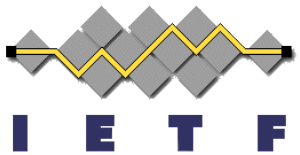
MMUSIC WG

Liaison from W3C WEBRTC WG

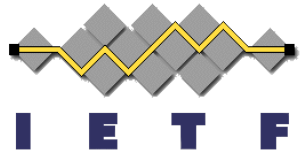
Bernard Aboba

March 30, 2017

IETF 98



W3C Liaison Request



- Request from W3C WEBRTC WG for MMUSIC WG consensus determination:
  - Issue: interpretation of text in Section 6.2 of draft-ietf-mmusic-4572-update (carried over from RFC 4572).
  - Relevant to open issue in WebRTC specification:
    - https://github.com/w3c/webrtc-pc/issues/849
- Original posting to MMUSIC WG list:
  - https://www.ietf.org/mail-archive/web/mmusic/current/msg17646.html
- Posting to IETF liaison web page in progress:
  - https://datatracker.ietf.org/liaison/

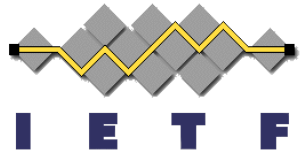
Section 6.2 text

Note that when the offer/answer model is being used, it is possible for a media connection to outrace the answer back to the offerer. Thus, if the offerer has offered a 'setup:passive' or 'setup:actpass' role, it MUST (as specified in RFC 4145 [7]) begin listening for an incoming connection as soon as it sends its offer. **However, it MUST NOT assume that the data transmitted over the TLS connection is valid until it has received a matching fingerprint in an SDP answer.** If the fingerprint, once it arrives, does not match the client's certificate, the server endpoint MUST terminate the media connection with a bad_certificate error, as stated in the previous paragraph.

Questions

1. May data received over the data channel be provided to the application prior to verification?
2. May received media be played out prior to verification?

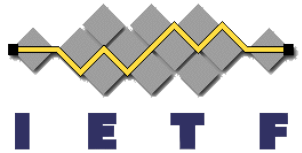
List Discussion



May data received over the data channel be provided to the application prior to verification?

- Martin: no, but holding data should be fine.
- EKR: Might be better to discard datachannel data, but not sure why it would be necessary.
- Inaki: Discarding data channel data could be catastrophic.

List Discussion (cont'd)



May received media be played out prior to verification?

- Martin: Of two minds. Could make origin-purity argument, but can isolate media from origin. Odds of attack would *seem* to be low.
- Roman: data is received, decoded and discarded until fingerprint is received and verified. This way DTLS handshake completes, key frames are decoded, but user is not presented with any unverified media.
- EKR: Ought to be safe to hold anything you receive prior to getting the fingerprint.
- Cullen: Policy question at the application layer.

Request

Can the consensus of the MMUSIC WG be determined?