Delegation Information (Referrals) Signer for DNSSEC
draft-fujiwara-dnsop-delegation-information-signer-00

K. Fujiwara
fujiwara@jprs.co.jp
dnsop WG, IETF 109
Motivation

• DNSSEC specifications don't protect the parent side NS RRSet and glue records in the delegation information.
  • It is a missing piece of DNSSEC
  • Why?
    • Parent side NS RRSet and glue records are not authoritative data of the parent zone
    • Parent zone cannot sign non-authoritative data
    • Authoritative servers can remove a part of glue records from response packets
    • Glue records are not well/exactly defined

• However, the referrals (parent side NS RRSet and glue records) are important information specified by customers for TLDs and RIRs (and Root)

• Currently, TLDs and RIRs (and Root) sign DS (and NSEC*) records only
Changes from 2005 (RFC 4033-4035)

• the word "in-domain" is defined by [RFC8499].
  • The in-domain glue is necessary and sufficient glue information for name resolution.

• draft-ietf-dnsop-glue-is-not-optional proposes:
  • “Glue records are expected to be returned as part of a referral and if they cannot be fitted into the UDP response, TC=1 MUST be set to inform the client that the response is incomplete and that TCP SHOULD be used to retrieve the full response.”

• Many DNS software developers understand that referrals (glue records) are non-authoritative data.

• Many DNS operators (includes TLDs, RIRs) avoid coexistence of parent zone and (direct) descendant zones on the same authoritative server.
One idea: Delegation information Signer (DiS)

• Reuse DS resource record
  • Assign a new DNSSEC Digest Type XX
    Delegation information Signer with SHA-256 (DISSHA256)
  • The key tag and algorithm field may require in further discussion.

• digest = SHA-256 hash( parent side NS RRSet | in-domain glue records)
  • NS RRSet and in-domain glue records are ordered as canonical order [DNSSEC]
  • Sibling and out-of-bailiwick glue records are not the data to calculate the hash
  • Another Idea: because sibling glue is also written in the parent zone, we can generate digest with all in-bailiwick glue records (need to determine)

• Parent zone signs DiS Resource Record as DS RRSet

• This proposal includes DiS data in the referral responses, DNSSEC validator can validate referral responses
An example of DiS record response

1. Remove old DiS
2. Generate new DiS
   2.1 Collect referral NS RRSet and in-domain glue
   2.2 Reorder NS RRSet and in-domain glue as DNSSEC canonical order [RFC 4034]
   2.3 Calculate SHA-256 hash
      SHA-256(  
      wide.ad.jp. 86400 IN NS ns.tokyo.wide.ad.jp.  
      wide.ad.jp. 86400 IN NS ns-wide.wide.ad.jp.  
      wide.ad.jp. 86400 IN NS mango.itojun.org.  
      wide.ad.jp. 7200 IN DS 32584 8 2 1D7EEF8BC...  
      );; ADDITIONAL SECTION:  
      ns.tokyo.wide.ad.jp. 86400 IN AAAA 2001:200:0:1::6  
      ns-wide.wide.ad.jp. 86400 IN AAAA 2001:200:0:1::f  
      ns.tokyo.wide.ad.jp. 86400 IN A 203.178.136.35  
      ns-wide.wide.ad.jp. 86400 IN A 203.178.136.59  
      wide.ad.jp. 86400 IN NS ns.tokyo.wide.ad.jp.  
      wide.ad.jp. 86400 IN NS ns-wide.wide.ad.jp.  
      wide.ad.jp. 86400 IN NS mango.itojun.org.  
      wide.ad.jp. 7200 IN A 203.178.136.59  
      ns-wide.wide.ad.jp. 86400 IN AAAA 2001:200:0:1::f  
      ns.tokyo.wide.ad.jp. 86400 IN A 203.178.136.35  
      ns.tokyo.wide.ad.jp. 86400 IN AAAA 2001:200:0:1::6  
2.4 Generated DiS data  
      wide.ad.jp 7200 IN DS 0 0 XX _SHA256_hash(NS|glue)  
3. Sign DS RRSet (contains generated DiS and original DS)
An example of DiS record validation

• dig +norec +dnssec @a.dns.jp wide.ad.jp

;; AUTHORITY SECTION:
wide.ad.jp. 86400 IN NS ns.tokyo.wide.ad.jp.
wide.ad.jp. 86400 IN NS ns-wide.wide.ad.jp.
wide.ad.jp. 86400 IN NS mango.itojun.org.
wide.ad.jp. 7200 IN DS 32584 8 2 1D7EEF8BC...
wide.ad.jp. 7200 IN DS 0 0 XX hash(NS|glue)
wide.ad.jp. 7200 IN RRSIG DS ...

;; ADDITIONAL SECTION:
ns.tokyo.wide.ad.jp. 86400 IN AAAA 2001:200:0:1::6
ns-wide.wide.ad.jp. 86400 IN AAAA 2001:200:0:1::f
ns.tokyo.wide.ad.jp. 86400 IN A 203.178.136.35
ns-wide.wide.ad.jp. 86400 IN A 203.178.136.59

• When a validating resolver receives a referral response with DS RRSet and the DS RRSet contains a DS resource record that have DISSHA256 digest type,
  • calculate digest from NS RRSet and in-domain glue from the referral response. (canonical order)
SHA-256(
wide.ad.jp. 86400 IN NS ns.tokyo.wide.ad.jp.
wide.ad.jp. 86400 IN NS ns-wide.wide.ad.jp.
wide.ad.jp. 86400 IN NS mango.itojun.org.
ns-wide.wide.ad.jp. 86400 IN A 203.178.136.59
ns-wide.wide.ad.jp. 86400 IN AAAA 2001:200:0:1::f
ns.tokyo.wide.ad.jp. 86400 IN A 203.178.136.35
ns.tokyo.wide.ad.jp. 86400 IN AAAA 2001:200:0:1::6)

• Compare the digest and the digest field from the DiS resource record
wide.ad.jp. 7200 IN DS 0 0 XX hash(NS|glue)
• If the digests differ, the referral is compromised or modified. The validating resolver can drop the referral.
Responses/Comments from dnsop mailing list

• Who signs?
  • DiS is a part of DS RRSet. It is signed by parent zone and it is the same as DS RRSet.

• TLD zone would become big. Because current DS registration ratio is very low, and DiS adds DS, NSEC/NSEC3, RRSIGs to all delegations.
  • It is not a problem for TLDs with a high DNSSEC deployment rate such as .SE.

• DNS is loosely coherent. DiS does not work when the sources of data are not coherent.
  • Many DNS operators (includes TLDs, RIRs) avoid coexistence of parent zone and (direct) descendant zones on the same authoritative server.
  • In-domain, or in-bailiwick glues are well defined
Questions?

- Why did not we decide signing referral information (parent NS + glue)?
- Is it a missing piece of DNSSEC?
- Do you have interests about signing referral information?
- Do you have another idea?
- Is it good to reuse DS resource record?
- Is the Delegation information signer idea good?