DNSSEC Project Outline

Olaf Kolkman

NLnet Labs document 2006-unansigned

December 14, 2006

Contents

About This Document

In order to deploy DNSSEC in existing infrastructure a number of steps will need to be made. This memo enumerates these steps. They can serve as the basis for the enumeration of a project plan.

This document was created during a workshop in Thailand and the version you received is only a snapshot of ongoing work. Feedback is appreciated.

The identifyer for this version of the document is svn: 79.

1 Project Milestones

1.1 Private Key policies and procedures

prerequisites none

description The policies and procedures concerning the private key handling are a prerequisite for designing your architecture. There are a number of issues that need thought, documentation and management signoff.

- The use of key signing and zone signing keys (KSK and ZSKs)
- Generation mechanism for keys
  - Who generates the keys
  - Where are the keys generated e.g. is there special hardware involved
  - How are the keys stored after generation

  - Technical consideration: what is the source of randomness.
  - What key lengths are used

- Who has access to the keys, is this different for KSKs and ZSKs
- Where and how are the keys stored in the production environment
- How long will the keys be used

Some of these decisions may influence the complexity of your operation. In practice the considerations will need to be based on a risk analysis *i.e.* what will happen if the key would be compromised.

1.2 Public Key policies and procedures

prerequisites

description The policies concerning the public key could be published publicly so that all users that use your key as a trust-anchor know what they are up to.

These policies are closely related to your private key policy and should document

- If and how a distinction can be made between zone signing keys (ZSKs) and key signing keys (KSK).
- Signing frequencies of KSK and ZSKs.
- Rollover frequencies of KSK and ZSKs.
- Rollover techniques used (Further considerations see [2] and [**?**]).
- How the keys are published and which off-band mechanism(s) for validation are offered.
- How changes to the policy are announced in a way such these announcements can be validated.
- How will emergencies be communicate and how can people validate such messages.

In appendix A we have reproduced an example public key policy statement inspired on the one in use by the RIPE NCC.

1.3 Signing infrastructure

prerequisites 1.2

description The signing infrastructure is all the infrastructure needed to turn unsigned records into signed records. The architecture of this setup depends on how your provisioning system generates data for the DNS and how the data is put into the DNS. If you use proprietary systems without zone-files you may not be able to depend on standard tools.

The design also depends on how access to the private keys (ZSK and KSKs) is arranged.

1.4 Server infrastructure

prerequisites External, software needs to support same features.

description All the servers, primary and secondary zones, need to be able to support the DNSSEC protocol. If one of the servers does not support DNSSEC there will be failures. If you choose to deploy NSEC3 all the servers will need to support NSEC3

There could be concerns with respect to growth of the size of the zonefiles as kept in memory or to increased traffic or CPU loads. In practice the memory concerns may be the most problematic. But the increase in memory can be predicted [3].

For well provisioned server infrastructure the increase in CPU or network traffic should not be a problem.

1.5 Monitoring tools

prerequisites 1.2

description Tools are essential to make sure that what is served is correct, that signatures will not expire and that your service levels are maintained.

When adding DNSSEC you will have to adapt or create monitoring tools.

1.6 Serving a Secured zone

prerequisites 1.4 1.5 1.2 1.2

description At this moment you are ready to load the first signed zone into your nameservers. It is also the moment you can publish your trust anchors.

1.7 Requesting secure delegation

prerequisites 1.6

description Once your zone is served you can request a secure delegation with your parent, or in absence of a signed parent approach ISC for an entry in their DLV registry.

1.8 Secure Delegation Provisioning

prerequisites 1.6

description For the provisioning of secure delegations you will have to perform two subtasks.

You will have to provide a method for the zone-owners to securely enter the key signing key into your provisioning system. It is good to realize that the method you use for exchanging NS RRs has the same security requirements as the method for exchanging the DS information.

The details of the system depend a lot on how your registry, and possibly registrars, are set up. For registry-registrar interaction it may be good to note that EPP[1] supports DNSSEC.

You are advised to device a method to prevent your children to enter secure entry-points for which there are no keys in the DNS *i.e.* you should try to prevent security lameness.

The second subtask is that the DS RRs should be pulled from your provisioning system into the nameservers. The details of this process are also dependent on your organization, but the process used for NS records can probably be cloned.

References

[1] S. Hollenbeck. *Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)*. RFC 4310 (Proposed Standard), December 2005. `http://www.ietf.org/rfc/rfc4310.txt`.

[2] O. Kolkman and R. Gieben. *DNSSEC Operational Practices*. RFC 4641 (Proposed Standard), September 2006. `http://www.ietf.org/rfc/rfc4641.txt`.

[3] Olaf Kolkman. *Measuring the resource requirements of DNSSEC*. RIPE NCC web pages. `http://www.ripe.net/ripe/docs/ripe-352.html`.

A Example DNSSEC key procedure

This is an example key policy, based on *i.e.* not a verbatim copy of, the key policy as developed for RIPE NCC.

- This procedure[1] applies to each zone that the is signed.
- Each zone with at least one Zone Signing Key (ZSK). A ZSK is zone specific.

[1] Based on the procedure published at the RIPE NCC

- The ZSK will be published in the DNSKEY Resource Record (RR) set and signed with a Key Signing Key (KSK).
- The KSKs will have a SEP flag set so that they can be distinguished from the ZSKs in the DNSKEY RR set.
- The ZSK may be rolled without making any announcement. The 'pre-publish rollover scheme' as published in RFC4641 [2] is used. This will avoid breaks in the chain of trust.
- During the first two years of deployment, the KSK of each signed zone will be rolled twice each year. The rollover scheme that we will follow is the 'double signature scheme' published in RFC4661[2]. There will be an overlap of three months to allow zone administrators to configure their new key. o At t=0 KSK1 signs the keyset. At t=3months KSK1 and KSK2 sign the keyset. DNS clients are expected to configure KSK2 during the three months that follow. At t=6months only KSK2 signs the keyset until (at t=9 months) KSK3 is introduced and a new rollover starts. o All zones at the RIPE NCC will roll their KSK simultaneously. Signatures are valid for one month. However, after announcing the change, the signing validity period may be changed to the shortest operationally possible period. Also see RFC4641[2] section 4.4.4. The ZSK will be an RSA/SHA1 key of 1200 bits (e RFC4641[2] section 3.5) The KSK will be an RSA/SHA1 key of 2048 bits.
- The KSKs to be used as 'trust-anchors' for our zones are published on a secure website in the format used in the 'trusted-keys' statement in BIND9 named configuration files.
- The KSK will also be published in the ISC DLV registry, but only until the root is signed.
- Any changes to this procedure and other announcements will be signed with our PGP key and published on our secure website and a dedicated mailing list.