Client Certificates in DANE TLSA Records

Shumon Huque & Viktor Dukhovni

IETF 93, DANE Working Group
July 20th 2015, Prague, Czech Republic

https://tools.ietf.org/html/draft-huque-dane-client-cert-01

Client Certificates in DANE TLSA Records

- Owner name format:

```
_service.<domain-name>  IN  TLSA  <.. rdata ..>
```

```
_smtp-client.device1.example.com. IN TLSA (
      3 1 1 d2abde240d7cd3ee6b4b28c54df034b9
            7983a1d16e8a410e4561cb106618e971 )
```

Authentication Model

- Client has an identity assigned corresponding to a DNS domain name.

- Client has a private/public key pair and a certificate binding the domain name to the public key.

- Domain Name + Certificate has a corresponding signed DNS TLSA record

Client identity in Certificate

- Two options, Subject Alternative Name’s:
    - dNSName type
    - SRVName type

Signaling Client Id

- Server may want an explicit indication from the client that it has a TLSA record, to avoid unnecessary DNS queries in-band with TLS handshake.

- If raw public keys are being used (RFC 7250), the client needs to convey its identity explicitly.

- Some deployed client software reacts badly to unexpected Certificate Request messages.

Signaling Client Id

- A new TLS extension is proposed to convey DNS client identity (I-D will go out in the near future)

Client Requirements

- Must have a signed TLSA record published corresponding to DNS name and X.509 client certificate

- Client's name must appear in the certificate's dNSName or SRVname fields of the Subject Alternative Name

- [Future: client uses a TLS extension to signal identity explicitly to the server]

Server Requirements

- Send Certificate Request message in TLS handshake.
- Extract client identity from presented certificate.
- Construct DNS query name for corresponding TLSA record.
- Lookup & authenticate TLSA record in DNS.
- Extract rdata of TLSA record and match it to the client certificate.

More details

https://tools.ietf.org/html/draft-huque-dane-client-cert-01