IKEv2 Configuration for Encrypted DNS

draft-btw-add-ipsecme-ike-03

IETF#111, July 2021

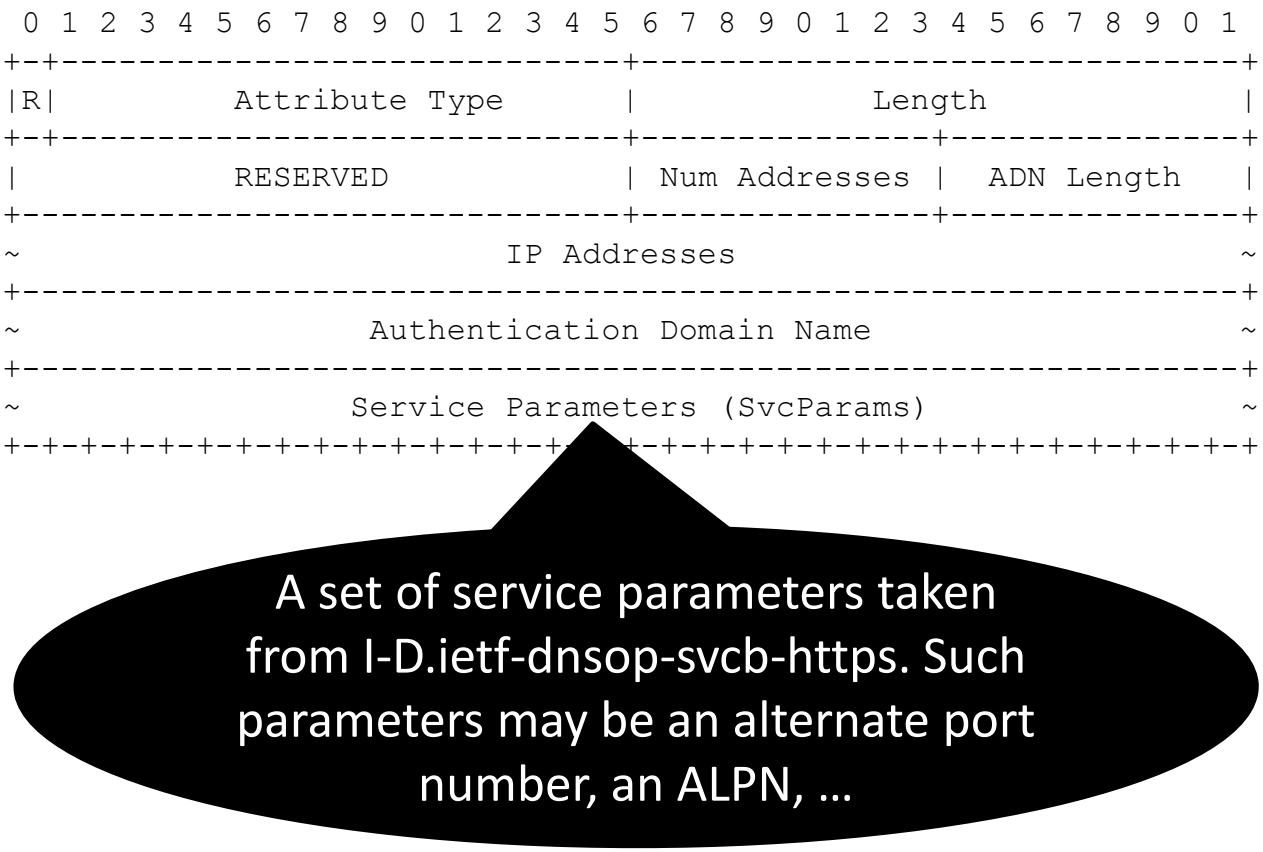
M. Boucadair (Orange)
T. Reddy (Akamai)
D. Wing (Citrix)
V. Smyslov (ELVIS-PLUS)

Changes Since IETF#110

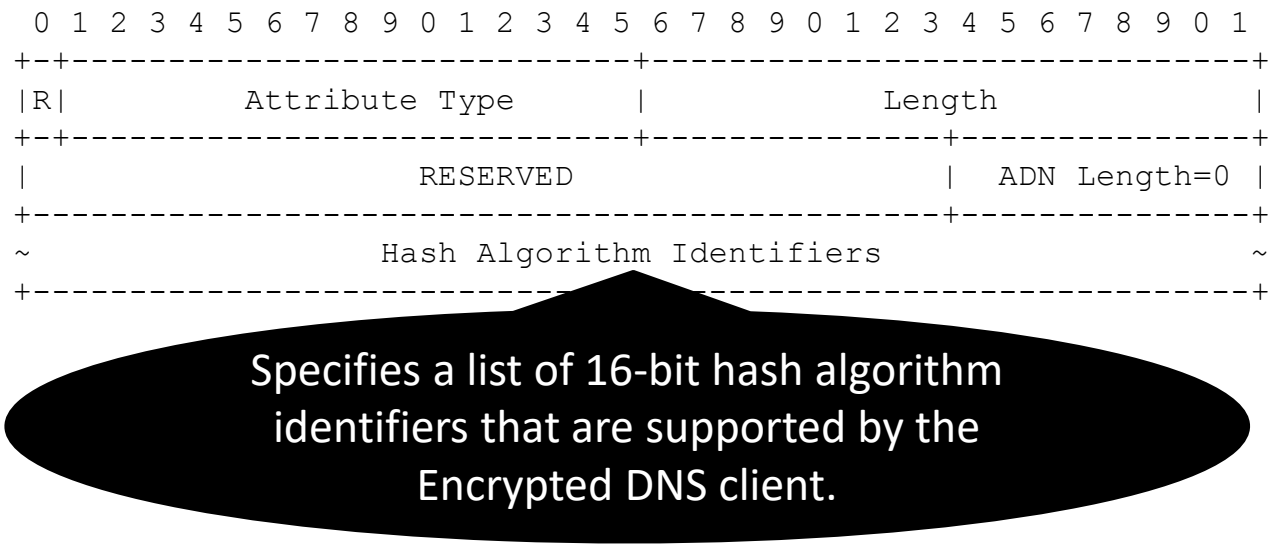
- ***Simplified design***
  - Align with recent I-D.ietf-add-dnr design (*ADD WG*)
  - Leverages SVCB

- Address comments raised by the WG in IETF#110
  - Move the deployment section to an appendix
  - ***Rely upon IKEv2 to validate the end-entity certificate***, instead of PKI: Add a new attribute ENCDNS_DIGEST_INFO

Simplified Design

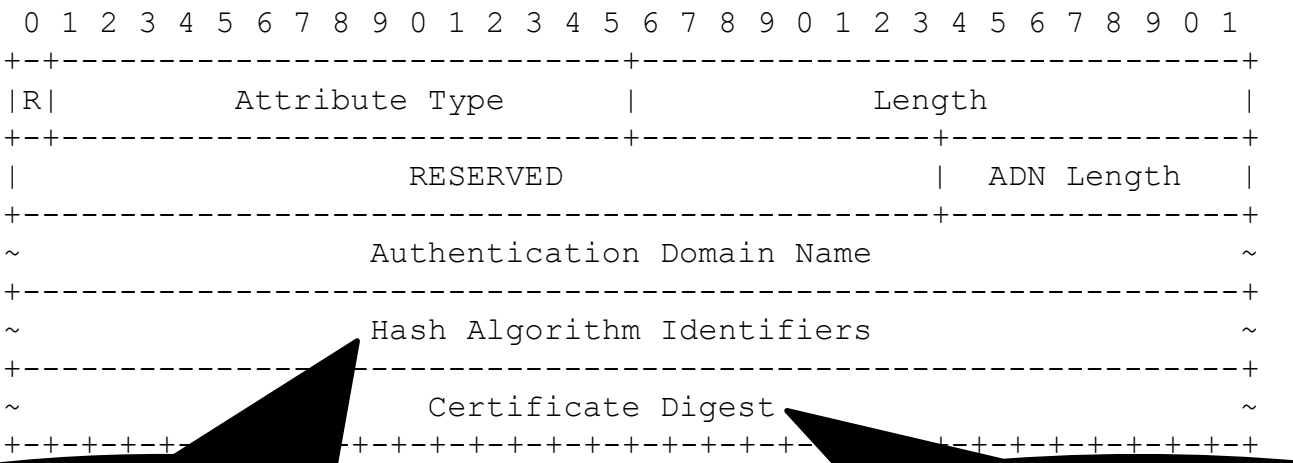


ENCDNS_DIGEST_INFO: Request



- No need for a new IANA registry
  - Values are taken from ***the IANA IKE's Hash Algorithm identifiers***
- SHA2-256 is mandatory-to-implement

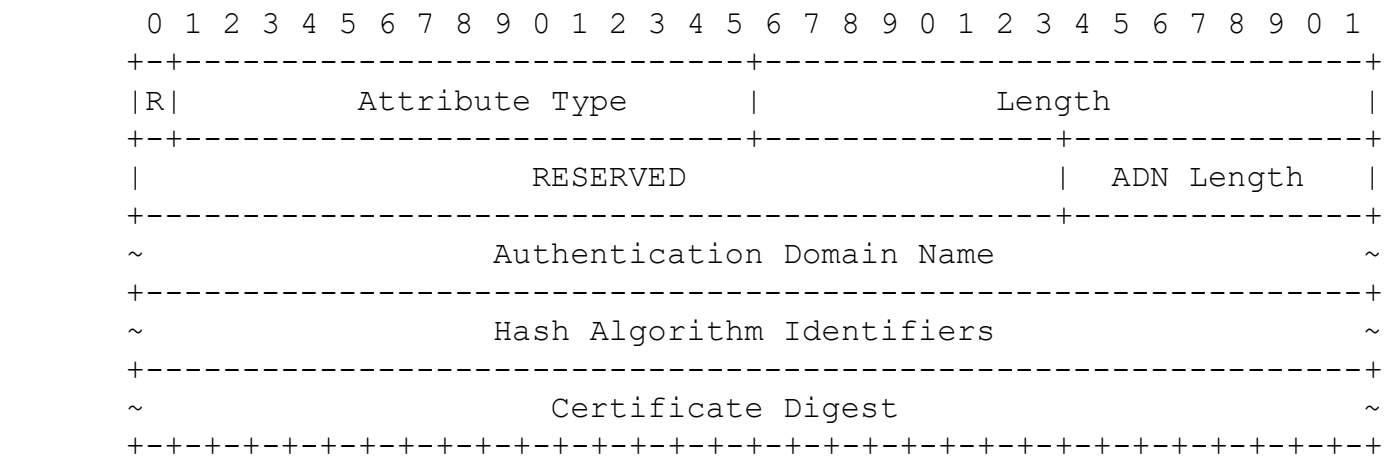
ENCDNS_DIGEST_INFO: Response

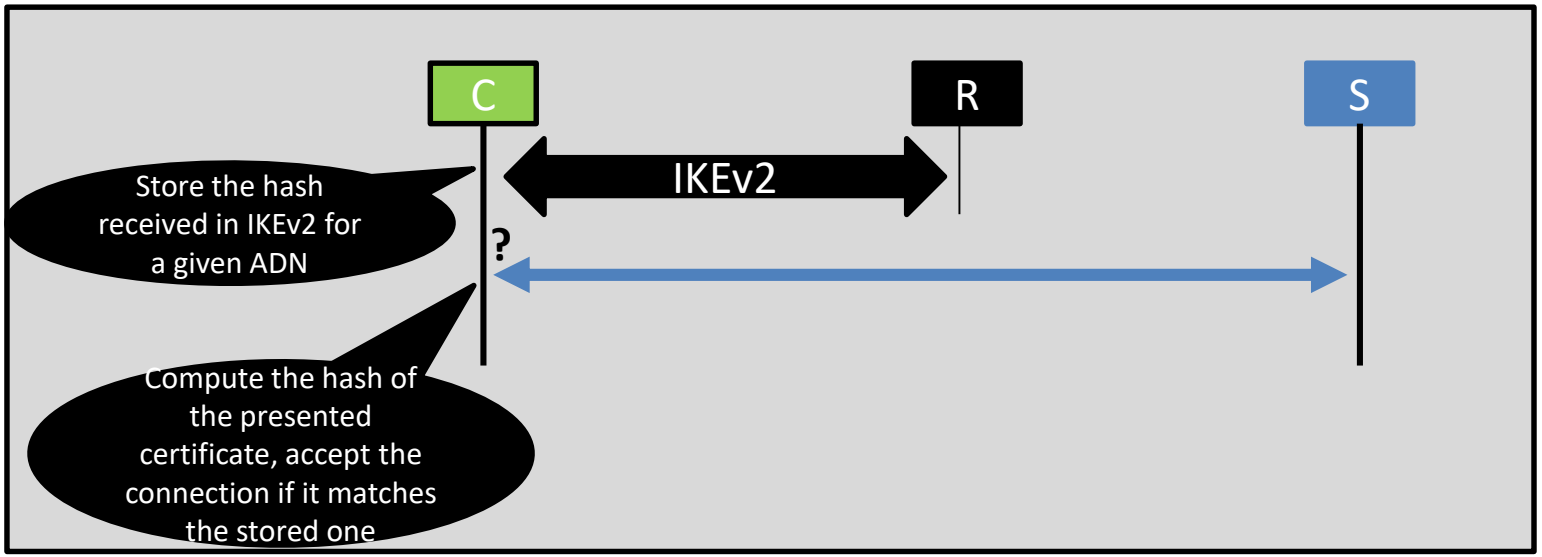


Specifies the hash algorithm identifier ***selected by the server*** to generate the digest of its certificate

Includes the digest of the Encrypted DNS server certificate using the selected hash algorithm

ENCDNS_DIGEST_INFO: Response





Next Steps

- Consider WG adoption