DNSSEC challenges

Ari-Matti Husa
ICANN56, Helsinki, Finland

Name: Ari-Matti Husa
Login: luru
Directory: /home/luru
Shell: /bin/bash
Never logged in.
No mail.
Project:

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.

No plan.
%

%
.FI in brief

- Registry administrated by FICORA for ~two decades now
- Roughly 388k active domains
- 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
- Primary a.fi and secondaries [bcdefgh].fi
- The website: domain.fi (ficora.fi)
- The web service interface for registrars
  - until September 2
- The whois service
- The Odata service
- The EPP interface for registrars
  - from September 5
.FI switching to registry-registrar model

- September 5, 2016 at 10 AM local time
- Domain holders can no longer register directly from FICORA
- No longer open only for Finnish registrants
- No working DNS servers required for registration
- So far not a great success of reducing the number of FICORA customers
  - more than 2000 registrars already registered
.FI and DNSSEC

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

  - 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 (to come)**
  - 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 by registrars only:
  - www user interface
  - EPP interface
.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)
  - Current device deployed 2014
- Root server and signing functions operated by CSC IT Center For Science Ltd.
Validating resolvers

• Biggest providers in Finland (seem to) offer DNSSEC validating resolvers
  - “Official” information or statements hard to find / nonexistent
Thank You!


ari-matti.husa@ficora.fi
domain@ficora.fi
fi-domain-tech@ficora.fi