draft-fanf-dane-smtp
draft-fanf-dane-mua

Presented by Paul Hoffman <paul.hoffman@vpnc.org>
Internet Drafts by Tony Finch <dot@dotat.at>

DNS-based Authentication of Named Entities

IETF 84 – Vancouver
Monday 30 July 2012

draft-fanf-dane-smtp

"Secure SMTP with TLS, DNSSEC and TLSA records"

- For SMTP between MTAs
  - message submission is covered by the next I-D
- Bigger goals than simply applying DANE to SMTP
  - Fix missing spec for which server identity to check
    - RFC 3207 (SMTP+TLS) does not say whether to check mail domain (MX owner) or host name (MX target)
  - Work around deployed base of unverifiable certs
    - Client needs indication that strict authentication should work
  - Prevent downgrade attacks
    - Otherwise what is the point? :-)
- Two main parts: one fairly solid, one somewhat speculative.
  - Sections 3 & 4: SMTP with TLSA
  - Sections 4 & 5: tracing use of DANE

draft-fanf-dane-smtp - sections 3 & 4

- Appendix B: Rationale
  - Why to authenticate SMTP server host name (MX target) not mail domain (MX owner)
  - Main consequence: DNSSEC is required regardless of DANE
- Section 3.1: MX lookup checks
  - Adds DNSSEC checks to RFC 5321 section 5
  - A "secure" result is required for the rest to apply else fall back to unauthenticated SMTP
  - *Question: does this section have the right level of detail?*
- Section 3.2: SMTP server checks
  - Applies RFC 6125 identity checking
  - And DANE checking
  - TLSA records imply strict transport security
- Section 4: how previous section applies to intra-domain SMTP

draft-fanf-dane-smtp - sections 5 & 6

Motivation: how can a postmaster track usage of TLSA records?

- Section 5: `Transmitted:` header field
  - Just like `Received:` but gives client's view of the connection
  - Includes TLSA marker in "`with`" clause
  - And which host name the client checked
    (can differ from server's idea of its name)
- Section 6: IANA considerations
  - New "`with`" protocol types
  - `Transmitted:` header field registration
  - "`dane`" MTA-name-type for use in delivery status notifications
- This is rather ugly and heavyweight and a bit crappy.

draft-fanf-dane-smtp - sections 5 & 6

Problems and alternatives:

- What to do when a message has a mixture of secure and insecure recipients for same server?
- Delivery status notifications are under-specified.
- Use an informational SMTP server extension instead of a header field?
- Put these sections in a separate document?

draft-fanf-dane-mua

"DNSSEC and TLSA for IMAP, POP3, and message submission"

- Builds on RFC 6186 "Use of SRV Records for Locating Email Submission/Access Services"
- TLSA records authenticate server host name
  - Same as draft-fanf-dane-smtp and draft-miller-xmpp-dnssec-prooftype
- TLSA records used to auto-configure transport security
  - Fixes an omission from RFC 6186
- Clarifies interaction with RFC 6125
  - Without DNSSEC the certificate must authenticate the mail domain (SRV owner) not the host name (SRV target)
  - At least one large mail provider got this wrong
- Grievously lacking in review & feedback!
  - Current text is probably too terse

draft-fanf-dane-mua - compatibility

Tricky coping with installed base

1. Old clients
   - Expect certificate to match server host name
   - Probably no TLS SNI
2. RFC 6186 clients
   - Ought to expect certificate to match mail domain
   - Might lack TLS SNI
3. DANE clients
   - Expect certificate to match server host name but mail domain is also OK
   - MUST have TLS SNI

- Can use SRV records to separate 1 from 2 & 3
- Can use TLS SNI to separate 2 from 3
- Can use multi-name certificates