DNS SIG(0)

DNS Public Key Based Authentication/Authorization

draft-eastlake-dnsop-rfc2931bis-sigzero-02

Donald Eastlake 3rd d3e3e3@gmail.com

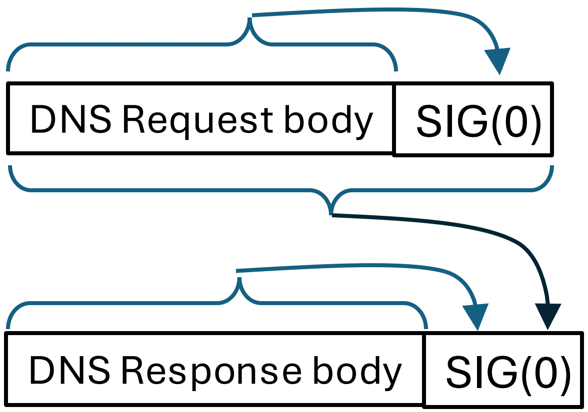
Johan Stenstam
johan.stenstam@internetstiftelsen.se

SIG(0)

- SIG(0) [RFC2931] is a meta DNS Resource Record (RR) providing DNS request and transaction security based on a public/private key signature. It has the structure of the RRSIG RR with a “Type covered” field of zero.
  - Being a meta (pseudo) RR means that it can be included in DNS messages, but it is not included in stored zone data.
- The corresponding public key is represented in a KEY RR [RFC2535] which has the structure of DNSKEY RR and can be stored in zone data or included, as is done in DNSSD Service Registration Protocol, in DNS messages.

SIG(0) uses

- Message integrity & origin/authority authentication
  - Request
    - Request signed by a private key at the requester
  - Transaction
    - Request and response signed by a private key at the server



- DNS UPDATE [RFC2136] Authorization
  - SIG(0) in request signed with a key indicating update authority for the zone.
- DNS based SRP FCFS UPDATE Authorization
  - SIG(0) in request signed with a key indicating continuity of the same requester [RFC9665].

TSIG

- TSIG (Transaction Signature, RFC 8945) is a meta RR providing efficient DNS request and transaction authentication based on a keyed hash algorithm and shared secret key. (transaction = concatenated request and response)
- TSSIG requires a shared secret key and does not apply to existing SRP. (However, it is possible by using TKEY [RFC2930] RRs and SIG(0) to dynamically configure secure shared secret keys.)

RFC 2931 SIG(0) RR Problems

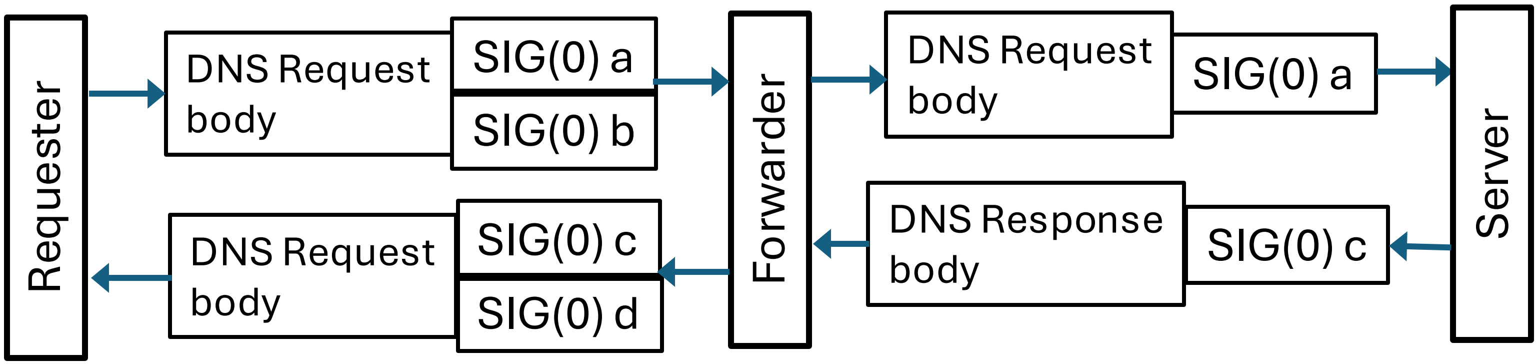
- Has no separate extended Error field, unlike TSIG and TKEY. So, an error separate from the overall DNS request error cannot be signaled.

- Has no Original ID field so forwarded authentication not obviously supported.
  - BIND supports multi-hop SIG(0) by forwarding with TCP with the same ID and maintaining a separate ID space per TCP connection.

SIG(0) Changes Being Considered

- [draft-eastlake-dnsop-rfc2931bis-sigzero-02]()
  - Removed statement that TCP support of SIG(0) is optional.
  - Added an EDNS(0) option to carry the Original ID and possibly return an error value.
  - Added section on considerations for forwarding servers.
  - Permits multiple SIG(0)s in a DNS message. (But not a SIG(0) and a TSIG and not multiple TSIGs.)
- [draft-berra-dnsop-keystate-01]()
  - Add an EDNS(0) option that can be used to synchronize SIG(0) key state.

Example of Multiple and Forwarded SIG(0)s



a) Authority and integrity for action at Server.

b) Integrity and possibly authorization at Forwarder.

c) Transaction integrity from Server.

d) Transaction integrity from Forwarder.

Questions?

END

Donald Eastlake 3rd d3e3e3@gmail.com

Johan Stenstam
johan.stenstam@internetstiftelsen.se

Historical RR Type Note

- Both DNS transaction security and DNSSEC data security originally used the
  - SIG (type = 24) and
  - KEY (type = 25) RRs [RFC2535].
- DNSSEC was changed to use the
  - RRSIG (type = 46) and
  - DNSKEY (type = 48) RRs [RFC4034].
- The corresponding RRs have the same field structure as each other. Transaction security continues to use the SIG and KEY RRs.