HÖGSKOLAN
I GÄVLE

AKADEMIN FÖR TEKNIK OCH MILJÖ
Avdelningen för industriell utveckling, IT och samhällsbyggnad

Robust internetinfrastruktur med DNSSEC och IPv6

En studie av DNSSEC- och IPv6-implementationen hos utvalda organisationer i Sverige

Magnus Eklund, Per Hedblom

2015

Examensarbete, Grundnivå (högskoleexamen), 15 hp
Datavetenskap
Dataingenjörsprogrammet

Handledare: Anders Hermansson
Examinator: Douglas Howie

Robust internetinfrastruktur med DNSSEC och IPv6

En studie av DNSSEC- och IPv6-implementationen hos utvalda organisationer i Sverige

av

Magnus Eklund
Per Hedblom

Akademin för teknik och miljö
Högskolan i Gävle

801 76 Gävle, Sverige

Email:
ntn11med@student.hig.se
ntn11phm@student.hig.se

Abstrakt

Domännamnssystemet DNS är en vital och ofrånkomlig del av internet. Det är dock sårbart för attacker. DNSSEC är ett sätt att minska sårbarheten hos DNS. I detta examensarbete har data om ett antal domäner samlats in med hjälp av *Zonemaster* och *domain information groper* för att sedan bearbetas med hjälp av bash-skript och java-kod. Detta data har sedan analyserats. Resultatet visar att användandet av och statusen på DNSSEC-implementeringen hos flera av de undersökta domänerna är bristfällig och lämnar utrymme för förbättringar.
Nyckelord: DNS, DNSSEC, internetinfrastruktur.

Innehållsförteckning

1. Introduktion

1.1 Syfte

Syftet med detta examensarbete är att undersöka de utvalda organisationernas robusthet dvs. stabilitet och stryktålighet avseende dess infrastruktur angående områdena DNS (Domain Name System) och DNSSEC (Domain Name System Security Extensions). Post och Telestyrelsen definierar robusthet som *"förmågan att motstå störningar och avbrott samt förmågan att minimera konsekvenserna om de ändå inträffar"* [1]. Det kommer även att framgå om de har implementerat IPv6 (Internet Protocol version 6). Tillgängliga verktyg för att kontrollera DNS, DNSSEC och IPv6 har använts för att samla in data, vilket avslöjar hur implementation och konfiguration av de nämnda systemen förhåller sig.

1.1.2 Frågeställningar

På vilket sätt har de undersökta organisationerna implementerat och konfigurerat internetinfrastrukturen med avseende på DNS, implementation av DNSSEC och IPv6?

Vilka följder kan organisationens uppbyggnad av internetinfrastruktur få om dessa system inte är implementerade eller konfigurerade korrekt?

1.2 Bakgrund

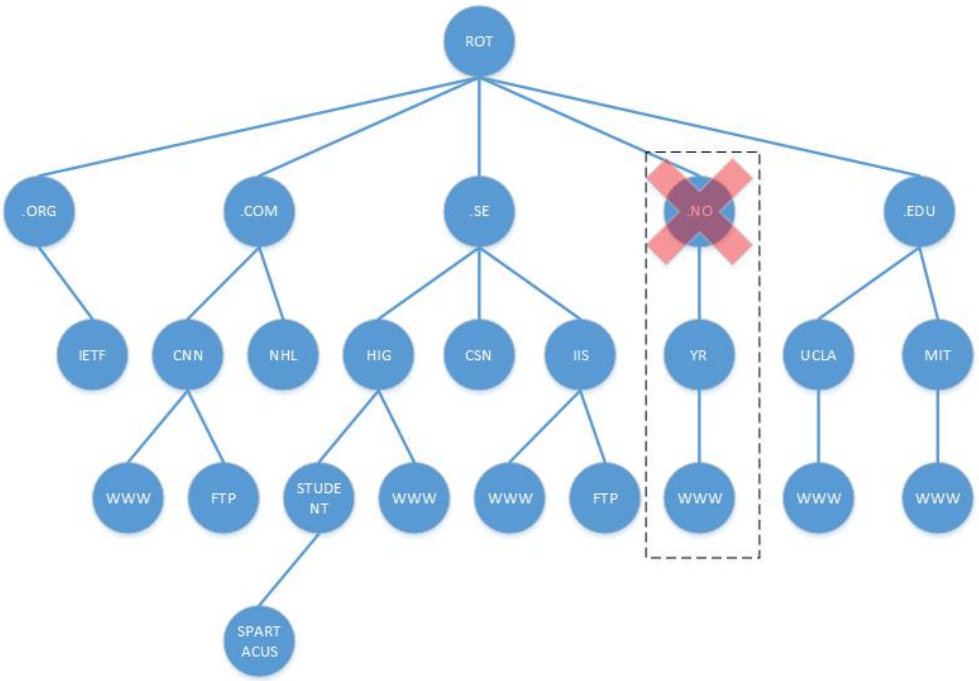
Kommuner och myndigheter eftersträvar att göra sig tillgängliga för allmänheten och skapa en enklare vardag för privatpersoner och företag. Goda förutsättningar skall ges för att tillhandahålla tjänster som bland annat genom självservice tillfredsställer människor och företags behov. I dagens samhälle innebär tillgänglighet även att det går att nå och kommunicera med, eller att använda tjänster över internet via exempelvis en kommuns hemsida när man så vill. Ett typiskt fall på en önskvärd tjänst kan vara att använda 1177-Vårdguiden för att söka information om sjukdomar, att använda deras e-tjänster för att förnya recept eller till att boka en tid. En annan funktion är att viktiga meddelanden till allmänheten kan spridas via en myndighets eller kommuns hemsida. Det är då essentiellt att kunna känna sig trygg i antagandet att meddelanden och information kommer ifrån den organisation man förväntar sig och inte har blivit manipulerat av en okänd aktör.

Enligt den digitala agenda som regeringen publicerade år 2011 fastställs att *"internet som bärare av tjänster skall vara tillgängligt och robust"* [2]. För att säkerställa detta krävs att man har ett väl fungerande och skyddat DNS. I den digitala agendan framgår även att alla myndigheter bör ha implementerat DNSSEC och vara nåbara över IPv6 senast 2013.

Studien har gjorts på uppdrag av företaget Interlan Gefle AB som är ett IT-konsultbolag.

1.3 Domain Name System

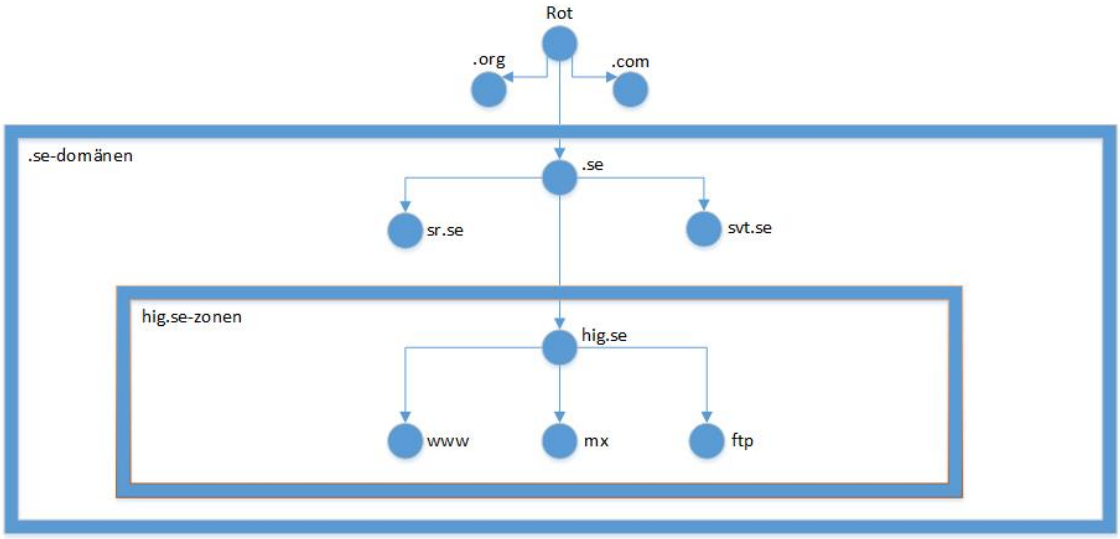
För att översätta mellan domännamn och IP-adresser i internets uppbyggnad används domännamnssystemet DNS [3]. DNS omfattar bl.a. hemside-adresser och även de domäner som används i e-postadresser. DNS är uppbyggd som en hierarkiskt distribuerad databas med totalt tretton stycken rot-servrar över världen. Rot-servrar använder sig av Anycast [4] vilket innebär att en server kan vara distribuerad över hela världen men ändå vara kopplad mot en och samma IP-adress. Informationen i DNS lagras i en trädstruktur. Tidskomplexiteten för sökning i trädstrukturer gör att det går snabbt att komma åt den information man är intresserad av. Medelhastigheten är O(log n). I och med att DNS är konstruerat med en hierarkisk struktur kommer DNS att fungera även om problem uppkommer på en lägre hierarkisk nivå. Exemplet i figur 1 visar att en förlust av TLD (Top Level Domain) *.no* inte påverkar de övriga TLD, utan endast de domäner som ligger under *.no*.



Figur 1 DNS-träd med utslagen domännivå

En zon i DNS är ett delegerat ansvarsområde inom en domän. Till exempel är *hig.se* en zon i domänen *.se*. Alla TLD är zoner tilldelade ansvar från rot. En zon behöver inte enbart innehålla IP-adresser utan kan ha vidare delegerat ansvar till underliggande domäner och har då endast vetskapen om vilken väg som ska användas för att få ytterligare information (figur 2).

Sökningar i DNS går att göra på både domännamn t.ex. *hig.se* men även på FQDN (Fully Qualified Domain Name) t.ex. *www.hig.se*.



Figur 2 Exempel på indelning av domäner och zoner.

En DNS-uppslagning kan resultera i att ett domännamn översätts till en IP-adress. I specifikationen för DNS [3] anges 2 möjliga metoder för namnuppslagning, nämligen iterativ eller rekursiv och den iterativa utställs vara den att föredra. I den praktiska användningen används båda delarna. Först kontaktar den applikation som vill göra en uppslagning en så kallad stubb-resolver. Stubb kontaktar en rekursiv resolver och väntar därefter på svar. Detta steg är att betrakta som rekursivt då stubb kommer att få det färdiga svaret (eller ett felmeddelande om uppslagningen misslyckades) utan någon ytterligare interaktion. En resolver är ansvarig för initiering och sekvensering av DNS-uppslagningar. Den resolver som ska användas tillhandahålls av t.ex. klientens ISP (Internet Service Provider). I många fall kan man dock välja att konfigurera om detta så man använder en annan resolver om behovet skulle uppstå. Den rekursiva resolvern kontrollerar om svaret finns i dess cache men om så inte är fallet så ställs frågan till en av rot-servrarna för att sedan starta en iterativ process där auktoritativa namnservrar kontaktas i ordning till rätt nivå i hierarkin har nåtts och svaret funnits.

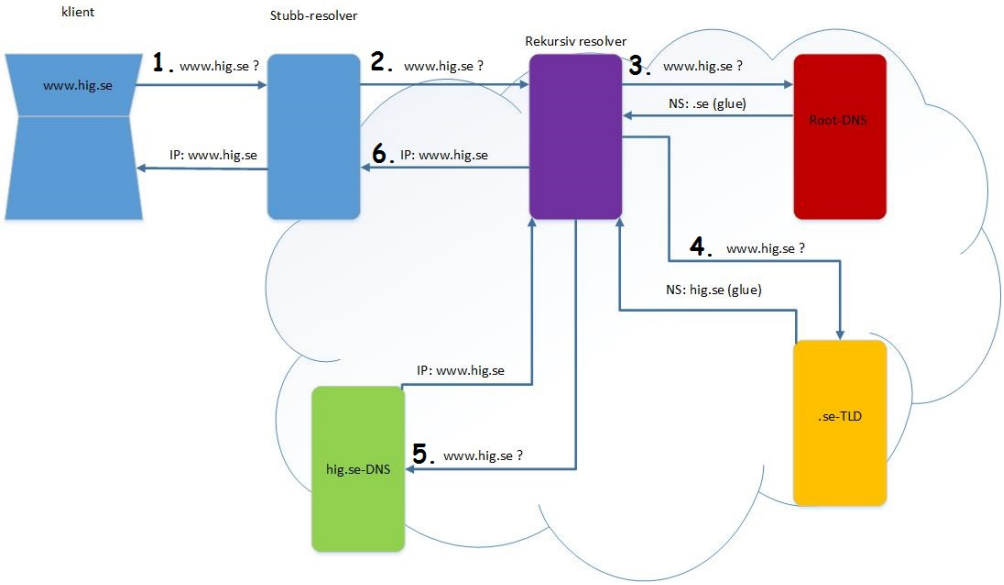
Enligt artikeln DNSSEC: A Protocol Toward Securing the Internet Infrastructure [5] så ska en rekursiv resolver som inte har det eftersökta resultatet lagrat i sin cache kontakta sin *parent* innan det numera normala förfarandet med iteration utifrån roten utförs.

Ett typiskt förfarande skulle kunna se ut på följande sätt (figur 3):

1. En person vill söka information på *www.hig.se* och skriver in URL:en i sin webbläsarklient. Klienten kontaktar då sin stubb-resolver för att få IP-adressen till domänen *www.hig.se*.
2. Om informationen inte finns lagrad i den lokala cachen så kontaktas den för operativsystemet inställda DNS resolvern. Om resolvern har IP-adressen lagrad i sin cache skickas ett svar tillbaka.
3. Annars får resolvern kontakta en av root-DNS:erna och frågar efter svar. Root-DNS:erna har delegerat ut ansvaret till olika TLD och kommer därför att svara resolvern med att den inte vet svaret men att vidare frågor kan skickas till *.se*. IP-adressen till.se skickas med i svaret till resolvern (kallas glue).
4. I nästa steg kontaktar resolvern TLD för den givna URL:en, i detta fall *.se*. TLD för *.se* vet inte vilken IP-adress som *www.hig.se* har

men den vet IP-adressen till *hig.se*. Det som nu händer är att *.se* svarar till resolvern att den inte vet adressen till *www.hig.se* men att resolvern kan fråga *hig.se*. IP-adressen till *hig.se* skickas med i svaret till resolvern.

5. Resolvern skickar nu samma fråga till *hig.se* och där finns svaret på vilken IP-adress som *www.hig.se* har.
6. Svaret från *hig.se* sparas i cachen hos den rekursiva resolvern och även i en cache i operativsystemet.



Figur 3 Process för DNS-uppslagning.

När DNS togs fram på 80-talet var det inte avsett att användas i så stor omfattning. Det har lett till att det finns allvarliga säkerhetsbrister i DNS som är förhållandevis lätta att utnyttja av illasinnade och därmed är inte säkerhetsnivån i DNS tillräckligt hög för att ha önskvärd motståndskraft mot attacker.
Ett antal av de brister som finns i DNS har listats i RFC 3833 [6] och förslag på lösningar på problemen ges också.

1.4 Domain Name System Security Extensions

Ett kryptografiskt skydd, DNSSEC [7] utvecklades för att tillföra säkerhet i DNS. DNSSEC motverkar möjligheten att en eventuell angripare manipulerar svar på DNS-frågor och på detta vis är det möjligt att försvåra man in the middle-attacker som exempelvis DNS-cache poisoning.

Cache poisoning innebär att en eventuell angripare förser en rekursiv resolver med ett falskt svar på en DNS-fråga. Svaret uppger en felaktig IP-adress för det efterfrågade domännamnet. Detta svar sparas i resolverns cache-minne och eftersom den som genomför attacken med stor sannolikhet har satt TTL (Time To Live)-värdet till ett värde som denne anser lämpligt kommer alla förfrågningar till det efterfrågade domännamnet att dirigeras om till angriparens egen server eller websida så länge som detta TTL-värde gäller. Angripare letar efter resolvers med gammal eller dåligt uppdaterad mjukvara vilket gör det lättare för dessa att genomföra cache poisoning-attacker.

År 2008 upptäckte datasäkerhetsforskaren Dan Kaminsky en allvarlig brist i DNS som gjorde det enkelt att genomföra cache poisoning [8]. Detta gjorde att tillverkare av programvaror som används i resolvers fick bråttom

att ge ut uppdaterade versioner av sina programvaror som skall ha bättre motståndskraft mot den så kallade Kaminskybuggen.

Det är arkitekturen i DNS som gör det möjligt att genomföra dessa attacker vilket gör att cache poisoning-problemen inte är möjliga att lösa helt med att endast uppdatera programvara. När DNS designades så var huvudmålet att det skulle vara enkelt att ansluta många datorer till nätet, säkerhetsaspekten var inte något som ägnades mycket uppmärksamhet.

DNSSEC förhindrar att innehållet i en DNS-fråga förändras eller att ett svar förfalskas av obehöriga genom att använda sig av digital signering. Den digitala signeringen verifierar DNS-datats ursprung och sker med hjälp av asymmetrisk kryptering. Denna signering sker i en kedja genom trädstrukturen i DNS ända från root-zonen, vilken ansvarar för DNS-förfrågningar på topp-nivå. DNS-root-zon skall tack vare ett säkert nyckelhanterings-förfarande vara att betrakta som pålitlig. Genom att organisationer som aktiverat DNSSEC också använder validering i sina resolvers säkerställs datats autenticitet. I och med att krypteringen som används i DNSSEC är asymmetrisk så har man en privat-nyckel och en publik-nyckel. Detta är dock inte tillräckligt säkert utan man använder även dubbla uppsättningar av nycklar för att öka säkerheten. Dessa nycklar (certifikat) kallas KSK (Key-Signing Key) och ZSK (Zone-Signing Key). KSK används till att signera ZSK så att dessa kan verifieras. ZSK används i den löpande signering som sker vid DNS-uppslagning för att man ska kunna verifiera att svaret kommer från rätt server och inte är förfalskat eller manipulerat.

DNSSEC standardiserades 1997 [9] men det upptäcktes snart att det var dåligt anpassat till storleken på det allt mer utbredda internet. Detta löstes med ett antal uppdateringar som genererade en ny standard vilken antogs av IETF (Internet Engineering Task Force) 2005 [7]. Trots det så är den önskvärda nivån på utbredning och användande av DNSSEC långt under vad som bör anses vara acceptabelt.

De tydligaste hindren i införandet av DNSSEC handlar till stor del om problem med arkitekturen hos domännamnssystemet och hur man på ett säkert sätt skall kunna hantera och distribuera krypteringsnycklar [10]. Även hårdvara som brandväggar och NAT (Network Address Translation) kan behöva uppdateras både mjukvaru- och hårdvarumässigt för att bland annat kunna ta emot större datapaket utan att dessa fragmenteras eller ogillas [11, 12].

1.5 Internetprotokoll version 6

IPv6 [13] är den version av internetprotokollet IP som är avsett att ta över efter IPv4 vilket är det internetprotokoll som till största del används idag. IPv4 har en adresslängd på 32 bitar som möjliggör ca 4,3 miljarder adresser (2^{32}). Dessa adresser är i praktiken redan slut. IPv6 använder sig av en adresslängd på 128 bitar vilket ger en avsevärd ökning av antalet möjliga adresser att nyttja (2^{128} eller $3,4 * 10^{38}$).

Att de organisationer som undersöks i studien har implementerat IPv6 är önskvärt då det är fördelaktigt att använda sig av IPv6 parallellt med IPv4 under en övergångsperiod för att säkerställa organisationens nåbarhet även i framtiden. Detta nämns i regeringens digitala agenda [2] som 2011 rekommenderade att alla myndigheter bör ha infört IPv6 och använda sig av DNSSEC under 2013.

2. Metod och material

2.1 Verktyg

Det primära verktyget för att analysera de utvalda domänerna är Zonemaster [14], vilket är ett verktyg som har tagits fram av .SE (Stiftelsen för internetinfrastruktur) [15] och deras franska motsvarighet afnic[1]. .SE är den organisation som ansvarar för den svenska toppdomänen *.se* och även domänen *.nu*. Post- och Telestyrelsen är tillsynsmyndighet för .SE. Zonemaster tar en domän som parameter och analyserar därefter den från TLD ner till den faktiska domänen så att hela kedjan kontrolleras. Exakt vad som kan kontrolleras går att läsa i Test requirements för Zonemaster[2]. Alla resultat från en körning med Zonemaster lagras i en mapp där varje domän motsvarar en fil som innehåller resultatet för den domänen och namnet på filen är domänens namn.

Ett annat verktyg är DIG (Domain Information Groper), vilket används till att göra DNS uppslagning av domännamn eller IP-adresser. Detta verktyg finns med i de vanliga distributionerna av operativsystemet Linux. DIG har använts för att komplettera med parametrar som inte omfattas av Zonemaster.

2.2 Skript

När data som insamlats med Zonemaster eller DIG ska behandlas används flera olika bash-skript för att utföra olika uppgifter. De flesta av dessa skript nyttjar den mapp som innehåller resultaten från Zonemaster och använder namnet på filerna (domännamnen) till att iterera igenom detta data.

Då ordningen av hur man exekverar skripten är av betydelse har vi en rekommenderad körordning (figur 4).

```
bash ttlDnssec.sh /usr/local/var/sverige/exjobb/result/dnscheck/ ttl
bash ttldnssecGettime.sh ttl ttltime/
bash signlife.sh /usr/local/var/sverige/exjobb/result/dnscheck/ lagra/
bash readli.sh lagra lagra2
java digParser.Startup lagra2/ temp/
bash catcherrors.sh /usr/local/var/sverige/exjobb/result/dnscheck temp
```

Figur 4 Rekommenderad körordning inklusive parametrar.

En av parametrarna som skulle undersökas var TTL på DNSKEY (DNS Public Key). Denna undersökning görs först i och med att resultatet cachas och därmed endast visar den totala TTL:en direkt efter att den har sparats i den lokala cachen. Därefter måste man invänta att TTL går ut innan man kan undersöka detta igen. Om någon då har en högt ställd TTL kan detta ta dagar eller veckor innan man kan repetera mätningen. Som alternativ till denna metod går det även att fråga auktorativa namnservrar direkt. T.ex.: *`dig dnskey uka.se @ns1.uka.se`*

[1] https://www.afnic.fr/

[2] https://github.com/dotse/zonemaster/blob/master/docs/requirements/TestRequirements.md

För att läsa TTL används följande skript i figur 5.

```
#!/bin/bash

for i in $1/* ; do
        name=${i##*/}
        if [ ”`dig +short ds $i`” ] ; then
                dig dnskey +multiline +noall +answer $name>>$2/$name
        fi
done
```

Figur 5 Skript för att kontrollera TTL på DNSKEY. (ttlDnssec.sh)

Skriptet tar 2 parametrar där den första är den mapp som innehåller resultatet från Zonemaster körningen. Detta är en lämplig mapp då den innehåller en fil för varje undersökt domän och att filnamnet är just den undersökta domänen. Den andra parametern är destinationsmappen. Där kommer en ny fil att skapas (om det inte redan finns en med det givna namnet) och resultaten kommer att skrivas in.

Kommandot *dig dnskey +multiline +noall +answer [domän]* ger ett resultat som kan se ut som i figur 6.

```
uka.se.                 3600 IN DNSKEY 256 3 7 (
                                AwEAAbV2TRMnbQOWUvj/JJ/H7ZsNZGFVXI+T9rPUpSSl
                                JtIRLCqruhY/FtKowQfgdKDK05EMG21j9io7lrRa2JbS
                                IgKx/G4gMwMx2qrQqx3EJ2ZgYe0BQYa0lcCzYndXMQHN
                                sRnzG7pB7kbDSxVYH5znO/cG5wM2IhuK974jz8yJfVQ9
                                ) ; ZSK; alg = NSEC3RSASHA1; key id = 10608
uka.se.                 3600 IN DNSKEY 257 3 7 (
                                AwEAAbzTw4FTAFd1POtSKkZaWmBOErj7O5T2A9gM0xVd
                                2nnzCI1gRf33/8mvnNcPkOyeRrFWpR5uBhzJt3z0U+r2
                                sntInmHh+6UfQn0VXNpvFAyr2fg+ggatYuxDuCrhnHJ7
                                RUtd5+XADLe6OX8HMwyPoQ42ZSv8/ZWcTtvRpatrzH33
                                eN9WFPeros+3zcwFZhdpWnl05ASlLysICmTJh89LUtGL
                                IpKPKqg5Uzhy4f1F9FYGixX2pm8CPzhU6fNpzL5mhAmV
                                VYkupFMbqlaIEbz5RdZT1qKP9/ZYVK5Y4htvj621hLMe
                                Plsx8y2CqwFAYyQo9I4lv1Q6RTFZ8EcQwRqRMl0=
                                ) ; KSK; alg = NSEC3RSASHA1; key id = 24466
```

Figur 6 Exempel på dig dnskey för utläsning av TTL.

Data från skriptet i figur 5 efterbehandlas sedan med skriptet i figur 7, vilket då skapar en fil med den undersökta domänen som filnamn och innehållet visar vilken nyckel som har vilken TTL.

```
#!/bin/bash

for i in $1/* ; do
   name=${i##*/}
   cat $i | while read line; do
      wordcount=1
      for word in $line; do
         if [ "$wordcount" = 2 ]; then
            if [ "`echo $word| grep ";" `" == "" ]; then
               echo $word>>$2/$name
            fi
         elif [ "$wordcount" = 3 ]; then
            if [ "`echo $word| grep "IN" `" == "" ]; then
               echo $word>>$2/$name
            fi
         fi
         wordcount=$((wordcount+1))
      done
   done
done
```

Figur 7 Efterbehandling av data från Figur 5. (ttldnssecGettime.sh)

Skriptet i figur 7 tar, precis som det ovan, 2 parametrar. Den första är mappen att läsa ifrån och den andra är destinationsmappen för det efterbehandlade resultatet.

Då skriptet i figur 7 har exekverats erhålls en fil vars innehåll ser ut som i figur 8.

```
3600
ZSK;
3600
KSK;
```

Figur 8 Exempel på efterbehandlad TTL.

När alla TTL-filer är färdigbehandlade analyseras signaturlivslängden. Skriptet i figur 9 kommer att köra DIG-kommandon där dnskey, soa, ns, mx och www för varje domän kontrolleras. Resultatet av varje kommando sparas i en temporär-fil.

```
#!/bin/bash

for i in $1/* ; do
        name=${i##*/}
        if [ "`dig +short ds $i`" ] ; then
                echo $name
                echo dnskey#####>$2/$name
                dig +dnssec dnskey $name>tmp
                cat tmp | grep "RRSIG *">>$2/$name
                echo soa#####>>$2/$name
                dig +dnssec soa $name>>tmp
                cat tmp | grep "RRSIG *">>$2/$name
                echo ns#####>>$2/$name
                dig +dnssec ns $name>tmp
                cat tmp | grep "RRSIG *">>$2/$name
                echo mx#####>>$2/$name
                dig +dnssec mx $name>tmp
                cat tmp | grep "RRSIG *">>$2/$name
                echo www#####>>$2/$name
                dig +dnssec www.$name>tmp
                cat tmp | grep "RRSIG *">>$2/$name
        fi
done
```

Figur 9 Skript med DIG-kommandon för utläsning av signaturlivslängd. (signlife.sh)

Skriptet i figur 9 tar två parametrar. Den första parametern är sökvägen till en mapp som innehåller filer vars namn är de domäner som skall undersökas. Den andra parametern är destinationsmappen där resultaten ska sparas. Exempel på hur detta ser ut finns i bilaga 4.

Nästa skript (figur 10) som används efterbehandlar den information som skriptet i figur 9 genererade. Resultatet blir en fil där parametrar har filtrerats ut för att underlätta vidare behandling.

```
#!/bin/bash

for i in $1/* ; do
   name=${i##*/}
   cat $i | while read line; do
      wordcount=1
      res=0
      str='RRSIG'
      for word in $line; do
         if [ "$wordcount" = 4 ]; then
            if [ "$word" = "$str" ]; then
               res=1
            fi
         elif [ "$wordcount" = 1 ]; then
            if [ "`echo $word| grep "#####" `" != "" ]; then
               res=1
            fi
         fi
         wordcount=$((wordcount+1))
```

```
      done
      if [ "$res" = 1 ]; then
         i=1
         for word2 in $line; do
            if [ "$i" = 1 ] || [ "$i" = 5 ] || [ "$i" = 9 ] || [ "$i" = 10 ]; then
               echo $word2>>$2/$name
            fi
            i=$((i+1))
         done
      fi
   done
done
```

Figur 10 Bash-skript för efterbehandling av resultatet från föregående skript. (readli.sh)

Precis som tidigare tar skriptet 2 parametrar där den första är mappen som innehåller filerna med data, vilka ska behandlas, och den andra är destinationsmappen där resultaten sparas. Exempel på hur detta ser ut återfinns i bilaga 5.

Steget därefter är att ett java-program (bilaga 1, bilaga 2, bilaga 3) körs. Programmet tar de filer som skriptet i figur 10 generade, går igenom informationen och beräknar hur länge de olika signaturerna är giltiga räknat i hela dagar. Informationen samlas sedan ihop och skrivs till en csv-fil. Detta program kräver att java-runtime finns installerat i systemet och det tar 2 parametrar som följer den tidigare fastslagna ordningen med mapp att läsa från först och destinationsmapp sist.

Efter att javakoden har körts får man ett resultat som exempelvis ser ut som i figur 11.

```
dnskey#####
nordanstig.se., DNSKEY, 20150625185301, 59
nordanstig.se., DNSKEY, 20150625185301, 60
soa#####
nordanstig.se., DNSKEY, 20150625185301, 60
nordanstig.se., DNSKEY, 20150625185301, 59
nordanstig.se., SOA, 20150625185301, 60
nordanstig.se., NS, 20150623185501, 60
ns1.nordanstig.se., A, 20150625185301, 60
ns#####
nordanstig.se., NS, 20150623185501, 60
ns1.nordanstig.se., A, 20150625185301, 60
mx#####
nordanstig.se., MX, 20150625185301, 60
nordanstig.se., NS, 20150623185501, 59
smtp1.interlan.se., A, 20150603143916, 40
smtp1.interlan.se., AAAA, 20150604211201, 40
ns1.nordanstig.se., A, 20150625185301, 59
www#####
www.nordanstig.se., A, 20150625185301, 59
nordanstig.se., NS, 20150623185501, 60
ns1.nordanstig.se., A, 20150625185301, 60
```

Figur 11 Exempel på data som har bearbetats av java-programmet.

Då resultatet från Zonemaster är omfattande (figur 12) och endast några rader är intressanta i varje fil, körs skriptet i figur 13. Dess syfte är att filtrera ut rader som innehåller vissa ord och spara dem i samma filer som java-koden använder.

```
/usr/local/var/sverige/exjobb/result/dnscheck$ cat nordanstig.se
0.00 nordanstig.se INFO SYSTEM GLOBAL_VERSION version=v1.0.1
0.01 nordanstig.se INFO SYSTEM CONFIG_FILE name=/usr/local/share/perl/5.18.2/auto/share/dist/Zonemaster/config.json
0.01 nordanstig.se INFO SYSTEM POLICY_FILE name=/usr/local/share/perl/5.18.2/auto/share/dist/Zonemaster/policy.json
1.07 nordanstig.se INFO BASIC PARENT_REPLIES parent=se
1.07 nordanstig.se INFO BASIC HAS_GLUE ns=ns1.nordanstig.se.,ns2.gavlenet.com., parent=se
1.82 nordanstig.se INFO BASIC IPV4_ENABLED ns=ns1.nordanstig.se/195.22.88.12, type=NS
1.84 nordanstig.se INFO BASIC HAS_NAMESERVERS ns=ns1.nordanstig.se.,ns2.gavlenet.com.,
source=ns1.nordanstig.se/195.22.88.12
1.84 nordanstig.se INFO BASIC IPV6_ENABLED ns=ns2.gavlenet.com/2001:b48::5, type=NS
```

```
1.84 nordanstig.se INFO BASIC HAS_NAMESERVERS ns=ns1.nordanstig.se.,ns2.gavlenet.com.,
source=ns2.gavlenet.com/2001:b48::5
1.84 nordanstig.se INFO BASIC IPV4_ENABLED ns=ns2.gavlenet.com/213.141.64.5, type=NS
1.85 nordanstig.se INFO BASIC HAS_NAMESERVERS ns=ns1.nordanstig.se.,ns2.gavlenet.com.,
source=ns2.gavlenet.com/213.141.64.5
1.85 nordanstig.se INFO BASIC HAS_NAMESERVER_NO_WWW_A_TEST name=nordanstig.se
2.21 nordanstig.se INFO ADDRESS NO_IP_PRIVATE_NETWORK
5.23 nordanstig.se INFO ADDRESS NAMESERVERS_IP_WITH_REVERSE
5.23 nordanstig.se INFO ADDRESS NAMESERVER_IP_PTR_MATCH
5.25 nordanstig.se INFO CONNECTIVITY NAMESERVER_HAS_UDP_53 address=195.22.88.12, ns=ns1.nordanstig.se
5.25 nordanstig.se INFO CONNECTIVITY NAMESERVER_HAS_UDP_53 address=2001:b48::5, ns=ns2.gavlenet.com
5.25 nordanstig.se INFO CONNECTIVITY NAMESERVER_HAS_UDP_53 address=213.141.64.5, ns=ns2.gavlenet.com
5.28 nordanstig.se INFO CONNECTIVITY NAMESERVER_HAS_TCP_53 address=195.22.88.12, ns=ns1.nordanstig.se
5.28 nordanstig.se INFO CONNECTIVITY NAMESERVER_HAS_TCP_53 address=2001:b48::5, ns=ns2.gavlenet.com
5.30 nordanstig.se INFO CONNECTIVITY NAMESERVER_HAS_TCP_53 address=213.141.64.5, ns=ns2.gavlenet.com
7.98 nordanstig.se INFO CONNECTIVITY IPV4_ASN asn=3292,16117
7.98 nordanstig.se INFO CONNECTIVITY IPV6_ASN asn=16117
7.98 nordanstig.se WARNING CONNECTIVITY NAMESERVERS_IPV6_WITH_UNIQ_AS asn=16117
7.98 nordanstig.se INFO CONNECTIVITY NAMESERVERS_WITH_MULTIPLE_AS asn=3292;16117
7.99 nordanstig.se INFO CONSISTENCY ONE_SOA_SERIAL serial=2015042601
7.99 nordanstig.se INFO CONSISTENCY ONE_SOA_RNAME rname=registry.it.nordanstig.se.
7.99 nordanstig.se INFO CONSISTENCY ONE_SOA_TIME_PARAMETER_SET expire=3628800, minimum=86400, refresh=28800,
retry=3600
7.99 nordanstig.se INFO CONSISTENCY ONE_NS_SET nsset=ns1.nordanstig.se.,ns2.gavlenet.com.
8.01 nordanstig.se INFO DNSSEC DS_FOUND keytags=12876
8.02 nordanstig.se INFO DNSSEC COMMON_KEYTAGS keytags=12876
8.02 nordanstig.se INFO DNSSEC DS_MATCHES_DNSKEY keytag=12876
8.02 nordanstig.se INFO DNSSEC DS_MATCH_FOUND
8.06 nordanstig.se INFO DNSSEC ALGORITHM_OK algorithm=8, description=RSA/SHA-256, keytag=12876
8.06 nordanstig.se INFO DNSSEC ALGORITHM_OK algorithm=8, description=RSA/SHA-256, keytag=63266
8.09 nordanstig.se INFO DNSSEC HAS_NSEC3
8.10 nordanstig.se INFO DNSSEC DELEGATION_SIGNED keytag=12876
8.10 nordanstig.se INFO DELEGATION ENOUGH_NS_GLUE count=2, glue=ns1.nordanstig.se;ns2.gavlenet.com, minimum=2
8.10 nordanstig.se INFO DELEGATION ENOUGH_NS count=2, minimum=2, ns=ns2.gavlenet.com;ns1.nordanstig.se
8.11 nordanstig.se INFO DELEGATION ENOUGH_NS_TOTAL count=2, minimum=2, ns=ns1.nordanstig.se;ns2.gavlenet.com
8.11 nordanstig.se INFO DELEGATION DISTINCT_IP_ADDRESS
8.13 nordanstig.se INFO DELEGATION ARE_AUTHORITATIVE
8.19 nordanstig.se INFO DELEGATION NS_RR_NO_CNAME
8.19 nordanstig.se INFO DELEGATION SOA_EXISTS
8.20 nordanstig.se INFO DELEGATION NAMES_MATCH names=ns1.nordanstig.se;ns2.gavlenet.com
8.20 nordanstig.se INFO SYSTEM POLICY_DISABLED name=Example
8.22 nordanstig.se INFO NAMESERVER NO_RECURSOR names=ns1.nordanstig.se,ns2.gavlenet.com
8.24 nordanstig.se INFO NAMESERVER EDNS0_SUPPORT
names=ns1.nordanstig.se/195.22.88.12,ns2.gavlenet.com/2001:b48::5,ns2.gavlenet.com/213.141.64.5
8.27 nordanstig.se INFO NAMESERVER AXFR_FAILURE address=195.22.88.12, ns=ns1.nordanstig.se
8.28 nordanstig.se INFO NAMESERVER AXFR_FAILURE address=2001:b48::5, ns=ns2.gavlenet.com
8.29 nordanstig.se INFO NAMESERVER AXFR_FAILURE address=213.141.64.5, ns=ns2.gavlenet.com
8.29 nordanstig.se INFO NAMESERVER SAME_SOURCE_IP
names=ns2.gavlenet.com/213.141.64.5,ns1.nordanstig.se/195.22.88.12,ns2.gavlenet.com/2001:b48::5
8.31 nordanstig.se INFO NAMESERVER AAAA_WELL_PROCESSED
names=ns2.gavlenet.com/213.141.64.5,ns1.nordanstig.se/195.22.88.12,ns2.gavlenet.com/2001:b48::5
8.31 nordanstig.se INFO NAMESERVER CAN_BE_RESOLVED
8.31 nordanstig.se INFO SYNTAX ONLY_ALLOWED_CHARS name=nordanstig.se
8.31 nordanstig.se INFO SYNTAX NO_ENDING_HYPHENS name=nordanstig.se
8.31 nordanstig.se INFO SYNTAX NO_DOUBLE_DASH name=nordanstig.se
8.31 nordanstig.se INFO SYNTAX NAMESERVER_SYNTAX_OK name=ns1.nordanstig.se
8.31 nordanstig.se INFO SYNTAX NAMESERVER_SYNTAX_OK name=ns2.gavlenet.com
8.31 nordanstig.se INFO SYNTAX RNAME_NO_AT_SIGN rname=registry.it.nordanstig.se.
8.32 nordanstig.se INFO SYNTAX RNAME_RFC822_VALID rname=registry@it.nordanstig.se
8.32 nordanstig.se INFO SYNTAX MNAME_SYNTAX_OK name=ns1.nordanstig.se
8.33 nordanstig.se INFO SYNTAX MX_SYNTAX_OK name=smtp1.interlan.se
8.45 nordanstig.se INFO ZONE MNAME_IS_AUTHORITATIVE mname=ns1.nordanstig.se, zone=nordanstig.se
8.46 nordanstig.se INFO ZONE REFRESH_MINIMUM_VALUE_OK refresh=28800, required_refresh=14400
8.46 nordanstig.se INFO ZONE REFRESH_HIGHER_THAN_RETRY refresh=28800, retry=3600
8.46 nordanstig.se INFO ZONE EXPIRE_MINIMUM_VALUE_OK expire=3628800, required_expire=604800
8.46 nordanstig.se INFO ZONE SOA_DEFAULT_TTL_MAXIMUM_VALUE_OK highest_minimum=86400, lowest_minimum=300,
minimum=86400
8.54 nordanstig.se INFO ZONE MNAME_IS_NOT_CNAME mname=ns1.nordanstig.se
8.60 nordanstig.se INFO ZONE MNAME_IS_NOT_CNAME mname=ns1.nordanstig.se
8.61 nordanstig.se INFO ZONE MX_RECORD_EXISTS info=MX=smtp1.interlan.se
```

Figur 12 Exempel på Zonemaster resultat.

Det som skriptet i figur 13 filtrerar ut är rader som innehåller orden ERROR, WARNING, CRITICAL och NOTICE, vilka alla är etiketter som Zonemaster använder i analysen av domänerna. Dessutom filtreras de rader som innehåller information om vilka AS (Autonomt System)-nummer den undersökta domänen har.

```
#!/bin/bash

for i in $1/* ; do
        name=${i##*/}
        echo $name
        cat $i | grep -i "ERROR *">>$2/$name
        cat $i | grep -i "WARNING *">>$2/$name
        cat $i | grep -i "CRITICAL *">>$2/$name
        cat $i | grep -i "NOTICE *">>$2/$name
        cat $i | grep "IPV4_ASN *">>$2/$name
        cat $i | grep "IPV6_ASN *">>$2/$name
done
```

Figur 13 Skript för att filtrera rådata från Zonemaster. (catcherrors.sh)

Resultatet av all denna databehandling ser ut som exemplet i figur 14.

```
7.98 nordanstig.se WARNING CONNECTIVITY
NAMESERVERS_IPV6_WITH_UNIQ_AS asn=16117
7.98 nordanstig.se INFO CONNECTIVITY IPV4_ASN asn=3292,16117
7.98 nordanstig.se INFO CONNECTIVITY IPV6_ASN asn=16117
```

Figur 14 Exempel på efterbehandlad data.

Resultaten från Zonemaster innehåller också information om så väl vilka DNS-servrar som är kopplade mot en domän som vilka e-postservrar som används. Båda dessa kan undersökas genom att skriva *`dig uka.se.`* Kommandot ovan ger ett resultat som kan ses i figur 15.

```
; <<>> DiG 9.9.5-3ubuntu0.2-Ubuntu <<>> uka.se
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32311
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;uka.se.                                IN      A

;; ANSWER SECTION:
uka.se.                 900     IN      A       212.85.68.108

;; Query time: 28 msec
;; SERVER: 213.141.64.2#53(213.141.64.2)
;; WHEN: Sat May 16 15:18:00 CEST 2015
;; MSG SIZE  rcvd: 51
```

Figur 15 Exempel på undersökning av en domäns IP-adress.

Om man sedan använder en whois-tjänst, eller som i figur 16 ett program som vanligtvis ingår i en linux-distribution, på den IP-adress som erhålls i resultatet från figur 15 kan man bland annat utläsa i vilket land som denna IP-adress är registrerad.

```
exjobb@exjobb:~$ whois 212.85.68.108
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '212.85.68.64 - 212.85.68.127'

% Abuse contact for '212.85.68.64 - 212.85.68.127' is 'abuse@bahnhof.net'

inetnum:        212.85.68.64 - 212.85.68.127
netname:        RID-0000190646
descr:          RID-0000190646
country:        SE
admin-c:        BD856-RIPE
tech-c:         BD856-RIPE
status:         ASSIGNED PA
mnt-by:         BAHNHOF-NCC
created:        2012-02-14T14:53:06Z
last-modified:  2012-02-14T14:53:06Z
source:         RIPE # Filtered

role:           Bahnhof DBM
address:        Bahnhof AB
address:        Isafjordsgatan 32B
address:        164 40 Kista
address:        Sweden
admin-c:        BD856-RIPE
tech-c:         BD856-RIPE
nic-hdl:        BD856-RIPE
```

```
mnt-by:          BAHNHOF-NCC
created:         2004-03-01T23:41:37Z
last-modified:   2012-08-16T09:14:55Z
source:          RIPE # Filtered

% Information related to '212.85.64.0/19AS8473'

route:           212.85.64.0/19
descr:           Bahnhof AB
origin:          AS8473
mnt-by:          BAHNHOF-NCC
created:         2006-01-13T16:10:18Z
last-modified:   2006-01-13T16:11:34Z
source:          RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.79.2 (DB-2)
```

Figur 16 Exempel på uppslagning av en IP-adress med whois.

I det första stycket med data kan man utläsa vart denna IP-adress finns på raden *`country: SE`*.

Motsvarande operationer kan utföras på de domännamn som finns för e-postservrarna.

2.3 Undersökta domäner

För att få en något så när hanterlig mängd med data har vi avgränsat antalet domäner som undersöks. Avgränsningen baseras på den geografiska placeringen av kommunen (Gävleborgs län) och utvalda myndigheter. Mediabolagen har avgränsats med avseende på närvaro i Gävleborgs län men också de rikstäckande Sveriges television, Sveriges radio och tv4 inkluderades. Dessa har delats in i några grupper, vilka presenteras nedan.

I tabell 1 finns de kommuner som ingår i Gävleborgs län.

Tabell 1 Kommuner i Gävleborgs län.

bollnas.se	hudiksvall.se	ockelbo.se	soderhamn.se
gavle.se	ljusdal.se	ovanaker.se	
hofors.se	nordanstig.se	sandviken.se	

tabell 2 innehåller landsting och de myndigheter som vi har valt att undersöka.

Tabell 2 Landsting och myndigheter.

aklagare.se	forsvarsmakten.se	pliktverket.se	riksdagen.se
arbetsformedlingen.se	lansstyrelsen.se	polisen.se	skatteverket.se
csn.se	lantmateriet.se	regeringen.se	smhi.se
datainspektionen.se	lg.se	regiongavleborg.se	socialstyrelsen.se
forsakringskassan.se	msb.se	riksbank.se	uka.se

De utvalda mediabolagen redovisas i tabell 3.

Tabell 3 Mediabolag.

arbetarbladet.se	helahalsingland.se	svt.se
gd.se	sr.se	tv4.se

3. Resultat

Vi har valt att dela in de undersökta domänerna i olika grupper baserat på utfallet av resultaten från de skript som har körts i metod-delen.

3.1 Domäner som saknar DNSSEC

Domänerna i tabell 4 har inte implementerat DNSSEC.

Tabell 4 Domäner utan DNSSEC.

aklagare.se	arbetarbladet.se	gd.se
helahalsingland.se	polisen.se	riksbank.se
sr.se	svt.se	tv4.se

3.2 Domäner som har implementerat DNSSEC men har problem

Domänerna i tabell 5 har en DNSSEC implementation men resultatet från Zonemaster-analysen visar på flera fel och eller varningar.

Tabell 5 Domäner med DNSSEC och fel/varningar.

csn.se	datainspektionen.se	forsakringskassan.se	hofors.se
lantmateriet.se	lg.se	ljusdal.se	msb.se
nordanstig.se	pliktverket.se	regeringen.se	regiongavleborg.se
riksdagen.se	socialstyrelsen.se	uka.se	

3.3 Domäner med väl implementerad DNSSEC

De domäner som listas i tabell 6 har en väl fungerande implementation av DNSSEC.

Tabell 6 Domäner med DNSSEC.

arbetsformedlingen.se	bollnas.se	forsvarsmakten.se	gavle.se
hudiksvall.se	lansstyrelsen.se	ockelbo.se	ovanaker.se
sandviken.se	skatteverket.se	smhi.se	soderhamn.se

3.4 TTL på DNSKEY

TTL:en för de nycklar som lagras i cache för de domäner som har implementerat DNSSEC redovisas i sin helhet i bilaga 10. Både Zone-Signing-Key och Key-Signing-Key kontrolleras samt hur många poster som varje typ av signatur har. De flesta följer rekommendationen på 3600 sekunder [16]. 7st domäner har en för högt ställd TTL. En domän har sin TTL för lågt ställd.

3.5 Signaturlivslängd

Den rekommenderade signaturlivslängden är enligt .SE 32 dagar [17]. Av de undersökta domänerna är det endast ett fåtal som uppfyller de givna rekommendationerna. De flesta domäner antingen överstiger eller understiger den tid som förordas kraftigt (bilaga 7).

3.6 Geografisk placering av DNS-servrar

De flesta av de undersökta domänerna har sin drift av DNS-servrar i landet. Dock har några valt att låta utländska leverantörer av DNS-tjänster sköta deras drift (bilaga 8).

3.7 Geografisk placering av e-posttjänster

Av de IP-adresser till e-postservrar som gått att få fram i undersökningen finns alla utom en i Sverige (bilaga 9). Många av domänerna har av servernamnet att döma en egen drift av e-post tjänster. 14 av de 36 undersökta domänerna har en extern leverantör inblandad i sin e-post-hantering.

3.8 Specifikation av fel och varningar

En analys av resultaten från Zonemaster visar att 15st av de undersökta domänerna har fel- och eller varningar i DNS-konfigurationen (bilaga 6). Dessa avvikelser kan indelas i följande kategorier:

- Endast en Internet Service Provider.
- Nameserver IP without reverse.
- No response.

Endast en Internet Service Provider innebär att domänen endast är ansluten till ett AS. Vilket i praktiken innebär att de saknar redundans vid eventuella störningar hos sin ISP.

Nameserver IP without reverse betyder att man inte har gjort sina PTR (pointer)-records tillgängliga för omvänd uppslagning, dvs. från IP-adress till domännamn.

No response uppträder i 2 varianter. Det ena fallet uppkommer när en NS (Name Server) ej svarar på UDP. Det andra fallet är NS inte svarar på TCP.

3.9 Internet Service Providers per domän

Zonemaster-data visar även information om hur många ASN som är kopplade mot de olika versionerna av Internet Protokoll. Resultaten finns i bilaga 11. En summering presenteras i tabell 7. De domäner som visas i tabellen saknar tillräcklig redundans eller saknar helt IPv6.

Tabell 7 Domäner med otillräcklig ISP-redundans.

Domän	IPv4	IPv6
arbetarbladet.se		0
csn.se	1	0
datainspektionen.se		1
gd.se		0
helahalsingland.se	1	0
lantmateriet.se		1
msb.se	1	1
nordanstig.se		1
pliktverket.se	1	1
polisen.se		1
regeringen.se	1	1
riksbanken.se	1	1
soderhamn.se		0
svt.se	1	1
uka.se	1	1

De fält som inte innehåller någon data skall utläsas som att det åtminstone finns två ISP:er där.

3.10 Sammanfattning av domänernas tillstånd

I tabell 8 ges en sammanfattning där de röd-färgade domänerna helt saknar DNSSEC. De gröna har inte bara implementerat DNSSEC utan har också en korrekt konfiguration. Vad gäller kolumnen med TTL bedöms 3600 sekunder eller mindre som ett bra resultat. För signaturer är bedömningen att de som har 30 dagar eller mer är acceptabla.

Tabell 8 Sammanfattning av status.

Domän	DNSSEC	Fel	Varningar	TTL	Signatur
aklagare.se					
arbetarbladet.se					
arbetsformedlingen.se	X			Ok	Fel
bollnas.se	X			Ok	Ok
csn.se			X	Fel	Fel
datainspektionen.se	X		X	Ok	Fel
forsakringskassan.se	X		X	Fel	Fel
forsvarsmakten.se	X			Ok	Ok
gavle.se	X			Ok	Ok
gd.se					
helahalsingland.se					
hofors.se	X	X	X	Ok	Ok
hudiksvall.se	X			Ok	Ok
lansstyrelsen.se	X			Ok	Fel
lantmateriet.se	X		X	Fel	Ok
lg.se	X		X	Ok	Ok
ljusdal.se	X	X	X	Ok	Ok
msb.se	X		X	Ok	Ok
nordanstig.se	X		X	Ok	Ok
ockelbo.se	X			Ok	Ok
ovanaker.se	X			Ok	Ok
pliktverket.se	X		X	Ok	Fel
polisen.se					
regeringen.se	X		X	Ok	Ok
regiongavleborg.se	X		X	Ok	Ok
riksbank.se					
riksdagen.se	X		X	Fel	Fel
sandviken.se	X			Ok	Ok
skatteverket.se	X			Fel	Fel
smhi.se	X			Fel	Fel
socialstyrelsen.se	X	X	X	Fel	Fel
soderhamn.se	X			Ok	Fel
sr.se					
svt.se					
tv4.se					
uka.se	X		X	Ok	Fel

4. Diskussion och slutsatser

De slutsatser vi har dragit vad gäller DNSSEC och dess implementation hos de undersökta organisationerna är baserat på RFC6781 [18] och på rekommendationerna i dokumentet - DNSSEC Säkerhetsdeklaration (DPS) .se [16]. Detta dokument är framtaget av Stiftelsen för internetinfrastruktur vilka ansvarar för toppdomänen *.se*.

Som resultaten av den undersökning vi genomfört visar, så finns det såväl myndigheter som landsting och kommuner vilka inte har tillfredställande skydd av DNS med DNSSEC.

Totalt 9st domäner saknar helt implementation av DNSSEC. Detta gör att de är mottagliga för attacker av typen DNS-cache poisoning vilket kan resultera i Denial of Service eller ännu värre - att en illasinnad aktör leder om datatrafiken till en server eller hemsida med skadligt innehåll.

Av de domäner som har väl implementerad DNSSEC enligt Zonemaster så finns det ändå en del övrigt att anmärka på. Som ett exempel så har domänen smhi.se en TTL på 2 dagar där rekommendationen är 1 timme. Även giltighetstiden på dess signaturer avviker kraftigt från de givna rekommendationerna.

Kommunerna i Gävleborgs län har överlag en god implementation av DNSSEC. När studien genomfördes hade 7 av 10 kommuner väl implementerad DNSSEC. Vill man få en överblicksbild av hur läget ser ut avseende DNSSEC och IPv6 kan man besöka sidan *kommunermedipv6.se*[3]. Där går att se en karta över Sverige med färgkodad status över alla kommuner och dess DNSSEC och IPv6 status. Som ett exempel kan det nämnas att ingen av Örebro läns 11 kommuner har tillfredställande implementationer av DNSSEC.

Några av de domäner som har fel/varningar enligt Zonemaster-resultaten har fått denna varning pga. de endast har ett AS-nummer knytet mot sig. Konsekvensen av detta är att man gör sig känslig för störningar hos sin ISP om man inte ser till att ha redundans i systemet. Dock går det inte att säga att de som har fler AS-nummer per automatik inte har ett inbördes beroende. Detta skulle kräva omfattande analys av det data som återfinns i bilaga 11 vilket faller utanför tidsramarna för detta examensarbete.

Analysen av antal ISP:er (tabell 7) visar att det finns myndigheter som endast är nåbara via IPv4. Enligt regeringens digitala agenda är rekommendationen att alla myndigheter bör gå att nå via IPv6 senast under 2013 [2].

Andra fel som framkommit är att det inte går att kommunicera med servrarna via UDP/TCP. I det fall där det endast är UDP eller TCP som inte svarar kan det sannolikt röra sig om en felkonfigurering eller ett temporärt fel under testperioden. När servern inte svarar på vare sig UDP eller TCP bör man kunna anta att servern inte är operativ. Konsekvensen av att en DNS-server inte svarar är dock inte så allvarlig under förutsättning att domänen har flera servrar. Då kommer användaren endast att uppleva en kortare fördröjning innan uppslagningen utförs, i och med att en av de andra servrarna kontaktas, och därefter kan sidan laddas.

Ett annat fel som ett fåtal av de undersökta domänerna hade var att de inte hade gjort sina PTR-records tillgängliga för DNS vilket resulterade i

[3] http://www.kommunermedipv6.se/maps.php

felet - `Name Server IP without reverse`. Vissa ISP:er kräver att det är möjligt att göra en omvänd DNS-uppslagning mot domänen för att på så sätt minska risken för spam [19]. En omvänd DNS-uppslagning (DNS reverse) är till skillnad mot en standard DNS-uppslagning (forward DNS) en procedur där IP-adressen översätts till ett FQDN.

Den geografiska placeringen av DNS-servrar är av betydelse för domänens tillgänglighet. Har man dessa servrar placerade på olika platser så minskar risken för att domänen skulle bli otillgänglig vid bortfall av en DNS-server eller störningar hos en ISP. Man bör även ta i beaktande var någonstans i världen leverantören av DNS-tjänsten har sina servrar. En betydande del av de undersökta domänerna har sina servrar placerade i Sverige. En tredjedel av domänerna har åtminstone en server placerad utanför Sverige.

Man kan dock inte likställa att en IP-adress till ett land verkligen innebär att en server är fysiskt placerad på platsen som är kopplad mot IP-adressen. Detta beror på att det är vanligt förekommande med s.k. Anycast-cluster, vilket innebär att de fysiska servrarna kan finns utspridda över världen men är kopplade mot samma IP-adress.

Det visar sig att två av de kanske mest betydande myndigheterna med samhällsviktig funktion, *regeringen.se* och *msb.se* (Myndigheten för Samhällsskydd och Beredskap) har sina DNS-servrar hos ett företag i USA vilket även innebär att de lyder under amerikansk lagstiftning. Detta företag nyttjar sig av Anycast vilket innebär att servrarna som används inte är placerade endast i USA. Dock är ingen av servrarna placerade i Sverige. Det medför att dessa myndigheter inte har någon egen DNS-infrastruktur inom landets gränser vilket gör det svårt att se hur tillgängligheten till dessa domäner skall kunna säkras i händelse av kris eller ofred. Dessa DNS:er är signerade med DNSSEC vilket betyder att en privat nyckel måste finnas hos företaget som tillhandahåller DNS-tjänsten. Om dessa nycklar förvaras hos främmande makt och obehöriga aktörer får tillgång till nycklarna kan manipulation och förfalskning av DNS-data ske vilket måste betraktas som mycket allvarligt.

De senaste åren har det framkommit en hel del avslöjanden om olika säkerhetstjänsters övervakning av kommunikation. Faktumet att ett antal av Sveriges viktigaste myndigheter har sina DNS-servrar placerade hos en leverantör utomlands borde inte göra uppgiften att avlyssna och övervaka trafiken över dessa direkt svårare.

Beträffande e-post-servrarnas placering så har alla utav de undersökta organisationerna utom en sina mx-tjänster placerade i Sverige. Dock har 14st mx-tjänster som tillhandahålls av extern leverantör. Resterande sköts sannolikt av organisationen självt. Ur ett konfidentiellitets- och integritets-perspektiv är externa leverantörer en potentiell säkerhetsrisk. Man får anta att kontrakt styr hur data ska/får behandlas av leverantören men det är svårt att veta hur t.ex. kvalitetssäkringen av deras personal genomförs. Därmed blir det problematiskt att garantera sitt datas säkerhet. Beroende på hur routingprocessen utförs finns dessutom ingen som helst garanti för att e-post som skickas från en server i landet till en annan server som också befinner sig i samma land inte passerar landets gränser när data routas vidare mot sin destination.

Ett scenario det går att dra paralleller till när det gäller bortfall av DNS var när ett datavirus drabbade Region Skånes regionala nät Skånet [20]. Vid angreppstillfället bestod nätet av ca 21000 arbetsstationer för administrativa ändamål och ca 1300 servrar/kluster. Utöver detta tillkom 3-4000 datorer i medicintekniska produkter och av forskare anslutna

datorer. Effekterna av denna virusattack var liknande de effekter man skulle uppleva vid ett bortfall av DNS. Exempelvis inloggningsproblem, begränsad eller obefintlig tillgång till system, problem med uppkoppling till e-post och internet. En allvarlig incident under perioden var att en medicinteknisk dator blockerades under pågående behandling av en patient vilket turligt nog inte skedde i ett kritiskt skede av behandlingen, vilket om så hade skett skulle ha medfört stor risk för allvarlig skada på patienten.

Detta är ju naturligtvis konsekvenser man borde försöka undvika i största möjliga utsträckning. Om DNS signeras med DNSSEC minskar risken betydligt för man-in-the-middle attacker, t.ex. cache-poisoning och därmed har man ett avsevärt säkrare och robustare DNS. På så sätt kan incidenter som den som beskrivs ovan undvikas eller i alla fall få ett begränsat genomslag.

För att kunna verifiera RRSIG används DNSKEY. Dessa publika nycklar cachas och har därmed ett TTL-värde. Enligt rekommendation ska detta vara satt till 1 timme (3600 sekunder) [17]. Problem som kan uppstå med för lågt ställd TTL blir att belastningen på servern ökar då fler förfrågningar görs. Detta kan eventuellt vara att föredra, i alla fall i jämförelse med att ha den satt till ett betydligt högre värde. När TTL är satt till ett högt värde, vissa av de undersöka domänerna har 2 dagar (172800 sekunder), så finns en betydande risk att ett nyckelbyte kommer resultera i att tjänsten ej kan nås inom rimlig tid. Ponera att Försäkringskassan försvinner från internet i två dagar kontra en timme. Detta skulle medföra att en myndighets e-tjänster och information skulle vara otillgängligt för besökare under en oacceptabelt lång tid och förmodligen även påverka allmänhetens uppfattning och förtroende för myndigheten på ett negativt sätt. Eftersom att nycklar måste bytas med jämna mellanrum är det viktigt att påverkan på tillgänglighet när ett nyckelbyte sker är så låg som möjligt [18]. Tiden på TTL som rekommenderas i säkerhetsdeklarationen gör att ett bortfall pga. nyckelbyte hålls på en rimlig nivå.

En nackdel med DNSSEC är att det kan förstärka effekten av DDoS (Distributed Denial of Service)-attacker i och med att ett svar signerat med DNSSEC är betydligt större än svaret från en vanlig DNS-uppslagning [6]. DNSSEC gör heller inget för att skydda innehållet i ett DNS-svar utan garanterar bara att det kommer från rätt källa. Dessa faktum är dock ingenting som har behandlats i denna studie men kan vara intressant att nämna ur säkerhetssynpunkt.

Utifrån detta har vi dragit följande slutsatser. DNS är en vital komponent i internetinfrastrukturen och i behov av adekvat skydd. Ett felaktigt konfigurerat DNS och avsaknad av DNSSEC, eller ett DNSSEC som inte är konfigurerat enligt rekommendationerna är att bädda för problem. DNS är i sin ursprungliga form väldigt enkelt att genomföra attacker mot. DNSSEC tillför gott skydd mot cache-poisoning vilket är en allvarlig attack mot DNS som kan ställa till med allvarliga problem och bör undvikas i största möjliga mån. Därför är det viktigt att man ser till att ha sin domän signerad med DNSSEC samt att det har konfigurerats korrekt i enlighet med rekommendationerna i säkerhetsdeklarationen.

Internet har blivit en på många vis integrerad del av vårt samhälle vilket gör det naturligt för kommuner och myndigheter att ha ambitionen att vara nåbara över detta medium. Att inte kunna komma åt en önskad tjänst hos en myndighet eller kommun är naturligtvis inte lika allvarligt som att en patients säkerhet äventyras som i det tidigare beskrivna scenariot, men är likväl en konsekvens av att DNS inte är tillgängligt. Att

för en myndighet eller kommun säkerställa en robust internetinfrastruktur bör vara av hög prioritet.

En sammanfattning av resultaten från de undersökta domänerna visar att mediabolagen helt har ignorerat hotet mot DNS. Av myndigheterna har flertalet infört DNSSEC och även korrekt konfigurerat detta. Det finns dock ett antal avvikelser som bör åtgärdas. Kommunerna är de som ligger bäst till både med avseende på implementation och konfiguration av DNSSEC. Endast ett fåtal anmärkningar finns där och de berör brister kring IPv6, AS och placering av e-posttjänster.

Ordförklaringar

AS (Autonoma system). Term för nätverk som kommunicerar med andra nätverk, kan likställas med ISP.

DDoS (Distributed Denial of Service) – en överbelastningsattack där många källor attackerar ett givet mål simultant.

DS (Delegation signer) – används till att autentisera DNSKEY. DS lagras på en högre nivå i hierarkin (parent) än DNSKEY.

DNSKEY (DNS public key) – ett RR som lagrar zonens publika nyckel, båda ZSK och KSK kan lagras.

Domän – en logisk instans i domännamnshierarkin.

Domännamn – t.ex. *hig.se*

FQDN (Fully Qualified Domain Name) t.ex. *www.hig.se*

IETF (Internet Engineering Task Force) – en organisation som arbetar med att få internet att fungera bättre ur en teknisk synvinkel.

IP (Internet Protocol) – ett protokoll för informationsöverföring på internet.

IPv4 – Internet Protocol version 4 (32 bitars adresslängd).

IPv6 – Internet Protocol version 6 (128 bitars adresslängd).

ISP (Internet Service Provider) – leverantör av anslutning mot internet.

KSK (Key-Signing key) – används i DNSSEC till att signera ZSK.

NS (Nameserver) – en server som innehåller DNS-data.

MX (Mail Exchange) - översätter FQDN till IP-adresser för e-post system.

NAT (Network Address Translation) – Möjliggör delning av externa IP-adress inom ett lokalt nätverk.

NSEC (Next secure) – innehåller en länk till nästa RR.

Resolver – är den del av DNS-systemet som praktiskt sköter om namnuppslagningen dvs. den letar i sin cache och om svaret ej finns där gör uppslagning mot de auktoritativa namnservrarna.

RR (Resource record) – den post i en zone-file som innehåller DNS-data.

RRSIG (Resource record signature) – används till att autentisera att ett RR kommer från en given källa.

SOA (Start Of Authority) – en post som innehåller information om en zon t.ex. kontaktuppgifter till zonansvarig, versionsnummer och zone-timers.

TCP (Transmission Control Protocol) – förbindelseorienterat dataöverföringsprotokoll för internetkommunikation.

TTL (Time-To-Live) - en term som används då man inom it och datorkommunikation ska ha en tidsbegränsning av något slag. Vanliga

användningsområden är att begränsa antalet hopp som ett IP-paket kan göra innan det kastas eller en giltighetsperiod mätt i lämplig tidsenhet. I denna rapport avser TTL hur länge ett RR cachas hos en resolver.

TLD (Top-Level Domain) – steget under rot-servrarna. Är indelat i 2 kategorier, landskoder som .se, .uk, .dk, .jp, och generiska koder som .com, .net, .org, .edu.

UDP (User Datagram Protocol) – förbindelselöst dataöverföringsprotokoll.

URL (Uniform Resource Locator) – webbadress.

whois – tjänst som används till att ta reda på ägare till IP-adressrymder eller domännamn.

Zon – en administrativ instans. En zon kan delegera ansvaret vidare till underdomäner, vilka då blir egna zoner som får ansvara för att svara på förfrågningar kring deras innehåll eller i sin tur delegera ansvaret vidare.

Zone-file – data för en given zon. Innehåller mappning mellan IP-adresser och domännamn samt eventuella delegeringar.

ZSK (Zone-Signing key) – används i DNSSEC till att signera underliggande zoner samt RRSIG för MX, NS, SOA och www. ZSK signeras med KSK.

Referenser

[1] A. Rafting. (2011). *Robust elektronisk kommunikation - vägledning för anskaffning*. Available: http://www.pts.se/upload/Rapporter/Internet/2011/V%C3%A4gledning%20f%C3%B6r%20%20anskaffning%20av%20robust%20elektronisk%20kommunikation_110823.pdf.
[2] Näringsdepartementet. (2011). *It i människans tjänst - en digital agenda för Sverige*. Available: http://www.regeringen.se/sb/d/14216/a/177256.
[3] P. Mockapetris. (1987, Nov 01). [DOMAIN NAMES - CONCEPTS AND FACILITIES]. Available: http://tools.ietf.org/html/rfc1034.
[4] J. Abley and K. Lindqvist. (2006). *Operation of Anycast Services*. Available: https://tools.ietf.org/html/rfc4786.
[5] A. Friedlander, A. Mankin, W. D. Maughan and S. D. Crocker, "DNSSEC: A Protocol Toward Securing the Internet Infrastructure," *Commun ACM,* vol. 50, pp. 44-50, jun, 2007.
[6] D. Atkins, IHTFP Consulting, R. Austein and ISC. (2004, August). *Threat Analysis of the Domain Name System (DNS)*. Available: http://tools.ietf.org/html/rfc3833.
[7] R. Arends, T. Instituut., R. Austein, ISC., M. Larson, VeriSign., D. Massey, C. S. University., S. Rose and NIST. (2005). *DNS Security Introduction and Requirements*. Available: http://tools.ietf.org/html/rfc4033.
[8] N. Alexiou, S. Basagiannis, P. Katsaros, T. Dashpande and S. A. Smolka, "Formal analysis of the kaminsky DNS cache-poisoning attack using probabilistic model checking," in *Proceedings of the 2010 IEEE 12th International Symposium on High-Assurance Systems Engineering,* 2010, pp. 94-103.
[9] D. Eastlake and C. Kaufman. (1997). *Domain Name System Security Extensions*. Available: https://tools.ietf.org/html/rfc2065.
[10] L. Yuan, C. Chen, P. Mohapatra, C. Chuah and K. Kant, "A Proxy View of Quality of Domain Name Service, Poisoning Attacks and Survival Strategies," *ACM Trans.Internet Technol.,* vol. 12, pp. 9:1-9:26, may, 2013.
[11] A. Herzberg and H. Shulman, "Retrofitting Security into Network Protocols: The Case of DNSSEC," *Internet Computing, IEEE,* vol. 18, pp. 66-71, 2014.
[12] E. Osterweil, M. Ryan, D. Massey and L. Zhang, "Quantifying the operational status of the DNSSEC deployment," in *Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement,* Vouliagmeni, Greece, 2008, pp. 231-242.
[13] S. Deering and R. Hinden. (1998). *Internet Protocol, Version 6 (IPv6) Specification*. Available: https://tools.ietf.org/html/rfc2460.
[14] dotse. The zonemaster project. [https://github.com/dotse/zonemaster;]. 2015. Available: https://github.com/dotse/zonemaster.
[15] Stiftelsen för internetinfrastruktur. (2015). *.SE*. Available: https://www.iis.se/.
[16] A. Eklund Löwinder. (). *DNSSEC Säkerhetsdeklaration (DPS) .se*. Available: https://www.iis.se/docs/dnssec-dps-sv.pdf.
[17] .SE. (2014). *Recommendations for DNSSEC deployment at municipal administrations and similar organisations*. Available: https://www.iis.se/docs/Recommendations_for_DNSSEC_deployment.pdf.
[18] O. Kolkman, W. Mekking and R. Gieben. (). *DNSSEC Operational Practices, Version 2*. Available: https://tools.ietf.org/html/rfc6781.
[19] D. Senie and A. Sullivan. (). *Considerations for the use of DNS Reverse Mapping*. Available: https://tools.ietf.org/html/draft-ietf-dnsop-reverse-mapping-considerations-06.
[20] Anonymous *IT-Haverier i Vården : Erfarenheter Och Förslag Till Åtgärder Från Aktuella Fall*. Stockholm: Socialstyrelsen, 2012.

Bilagor

Bilaga 1 main-program för java-applikation.

```
package digParser;

public class Startup {

   public static void main(String[] args) {
      LogReader lr = new LogReader(args[0], args[1]);
      boolean res = lr.parseTargetFolder();
      if (res)
         System.out.println("Folder parsed Ok!");
      else
         System.out.println("Parsing failed!");
   }
}
```

Bilaga 2 Javaklass som beräknar dagar.

```
package digParser;

import java.util.Calendar;
import java.util.Date;

public class DateLoader {
   private Calendar cal;
   private String input;

   public DateLoader(String dateString) {
      this.input = dateString;
      this.cal = Calendar.getInstance();
      loadDate();
   }

   public Date getDate() {
      Date date = new Date();
      date = cal.getTime();
      return date;
   }

   private void loadDate() {
      String yearS = "";
      for (int i = 0; i < 4; i++)
         yearS += input.charAt(i);
      int year = Integer.parseInt(yearS);
      String monthS = "";
      for (int i = 4; i < 6; i++)
         monthS += input.charAt(i);
      int month = Integer.parseInt(monthS);
      String dayS = "";
      for (int i = 6; i < 8; i++)
         dayS += input.charAt(i);
      int day = Integer.parseInt(dayS);
      String hourS = "";
      for (int i = 8; i < 10; i++)
         hourS += input.charAt(i);
      int hour = Integer.parseInt(hourS);
      String minS = "";
      for (int i = 10; i < 12; i++)
         minS += input.charAt(i);
      int min = Integer.parseInt(minS);
      String secS = "";
      for (int i = 12; i < 14; i++)
         secS += input.charAt(i);
      int sec = Integer.parseInt(secS);
      cal.set(year, month, day, hour, min, sec);
   }
}
```

Bilaga 3 Javaklass som läser in datafiler.

```
package digParser;

import java.io.BufferedReader;
import java.io.File;
import java.io.FileReader;
import java.io.IOException;
import java.nio.file.Files;
import java.nio.file.Path;
import java.nio.file.Paths;
import java.nio.file.StandardOpenOption;
import java.util.Date;

public class LogReader {
   private String targetPath;
   private String destination;
   private String fileName;
   private File file;
   private Path filePath;

   public LogReader(String targetPath, String destination) {
      this.targetPath = targetPath;
      this.destination = destination;
   }

   public boolean parseTargetFolder() {
      boolean result = true;
      File path = new File(targetPath);
      if (path.exists() && path.isDirectory())
         if (new File(destination).exists() && new File(destination).isDirectory()) {
            parserMain();
         } else
            System.out.println("Destination isn't a folder! (args 1)");
      else
         System.out.println("TargetPath isn't a folder! (args 0)");
         return result;
   }

   private void parserMain() {
      File path = new File(targetPath);
      File[] listFiles = path.listFiles();
      if (listFiles != null)
         for (File file : listFiles)
            if (file.isFile()) {
               this.file = file;
               try {
                  BufferedReader reader = new BufferedReader(new FileReader(this.file));
                  String line;
                  String buildLine = "";
                  int index = 0;
                  Date date = new Date();;
                  while ((line = reader.readLine()) != null) {
                     if (line.contains("#####")) {
                        this.filePath = Paths.get(destination+File.separatorChar+file.getName());
                        createFile();
                        printToFile(line);
                     } else {
                        if (index == 0 && line != "") {
                           buildLine = line + ", ";
                           index++;
                        } else if (index == 1) {
                           buildLine += line + ", ";
                           index++;
                        } else if (index == 2) {
                           buildLine += line + ", ";
                           DateLoader dl = new DateLoader(line);
                           date = dl.getDate();
                           index++;
                        } else if (index == 3) {
                           DateLoader dl = new DateLoader(line);
                           Date oldDate = dl.getDate();
                           Long diff=(long)(date.getTime() - oldDate.getTime()) / (1000 * 3600 * 24);
                           buildLine += diff.toString();
                           index = 0;
                           printToFile(buildLine);
                        }
                     }
                  }
                  reader.close();
               } catch (IOException e) {
               } catch (IllegalArgumentException a) {}
            }
        }

   private void createFile() throws IOException {
      if (!Files.exists(filePath)) {
         Files.createFile(filePath);
      }
   }

   private void printToFile(String text) throws IOException {
      String newLine = System.getProperty("line.separator");
      text += newLine;
      Files.write(filePath, text.getBytes(), StandardOpenOption.APPEND);
   }
}
```

Bilaga 4 Exempel på utläsning av signaturlivslängd.

```
dnskey#####
uka.se.                 3596    IN      RRSIG   DNSKEY 7 2 3600 20150502100137 20150425201049 24466 uka.se.
p1bDhXea88R/+qlFFy/KYPIT/kHT8PYANV5RgkJv9+PjIsVDFwcOFy+t /H7RqnQBZEvEtKBogGfn6bV0zu0FJN2AUIex+2glLKhttSyWG0SamFGq
rP95ioKWY+3/cliDCMUMxJs/SMsC0XrHvq+3HnmmVYgg6J508WYnXumW vfINOvYBPelSQS7ZCaiDamtVpHujyyJAyRV8k9k5Mc3Y9kIINRuSRShd
bqqlA/vPJvPh7BE+QmP/KYgZfCBgHqjiUo0edz+s/xsk0NlbuGu9y41+ OH9k9gzG4blgDCMW6OIn5j58rdBBBiohhvOJ0dSQE2rvH+xgjKBnoDwm vYXU4w==
soa#####
uka.se.                 3596    IN      RRSIG   DNSKEY 7 2 3600 20150502100137 20150425201049 24466 uka.se.
p1bDhXea88R/+qlFFy/KYPIT/kHT8PYANV5RgkJv9+PjIsVDFwcOFy+t /H7RqnQBZEvEtKBogGfn6bV0zu0FJN2AUIex+2glLKhttSyWG0SamFGq
rP95ioKWY+3/cliDCMUMxJs/SMsC0XrHvq+3HnmmVYgg6J508WYnXumW vfINOvYBPelSQS7ZCaiDamtVpHujyyJAyRV8k9k5Mc3Y9kIINRuSRShd
bqqlA/vPJvPh7BE+QmP/KYgZfCBgHqjiUo0edz+s/xsk0NlbuGu9y41+ OH9k9gzG4blgDCMW6OIn5j58rdBBBiohhvOJ0dSQE2rvH+xgjKBnoDwm vYXU4w==
uka.se.                 2816    IN      RRSIG   SOA 7 2 3600 20150504021527 20150427041120 10608 uka.se.
LTF0pnc6ptNYATGHPgNaoIMe6HjzC8ym372ACkOFy3XzGL1oUbto5YEn V4PA+tNV5LPXrNQ+3HMJwbTm62bNnIsvqTSTagbB4vTUUeU/vv6O0Rs7
IhcQrIEx0M+5jUnTCyMp/3W7zI6pa+LxRVCh2pHfcuOp4IlOv+iYRxx8 c2A=
uka.se.                 116     IN      RRSIG   NS 7 2 900 20150502064416 20150425101039 10608 uka.se.
nSZfX1laM40detHQ/pjjGLp2U7mE4OCHy4LTrbM+PfdiyAsgOajzuL2f 4X4TnaE438zjqaVAaeENGUoezQlrSF6AHKo1OEsSDJIBpEIPP7cCjb4V
lBXYKd5V5yJK5QlGlLxGNvURBbymoFzhaDtvPkFJl4lSzxhgLVo4C+hI lXs=
ns1.uka.se.              116     IN      RRSIG   A 7 3 900 20150501061451 20150424101005 10608 uka.se.
g9V9hZYDIjS6qKrdsc+iGdUyjlC0fRLNrExOhYhNolZ2IYGXeuxtv4dd 52Pev3SL2btGild/GzdxIKyr1EvUZMOE2d3EqlhRe35Gf4s8wNvCRPV2
YS/W7cNdXVuIab6juMWthxdKM4X9yzg4DdRwKyjZSh5GiEoyXdv9eoz9 MIQ=
ns1.uka.se.              116     IN      RRSIG   AAAA 7 3 900 20150430223906 20150424020950 10608 uka.se.
LnZGabudkBGqPdZK2zUbXusiFi/3m+z5tdMom09IN17fyzeGR9soD6iU Tu8m5eF7W90h+JVcMHpoqJdocRTqge/IcSrB39Ixi1APQwNNm1woCr4
xxmWQfDKv4gdT4cr89ju8BEgz0HKCYv7nllTAJGrYpvZASOJ3O6dyedh 90c=
ns2.uka.se.              116     IN      RRSIG   A 7 3 900 20150501223754 20150425021028 10608 uka.se.
io9p4RYVXQVqQvIBOPosAKvanKawKnu5SXC7pWyJYkLAea9BFz312bRY oUKo1aZh7IypY9mHrZn41Qgzixwu5rAP8dkjPsLS16uX4ynY84S1yjmt
fyzKXf8/JRvtvYSNgLjoqo44kbcewelVyJKPukPhsZUXjcvLMH3n4lB7 MuE=
ns2.uka.se.              116     IN      RRSIG   AAAA 7 3 900 20150502035522 20150425041032 10608 uka.se.
HhwdKxU7ttk4fv4MFwPEaMHit3CClHZ7AEn99/5KtL5R6lgO8dotzboe nkmmINiTZgySPrAp6mPwN3oM/B5DPOl96uaavWCR/dXUSS+jSknusbeS
M5nMav6rpHjZwLyOuBZCvpP9ZXUL3Q7I8xpAXPOzMzfVjMcQMItcS9V4 5wU=
sunic.sunet.se.          946     IN      RRSIG   A 8 3 86400 20150505033457 20150425023457 7636 sunet.se.
x4PdDzUEXGVBNtQCdtUvsSEsp/AAc63bSMeDOanPXDzERjqcyxzMRXHk yJmmSWJsxBYCEKNl7Rab8rH23uc9ys/CA39PSkz8PWPCqudXFlSjeGXU
pakiDno+uuSLaODXpj+j96R3cZs3UlNKp7NzeZfJXMPs5lD1KhzNotn7 9UE=
sunic.sunet.se.          946     IN      RRSIG   AAAA 8 3 86400 20150505033457 20150425023457 7636 sunet.se.
heNpGX1iucZypEKXhaE4EC5t3zpnhOjY2zbONyABcAjz61qpdRY283ER HcEvn/Xlsa8/i9UdMorWb7HcKpnCGrD/fh2i+sHganmiXHmNghwyKpwc
s0N+R/lUVp96F0c4ZRHG/qlSO9KL3Dcwci8GWd84bSpYy3WK1xUYSWA4 zrc=
ns#####
uka.se.                 116     IN      RRSIG   NS 7 2 900 20150502064416 20150425101039 10608 uka.se.
nSZfX1laM40detHQ/pjjGLp2U7mE4OCHy4LTrbM+PfdiyAsgOajzuL2f 4X4TnaE438zjqaVAaeENGUoezQlrSF6AHKo1OEsSDJIBpEIPP7cCjb4V
lBXYKd5V5yJK5QlGlLxGNvURBbymoFzhaDtvPkFJl4lSzxhgLVo4C+hI lXs=
ns1.uka.se.              116     IN      RRSIG   A 7 3 900 20150501061451 20150424101005 10608 uka.se.
g9V9hZYDIjS6qKrdsc+iGdUyjlC0fRLNrExOhYhNolZ2IYGXeuxtv4dd 52Pev3SL2btGild/GzdxIKyr1EvUZMOE2d3EqlhRe35Gf4s8wNvCRPV2
YS/W7cNdXVuIab6juMWthxdKM4X9yzg4DdRwKyjZSh5GiEoyXdv9eoz9 MIQ=
ns1.uka.se.              116     IN      RRSIG   AAAA 7 3 900 20150430223906 20150424020950 10608 uka.se.
LnZGabudkBGqPdZK2zUbXusiFi/3m+z5tdMom09IN17fyzeGR9soD6iU Tu8m5eF7W90h+JVcMHpoqJdocRTqge/IcSrB39Ixi1APQwNNm1woCr4
xxmWQfDKv4gdT4cr89ju8BEgz0HKCYv7nllTAJGrYpvZASOJ3O6dyedh 90c=
ns2.uka.se.              116     IN      RRSIG   A 7 3 900 20150501223754 20150425021028 10608 uka.se.
io9p4RYVXQVqQvIBOPosAKvanKawKnu5SXC7pWyJYkLAea9BFz312bRY oUKo1aZh7IypY9mHrZn41Qgzixwu5rAP8dkjPsLS16uX4ynY84S1yjmt
fyzKXf8/JRvtvYSNgLjoqo44kbcewelVyJKPukPhsZUXjcvLMH3n4lB7 MuE=
ns2.uka.se.              116     IN      RRSIG   AAAA 7 3 900 20150502035522 20150425041032 10608 uka.se.
HhwdKxU7ttk4fv4MFwPEaMHit3CClHZ7AEn99/5KtL5R6lgO8dotzboe nkmmINiTZgySPrAp6mPwN3oM/B5DPOl96uaavWCR/dXUSS+jSknusbeS
M5nMav6rpHjZwLyOuBZCvpP9ZXUL3Q7I8xpAXPOzMzfVjMcQMItcS9V4 5wU=
sunic.sunet.se.          946     IN      RRSIG   A 8 3 86400 20150505033457 20150425023457 7636 sunet.se.
x4PdDzUEXGVBNtQCdtUvsSEsp/AAc63bSMeDOanPXDzERjqcyxzMRXHk yJmmSWJsxBYCEKNl7Rab8rH23uc9ys/CA39PSkz8PWPCqudXFlSjeGXU
pakiDno+uuSLaODXpj+j96R3cZs3UlNKp7NzeZfJXMPs5lD1KhzNotn7 9UE=
sunic.sunet.se.          946     IN      RRSIG   AAAA 8 3 86400 20150505033457 20150425023457 7636 sunet.se.
heNpGX1iucZypEKXhaE4EC5t3zpnhOjY2zbONyABcAjz61qpdRY283ER HcEvn/Xlsa8/i9UdMorWb7HcKpnCGrD/fh2i+sHganmiXHmNghwyKpwc
s0N+R/lUVp96F0c4ZRHG/qlSO9KL3Dcwci8GWd84bSpYy3WK1xUYSWA4 zrc=
mx#####
uka.se.                 900     IN      RRSIG   MX 7 2 900 20150501200614 20150425001025 10608 uka.se.
KmyOub01IArNe1foWpyjS/fbj1Hgib40MEqgdPrtBf2kqKPgkCRbnou4 X1mGEqOJnVLaygVz9PccmwAKqAoFXx78Fpa5dcEENzpPbTeDyTORCW2y
NP1YDVfW59ZFN2/JWfCl28CKlh6y9rXSO3visnFn8Yrc01dw6BWaUOAy kdM=
uka.se.                 115     IN      RRSIG   NS 7 2 900 20150502064416 20150425101039 10608 uka.se.
nSZfX1laM40detHQ/pjjGLp2U7mE4OCHy4LTrbM+PfdiyAsgOajzuL2f 4X4TnaE438zjqaVAaeENGUoezQlrSF6AHKo1OEsSDJIBpEIPP7cCjb4V
lBXYKd5V5yJK5QlGlLxGNvURBbymoFzhaDtvPkFJl4lSzxhgLVo4C+hI lXs=
ns1.uka.se.              115     IN      RRSIG   A 7 3 900 20150501061451 20150424101005 10608 uka.se.
g9V9hZYDIjS6qKrdsc+iGdUyjlC0fRLNrExOhYhNolZ2IYGXeuxtv4dd 52Pev3SL2btGild/GzdxIKyr1EvUZMOE2d3EqlhRe35Gf4s8wNvCRPV2
YS/W7cNdXVuIab6juMWthxdKM4X9yzg4DdRwKyjZSh5GiEoyXdv9eoz9 MIQ=
ns1.uka.se.              115     IN      RRSIG   AAAA 7 3 900 20150430223906 20150424020950 10608 uka.se.
LnZGabudkBGqPdZK2zUbXusiFi/3m+z5tdMom09IN17fyzeGR9soD6iU Tu8m5eF7W90h+JVcMHpoqJdocRTqge/IcSrB39Ixi1APQwNNm1woCr4
xxmWQfDKv4gdT4cr89ju8BEgz0HKCYv7nllTAJGrYpvZASOJ3O6dyedh 90c=
ns2.uka.se.              115     IN      RRSIG   A 7 3 900 20150501223754 20150425021028 10608 uka.se.
io9p4RYVXQVqQvIBOPosAKvanKawKnu5SXC7pWyJYkLAea9BFz312bRY oUKo1aZh7IypY9mHrZn41Qgzixwu5rAP8dkjPsLS16uX4ynY84S1yjmt
fyzKXf8/JRvtvYSNgLjoqo44kbcewelVyJKPukPhsZUXjcvLMH3n4lB7 MuE=
ns2.uka.se.              115     IN      RRSIG   AAAA 7 3 900 20150502035522 20150425041032 10608 uka.se.
HhwdKxU7ttk4fv4MFwPEaMHit3CClHZ7AEn99/5KtL5R6lgO8dotzboe nkmmINiTZgySPrAp6mPwN3oM/B5DPOl96uaavWCR/dXUSS+jSknusbeS
M5nMav6rpHjZwLyOuBZCvpP9ZXUL3Q7I8xpAXPOzMzfVjMcQMItcS9V4 5wU=
sunic.sunet.se.          945     IN      RRSIG   A 8 3 86400 20150505033457 20150425023457 7636 sunet.se.
x4PdDzUEXGVBNtQCdtUvsSEsp/AAc63bSMeDOanPXDzERjqcyxzMRXHk yJmmSWJsxBYCEKNl7Rab8rH23uc9ys/CA39PSkz8PWPCqudXFlSjeGXU
pakiDno+uuSLaODXpj+j96R3cZs3UlNKp7NzeZfJXMPs5lD1KhzNotn7 9UE=
sunic.sunet.se.          945     IN      RRSIG   AAAA 8 3 86400 20150505033457 20150425023457 7636 sunet.se.
heNpGX1iucZypEKXhaE4EC5t3zpnhOjY2zbONyABcAjz61qpdRY283ER HcEvn/Xlsa8/i9UdMorWb7HcKpnCGrD/fh2i+sHganmiXHmNghwyKpwc
s0N+R/lUVp96F0c4ZRHG/qlSO9KL3Dcwci8GWd84bSpYy3WK1xUYSWA4 zrc=
www#####
www.uka.se.             900     IN      RRSIG   A 7 3 900 20150502205552 20150425101039 10608 uka.se.
dv9O+X0mekfhqhiQmYy4ZEOznfLIVHPtR853NhonrePb+PYzkvmTRlFt MG5D+d29PGasq1B24kSPqv42kvalLovDCZoq6YT6AsAJj9CQoPru7ACu
spvdDKT5v7Wm0Q+7Tf85+YvYHP/3ziOVGKVhVK2obei5TToQMGOzdXpA eJ8=
uka.se.                 114     IN      RRSIG   NS 7 2 900 20150502064416 20150425101039 10608 uka.se.
nSZfX1laM40detHQ/pjjGLp2U7mE4OCHy4LTrbM+PfdiyAsgOajzuL2f 4X4TnaE438zjqaVAaeENGUoezQlrSF6AHKo1OEsSDJIBpEIPP7cCjb4V
lBXYKd5V5yJK5QlGlLxGNvURBbymoFzhaDtvPkFJl4lSzxhgLVo4C+hI lXs=
ns1.uka.se.              114     IN      RRSIG   A 7 3 900 20150501061451 20150424101005 10608 uka.se.
g9V9hZYDIjS6qKrdsc+iGdUyjlC0fRLNrExOhYhNolZ2IYGXeuxtv4dd 52Pev3SL2btGild/GzdxIKyr1EvUZMOE2d3EqlhRe35Gf4s8wNvCRPV2
YS/W7cNdXVuIab6juMWthxdKM4X9yzg4DdRwKyjZSh5GiEoyXdv9eoz9 MIQ=
ns1.uka.se.              114     IN      RRSIG   AAAA 7 3 900 20150430223906 20150424020950 10608 uka.se.
LnZGabudkBGqPdZK2zUbXusiFi/3m+z5tdMom09IN17fyzeGR9soD6iU Tu8m5eF7W90h+JVcMHpoqJdocRTqge/IcSrB39Ixi1APQwNNm1woCr4
xxmWQfDKv4gdT4cr89ju8BEgz0HKCYv7nllTAJGrYpvZASOJ3O6dyedh 90c=
ns2.uka.se.              114     IN      RRSIG   A 7 3 900 20150501223754 20150425021028 10608 uka.se.
io9p4RYVXQVqQvIBOPosAKvanKawKnu5SXC7pWyJYkLAea9BFz312bRY oUKo1aZh7IypY9mHrZn41Qgzixwu5rAP8dkjPsLS16uX4ynY84S1yjmt
fyzKXf8/JRvtvYSNgLjoqo44kbcewelVyJKPukPhsZUXjcvLMH3n4lB7 MuE=
ns2.uka.se.              114     IN      RRSIG   AAAA 7 3 900 20150502035522 20150425041032 10608 uka.se.
HhwdKxU7ttk4fv4MFwPEaMHit3CClHZ7AEn99/5KtL5R6lgO8dotzboe nkmmINiTZgySPrAp6mPwN3oM/B5DPOl96uaavWCR/dXUSS+jSknusbeS
M5nMav6rpHjZwLyOuBZCvpP9ZXUL3Q7I8xpAXPOzMzfVjMcQMItcS9V4 5wU=
sunic.sunet.se.          944     IN      RRSIG   A 8 3 86400 20150505033457 20150425023457 7636 sunet.se.
x4PdDzUEXGVBNtQCdtUvsSEsp/AAc63bSMeDOanPXDzERjqcyxzMRXHk yJmmSWJsxBYCEKNl7Rab8rH23uc9ys/CA39PSkz8PWPCqudXFlSjeGXU
pakiDno+uuSLaODXpj+j96R3cZs3UlNKp7NzeZfJXMPs5lD1KhzNotn7 9UE=
sunic.sunet.se.          944     IN      RRSIG   AAAA 8 3 86400 20150505033457 20150425023457 7636 sunet.se.
heNpGX1iucZypEKXhaE4EC5t3zpnhOjY2zbONyABcAjz61qpdRY283ER HcEvn/Xlsa8/i9UdMorWb7HcKpnCGrD/fh2i+sHganmiXHmNghwyKpwc
s0N+R/lUVp96F0c4ZRHG/qlSO9KL3Dcwci8GWd84bSpYy3WK1xUYSWA4 zrc=
```

Bilaga 5 Exempel på efterbehandling av signaturlivslängd.

dnskey#####	soa#####	ns#####	mx#####	www#####
uka.se.	uka.se.	uka.se.	uka.se.	www.uka.se.
DNSKEY	DNSKEY	NS	MX	A
20150502100137	20150502100137	20150502064416	20150501200614	20150502205552
20150425201049	20150425201049	20150425101039	20150425001025	20150425101039
	uka.se.	ns1.uka.se.	uka.se.	uka.se.
	SOA	A	NS	NS
	20150504021527	20150501061451	20150502064416	20150502064416
	20150427041120	20150424101005	20150425101039	20150425101039
	uka.se.	ns1.uka.se.	ns1.uka.se.	ns1.uka.se.
	NS	AAAA	A	A
	20150502064416	20150430223906	20150501061451	20150501061451
	20150425101039	20150424020950	20150424101005	20150424101005
	ns1.uka.se.	ns2.uka.se.	ns1.uka.se.	ns1.uka.se.
	A	A	AAAA	AAAA
	20150501061451	20150501223754	20150430223906	20150430223906
	20150424101005	20150425021028	20150424020950	20150424020950
	ns1.uka.se.	ns2.uka.se.	ns2.uka.se.	ns2.uka.se.
	AAAA	AAAA	A	A
	20150430223906	20150502035522	20150501223754	20150501223754
	20150424020950	20150425041032	20150425021028	20150425021028
	ns2.uka.se.	sunic.sunet.se.	ns2.uka.se.	ns2.uka.se.
	A	A	AAAA	AAAA
	20150501223754	20150505033457	20150502035522	20150502035522
	20150425021028	20150425023457	20150425041032	20150425041032
	ns2.uka.se.	sunic.sunet.se.	sunic.sunet.se.	sunic.sunet.se.
	AAAA	AAAA	A	A
	20150502035522	20150505033457	20150505033457	20150505033457
	20150425041032		20150425023457	20150425023457
	sunic.sunet.se.		sunic.sunet.se.	sunic.sunet.se.
	A		AAAA	AAAA
	20150505033457		20150505033457	20150505033457
	20150425023457		20150425023457	20150425023457
	sunic.sunet.se.			
	AAAA			
	20150505033457			
	20150425023457			
	20150425023457			

Bilaga 6 Specifering av fel och varningar.

Domän	Kategori	Benämning	Orsak
csn.se	WARNING	NAMESERVERS_IPV4_WITH_UNIQ_AS	Endast 1 IPv4 ISP
datainspektionen.se	WARNING	CONNECTIVITY NAMESERVERS_IPV6_WITH_UNIQ_AS	Endast 1 IPv6 ISP
forsakringskassan.se	WARNING	ADDRESS NAMESERVER_IP_WITHOUT_REVERSE	Felaktig konfigurering ?
hofors.se	ERROR	CONNECTIVITY NAMESERVER_NO_UDP_53	Svarar ej på UDP
	WARNING	CONSISTENCY NO_RESPONSE	DNS server svarar inte
lantmateriet.se	WARNING	CONNECTIVITY NAMESERVERS_IPV6_WITH_UNIQ_AS	Endast 1 IPv6 ISP
lg.se	WARNING	ADDRESS NAMESERVER_IP_WITHOUT_REVERSE	Felaktig konfigurering ?
ljusdal.se	ERROR	CONNECTIVITY NAMESERVER_NO_UDP_53	Svarar ej på UDP
	WARNING	CONSISTENCY NO_RESPONSE	DNS server svarar inte
msb.se	WARNING	CONNECTIVITY NAMESERVERS_IPV4_WITH_UNIQ_AS	Endast 1 IPv4 ISP
	WARNING	CONNECTIVITY NAMESERVERS_IPV6_WITH_UNIQ_AS	Endast 1 IPv6 ISP
nordanstig.se	WARNING	CONNECTIVITY NAMESERVERS_IPV6_WITH_UNIQ_AS	Endast 1 IPv6 ISP
pliktverket.se	WARNING	CONNECTIVITY NAMESERVERS_IPV4_WITH_UNIQ_AS	Endast 1 IPv4 ISP
	WARNING	CONNECTIVITY NAMESERVERS_IPV6_WITH_UNIQ_AS	Endast 1 IPv6 ISP
regeringen.se	WARNING	CONNECTIVITY NAMESERVERS_IPV4_WITH_UNIQ_AS	Endast 1 IPv4 ISP
	WARNING	CONNECTIVITY NAMESERVERS_IPV6_WITH_UNIQ_AS	Endast 1 IPv6 ISP
regiongavleborg.se	WARNING	ADDRESS NAMESERVER_IP_WITHOUT_REVERSE	Felaktig konfigurering ?
riksdagen.se	WARNING	ADDRESS NAMESERVER_IP_WITHOUT_REVERSE	Felaktig konfigurering ?
socialstyrelsen.se	ERROR	CONNECTIVITY NAMESERVER_NO_UDP_53	Svarar ej på UDP
	ERROR	CONNECTIVITY NAMESERVER_NO_TCP_53	Svarar ej på TCP
	WARNING	CONNECTIVITY NAMESERVERS_IPV4_WITH_UNIQ_AS	Endast 1 IPv4 ISP
	WARNING	CONNECTIVITY NAMESERVERS_IPV6_WITH_UNIQ_AS	Endast 1 IPv6 ISP
	WARNING	CONSISTENCY NO_RESPONSE	DNS server svarar inte
uka.se	WARNING	CONNECTIVITY NAMESERVERS_IPV4_WITH_UNIQ_AS	Endast 1 IPv4 ISP
	WARNING	CONNECTIVITY NAMESERVERS_IPV6_WITH_UNIQ_AS	Endast 1 IPv6 ISP

Bilaga 7 Signaturlivslängd.

Domän	Typ	Namn	Längd (dagar)
arbetsformedlingen.se	DNSKEY	arbetsformedlingen.se	15
	SOA	arbetsformedlingen.se	15
	NS	arbetsformedlingen.se	15
	MX	arbetsformedlingen.se	15
	www	www.arbetsformedlingen.se	15
bollnas.se	DNSKEY	bollnas.se	39
	SOA	bollnas.se	39
	NS	bollnas.se	40
	MX	bollnas.se	39
	www	www. bollnas.se	40
csn.se	DNSKEY	csn.se	4
	SOA	csn.se	4
	NS	csn.se	4
	MX	csn.se	4
	www	www.csn.se	4
	www	wpl.csn.se	4
datainspektionen.se	DNSKEY	datainspektionen.se	15
	SOA	datainspektionen.se	15
	NS	datainspektionen.se	15
	MX	datainspektionen.se	15
	www	www.datainspektionen.se	15
forsakringskassan.se	DNSKEY	forsakringskassan.se	4
	SOA	forsakringskassan.se	4
	NS	forsakringskassan.se	4
	MX	forsakringskassan.se	4
	www	www. forsakringskassan.se	4
forsvarsmakten.se	DNSKEY	forsvarsmakten.se	36
	SOA	forsvarsmakten.se	36
	NS	forsvarsmakten.se	36
	MX	forsvarsmakten.se	36
	www	www.forsvarsmakten.se	36
gavle.se	DNSKEY	gavle.se	50
	SOA	gavle.se	50
	NS	gavle.se	50
	MX	gavle.se	50
	www	www.gavle.se	50
hofors.se	DNSKEY	hofors.se	60
	SOA	hofors.se	60
	NS	hofors.se	60
	MX	hofors.se	60
	www	www.hofors.se	59
hudiksvall.se	DNSKEY	hudiksvall.se	60
	SOA	hudiksvall.se	60
	NS	hudiksvall.se	60
	MX	hudiksvall.se	60
	www	www.hudiksvall.se	60
lansstyrelsen.se	DNSKEY	lansstyrelsen.se	22
	SOA	lansstyrelsen.se	21
	NS	lansstyrelsen.se	22
	MX	lansstyrelsen.se	22
	www	www.lansstyrelsen.se	21
lantmateriet.se	DNSKEY	lantmateriet.se	31
	SOA	lantmateriet.se	31
	NS	lantmateriet.se	31
	MX	lantmateriet.se	31
	www	www.lantmateriet.se	31
lg.se	DNSKEY	lg.se	40
	SOA	lg.se	40
	NS	lg.se	40
	MX	lg.se	40
	www	www.lg.se	40
ljusdal.se	DNSKEY	ljusdal.se	60
	SOA	ljusdal.se	60
	NS	ljusdal.se	60
	MX	ljusdal.se	60
	www	www.ljusdal.se	60
	www	ljusdal.se	60

msb.se	DNSKEY	msb.se	31
	SOA	msb.se	31
	NS	msb.se	31
	MX	msb.se	31
	www	www.msb.se	31
nordanstig.se	DNSKEY	nordanstig.se	59
	SOA	nordanstig.se	60
	NS	nordanstig.se	60
	MX	nordanstig.se	60
	www	www.nordanstig.se	59
ockelbo.se	DNSKEY	ockelbo.se	50
	SOA	ockelbo.se	50
	NS	ockelbo.se	50
	MX	ockelbo.se	50
	www	www.ockelbo.se	50
ovanaker.se	DNSKEY	ovanaker.se	40
	SOA	ovanaker.se	39
	NS	ovanaker.se	40
	MX	ovanaker.se	40
	www	www.ovanaker.se	40
pliktverket.se	DNSKEY	pliktverket.se	22
	SOA	pliktverket.se	22
	NS	pliktverket.se	22
	MX	pliktverket.se	22
	www	pliktverket.se	22
regeringen.se	DNSKEY	regeringen.se	31
	SOA	regeringen.se	31
	NS	regeringen.se	31
	MX	regeringen.se	31
	www	regeringen.se	31
regiongavleborg.se	DNSKEY	regiongavleborg.se	40
	SOA	regiongavleborg.se	40
	NS	regiongavleborg.se	40
	MX	regiongavleborg.se	40
	www	www.regiongavleborg.se	40
riksdagen.se	DNSKEY	riksdagen.se	22
	SOA	riksdagen.se	22
	NS	riksdagen.se	22
	MX	riksdagen.se	22
	www	www.riksdagen.se	22
sandviken.se	DNSKEY	sandviken.se	60
	SOA	sandviken.se	60
	NS	sandviken.se	59
	MX	sandviken.se	60
	www	www.sandviken.se	60
skatteverket.se	DNSKEY	skatteverket.se	11
	SOA	skatteverket.se	10
	NS	skatteverket.se	11
	MX	skatteverket.se	10
	www	www.skatteverket.se	11
smhi.se	DNSKEY	smhi.se	4
	SOA	smhi.se	5
	NS	smhi.se	4
	MX	smhi.se	4
	www	www.smhi.se	5
socialstyrelsen.se	DNSKEY	socialstyrelsen.se	4
	SOA	socialstyrelsen.se	5
	NS	socialstyrelsen.se	5
	MX	socialstyrelsen.se	4
	www	www.socialstyrelsen.se	4
soderhamn.se	DNSKEY	soderhamn.se	15
	SOA	soderhamn.se	15
	NS	soderhamn.se	15
	MX	soderhamn.se	15
	www	www.soderhamn.se	15
uka.se	DNSKEY	uka.se	7
	SOA	uka.se	7
	NS	uka.se	7
	MX	uka.se	7
	www	www.uka.se	8

Bilaga 8 Placering av DNS-servrar

Domän	DNS-server	Land
arbetsformedlingen.se	ns.cafax.se	SE
	ns1.frobbit.se	USA
	ns2.frobbit.se	SE
	ns3.frobbit.se	USA
bollnas.se	ns.interlan.se	SE
	ns3.interlan.se	UK
csn.se	nse1.edb.se	SE
	nse2.edb.se	SE
datainspektionen.se	ns3.binero.se	USA
	ns4.binero.se	USA
	ns5.binero.se	USA
	ns6.binero.se	USA
	ns7.binero.se	SE
forsakringskassan.se	sadbnsy1.sfa.se	
	sadbsmtpy1.sfa.se	
forsvarsmakten.se	dns5.telia.com	SE
	dns6.telia.com	SE
	ns.mil.se	SE
	ns2.mil.se	SE
	ns3.mil.se	
	pitea.dns.swip.net	SE
gavle.se	ns.gavle.se	SE
	ns2.gavlenet.com	SE
hofors.se	ns1.hofors.se	
	ns1.ipv6dns.se	SE
	ns2.ipv6dns.se	UK
hudiksvall.se	a.dns.tdc.se	SE
	b.dns.tdc.se	SE
	c.dns.tdc.se	SE
	ns.hudiksvall.se	
lansstyrelsen.se	nic.fassberg.se	
	ns1.lst.se	SE
	ns2.lst.se	SE
	sunic.sunet.se	SE
lantmateriet.se	ns01.lm.se	SE
	ns02.lm.se	SE
	ns04.lm.se	SE
	ns05.lm.se	SE
lg.se	a.dns.tdc.se	SE
	b.dns.tdc.se	SE
	ns-1.lg.se	
	ns-2.lg.se	
ljusdal.se	ns.ljusdal.se	
	ns1.ipv6dns.se	SE
	ns2.ipv6dns.se	UK
msb.se	ns1.p21.dynect.net	USA
	ns2.p21.dynect.net	USA
	ns3.p21.dynect.net	USA
	ns4.p21.dynect.net	USA
nordanstig.se	ns1.nordanstig.se	
	ns2.gavlenet.com	SE
ockelbo.se	ns.gavle.se	SE
	ns2.gavlenet.com	SE
ovanaker.se	ns.interlan.se	SE
	ns3.interlan.se	UK
pliktverket.se	dns9.telia.com	SE
	dns10.telia.com	SE
regeringen.se	ns1.p21.dynect.net	USA
	ns2.p21.dynect.net	USA
	ns3.p21.dynect.net	USA
	ns4.p21.dynect.net	USA
regiongavleborg.se	ns-1.lg.se	
	ns-2.lg.se	
riksdagen.se	ns1.riksdagen.se	
	ns2.riksdagen.se	
sandviken.se	ns.sandviken.se	
	ns2.gavlenet.com	SE

skatteverket.se	a.dns.tdc.se	SE
	b.dns.tdc.se	SE
	c.dns.tdc.se	SE
	dns5.telia.com	SE
	ystad.dns.swip.net	SE
smhi.se	a.dns.tdc.se	SE
	b.dns.tdc.se	SE
	c.dns.tdc.se	SE
	dns5.telia.com	SE
	dns6.telia.com	SE
socialstyrelsen.se	ns1.socialstyrelsen.se	SE
	ns2.socialstyrelsen.se	SE
soderhamn.se	a4.nstld.com	USA
	f4.nstld.com	USA
	ns1.ascio.net	
	ns4.ascio.net	USA
uka.se	ns1.hsv.se	
	ns1.uka.se	
	ns2.hsv.se	
	ns2.uka.se	
	sunic.sunet.se	SE
aklagare.se	a.dns.tdc.se	SE
	b.dns.tdc.se	SE
	c.dns.tdc.se	SE
	ns.wineasy.se	SE
	ns2.wineasy.se	SE
arbetarbladet.se	ns.gd.se	SE
	ns01.sth.basefarm.net	SE
	ns1.mittmedia.se	
	ns1.osl.basefarm.net	NO
	ns2.mittmedia.se	
gd.se	ns.gd.se	SE
	ns01.sth.basefarm.net	SE
	ns1.mittmedia.se	
	ns1.osl.basefarm.net	NO
	ns2.mittmedia.se	
helahalsingland.se	ns1.mittmedia.se	
	ns2.mittmedia.se	
polisen.se	dns5.telia.com	SE
	ns1.police.se	SE
	ns2.police.se	SE
riksbank.se	ns-hk.riksbank.se	SE
	ns-s2.riksbank.se	SE
	pitea.dns.swip.net	SE
sr.se	a.ns.ip-only.net	SE
	atos.sr.se	SE
	c.ns.ip-only.net	SE
	dart.sr.se	SE
	dart2.sr.se	
svt.se	a.ns.ip-only.net	SE
	b.ns.ip-only.net	SE
	c.ns.ip-only.net	SE
	hermes.svt.se	SE
	mercury.svt.se	SE
tv4.se	dns1.cscdns.net	USA
	dns2.cscdns.net	USA

Bilaga 9 Placering av e-post servrar.

Domän	Mail-server	Land
arbetsformedlingen.se	smtp.arbetsformedlingen.se	SE
bollnas.se	smtp-in.sto-ste.se.stejtech.net	SE
	smtp-in.sto-hy.se.stejtech.net	SE
csn.se	smtp-in.sto-ste.se.stejtech.net	SE
	smtp-in.sto-hy.se.stejtech.net	SE
datainspektionen.se	smtp-in.sto-ste.se.stejtech.net	SE
	smtp-in.sto-hy.se.stejtech.net	SE
forsakringskassan.se	maily2.forsakringskassan.se	SE
	maily1.forsakringskassan.se	SE
forsvarsmakten.se	193.44.157.193	SE
	193.44.157.219	SE
gavle.se	mail1.gavle.se	SE
	mail2.gavle.se	SE
hofors.se	smtp1.interlan.se	SE
hudiksvall.se	katla.teknikpark.se	SE
lansstyrelsen.se	external-mx.lst.se	SE
lantmateriet.se	profi.lmv.lm.se	SE
	ipv6mailrelay.lmv.lm.se	
lg.se	mailgw1.lg.se	SE
	mailgw2.lg.se	SE
ljusdal.se	sbg1.ljusdal.se	SE
msb.se	mailgw-01.msb.se	SE
	mailgw-02.msb.se	SE
nordanstig.se	smtp1.interlan.se	SE
ockelbo.se	mail1.gavle.se	SE
	mail2.gavle.se	SE
ovanaker.se	smtp1.interlan.se	SE
pliktverket.se	mailx.pliktverket.se	SE
regeringen.se	hnikud.ministry.se	SE
	eyfura.ministry.se	SE
	rollaug.ministry.se	
	hnikar.ministry.se	SE
	eylime.ministry.se	SE
regiongavleborg.se	mailgw1.lg.se	SE
	mailgw2.lg.se	SE
riksdagen.se	mailgw.riksdagen.se	SE
	mailgw2.riksdagen.se	SE
sandviken.se	mail2.sandviken.se	SE
	mail3.sandviken.se	SE
skatteverket.se	knatte.skatteverket.se	SE
	fnatte.skatteverket.se	SE
	tjatte.skatteverket.se	SE
smhi.se	smtp-in.sto-ste.se.stejtech.net	SE
	smtp-in.sto-hy.se.stejtech.net	SE
socialstyrelsen.se	Info om mx saknas	
soderhamn.se	katla.teknikpark.se	SE
uka.se	smtp-in.sto-ste.se.stejtech.net	SE
	smtp-in.sto-hy.se.stejtech.net	SE
aklagare.se	mail.aklagare.se	
	mail1.aklagare.se	SE
	mail2.aklagare.se	SE
arbetarbladet.se	smtp-in.sto-ste.se.stejtech.net	SE
	smtp-in.sto-hy.se.stejtech.net	SE
gd.se	smtp-in.sto-ste.se.stejtech.net	SE
	smtp-in.sto-hy.se.stejtech.net	SE
helahalsingland.se	smtp-in.sto-ste.se.stejtech.net	SE
	smtp-in.sto-hy.se.stejtech.net	SE
polisen.se	mail1.polisen.se	SE
	mail2.polisen.se	SE
riksbank.se	mail1.riksbank.se	SE
	mail2.riksbank.se	SE
sr.se	mail-1.sr.se	SE
	mail-2.sr.se	SE
	mail-3.sr.se	SE
svt.se	svt-se.mail.protection.outlook.com	UK
tv4.se	mx10-se.staysecuregroup.com	SE
	mx20-se.staysecuregroup.net	SE

Bilaga 10 Sammanställning av TTL på DNSKEY.

Domän	ZSK TTL	ZSK antal	KSK TTL	KSK antal
arbetsformedlingen.se	3600	2	3600	1
bollnas.se	3600	2	3600	1
csn.se	172800	2	172800	2
datainspektionen.se	3600	2	3600	1
forsakringskassan.se	172800	1	172800	1
forsvarsmakten.se	1800	1	1800	1
gavle.se	3600	1	3600	1
hofors.se	3600	1	3600	1
hudiksvall.se	3600	1	3600	1
lansstyrelsen.se	3600	1	3600	1
lantmateriet.se	43200	2	43200	2
lg.se	3600	1	3600	1
ljusdal.se	3600	1	3600	1
msb.se	3600	4	3600	2
nordanstig.se	3600	1	3600	1
ockelbo.se	3600	1	3600	1
ovanaker.se	3600	2	3600	1
pliktverket.se	3600	2	3600	1
regeringen.se	3600	2	3600	1
regiongavleborg.se	3600	1	3600	1
riksdagen.se	907200	2	907200	1
sandviken.se	3600	1	3600	1
skatteverket.se	14400	1	14400	1
smhi.se	172800	1	172800	2
socialstyrelsen.se	172800	1	172800	2
soderhamn.se	3600	1	3600	1
uka.se	3600	1	3600	1

Bilaga 11 Internet Service Providers per domän

Domän	AS nummer IPv4	AS nummer IPv6
aklagare.se	1653	1653
	3292	3292
arbetarbladet.se	1257	
	8523	
	25148	
arbetsformedlingen.se	42	42
	1257	1257
	6939	6939
	34244	34244
bollnas.se	15830	15830
	16117	16117
	20473	20473
	44136	44136
csn.se	28726	
datainspektionen.se	12008	12008
	41528	
forsakringskassan.se	3301	3301
	197942	197942
forsvarsmakten.se	1257	1257
	3301	3301
	8674	8674
	9201	9201
gavle.se	16117	16117
	41848	41848
gd.se	1257	
	8523	
	25148	
helahalsingland.se	1257	
hofors.se	3292	
	15830	15830
	16117	16117
	20473	20473
	44136	44136
hudiksvall.se	1653	1653
	3292	3292
	28954	
lansstyrelsen.se	1653	1653
	12597	12597
	24605	
	198476	198476
lantmateriet.se	3301	3301
	199902	
lg.se	3301	3301
	3292	3292
ljusdal.se	15830	15830
	16117	16117
	20473	20473
	25417	25417
	44136	44136
msb.se	33517	33517
nordanstig.se	3292	
	16117	16117
ockelbo.se	16117	16117
	41848	41848
ovanaker.se	15830	15830
	16117	16117
	20473	20473
	44136	44136
pliktverket.se	3301	3301
polisen.se	2799	
	3301	3301
regeringen.se	33517	33517
regiongavleborg.se	3292	3292
	3301	3301
riksbank.se	1257	1257
riksdagen.se	1653	1653
	3301	3301

sandviken.se	16117	16117
	20626	20626
skatteverket.se	1257	1257
	1653	1653
	3292	3292
	3301	3301
smhi.se	1653	1653
	3292	3292
	3301	3301
socialstyrelsen.se	1257	1257
soderhamn.se	33070	
	34922	
	36617	
	36620	
	36622	
	36623	
	36625	
	36626	
	36628	
	36632	
sr.se	3301	
	12552	12552
	47708	47708
svt.se	12552	12552
tv4.se		36616
	36617	
	36619	
	36620	
	36622	36622
	36623	
	36624	
	36625	
	36626	
	36628	
	36632	
uka.se	1653	1653