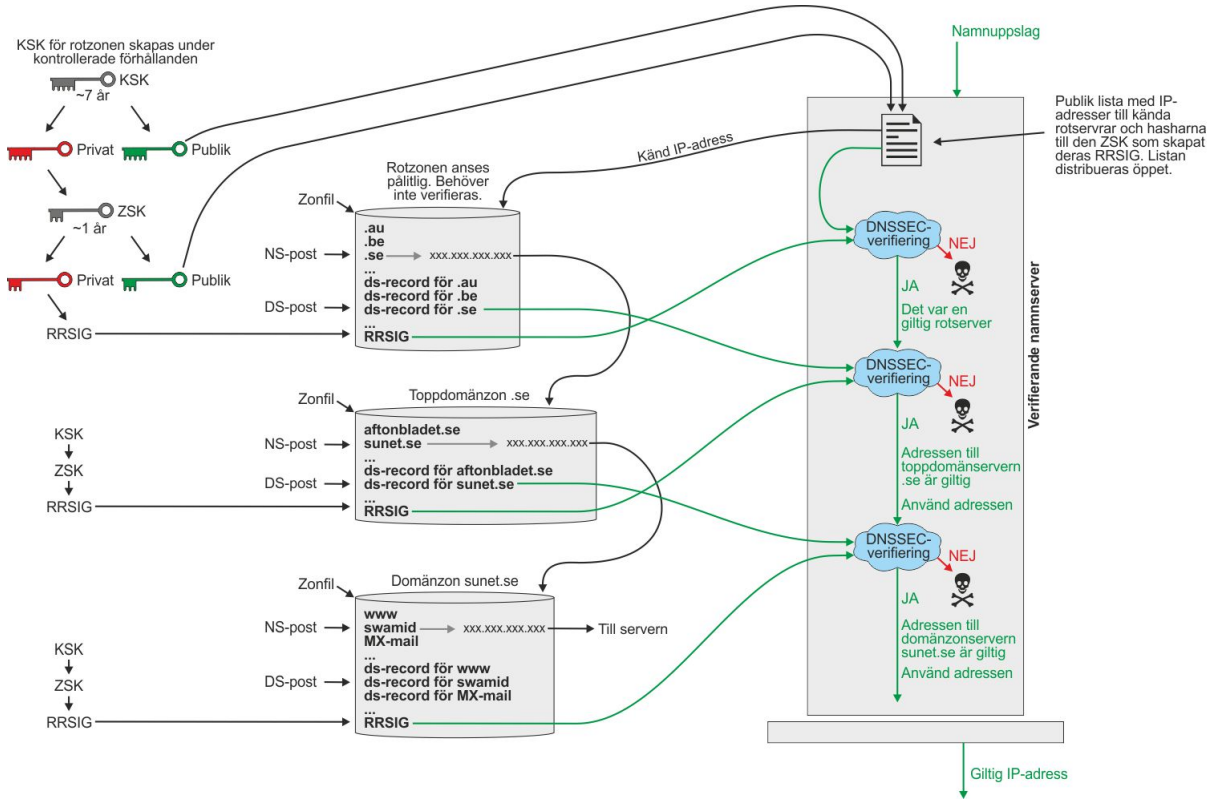
SE UPP! Säg inte DNS-förgiftning (DNS poisoning) för det är inte DNS-tjänsten som sådan som förgiftats. Det är din cache som förgiftats.

DNSSEC

DNSSEC betyder Domain Name System Security Extensions (DNSSEC), helt enkelt ett system som utökar DNS med förbättrad säkerhet. Ingen maskinvara i den befintliga DNS-systemet behöver ändras. Det är bara informationen i zonfilerna som utökas.

DNSSEC är inte kryptering utan ett sätt att säkra att informationen i DNS inte är falsk. Genom att använda sig av de nycklar som finns i zonfilernas utökade poster kan man verifiera att den information man fått är sann och kommer från rätt server. Det görs med en verifikationsprocess i namnservern som resulterar i en autentisering.

Man behöver inte använda DNSSEC. En DNS-server med DNSSEC tillåter dig att fråga om namn på precis samma sätt som innan DNSSEC, men du får ett osäkert svar.



Bilden visar bara verifikationsprocessen. Namnuppslaget görs på samma sätt som tidigare, men bara om man få JA på alla frågor. Se ovan.

Zonfilen har utökats med (bland annat) två nya posttyper: **DS-posterna** och **RRSIG** (Resource Record Set Signature).

DS-posten innehåller en kryptografisk hash med vilken man kan verifiera nyckeln RRSIG som hämtas från nästa domänserver längre ned i kedjan, den vars IP-adress som pekas ut av NS-posten. Det finns en DS-post för varje NS-post, eftersom varje NS-post pekar ut en ny domänserver och varje påföljande domänserver måste kunna autentiseras.

Hashen är en förkortad version av en riktig kryptonyckel, som används av praktiska skäl. Den är inte ”sämre”, bara kortare.

1. Låt oss anta att vi litar på rotservern, för den är garanterad av IANA och dess adress är känd i förväg.
2. Frågar man den om **.se** får man IP-adressen (NS-posten) till en svensk toppdomänserver. Man får också information för att verifiera sagda toppdomänserver (DS-posten). Dessa uppgifter är alltså redan betrodda.
3. Man frågar toppdomänservern för **.se** om IP-adressen till **sunet.se**. Som svar får man en IP-adress till SUNETs domänserver och toppdomänserverns RRSIG.
4. Genom att autentisera toppdomänserverns RRSIG mot DS-posten från rotservern kan vi veta att toppdomänservern var betrodd att svara på frågan om adressen till **sunet.se**. Sålunda kan vi lita på toppdomänserverns svar.
5. Man frågar domänservern för **sunet.se** om IP-adressen till **www.sunet.se**. Som svar får man en IP-adress till SUNETs webbserver och domänserverns RRSIG.
6. Genom att autentisera domänserverns RRSIG mot DS-posten från toppdomänservern kan man veta att domänservern var betrodd att svara på frågan om adressen till **www.sunet.se**. På så sätt kan man lita på svaret.

Sålunda har en kedja av betrodda servrar byggts upp från roten till den slutliga servern. Det är vår förtroendekedja, chain of trust.

Får man i något steg ett NEJ kan det ha flera orsaker, som att RRSIG saknas eller någon skickat in falsk information. En ansvarskännande användare bör stanna där.

KSK OCH ZSK OCH FÖRTROENDET FÖR ROTZONEN

Antag att man inte litar på rotservern. Hur verifierar man att rotservern är den rätta, dvs att den lämnar en riktig RRSIG, när den inte har någon överliggande server att ta en DS-post ifrån?

Hashen för den publika delen av den nyckel som användes för att generera RRSIG för rotservern är känd och kan användas för att autentisera rotservern. RRSIG är generad ur ZSK för rotzonen, som i sin tur är genererad ur KSK för rotzonen. Det enda i denna värld vi obetingat måste lita på är KSK för rotzonen. Det är därför den är skyddad av så omfattande säkerhetsprocedurer vid genereringen.

Varje namnserver har redan en publik lista med alla **IP-adresser till kända rotservrar** och en lista med **hashar till** deras RRSIG, som skapats ur **ZSK för rotzonen**. Eftersom KSK är betrodd är även ZSK betrodd och därmed även den RRSIG som skapats ur den.

Genom att utföra ytterligare en DNSSEC Verify-process mellan rotserverns RRSIG och den kända hashen för ZSK för rotzonen kan man autentisera rotservern. Detta bör utföras vid varje namnuppslag.

ATT SIGNERA ROTZONEN

Den kryptografiska kedjan börjar med att man skapar en nyckel som signerar rotzonen, en sk Key Signing Key (KSK). Den är mycket betydelsefull eftersom den är kärnan till all säkerhet i hela DNSSEC-systemet. Den är ingalunda offentlig utan förvaras bakom lås och bom hos IANA (Internet Assigned Numbers Authority).

KSK är lång och tar lång tid att verifiera. För att snabba på verifikationen använder man en kortare nyckel, med kortare livslängd. Denna kallas för Zone Signing Key (ZSK) och har en livslängd på cirka ett år.

Både KSK och ZSK är asymmetriska nyckelpar, som har en privat och en offentlig del.

- Med den privata delen av KSK skapar man en signatur som används för att generera en ZSK.
- Med den privata delen av ZSK skapar man en signatur som används för att generera en RRSIG.

Med ”generera” avses den kryptografiska processen att skapa en ny nyckel och den processen behöver ett startvärde, till vilket man använder signaturen. (Man hade kunnat välja ”nisse” men väljer istället ”8756a28746837298b5743e97562f58075895c680d29”).

- Den publika delen av KSK lagras i DNS-servern och används för att autentisera ZSK.
- Den publika delen av ZSK lagras i DNS-servern och används för att autentisera RRSIG.

Kan man läsa ut RRSIG ur en rotserver och verifiera den mot den publika delen av ZSK-nyckeln som finns i den publika listan vet man att man träffat på en giltig rotserver.

- Varje domänoperatör får generera sin egen KSK, ZSK och RRSIG och gömma den privata delen och lagra den publika delen på sin egen domänserver. Det är upp till operatören att se till att dennes RRSIG faktiskt stämmer med DS-posten i överliggande domänserver genom att rapportera ändringar uppåt till överliggande server.
- Så fort en ny domän tillkommer måste RRSIG genereras om, vilket ger som resultat att även den DS-post som pekar ut denna domänserver måste genereras om.

DEN SVENSKA NYCKELPIGAN

När vi nu sätter vår tilltro till en KSK för rotzonen (hela Internet), hur skapas detta förtroende? Det sker genom en nyckel-skapar-cermoni där ett antal betrodda personer är med när den nya KSK-nyckeln skapas och verifieras. Ceremonin direktsänds som strömmande video.

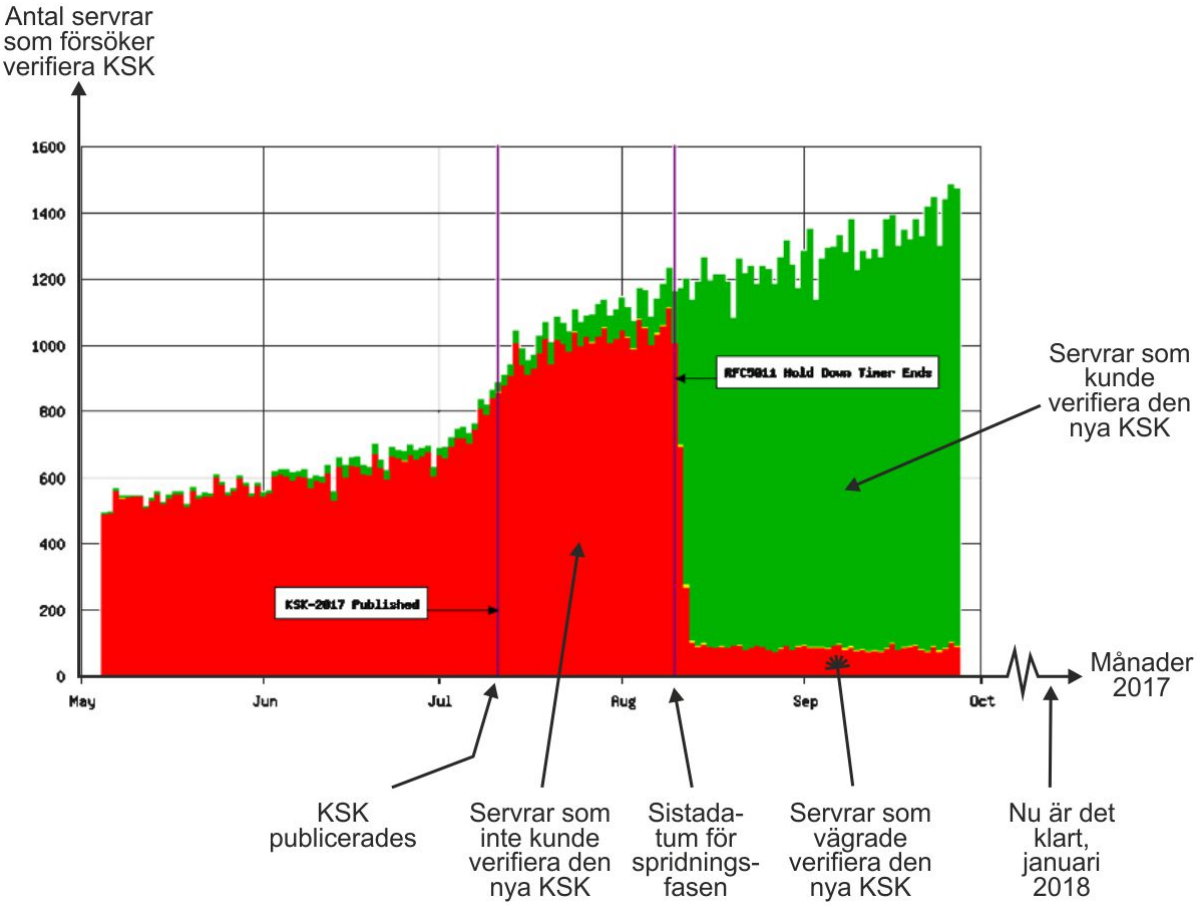
En av dessa personer är svenska Anne-Marie Eklund Löwinder som jobbar på Internetstiftelsen i Sverige. Hon kallas ibland för ”den svenska nyckelpigan” då hon utöver att vara en betrodd person även bär på sin lilla del av den fysiska nyckel som används vid ceremonierna.

NYCKELUTRULLNING – KEY SIGNING KEY ROLLOVER

Den översta KSK har en livslängd på sju år, medan den ZSK man genererar ur denna endast har en livslängd på ett år. 2017 var det dags att skapa en ny KSK. Det hade aldrig provats förut, men tidsschemat var helt klart och publicerades av IANA i maj 2016.

Så snart en ny KSK skapas, skapar man också en ny RRSIG för alla rotservrar. Om DNS-operatörerna och internetleverantörerna inte klarar av att hämta den publika delen av KSK, eller egentligen ZSK som skapas ur KSK, kan de inte verifiera RRSIG för rotservrarna och då blir rotzonen opålitlig.

Drygt ett år senare, i juli 2017, publicerades den publika delen av nya nyckeln i alla rotservrar så att alla skulle kunna verifiera den nya KSK, den sk spridningsfasen. Den 11 oktober 2017 var det tänkt att alla skulle ha skaffat sig möjligheter att verifiera den nya nyckeln. Då skulle den gamla nyckeln tas bort.



Den 11 oktober stod det dock klart att inte alla DNS-operatörer hade möjlighet att verifiera den nya KSK-nyckeln och borttagningen av den gamla stoppades tills vidare. I början av 2018 kunde emellertid alla verifiera den nya nyckeln.

Varje gång man byter KSK-nyckel, sk rollover, så använder man de båda KSK-nycklarna parallellt. Det börjar med att man introducerar den nya nyckeln, fortsätter med att man migrerar över till att använda den nya, för att sedan ta den gamla ur drift.

Problemet som uppstod var att flera viktiga infrastrukturer saknade en fungerande metod och därmed tidplan för att rulla ut nya trust anchors på sina servrar, vilket skulle innebära att när KSK för rotzonen byts, så skulle den inte längre matcha deras verifiering som var mot den gamla KSK, och därmed skulle hela DNSSEC förtroendekedja fallera. För att kunna hantera detta tvingades man ge dem mer tid på sig att rulla ut den nya trust anchor så att de kunde verifiera den nya nyckeln.

Så vad hände? Faktiskt hände inget alls. Det löste sig av sig själv efter ett par månader. De som har hand om nycklarna hos IANA tror på redundans och god ingenjörssed. Om fler hade trott på dessa två nyckelfaktorer hade vi haft betydligt färre IT-katastrofer i samhället.

INTRESSANTA MISSAR

Under 2017 fick vi uppleva stora attacker mot DNS-tjänster, som bland annat gjorde det svårt att nå **krisinformation.se** och **regeringen.se**.

Vad till exempel Myndigheten för Samhällsskydd och Beredskap (MSB) hade missat var att använda sig av robust DNS. De använde endast en DNS-leverantör kallad Dyn i USA, alltså på långt håll och Dyn blev DDoS-attackerad och satt ur spel. Då kunde ingen få några svar om de interna servrarna hos MSB och alltså aldrig nå fram till https://www.krisinformation.se/. Det är allvarligt, då det är del av den kommunikationsväg som finns för viktig information till allmänheten, dvs det blev en attack mot samhällets infrastruktur. Att MSB använder https, alltså krypterad dataöverföring av själva webbsidan, är helt utan betydelse. (Installera gärna DNSSEC/TLSA Validator, nedan, och se efter om de lärt sig när du läser den här artikeln.)

Det spelar ingen roll hur många gigabit per sekund eller rent av terabit per sekund din serverpark klarar av att leverera, om ingen ens vet IP-addresserna till den. Därför är DNS-servrarna plötsligt en attackvektor och svag punkt.

Lösningen är att specificera DNS-tjänsten korrekt och därefter betala, så får man ett system som håller igång oavsett attacker. Det går inte att påstå att man inte kan skydda sig.

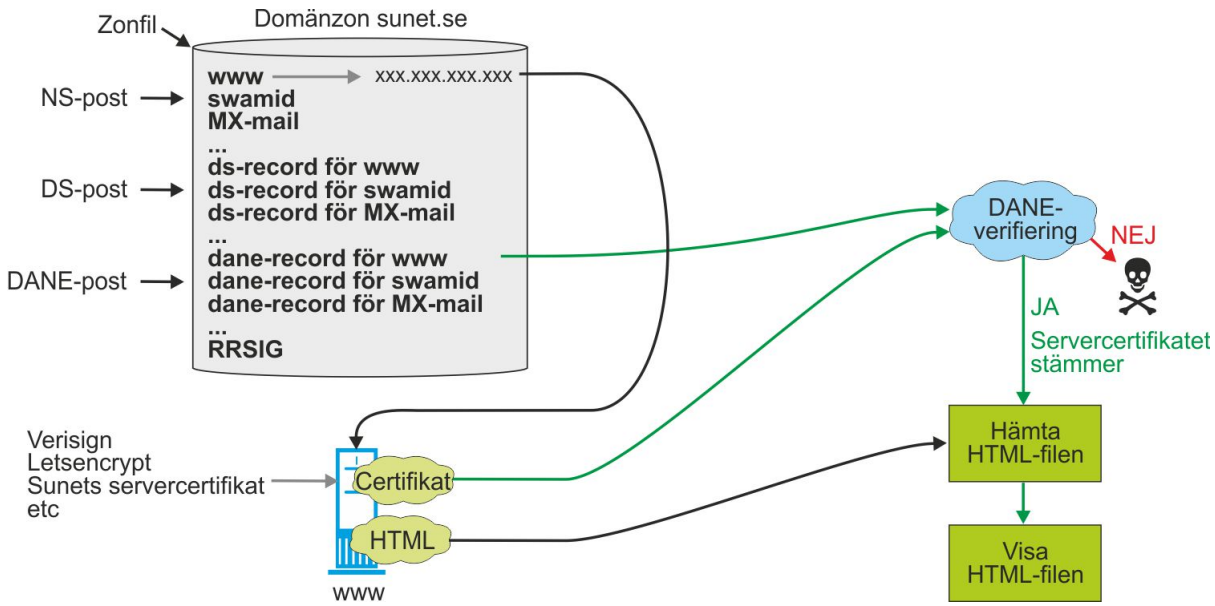
Genom att ha bra geografisk spridning på sina namnservrar kan man minska inverkan av sådana attacker.

SISTA BITEN – DANE

Nu kommer vi in på överkursen. Namnservern har fått en pålitlig IP-adress till www.sunet.se av SUNETs domänserver. Men hur kan man veta att man faktiskt får tag i den genuina www.sunet.se och inte en falsk server som har fuskats in på samma adress?

Webbservern kan ju ha ett certifikat från en pålitlig Certificate Authority som Verisign, men sådana är dyra. Man kan skapa egna certifikat, men om de inte godkänns av webbläsaren kommer ett otrevligt felmeddelande. SUNETs TCS-certifikat är gratis och det vore tråkigt om de inte kunde användas av alla.

Nu kommer grädden på moset. Man kan fortsätta använda DNS-kedjan för att verifiera själva webbservern också. Metoden kallas DANE (DNS-based Authentification of Named Entities).



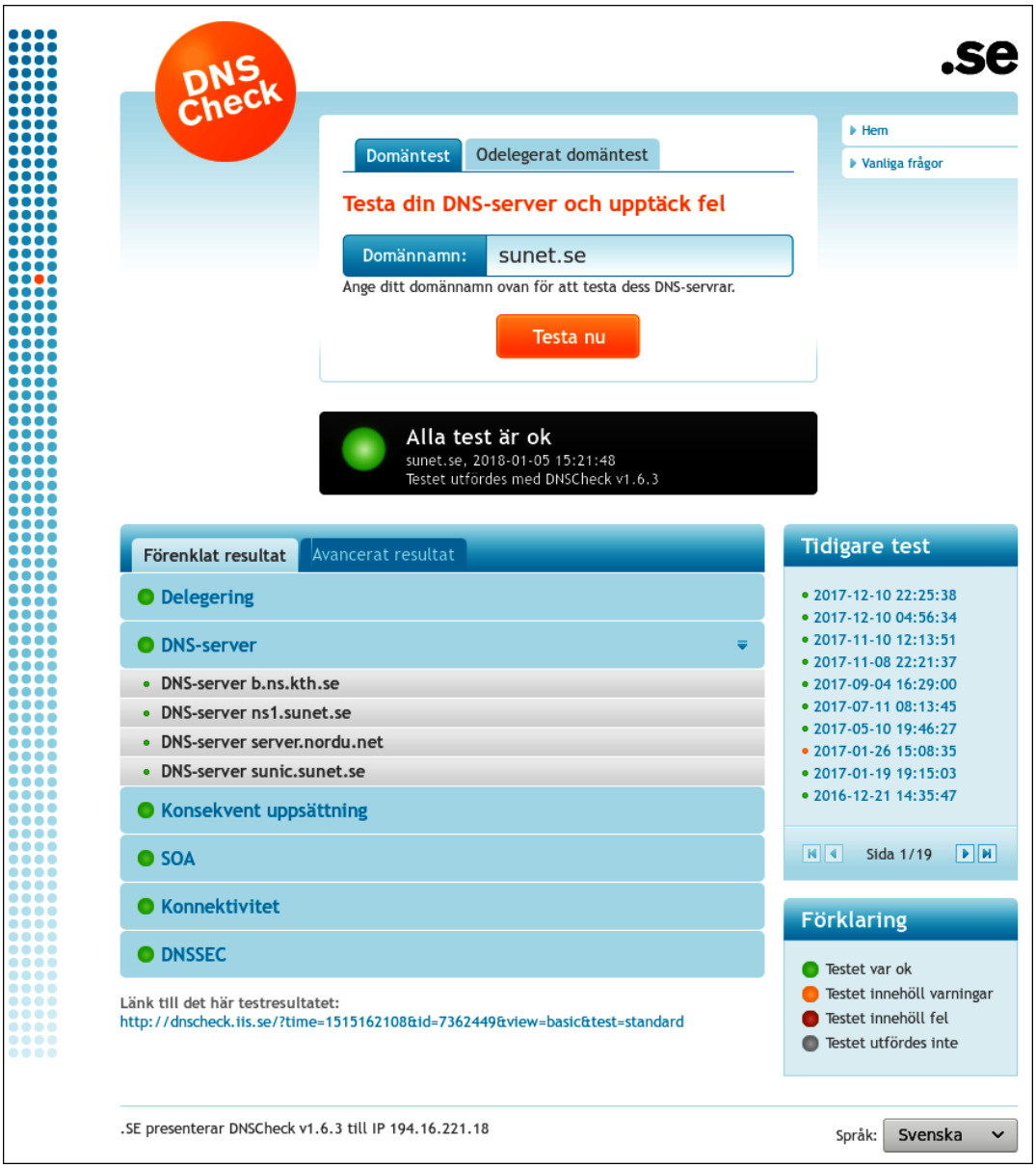
Genom att föra in ytterligare en form av metadata i domänservens zonfil, utöver NS-posterna, DS-posterna och RRSIG, nämligen en DANE-post, kan man använda denna, tillsammans med certifikatet i webbserven och genom en verifikationsprocess som är mer eller mindre lik DNSSEC-verifikationen, även autentisera webbservern.

Då kan webbserverägaren själv skapa ett certifikat som denne litar på och lägga in lämpliga DANE-poster i sin domänserver och därigenom få sin server godkänd. Det blir en oberoende verifiering, ett parallellt alternativ till andra certifikatutgivare.

Allt är demokratiskt på Internet och namnservern kan välja att tro på Verisigns certifikat och inte gå vidare i processen, eller också välja att verifiera certifikatet med DANE.

VALIDERINGSVERKTYG FÖR DNS-ADMINISTRATÖREN

Ett grundläggande verktyg för den som underhåller egna DNS-servrar är DNSCheck, som finns hos IIS.se, på http://dnscheck.iis.se/. Användningen är ganska rättfram. Ange den domän du vill testa i rutan **Domännamn** och klicka på knappen **Testa nu**.



Testservern hos IIS undersöker zonen (i detta fall sunet.se) och noterar grundläggande egenskaper, såväl som DNSSEC-egenskaper.

Punkten **Delegering** anger hur väl utpekningen av sunet.se sker från toppdomänservern, eller om data saknas osv.

Punkten **DNS-server** visar upp alla SUNETs DNS-servrar som listas av toppdomänen. Det finns, som tidigare nämnt, två hos SUNET, en hos NORDUnet och en på KTH. Inte nog med det: de fungerar.

Punkten **Konsekvent uppsättning** skärskådar SOA, rubrikdelen av zonfilen. Dessutom undersöks om alla servrarna har samma serienummer och därigenom är uppdaterade. För varje uppdatering ändrar man regelmässigt serienumret. Uppdaterade bör de ju vara, för de representerar samma zon. SUNETs servrar svarar på ett konsekvent sätt.

Punkten **SOA** kvalitetsprovar innehållet i zonfilens SOA. Time To Live får till exempel inte vara för kort, eller för lång. Tider mellan en och 24 timmar är utmärkta.

Punkten **Konnnektivitet** är ett prov av om alla DNS-servrar kan nås på alla de adresser som finns registrerade för dem, både IPv6 och IPv4.

Punkten **DNSSEC** provar om DNSSEC finns, om det finns signeringsinformation i zonfilen (DS-postern i toppdomänen .se letas fram varefter funktionen utför verifikationen), om livslängden för RRSIG är godkänd, att nycklar har lämpliga längder med mera.

Fliken **Avancerat resultat** visar upp alla detaljer i svaren från de olika servrarna, till exempel om servrarna svara på IPv6.

SUNET klarar provet med flaggan i topp.

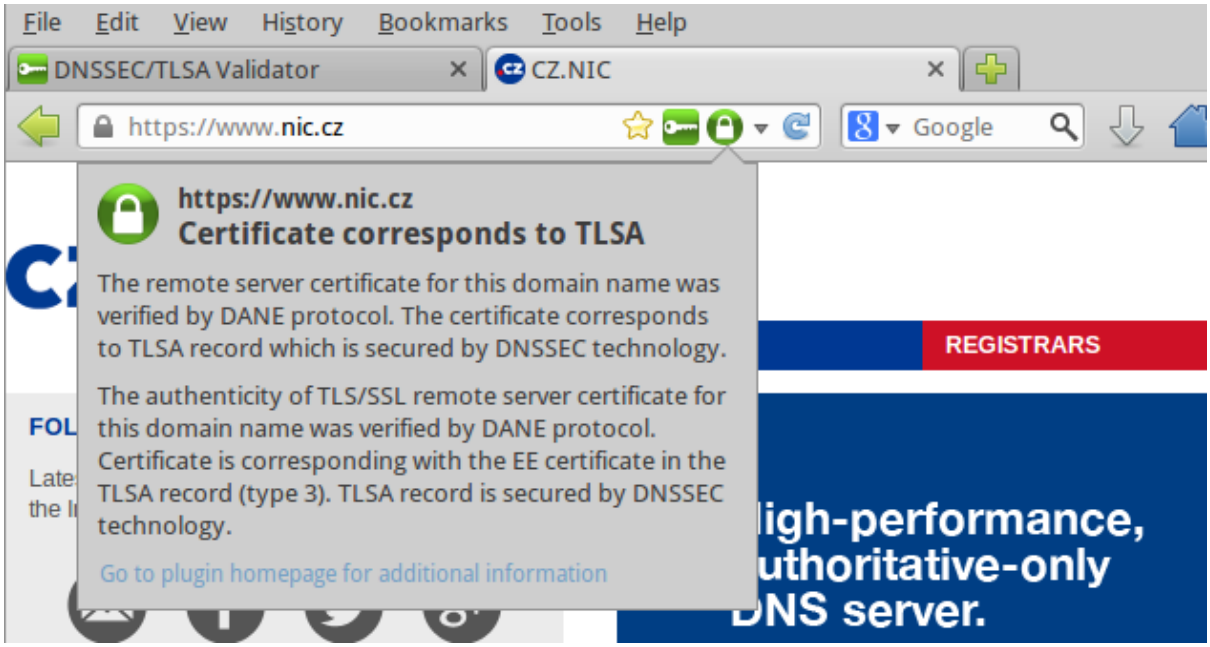
DANE testas inte, för det är inte en del av ursprungliga DNSSEC.

Ett annat testverktyg hos IIS är **Zonemaster** som du hittar på https://www.iis.se/vad-vi-gor/testverksamhet/zonemaster/. Den testar med lite andra kriterier, och visar svaret på lite annat sätt, men gör ungefär samma sak som DNSCheck.

Ytterligare ett verktyg heter **DNSViz**, DNS visualizer och återfinns på http://dnsviz.net/. Verktyget visualiserar hela DNS-kedjan från roten och ned. Alla nycklar visas, samt hur de används för autentisering av nästa domän. Sålunda kan du nu se hela chain of trust.

VERKTYG FÖR DEN INTRESSERADE ANVÄNDAREN

Du kan själv installera en validerare som en insticksmodul i din webbläsare för att vara säker på att den webbsida du ser, verkligen är vad den utger sig för att vara. Modulen heter **DNSSEC/TLSA Validator** och kan hittas på https://www.dnssec-validator.cz/.

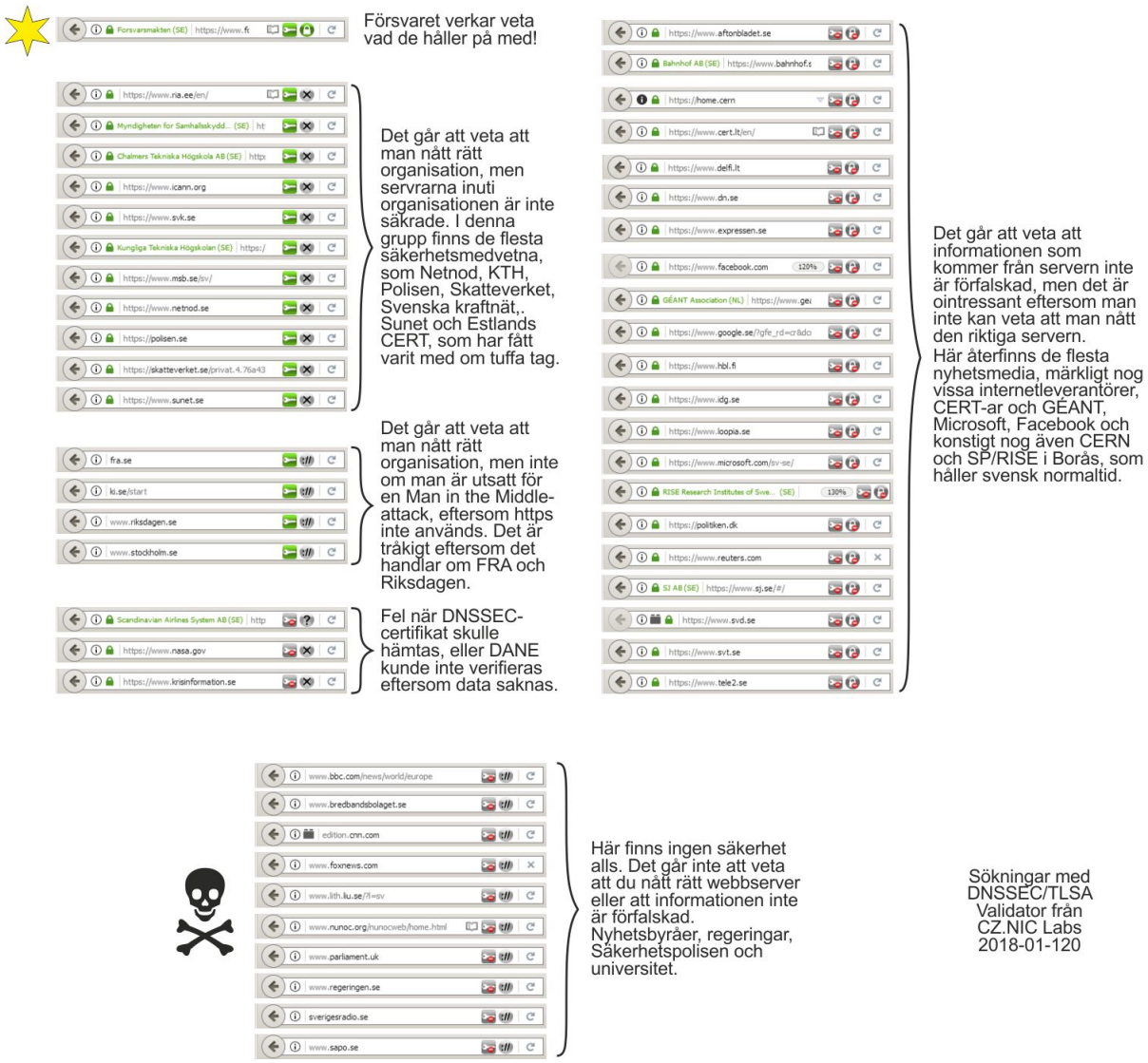


Verktyget visar hela tiden om de webbplatser du besöker fungerar korrekt med DNSSEC genom att visa en grön nyckel.

Eftersom du som användare också vill se slutresultatet, alltså en webbsida, verifieras även DANE-posterna, med ett grönt hänglås.

VEM KAN MAN LITA PÅ?

En liten rundfrågning på Internet efter de vanligaste nyhetsmedierna, regeringsorganen, försvaret osv gav inga särskilt upplyftande resultat. Man kunde tro att åtminstone teknikerorganisationer skulle ha kontroll på säkerheten, men icke.



De dödskallemärkta webbplatserna nederst är särskilt oroande. Kan du veta att du har kommit till rätt webbsida? Nej. De kanske har egna certifikat från exempelvis Verisign som din webbläsare kan verifiera, men har de inte det, är du förlorad. Och certifikat har förfalskats förr.

Kära svenska media: Bråka inte när ni blivit spoofade! Lösningen är, som synes, ganska enkel.

Kära svenska universitet och högskolor: För er egen säkerhet, inför DNSSEC i hela organisationen.

Kära användare: Säg inte att du inte har blivit varnad och att det inte finns verktyg för att hjälpa dig hitta rätt på Internet.

LÄS MER

Alla toppdomäner: https://sv.wikipedia.org/wiki/Toppdom%C3%A4n
Kända adresser till rotservrar: https://www.iana.org/domains/root/servers
Här finns rotservrarna: http://www.root-servers.org/
Mera information om myndigheters DNS-säkerhet finns här: https://www.myndighetermeddnssec.se/
Anne-Marie Eklund Löwinders blogg: https://www.iis.se/bloggare/anne-marie/
Vill du gå längre? Skaffa boken DNS and Bind: https://www.amazon.com/DNS-BIND-5th-Cricket-Liu/dp/0596100574/ref=sr_1_1?ie=UTF8&qid=1516876459&sr=8-1&keywords=dns+and+bind

KSK rollover

Tidsplanen publicerades i maj: https://www.icann.org/news/blog/changing-the-keys-to-the-domain-name-system-dns-root-zone
Den nya nyckeln publicerades i juni: https://www.icann.org/resources/pages/ksk-rollover
Utbytet senarelades i oktober: https://www.icann.org/news/announcement-2017-09-27-en

https://www.internetsociety.org/blog/2017/09/icann-postpones-dnssec-root-ksk-rollover-october-11-will-not-big-day/
Om IANA: https://www.iana.org/

Validerare

DNSCheck: http://dnscheck.iis.se/
Zonemaster: https://www.iis.se/vad-vi-gor/testverksamhet/zonemaster/
DNSViz: http://dnsviz.net/
DNSSEC/TLSA Validator: https://www.dnssec-validator.cz/
Felkoderna i DNSSEC/TLSA Validator https://www.dnssec-validator.cz/pages/documentation.html

SVÅRA ORD

Engelska	Svenska	Förkortning	Förklaring
AAAA-record			Namn på den IPv6-adress man får ur en DNS-server
A-record			Namn på den IPv4-adress man får ur en DNS-server
DNS-based Authentification of Named Entities		DANE	Sista biten av DNSSEC för att verifiera att servern som slutligen levererar tjänsten, är den rätta
Domain Name System		DNS	Adressboken på Internet, den osäkra versionen
Domain Name System Security Extensions		DNSSEC	Adressboken på Internet, den säkra versionen
Dynamic Host Configuration Protocol		DHCP	Automatisk möjlighet att ge nätverksinformation åt datorer och tilldela datorerna IP-adresser
Internet Assigned Numbers Authority		IANA	Ansvarar bland annat för fördelningen av namn och adresser på Internet, del av ICANN
Internet Corporation for Assigned Names and Numbers		ICANN	Ansvarar för namn och nummer på Internet, samt för rotservrarna
Internet Protocol version 4		IPv4	Den gamla typen av adresser på Internet. Dessa adresser är slut!
Internet Protocol version 6		IPv6	Den nya typen av adresser på Internet. Dessa finns i ett oändligt förråd!
Internet Service Provider		ISP	Internetleverantör
Key Signing Key		KSK	Den högsta autentiseringsnyckeln i DNS-strukturen
Registrar			Kommersiell organisation som säljer toppdomäner
Resource Record Set Signature		RRSIG	Den kryptografiska signaturen för posterna i en zonfil

Root Server	Rotserver		Översta servern i DNS-strädet
Spoofing	Parodiering		Att låtsas vara en annan server, eller att skicka ett anrop till fel server
Start Of Authority		SOA	Början av zonfilen, innehåller grunddata om zonfilen
Time To Live		TTL	Bäst-före-datum för en post i en DNS-server
Top Level Domain	Toppdomän	TLD	Landsdomäner som .se
Transport Layer Security Protocol		TLSA	Protokollet som används för HTTPS
User Datagram Protocol		UDP	Ett protokoll för kommunikation utan inbyggd säkerhet i överföringen
Zone Signing Key		ZSK	En enklare nyckel, utvunnen ur KSK

Skriven av

JÖRGEN STÄDJE

Jag heter Jörgen Städje och har skrivit om teknik och vetenskap sedan 1984. Friskt kopplat, hälften brunnet!