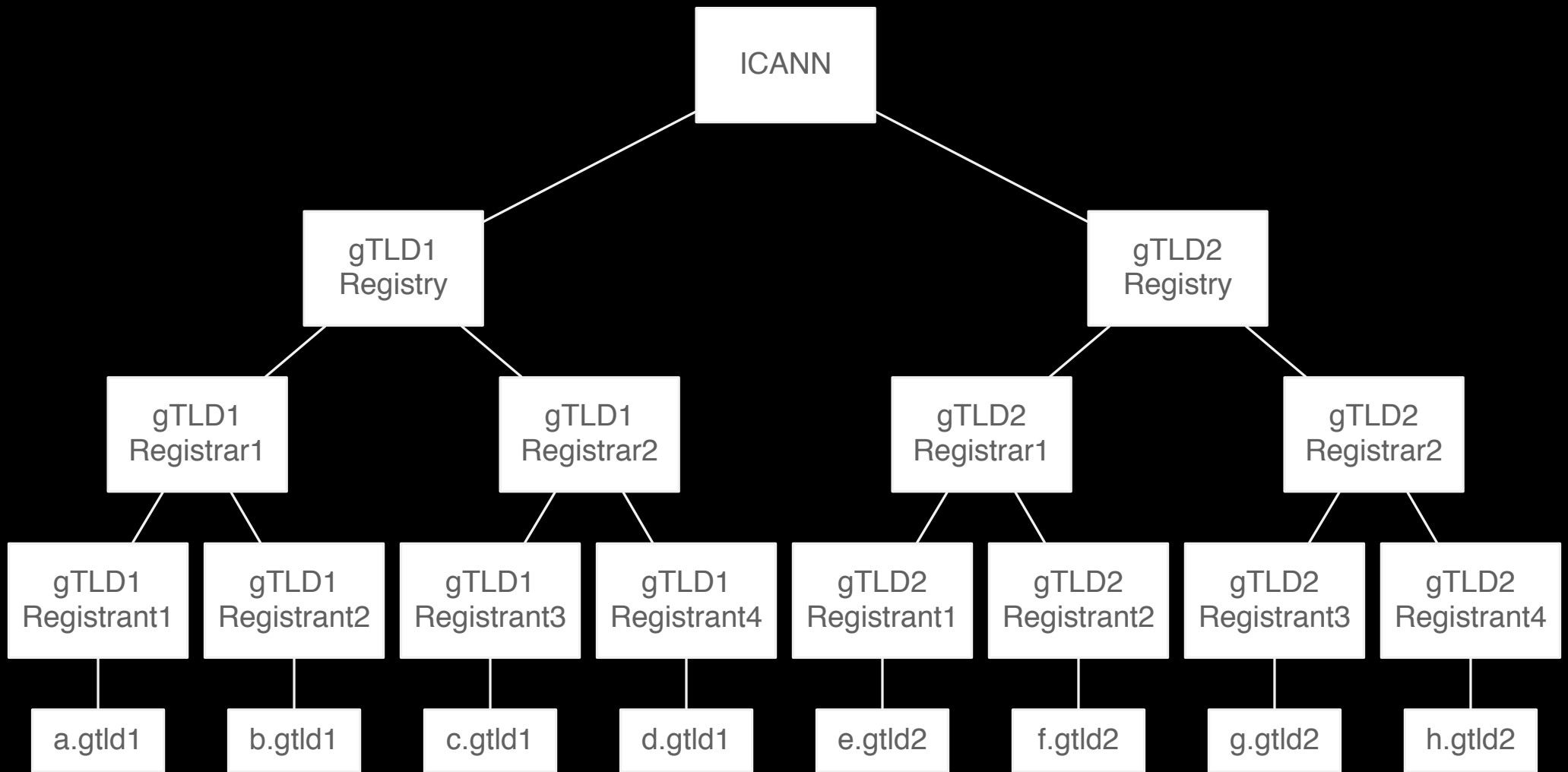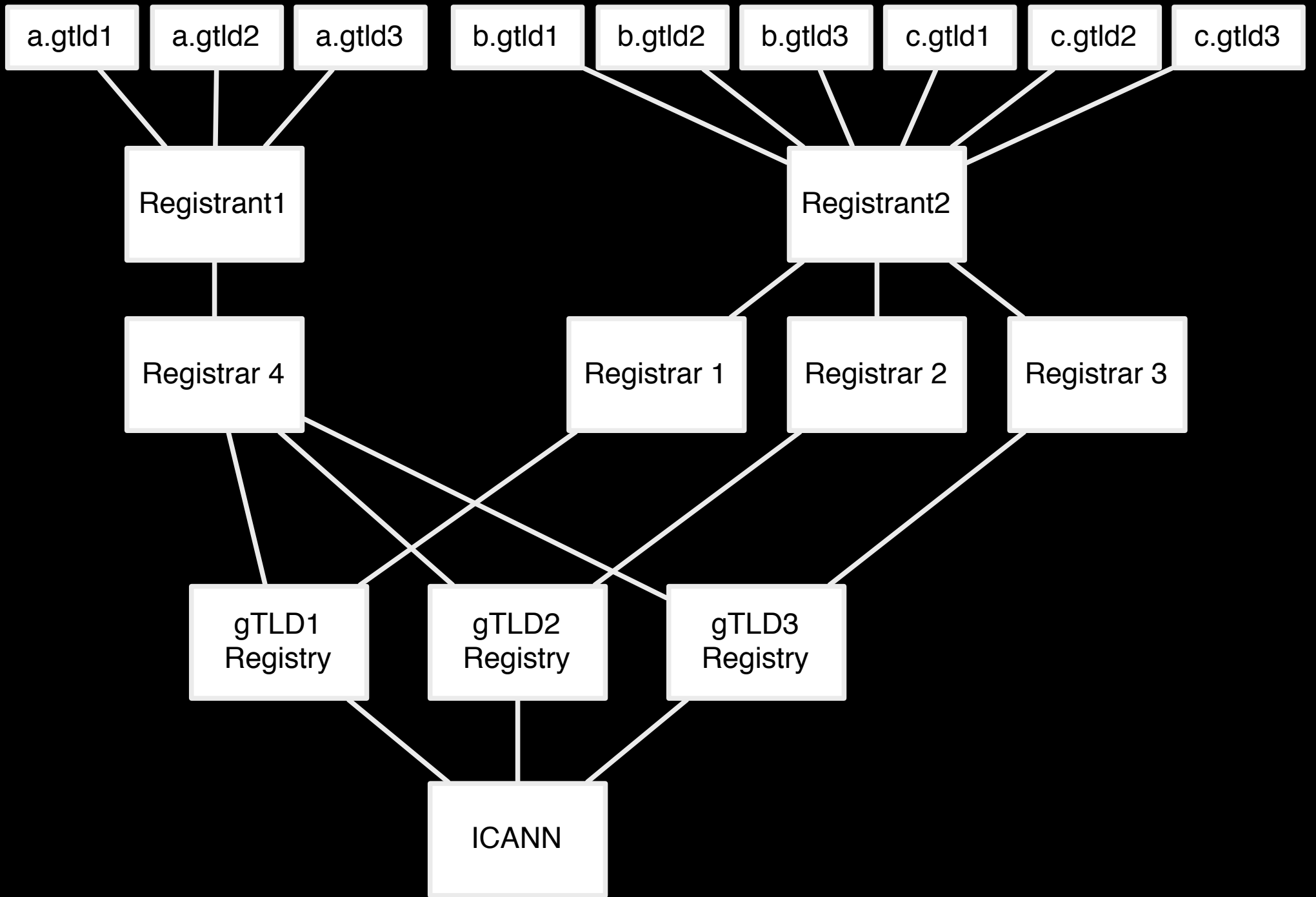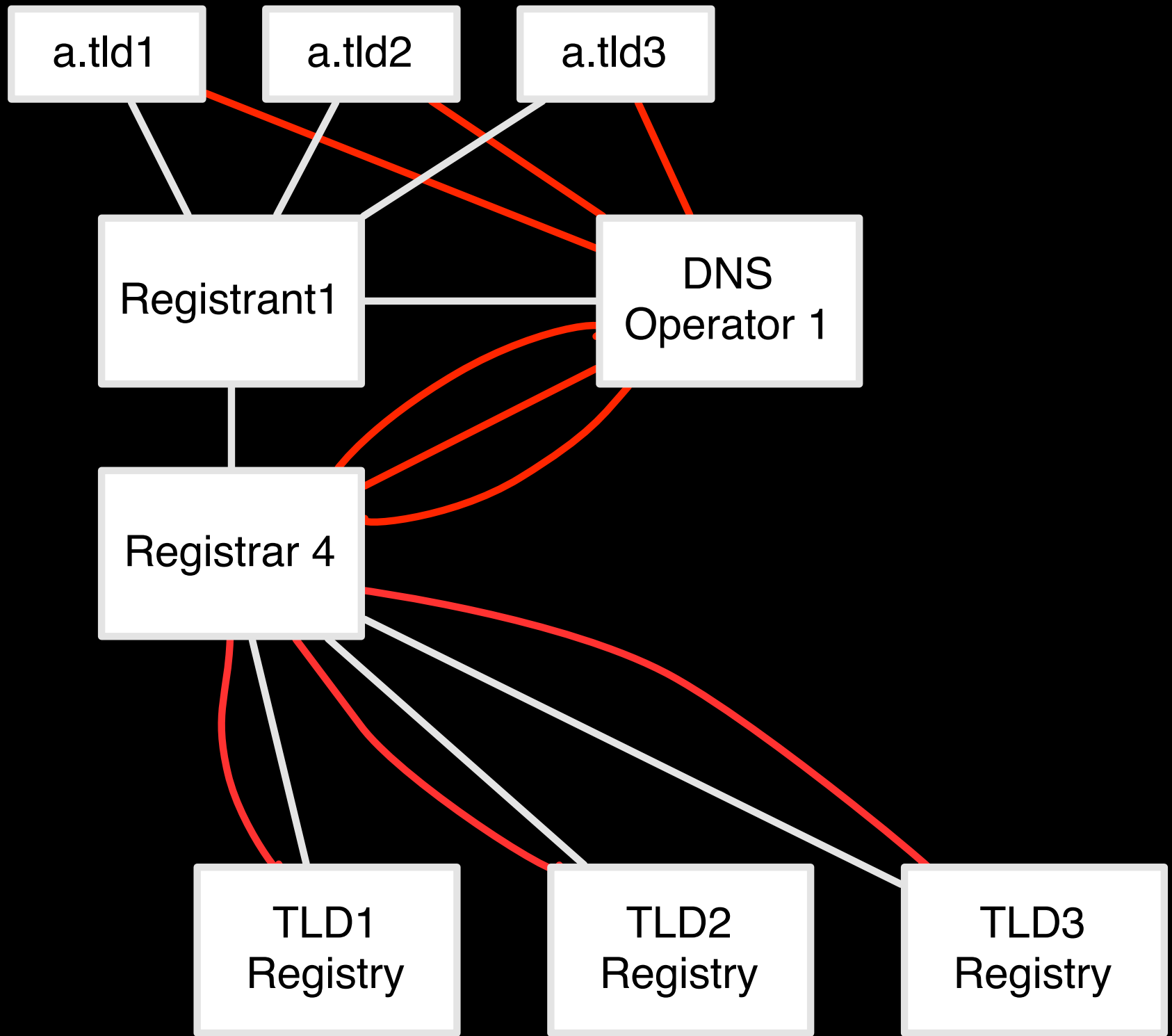DNSSEC and Registrars?

# Who am I?

- Employed by Netnod

  - IX, DNS, Root, NTP

- 50% owner of Frobbit!

  - Registrar ccTLD

  - DNS hosting etc

- SSAC Chair

# Perl Library Net::DRI version 0.96

- Net::DRI::DRD - Superclass of all Net::DRI Registry Drivers

- 48 different: ASIA, AT, AU, AdamsNames, BE, BIZ, BR, BZ, CAT, CIRA, COOP, CZ, CoCCA, DENIC, EURid, GL, Gandi, HN, ICANN, IENUMAT, IM, INFO, IRegistry, IT, LC, LU, ME, MN, MOBI, NAME, NO, NU, Nominet, ORG, OVH, OpenSRS, PL, PRO, PT, SC, SE, SIDN, SWITCH, TRAVEL, US, VC, VNDS and WS

- Net::DRI::Protocol::EPP::Extensions - Various extensions

- 34 different: AERO, AFNIC, ARNES, ASIA, AT, AU, Afilias, BR, CAT, CIRA, COOP, CZ, CentralNic, DNSBE, EurID, FCCN, GracePeriod, IENUMAT, IRegistry, IT, LU, MOBI, NAME, NO, NSgroup, NeuLevel, Nominet, PL, PRO, SE, SIDN, SWITCH, US and VeriSign

# Specifically for DNSSEC

5910 Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP). J. Gould, S. Hollenbeck. May 2010. (Format: TXT=72490 bytes) (Obsoletes RFC4310) (Status: PROPOSED STANDARD)

# 4.  DS Data Interface and Key Data Interface

This document describes operational scenarios in which a client can create, add, and remove Delegation Signer (DS) information or key data information for a domain name.  There are two different forms of interfaces that a server can support.  The first is called the "DS Data Interface", where the client is responsible for the creation of the DS information and is required to pass DS information when performing adds and removes.  The server is required to pass DS information for <domain:info> responses.  The second is the "Key Data Interface," where the client is responsible for passing the key data information when performing adds and removes.  The server is responsible for passing key data information for <domain:info> responses.

4.  DS Data Interface and Key Data Interface

   This document describes operational scenarios in which a client can create, add, and remove Delegation Signer (DS) information or key data information for a domain name.  There are two different forms of interfaces that a server can support.  The first is called the "DS Data Interface", where the client is responsible for the creation of the DS information and is required to pass DS information when performing adds and removes.  The server is required to pass DS information for <domain:info> responses.  The second is the "Key Data Interface," where the client is responsible for passing the key data information when performing adds and removes.  The server is responsible for passing key data information for <domain:info> responses.

# Why two?

- Search for accepting DS vs DNSKEY and you find discussions that have been going on for as long as we have been discussing DNSSEC, registry/registrar model and epp.

- We have not been able to converge...

# What's up?

- DNS operator passes DS **or** DNSKEY to registrar

- Registrar passes DS **or** DNSKEY to registry

- Registry places signed DS in their zone

# What's problematic?

- Some registries want DS, others DNSKEY

- Changing DNS operator is difficult

- Changing Registrar is difficult

- Being DNS operator and not registrar is difficult

- Synchronizing change of DNSSEC data in parent and child zone is…almost impossible

# Solutions?

- Out of band mechanism for bootstrap

- If one have trust via DNSSEC, and data is published, data can be fetched from the child zone

- Data should be fetched by **the registrar**

- Does still not solve the problem with different registries having different policies

# draft-ietf-dnsop-delegation-trust-maintainance?

Abstract

This document describes a method to allow DNS operators to more easily update DNSSEC Key Signing Keys using DNS as communication channel.  This document does not address the initial configuration of trust anchors for a domain. The technique described is aimed at delegations in which it is currently hard to move information from the child to parent.

# Patrik Fältström

Head of research and development
Netnod

Tel: +46-70-6059051
SIP/XMPP/Email: paf@netnod.se