Interim DANE WG

DNS-based Authentication of Named Entities

Telephone / Webex - 2014-12-02

Welcome to DANE

Chairs:

- Olafur Gudmundsson <ogud@ogud.com>
- Warren Kumari <warren@kumari.net>

~~Jabber Scribe:~~

- ~~dane@ietf.jabber.org~~

Minutes:

http://tools.ietf.org/wg/dane/minutes

- Note Well.
- Agenda Bashing.

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Process

- First time we are doing an interim - unclear on how to run this well.
- Please mute when not speaking.
- Please keep in mind that folk cannot see you, and so remarks may get misinterpreted.
- Planning on watching the jabber-room for comments / questions / requests to speak.
- Some folk have the tendency to pontificate at the mic. Please try and keep this under control.

Agenda

Very open agenda.

Here to discuss:
draft-ietf-dane-smime-07
draft-osterweil-dane-ent-email-reqs
draft-ietf-dane-openpgpkey-usage-01

Discussion on what is allowed to sign, and what is allowed to encrypt, and some discussion on revocation.
[Can / should that sign vs encrypt be in the certificate, or should it be in the DNS?]

Bob writes a mail on March 1st and then leaves the Acme, Inc. on March 2nd. Alice finally gets around to opening the mail 10 years later - should it validate?”
[Opens the whole “Difference between reception and acted on” - decrypt and store decrypted can of worms]

"Bob gets fired on March 2nd and is understandably disgruntled. He has his laptop at home and sends mail on March 3rd. Can Acme, Inc prevent this / invalidate the keys?
[Is simply removing the key good enough? Do we need a “This key explicitly revoked” option? Is lack of TLS revocation a good signal?]

Agenda (cont.)

```
Should we in the S/MIME DANE documents explicitly support “policy
expressions” ?
  e.g: A way to publish that all email from an organization / domain
is signed?
```