RIPE NCC DNSSEC Policy

Doc-Id: RIPE-359
Author: RIPE NCC

October 2005

Introduction

The RIPE NCC is committed to supporting the deployment of DNS Security Extensions (DNSSEC) [1,2,3]. DNSSEC is a set of security extensions to the DNS that allows validating DNS resolvers to establish 'chains of trust' from known public keys to the data being validated. A full explanation of DNSSEC is out of the scope of this document. If you want this sort of information, please see [1,2,3,4 and 5].

During the resolution process, DNSSEC aware nameservers will provide secure delegations. These consist of a regular delegation (the NS record) to the nameservers that are authoritative for the child zone, as well as a signed pointer (the DS record) to a key that is authorised to sign the child zone. When the child and parent zone have exchanged keys, we can provide a secure delegation.

This document describes our policy for serving secured DNS data and key exchange. It does not cover deployment of DNSSEC by Local Internet Registries (LIRs) or others in our service region.

You should read this document alongside the Policy for Reverse Address Delegation of IPv4 and IPv6 Address Space in the RIPE NCC Service Region.

Policy

It is possible to secure delegations from the RIPE NCC under the Policy for Reverse Address Delegation of IPv4 and IPv6 Address Space in the RIPE NCC Service Region.

Our operational staff will deploy DNSSEC zone by zone. We will only exchange keys when parent domains are being signed. This will keep information current.

Key exchange between parent and child is based on the same authorisation and authentication mechanisms as the exchange of nameserver delegation information.

We will sign any announcements about secured DNS, such as changes in

RIPE NCC procedures, with our PGP key. We will publish procedures and announcements on our secure website (https://www.ripe.net/reverse/dnssec/) and also post these to an announcement mailing list (ripe-list@ripe.net). Procedures

The Public Key Procedure explains the procedure that we will follow with our keys. You will need this document if you plan to configure the RIPE NCC as a 'trust anchor' or if you receive a secure delegation from us.

The Registry Procedure explains how you can get a secure delegation.

Disclaimer

This policy and the related procedure are tailored towards the operation of a secured Domain Name System. They are not in any way tailored to the establishment of a certification authority similar to CAs used for X509 PKIs.

References

[1] DNS Security Introduction and Requirements, Arends et al, RFC4033, http://www.ietf.org/rfc/rfc4033.txt

[2] Resource Records for the DNS Security Extensions, Arends et al, RFC4034, http://www.ietf.org/rfc/rfc4034.txt

[3] Protocol Modifications for the DNS Security Extensions, Arends et al, RFC4035, http://www.ietf.org/rfc/rfc4035.txt

[4] DNSSEC HOWTO, O.M. Kolkman, RIPE NCC, http://www.ripe.net/projects/disi/dnssec_howto/

[5] http://www.dnssec.net/ a DNSSEC information portal