

DANE WG

DNS-based Authentication of Named Entities

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.
- Blue Sheets.
- 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.

Blue Sheets

- Please fill these in.

Agenda

Administrivia DANE status.

Chairs - 5 min

DANE activities in Other WGS

Chairs - 5 min

Working group documents: est 16:50

SRV and & SMTP status

<http://tools.ietf.org/html/draft-ietf-dane-smtp-with-dane-10>

<http://tools.ietf.org/html/draft-ietf-dane-srv-06>

Chairs 10 min

OPENPGP and SMIME status

<http://tools.ietf.org/html/draft-ietf-dane-openpgp-00>

<http://tools.ietf.org/html/draft-ietf-dane-openpgpkey-usage-00>

<http://tools.ietf.org/html/draft-ietf-dane-smime-06>

Chairs 5 min

DANEbis and operational guidance

<http://tools.ietf.org/html/draft-ietf-dane-ops-05>

Wes Hardaker - 30 minutes.

Agenda (cont.)

TLSA Raw Keys

<http://tools.ietf.org/html/draft-ietf-dane-rawkeys-00>

Paul Wouters 20 min

New proposals for DANE est 17:55

A DANE based solution for improving the security of HTTPS in CDN

<http://netsec.ccert.edu.cn/duanhx/files/2014/05/httpsincdn.pdf>

Haixin Duan -- 25 min

Only if there is time:

"Reverse DANE" i.e. can server check TLSA records for client?

<no draft>

Chairs - 10 min

End of meeting

SRV and & SMTP status

<http://tools.ietf.org/html/draft-ietf-dane-smtp-with-dane-10>

<http://tools.ietf.org/html/draft-ietf-dane-srv-06>

OPENPGP and SMIME status

<http://tools.ietf.org/html/draft-ietf-dane-openpgp-00>

<http://tools.ietf.org/html/draft-ietf-dane-openpgpkey-usage-00>

<http://tools.ietf.org/html/draft-ietf-dane-smime-06>

DANEbis and operational guidance

<http://tools.ietf.org/html/draft-ietf-dane-ops-05>

Wes Hardaker

TLSA Raw Keys

<http://tools.ietf.org/html/draft-ietf-dane-rawkeys-00>

Paul Wouters 20 min

A DANE based solution for HTTPS in CDN

<http://netsec.ccert.edu.cn/duanhx/files/2014/05/httpsincdn.pdf>
Haixin Duan -- 25 min

Reverse DANE!

Topic: How/if can a server lookup client DANE key?
Some protocols send names via handshake
some protocols only have the address of the client

How to scope this potential work ?
Are there general principles or does this need to be on a
protocol by protocol basis?