.SE DNSSEC Practice Statement

Why and what?

.se

Based on RFC Draft defining a DPS framework

- DNSSEC Signing policy and practice statement framework.
- https://datatracker.ietf.org/doc/draft-ietf-dnsop-dnssec-dps-framework/

Authors:
Anne-Marie Eklund Löwinder, .SE

amel@iis.se

Fredrik Ljunggren, Kirei AB

fredrik@kirei.se

Tomofumi Okubo, Verisign

tookubo@verisign.com

Status of the framework draft

A second draft:

draft-ietf-dnsop-dnssec-dps-framework-01

Currently working on text for Definitions and Concepts. Then suggesting working group Last Call.

What is a DPS?

- Defines the establishment and management of keys to be used by a TLD*) in conjunction with DNSSEC.
- Describes the verification process for the links between a domain, a public key, a physical individual or legal entity (the registrant of the domain) and the name service provider (technical contact) for that domain.
- Contains a brief description of the verification procedures, the operational procedures ran by the TLD*) and how the TLD*) manages its keys.
- is intended to enable trusting parties to determine the level of trust they wish to grant to the TLD's*) DNSSEC management.

*) Or a second level domain

.se

.se

Why a DPS?

- To provide transparency to the relying parties.
- To gain trust.

To provide means for the relying parties to evaluate the trust and strength of the chain, registries may choose to publish DNSSEC Practice Statements (DPSs), comprising statements of critical security controls and procedures relevant to the relying parties.

Who should publish a DPS?

Registries on different levels of the DNS hierarchy:

- Root
- TLDs
- Large registrars performing signing of customers domains

Who should be interested in a DPS?

- High-value domain holders
- Trusting parties
- The DNS community

The framework - motivation

- Supports the harmonization of DNSSEC Policy and Practice Statements (DPS)
- Assist writers of DPSs
- Increased transparency may have a positive effect on security controls at registries

The framework - content

- Outline of topics that should be covered in a DPS
- Explanation of each topic
- Does not suggest security controls or DNSSEC parameters

.SE's DPS

- In conformance with the RFC Draft
- Published under the CC license
  http://creativecommons.org/licenses/by/2.5/

.se

Publication of DPS and other relevant DNSSEC information (1)

- .SE publishes DNSSEC-relevant information on .SE's web site at https://www.iis.se/en/domaner/dnssec/
- The electronic version of the DPS at this specific address is the official version.
- Notifications relevant to DNSSEC in .SE will be distributed by e-mail: dnssec-announce@lists.nic.se

Publication of DPS….(2)

- .SE publishes KSKs in the form of a DNSKEY and DS as follows:
  - IANA Interim Trust Anchor Repository (ITAR), https://itar.iana.org
  - .SE's web site http://www.iis.se/en/domaner/dnssec/publika-nycklar-for-dnssec/
  - Directly in the root zone (only DS; when available)
  - Emergency KSK sha256:

    se. 3600 IN DS 59461 5 2 6db388ddf76f74ec785a152ffb3479b2055cff7db44504b414f9052b0111b62c

- The public part of the .SE key Signing Key is signed with .SE's official PGP-key which may be found at http://subkeys.pgp.net:11371/pks/lookup?op=get&search=0xFCEC5128F440EE9B

.SE's DPS - content

- Operational requirements
- Management, operational and physical control
- Technical security controls
- Zone signing
- Compliance audit
- Legal matters

Thank you…

Questions?

Anne-Marie Eklund-Löwinder <anne-marie.eklund-lowinder@iis.se>