

Secure DNS Concerns at RIPE

Jim Reid, DNS WG Chairman
`dns-wg-chair@ripe.net`

Background

- Presentation to RIPE DNS Working Group at RIPE54 in Tallinn from TeliaSonera requesting a central repository for DNSSEC keys
 - Suggested criteria:
 - Neutral, trusted, operational expertise, etc.
 - Could/should RIPE NCC do this?

Working Group Debate

- Almost a 50-50 split
 - Half the WG felt a trusted key repository was needed
 - Other half didn't...
 - Or didn't want RIPE NCC to run it
- Suggested forming a task force to examine the options
 - Should report to WG at RIPE55 in October

RIPE DNS WG Concerns - I

- Proliferation of ad-hoc solutions:
 - DLV, “the next good/bad idea”, embedding trust anchors in name server configurations, etc.
 - Plenty of scope for interoperability problems and confusion
 - Worries over exit strategies, open-ended commitments, liability, authentication and so on
- All of these troubling and potentially destabilising
 - What if a name server using ad-hoc kludge A comes across a zone signed with ad-hoc kludge B?

RIPE DNS WG Concerns -2

- Use of ad-hoc solutions takes the pressure off those who should be leading DNSSEC deployment
- Why should the root or some TLD be signed if zones can “rely” on trust anchors elsewhere?
 - Alternate solutions short-circuit the demand for getting parent zones signed
 - DNSSEC-aware user base can go elsewhere
 - => reduced involvement in policy development

Consensus

- Working group agreed that they didn't want workaround solutions
- They wanted The Real Thing
- A public statement was necessary
- Should be supported by the entire RIPE community, not just the DNS Working Group

OUTCOME

- WG prepared a statement expressing concern at the lack of progress in DNSSEC deployment and calling on ICANN to expedite matters
 - Unanimously approved by DNS Working Group
 - Requested endorsement from wider RIPE community
 - Unanimous support at RIPE54 Closing Plenary
- Letter sent to Vint Cerf and Paul Twomey by RIPE NCC on behalf of RIPE community

The lack of progress towards the deployment of DNSSEC is undermining the stability and security of the internet. Operators and implementers are compelled to adopt ad-hoc, short-term solutions which will create long-term problems. The RIPE community urges ICANN to speed up and improve its efforts to get the root zone signed.