DPS framework

DNSSEC Signing policy and practice statement framework.

draft-ljunggren-dps-framework-00.xml
Anne-Marie Eklund Löwinder, .SE
amel@iis.se

Fredrik Ljunggren, Kirei AB
fredrik@kirei.se

...
DNSSEC

- Builds a chain of trust based on best effort
- The higher up in the DNS hierarchy, the higher the value
- KSK's needs to be known to the public – one way is using Trust Anchor Repositories (TAR's)
- Signed root eliminates need for TAR's
What is a DPS

- Defines the establishment and management of keys to be used by a registry in conjunction with DNSSEC.
- Defines roles and responsibilities.
- 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 operational procedures ran by the registry.
- Is intended to enable trusting parties to determine the level of trust they wish to grant to the registry's DNSSEC management.
PKI - a comparison

- CP + CPS
- Webtrust audit
- "Trusted" CA certificates gets distributed by vendors
Why a DPS?

• Provide transparency to the relying parties
• Gain trust
Who should publish a DPS?

- Registries
- ...

\[\text{se} \quad \text{kirei}\]
Who should be interested in a DPS?

- High-value domain holders
- Relying parties
- The DNS community
DPS framework - motivation

• Supports the harmonisation of DNSSEC Policy and Practice Statements (DPS).

• Assist writers of DPS's.

• Increased transparency may have a positive effect on security controls at registries.
The framework
content and scope

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