.FI AND DNSSEC

Ari-Matti Husa

TREX Workshop 2016

Today's menu

```
% finger luru

Ari-Matti Husa, Network specialist at FICORA (2015-)

Information security specialist at FICORA (CERT-FI, NCSC-FI) (2006-2014)

IBM, Elisa, Kolumbus Internet, Helsingin Puhelin, HPY... (1997-2006)

University of Oulu


Background:

Internet services at large, ex-hostmaster@kolumbus.fi

Unix, Linux, a little bit of IOS (the older one)

Windows, not so much.

%
```

Today's menu

- Brief review of .FI
- Brief review of .FI DNSSEC – past and present
- The .FI DNSSEC deployment
- The law is changing, what will change?
- What else is new?

.FI in brief

- Registry administrated by FICORA for ~two decades now
- Roughly 388k active domains
- Growth not yet stalled (5.3%)
- New TLDs may be considered as 'a threat'
- IDN, DNSSEC, IPv6 supported
- The domain requirements will be relaxed soon
- Note: Åland Islands domain (.ax) NOT managed by FICORA

The .FI registry infrastructure

- The .fi domain database system at FICORA
- The website domain.fi (ficora.fi)
- The web service interface for registrars
  - Until September 2, 2016 at 16.15 local time
- The whois service
- The Odata service
- The EPP interface for registrars
  - From September 5, 2016 at 10 AM local time

The .FI root name server infrastructure

- Primary (master): a.fi (CSC)
- Secondaries (slaves): b.fi, c.fi, d.fi, e.fi, f.fi (Ficora), g.fi, h.fi (FICIX)
- operated by various service providers
- diverse name server software and hardware used
- also anycast for resiliency
- IPv6 access to the service

.FI and DNSSEC

- .FI zone signed 2010
- support for fi-domains, late 2010
- DNSSEC not exactly a hit
- 329 signed fi-domain zones (0.1%)
- comparison:
  - .se 651k = 47.5%
  - .no 408k = 58.5%
- so, not a huge marketing success
- too complicated or failure to justify the trouble?

How it is done

Näin allekirjoitat .fi domainisi

Asenna linux-serveriisi bind9. Lisää rivi /etc/bind/named.conf tiedoston { options } –osioon:

```
dnssec-enable yes;
```

luo hakemisto /etc/bind/dnssec/ ja sen alle hakemisto kullekin allekirjoitettavalle domainille

esimerkiksi `/etc/bind/dnssec/73.fi/`

Siirry tekemääsi hakemistoon ja anna komennot:

```
dnssec-keygen -a RSASHA256 -b 2048 -r /dev/urandom -n ZONE 73.fi
dnssec-keygen -f KSK -a RSASHA256 -b 2048 -r /dev/urandom -n ZONE 73.fi
```

vaihda kuitenkin komennoista domainin nimi oikeaksi.

Listaa luotujen julkisten avaimien nimet

```
ls /etc/named/dnssec/73.fi/*.key
```

ja lisää ne zone-tiedoston /etc/named/pri/73.zone loppuun

```
$include /etc/named/dnssec/73.fi/K73.fi.+005+12345.key
$include /etc/named/dnssec/73.fi/K73.fi.+005+23456.key
```

Tämän jälkeen voit allekirjoittaa zonen.

```
dnssec-signzone -r /dev/urandom -K /etc/named/dnssec/73.fi -N unixtime -g -o 73.fi /etc/named/pri/73.zone
```

Vaihda /etc/bind/named.conf tiedostossa zone-tiedostoksi:

```
file "pri/73.zone.signed";
```

Käynnistä bind uudelleen ja huolehdi että slave-DNS:t saavat uuden allekirjoitetun määrittelytiedoston.

Kirjaudu `domain.fi` palveluun ja päivitä domainiin DNSSEC-tiedot.

Klikkaa [Hae], valitse tietue ja [Hyväksy]

Zone täytyy oletusasetuksilla allekirjoittaa uudelleen 30 päivän sisällä, joten allekirjoitus on hyvä laittaa crontabiin. Zonen muokkauksen jälkeen luonnollisesti tarvitaan myös allekirjoitus.

.FI DNSSEC specification

- https://domain.fi/info/en/index/palveluntarjoajille/dnssec.html
  - hash function: SHA-256
  - signature algorithm: RSA
  - NSEC3
  - Opt-Out
  - Zone Signing Key (ZSK): RSA 1024-bit
  - Key Signing Key (KSK): RSA 2048-bit
- RFC6605: new key algorithms (elliptic curves)
  - 13: ECDSA Curve P-256 with SHA-256
  - 14: ECDSA Curve P-384 with SHA-384
  - will be supported, probably by the end of this year

.FI DNSSEC management

- Currently, domain holders can add DS records for their signed zones to .FI root zone by
  - www user interface
  - web service interface (for registrars)
  - https://domain.fi/info/attachments/lomakkeet/sxqK4PYBw/WS_toiminnallisuuspalvelukuvaus_EN.pdf
- After September 5 changes will be managed through registrars only:
  - www user interface
  - EPP interface
  - https://domain.fi/info/attachments/.fi_uudistuu_2016/9DcJsqr8G/EPP_Interface.pdf

.FI zone deployment with DNSSEC

- Zone data stored in FICORA domain database
- .FI root zone created, exported, sanity-checked, signed and deployed to the primary (master) server a.fi
- HSM module for signing
  - Safenet Network HSM (was Luna SA HSM)
  - Deployed 2014
- Operated by CSC IT Center For Science Ltd.

Validating resolvers

- Resolvers should validate DNSSEC records
- The biggest providers provide validation, too
- There are some things to consider, however
  - Size of DNS-packets grows
  - Resolver load and delay will increase
  - Resolver's clock must be accurate
  - and others...
- Excellent (short) article about DNSSEC's effects on resolvers and end users (in Finnish):
  - https://wiki.eduuni.fi/pages/viewpage.action?pageId=23691410

.FI registration will soon change

- https://domain.fi/info/en/index/fi_uudistuu.html
  - No longer open only for Finnish registrants
  - Any domain name can be registered
    - No trade mark infringements or existing company names, however
  - Registry-registrar model implemented
    - No direct registrant contacts or registrations to FICORA
  - No working DNS servers required
    - storing domains without technically working setup possible
    - if name servers registered, they still must work properly
  - Registrars can name their price, bundle services
    - No major price changes anticipated

.FI domain registration will soon change

- ALL domain holders MUST find a registrar!
  - registered domains do not prematurely expire
  - however, no changes can be made without registrar
- Friday, September 2, 16:15 local time
  - The old domain database and its user interfaces will be closed for upgrade
- Monday, September 5, 10:00 local time
  - The new domain database and interfaces will be opened for registrars
- Wednesday, September 7, 10:00 local time
  - The list of forbidden domain names is removed and restrictions for their registration lifted

Thank You!

http://www.viestintavirasto.fi/en/index.html

https://domain.fi/info/en/index.html

ari-matti.husa@ficora.fi

domain@ficora.fi

fi-domain-tech@ficora.fi