

DANCE Last Call(s) Discussion @ IETF-118

Joey Salazar and Wes Hardaker

November 6, 2023

Outline

Background

Last call comment discussion: [draft-ietf-dance-client-auth](#)

Last call comments about [draft-ietf-dance-tls-clientid](#)

Last Call Comments

- ▶ A number of comments received on both
- ▶ Some discussion on the list
- ▶ Mostly radio silence afterward

Goal today

- ▶ **Goal:** Resolve these finally with mic discussion
- ▶ **Discussion structure:**
 - ▶ We describe the comment
 - ▶ We propose a "Suggestion" path forward based on the comment/discussion to date
 - ▶ You talk
 - ▶ We take consensus
- ▶ DANCE!
- ▶ (and we verify the results on the list)

Comments on

- ▶ Resolving LC comments about [draft-ietf-dance-client-auth](#)

Examples needed

Comment From: Rick van Rein

Notes:

- ▶ could use examples for:
 - ▶ domain names
 - ▶ wildcards and DANE-TA

Suggestion: Volunteer needed to add an easy example

Suggestion: /or/ point to architecture document?

Suggestion: /or/ point to use-cases document?

Encoding the transport label

Comment From: Michael Richardson

Notes:

- ▶ The transport label encoding may not be needed,
- ▶ both TLS and DTLS are functionally dual-usable already
- ▶ the current draft already says the transport label is not needed

Suggestion: leave as is

clarity on the security considerations

Comment From: Robert Moskowitz

Notes:

- ▶ Are there privacy concerns because of client identity harvesting in DANCE?
- ▶ do we need a better security consideration section description?

Suggestion: Mention this consideration in the security consideration

X.509 certificates should be a MUST

Comment From: Michael Richardson

Notes:

- ▶ Why is there an exception that allows for SHOULD when using X.509 certificate

Suggestion: Change it to MUST

Comment From: Michael Richardson

Notes:

- ▶ Smaller wording suggestions and nits IRT DNSSEC validation, distinction between TLS and DTLS, [_service] and device notation, references for both RFCs and inactive drafts
- ▶ Message-ID: 763667.1668330590@dias

Suggestion: Accept and act on the nits

LC comments

- ▶ resolving LC comments for [draft-ietf-dance-tls-clientid](#)

Needs a check regarding the supported TLS version

Comment From: Michael Richardson

Notes:

- ▶ We have a reference to TLS 1.2 and 1.3 and DTLS 1.3
- ▶ We have a reference to RFC8446 (framing extension)

Suggestion: This extension supports both TLS 1.2 [RFC5246] and TLS 1.3 [RFC8446], and future TLS versions. DTLS [RFC6347] is also supported. The term TLS in this document is used generically to describe all protocols.

Suggestion: A reference to RFC6066 is not needed (TLS extensions)

Request for clarity on the ClientName limit definition

Comment From: Rick van Rein and Michael Richardson

Notes:

- ▶ dane_clientid extensions defined as <1..255>
- ▶ TLS encodes names as ascii
- ▶ DNS encodes them as 255 character limit names
 - ▶ (with a trailing dot/null indicating the root zone)

The decode_error alert and a closedown of the connection when using empty dane_clientid extensions defined as <1..255>

- ▶ We require ClientName to be non-empty
- ▶ Do we ever need to require an extension with a zero-length ClientName?

Suggestion: ensure the text properly shows the difference between the TLS length required vs the DANE request length required.

Use stiffer requirements

Comment From: Rick van Rein and Michael Richardson

Notes:

- ▶ More stiff requirements suggested in order to improve interoperability and reduce code complexity
- ▶ "When using X.509 certificate authentication, it SHOULD send this extension."

Suggestion: SHOULD -> MUST

The draft SHOULD say what RR content it expects

Comment From: Robert Moskowitz

Notes:

- ▶ Interpretation: DANE has multiple usage/etc models now, should we specify which are usable in this context?

Suggestion: drop this suggestion as it adds more strictness than is necessary. Disagreement about whether or not this should go into this document vs a more specific one if needed.

Use case for mixed environments in terms of certificate_authorities

Comment From: Rick van Rein?

Notes:

- ▶ Use case for mixed environments in terms of certificate_authorities
- ▶ likely in the context of an ownership change

Suggestion: ???