

# DANE Authentication for Network Clients Everywhere (DANCE)

Chairs:

Wes Hardaker

Joey Salazar

Mailing List:

<https://www.ietf.org/mailman/listinfo/dance>



# Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

By participating in the IETF, you agree to follow IETF processes and policies.

If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.

As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.

Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (<https://www.ietf.org/contact/ombudsteam/>) if you have questions or concerns about this.

# Note Well, page 2

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

[BCP 9](#) (Internet Standards Process)

[BCP 25](#) (Working Group processes)

[BCP 25](#) (Anti-Harassment Procedures)

[BCP 54](#) (Code of Conduct)

[BCP 78](#) (Copyright)

[BCP 79](#) (Patents, Participation)

<https://www.ietf.org/privacy-policy/> (Privacy Policy)

# IETF Code Of Conduct Guidelines

RFC7154

1. Treat colleagues with respect
2. Speak slowly and limit the use of slang
3. Dispute ideas by using reasoned argument
4. Use best engineering judgment
5. Find the best solution for the whole Internet
6. Contribute to the ongoing work of the group and the IETF

Please keep these in mind both at the mic and on Jabber/Meetecho IM

# DANCE WG Information

## **DANCE information:**

Datatracker: <https://datatracker.ietf.org/group/dance/about/>

Purpose: Extend DANE to encompass TLS client authentication using certificates or Raw Public Keys (RPK).

## **Mailing list information:**

List: [dance@ietf.org](mailto:dance@ietf.org)

Subscribe: <https://www.ietf.org/mailman/listinfo/dance>

## **Active drafts to consider:**

draft-dance-architecture-01

draft-dance-tls-dane-clientid-01

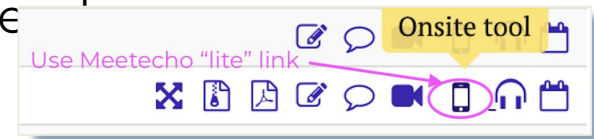
draft-dance-dane-client-cert-01



# This session is being recorded

## In-person participants

- Make sure to sign into the session using the Meetecho (usually the “onsite tool” client) from the Datatracker age
- Use Meetecho to join the mic queue
- *Keep audio and video off if not using the onsite version*



## Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session
- Use of a headset is strongly recommended

# Agenda

- |                                |                      |     |
|--------------------------------|----------------------|-----|
| 1. WG Introduction             | Chairs               | 5m  |
| ○ Note-takers: needed!         |                      |     |
| 2. DANCE Last Call discussion  | Chairs               | 25m |
| 3. IoT authentication in AfNIC | Gaël Berthaud-Muller | 20m |
| 4. Open MIC / Future of DANCE  | WG                   | 10m |

# last call summary: [draft-dance-tls-dane-clientid](#)

## Comment Summary:

- The draft SHOULD say what RR content it expects
- Needs a check regarding the supported TLS version, the reference used for framing extensions (RFC6066 vs RFC8446) and for the architecture document
- Request for clarity on the ClientName limit definition and the decode\_error alert and a closedown of the connection when using empty dane\_clientid extensions defined as <1..255>
- Request for consideration of the use case for mixed environments in terms of certificate\_authorities
- More stiff requirements suggested in order to improve interoperability and reduce code complexity

Conclusion: update needed but otherwise ready to go



# last call summary: [draft-dance-dane-client-cert](#)

## Comment Summary:

- Request to add domain name example and text on the use of wildcards and DANE-TA
- Request to consider the potential need to encode the transport label
- Request for clarity on the security considerations from RFCs 6698 and 7671
- Request for clarity on the exception that allows for SHOULD when using X.509 certificate and a suggestion to change it to MUST
- Smaller wording suggestions and nits IRT DNSSEC validation, distinction between TLS and DTLS, [\_service] and device notation, references for both RFCs and inactive drafts

Conclusion: update needed but otherwise ready to go

## DANCE Last Call results

**Update from the authors coming soon**



# Agenda

- |   |                  |     |
|---|------------------|-----|
| 1. WG Introduction                            | Chairs           | 5m  |
| ○ Note-takers: Korry Luke, Michael Richardson |                  |     |
| 2. DANCE Last Call results                    | Chairs           | 10m |
| 3. Updates on dance-architecture              | Olle and Michael | 20m |
| 4. Open MIC / Use Case Reports                | WG               | 15m |
| ● Wataru “Alt” Ohgai                          |                  |     |

