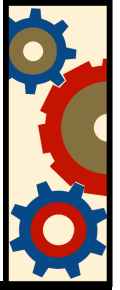


# DNSSEC Lookaside Validation (DLV)

Sofia, 2006



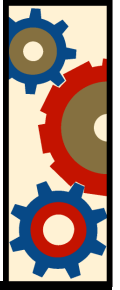
# Contents



- DNSSEC technical status
- The DNSSEC bootstrapping problem
- DNSSEC political status
- DLV
- DLV technical
- DLV registries



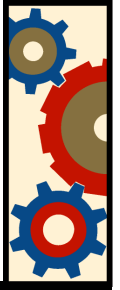
# DNSSEC technical status



- DNSSEC has been standardised at the IETF
  - Work continues in the dnsext working group
- DNSSEC servers exist (BIND, NSD, ...)
- DNSSEC resolvers exist (BIND, ...)



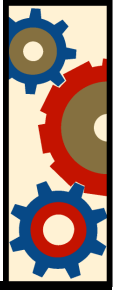
# The DNSSEC Bootstrapping Problem



- DNSSEC uses a hierarchical model
- The top is one or more “trust anchors”
  - Basically public keys that you configure
- Simplest solution is to start at the root
- If root is *not* signed, configure each TLD
  - Hundreds of TLDs, each with different keys
  - Maintenance would be a nightmare



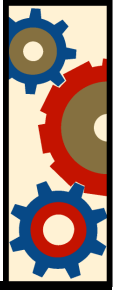
# DNSSEC political status



- The root zone is unsigned...
- ...and is not expected to be for a long time...
- ...if ever.



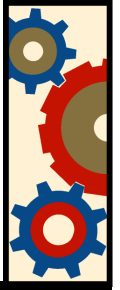
# DNSSEC political status



- Almost all TLD are unsigned.
- Some exceptions:
  - .SE
  - .RU (via forward)
  - .ORG/.MX testbeds
- Some other “important” zones are signed:
  - RIPE NCC reverse DNS trees
  - ISC.ORG ; )



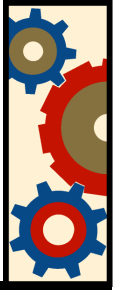
# DLV



- DNSSEC Lookaside Validation
- Repository of trust anchors
  - Remote
  - Signed
  - Accessed via DNS



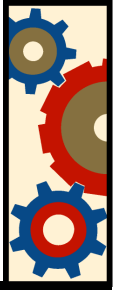
# DLV



- DLV is *NOT* meant to be permanent
  - Intended to ease bootstrapping
- DLV is not a change of protocol
  - There is a DLV record type, used instead of DS



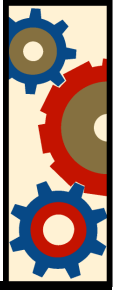
# DLV



- Documented in several places, including:
  - ISC-TN-2006-1 (ISC technical note)
  - Draft in IETF
- Currently implemented in BIND
- Not an IETF standardisation effort



# DLV technical

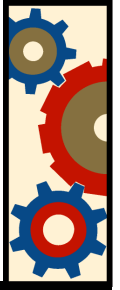


How does it work?

1. A DLV-enabled resolver tries to find a secure entry point using regular DNSSEC



# DLV technical

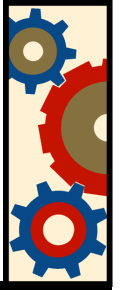


How does it work?

2. If the answer is provably unsecured, and DLV is configured, the resolver will try the DLV tree.



# DLV technical



How does it work?

3. The resolver strips off one domain at a time and queries the DLV server:

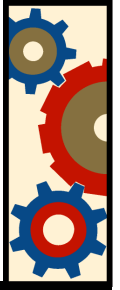
`www.example.org.dlv.isc.org`

`example.org.dlv.isc.org`

`org.dlv.isc.org`



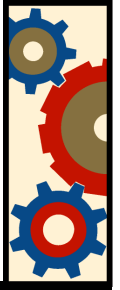
# DLV technical



- Separate DLV trees can be configured
  - Similar to how configuring trust anchors
  - Example: `dlv.isc.org` for root, `dlv.mil` for MIL
- DLV violates usual DNS chain of trust
  - Can be mitigated a bit if TLD join DLV



# DLV registries



- A DLV registry is a signed trust repository
- ISC operates one, `dlv.isc.org`
  - Open to any domain holder
  - Free
  - Especially interested in TLD participation
- Possible other groups will run others



# Questions, Discussion...

