TRAFICOM
Transport- och kommunikationsverket

DNSSEC

Garanterar ett säkert internet

Rutter säkras med
DNSSEC

Vad är DNSSEC?

DNSSec är ett tillägg i Domain Name System (DNS), som säkrar DNS-svarens äkthet och integritet. Tekniska åtgärder tillämpas vilket gör att den dator som lämnar en förfrågan (t.ex. en webbläsare) nukan se om svaret från en internetadress i DNS verkligen kommer från den server som registrerats av oss som behörig. Samtidigt säkrar DNSSEC att detta svar inte har modifierats när det sänts över internet.

Enkelt uttryckt: DNSSEC är en sorts försäkring som garanterar att internetanvändare endast visas till den webbsida som de verkligen tänkte koppla upp sig mot.

Detta garanteras tack vare kryptografiska signaturer. Ingen information krypteras i DNSSEC. All data förblir allmänt åtkomlig, liksom befintlig DNS.

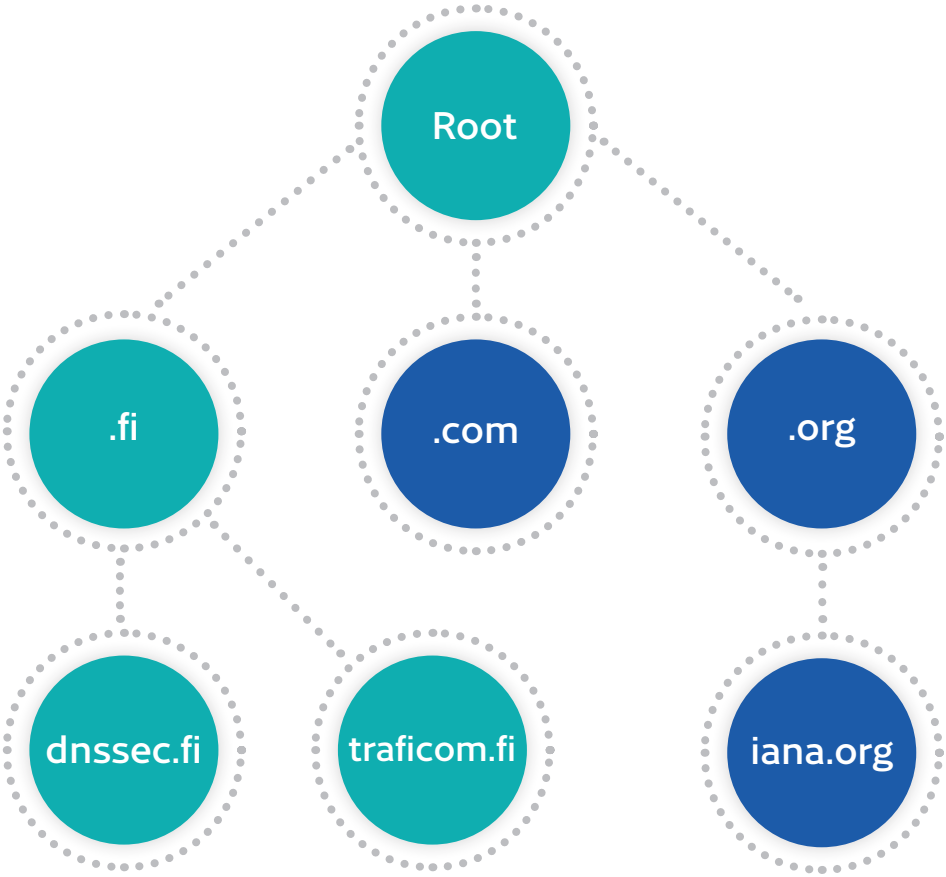
Varför behövs DNSSEC?

Observanta läsare har säkert noterat att webbläsare ju redan har inbyggd teknik som skapats för att säkra att användaren kommer till ”korrekt” webbsida. Webbsidor av denna typ är vanligen krypterade med SSL (Secure Sockets Layer), vilket visas i webbläsaren i form av en nyckel-symbol.
DNSSEC utvecklades inte för att ersätta SSL-kryptering. Tvärtom. DNSSEC är ett komplement till SSL och förhindrar situationer där användaren hamnar på en felaktig server redan innan anslutningen har säkrats av SSL.

Hur fungerar DNS (Domain Name System)?

Det internet vi känner idag baseras på det globala Domain Name System. Vi sammanfattar nedan, helt kort, hur detta system fungerar. DNS kan ses som ett världsomspännande distribuerat telefonregister, som tilldelar de globalt unika domännamnen (www.dnssec.fi) motsvarande globalt unika internetadresser (87.239.124.120). Internetadresser, dvs. domännamn används därför att de är enklare att komma ihåg. Suomen palvelimiin (”fi”) ja edelleen DNSSEC-palvelimiin (”dnssec.fi”). Yksittäisten vyöhykkeiden tehtävät on jaettu eli delegoitu hierarkiassa. För att inte de olika förfrågningarna alla ska hamna på samma server har DNS skapats med en hierarkisk struktur.

Namnutrymmet är uppdelat i så kallade zoner. I fallet med www.dnssec.fi följs hierarkins toppnivå (root) av servrarna för Finland (”fi”) och därefter av DNSSECservrarna (”dnssec.fi”). De individuella zonernas ansvar delas upp (delegeras) inom hierarkin. Om du vill kontakta webbsidan www.dnssec.fi från din dator så undersöker din internetleverantörs server alla nivåer i hierarkin, den ena efter den andra. Varje nivå som inte har svaret på måladressen sänder ett meddelande till nivån under. Servern på den lägsta nivån i hierarkin kommer sedan till slut att kunna erbjuda svaret på adressen.

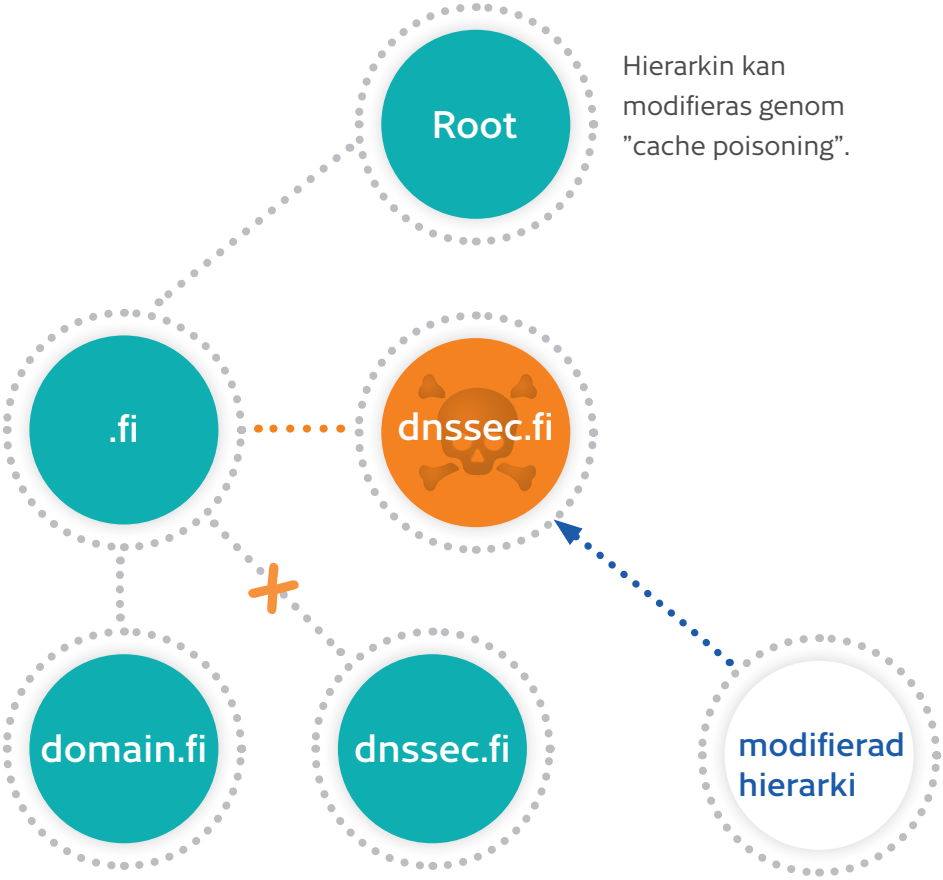


Domain Name System (DNS) har en hierarkisk struktur. Namnservrar för ”fi” vidarebefordrar automatiskt förfrågningar för domännamn som slutar på ”fi” (t.ex. dnssec.fi) till korrekt adress.

Vad är syftet med DNSSEC?

Tänk dig en situation där någon lyckas ändra uppgifter i telefonkatalogen. Du slår alltså upp numret till domännamnsservice vid Traficom och hittar ett felaktigt nummer. Skulle du ha någon egentlig möjlighet att upptäcka detta? Antagligen inte. Ett sådant scenario skulle vara möjligt på internet om en angripare gjorde ändringar i den hierarki som beskrivs ovan. Om en angripare till exempel lyckas med att smuggla in inkorrekt data i din leverantörs server (”cache poisoning”) skulle du komma till en annan webbsida när du kontaktade www.dnssec.fi. Det är bäst att inte tänka på vad som skulle kunna hända om den förfalskade webbsidan tillhörde din bank.

Eller om du skulle skicka ditt företags senaste strategi till en partners förfalskade e-postserver. Eftersom internet i dag används för en rad olika ändamål kan hacker-attacker få långtgående konsekvenser. DNSSEC ger ett grundläggande skydd mot attacker av denna typ – och inte bara när webbsidor kontaktas. DNSSEC kan inte ge ett övergripande skydd mot nätfiske. Det ger dock ett effektivt skydd mot attacker på DNS. Detta är viktigt, eftersom de flesta nätfiskeattacker kan identifieras och förebyggas av uppmärksamma internetanvändare. Men till och med experter har svårt att upptäcka attacker mot DNS.



Hierarkin kan modifieras genom ”cache poisoning”.

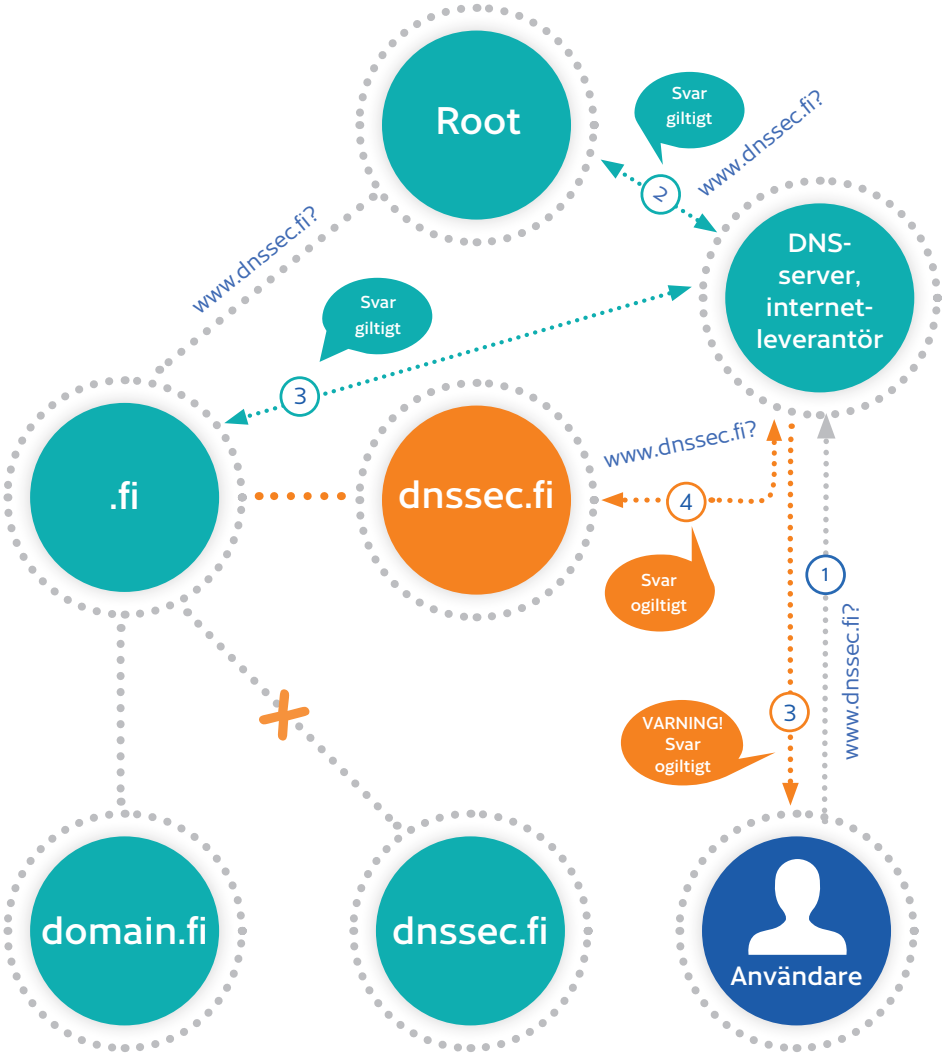
DNSSEC i detalj

Som redan har nämnts baseras DNSSEC på kryptografiska signaturer med vilka de aktuella DNS-posterna signerats. Alla med ansvar för ett domännamn på internet kan skydda sin information med hjälp av DNSSEC. All den information som en tjänsteleverantör är ansvarig för signeras med denna tjänsteleverantörs privata nyckel och signaturerna skrivs in i DNS (RRSIG record).

Ett exempel med DNSSEC:
Din internetleverantörs namnserver följer återigen den bekanta hierarkin för att lösa en förfrågan. Denna gång kan den emellertid kontrollera, på grundval av de signaturer som erhålls, om ursprunget till svaren är korrekt och om ett svar har modifierats på vägen. Namnservern svarar endast om all information är korrekt.

Hur kan alla dessa signaturer kontrolleras?

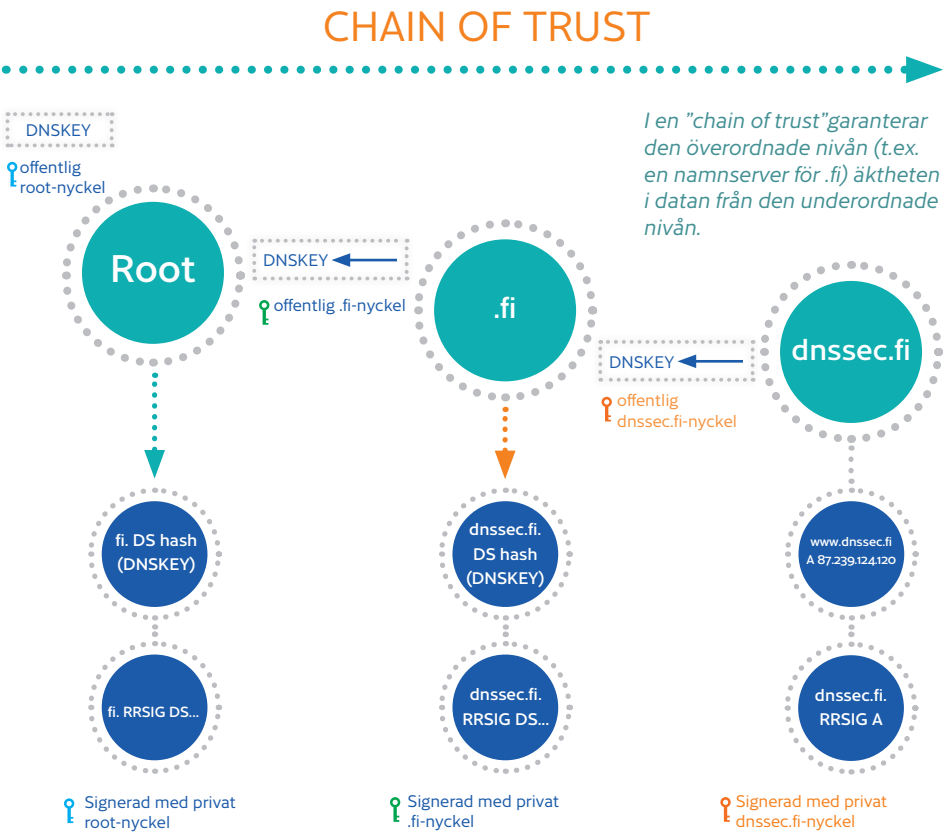
För att sammanställa digitala signaturer genereras ett par nycklar. Ett par nycklar av detta slag består av en privat och en offentlig nyckel (asymmetriskt kryptosystem). Som namnet antyder är den privata delen hemlig och förblir hos ägaren. Den offentliga delen publiceras i DNS (DNSKEY record). Med hjälp av den offentliga nyckeln är det nu möjligt att kontrollera och validera en signatur som signerats med den privata nyckeln.
Därför är det nödvändigt att ha förtroende för en offentlig nyckel innan du kan kontrollera signaturen. Eftersom det inte är möjligt att lita på alla nycklar på internet används en nyckel-hierarki liknande DNS-hierarkin (”chain of trust”). Detta kan verka förvirrande vid första anblicken, men dess enda syfte är att säkra att alla signaturer kan verifieras med en enda offentlig nyckel.



Med hjälp av DNSSEC kan din internetleverantörs namnserver känna igen en hierarki som har modifierats med ”cache poisoning”.

”Chain of trust” i detalj

En avbildning av den offentliga nyckeln aviseras till nästa nivå i hierarkin i varje enskilt fall. Den högre nivån skriver in avbildningen i sin zon (DS record) och garanterar dess äkthet genom att underteckna den. Denna offentliga nyckel för denna nivå aviseras i sin tur till nästa överliggande nivå.



Vad behöver jag för att använda DNSSEC?

Som internetanvändare behöver du inte göra någonting. Om din ADSL- eller kabelmodem-leverantör har stöd för DNSSEC kommer alla signaturkontroller att göras på deras DNS-servrar. Om du är innehavare av ett domännamn måste din webbsideadministratör installera DNSSEC åt dig. Eftersom användningen av DNSSEC initialt inte kommer att vara så utspridd kommer det förmodligen till att börja med vara administratörer av webbsidor som kräver skydd (t.ex. banker) som kommer att skydda sina domännamn med DNSSEC.

Broschyrens text baserar sig på materialet från the Swiss education and research network (www.switch.ch).

Kundservice kundservice
p. 0295 345 656 / Kundservice / Mån-Fre 9-15
p. 0295 34 5000 / Växel / Mån-Fre 8-16.15

Transport- och kommunikationsverket Traicom
Gumtäktsvägen 9
Helsingfors, PL 320
00059 TRAFICOM
domain.fi / traficom.fi

TRAFICOM
Transport- och kommunikationsverket