Audio/Video Transport Core Maintenance Working Group

Magnus Westerlund
Roni Even

http://tools.ietf.org/wg/avtcore/charters

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

– 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.

Agenda bash - Monday

13:00   AVTCore Status Update   (Chairs, 15)

13:15   Circuit Breakers for Unicast RTP Sessions   (Colin Perkins, 10)

13:25   Sending Multiple Media Streams in a Single RTP Session   (Magnus Westerlund, 20)

13:45   Requirements for Private Media in a Switched Conferencing Environment (Paul Jones, 15)

14:00   A Solution Framework for Private Media in a Switched Conferencing (Paul Jones, 30)

14:30   Encrypted Key Transport for Secure RTP   (John Mattsson, 15)

14:45   Multiplexing Scheme Updates for SRTP Extension DTLS   (Marc Petit-Huguenin, 15)

15:00   End

Document Status

- RFC Published - none
- IESG processing
  - draft-ietf-avtcore-srtp-aes-gcm-14
    - Waiting for conclusion - separate slide
  - draft-ietf-avtcore-aria-srtp-07
    - Was waiting for draft-ietf-avtcore-srtp-aes-gcm
    - Waiting for authors to split the document as agreed in last meeting

Document Status

- Other documents – not presented
  - Multipath RTP in draft-ietf-avtcore-mprtp-00
    - Now a WG document
  - RTP topologies indraft-ietf-avtcore-rtp-topologies-update-06
    - Done - going to IESG

Document Status

- Other documents – not presented
  - Sending Multiple Types of Media in a Single RTP Session in draft-ietf-avtcore-multi-media-rtp-session-07
    - Ready for WGLC
  - Sending Multiple Media Streams in a Single RTP Session: Grouping RTCP Reception Statistics and Other Feedback in draft-ietf-avtcore-rtp-multi-stream-optimisation-05
    - Ready for WGLC
  - Guidelines for using the Multiplexing Features of RTP to Support Multiple Media Streams in draft-ietf-avtcore-multiplex-guidelines-03
    - Need editorial work

AES-GCM and AES-CCM Authenticated Encryption in Secure RTP (SRTP)

- draft-ietf-avtcore-srtp-aes-gcm-14

- Is in IESG Evaluation
  - Stephen Farrel (Sec AD) raised an issue
    - The number of protection profiles was large (TLS has real issue)

- Mailing list and phone conference resulted in
  - AES-CCM is removed from draft
    - No plan to publish it – Raise requirements if you need it
  - AES-GCM a smaller number of profiles was selected:
    - AEAD_AES_128_GCM (with 16 byte authentication tag)
    - AEAD_AES_128_GCM_64 (with 8 byte authentication tag)
    - AEAD_AES_256_GCM (with 16 byte authentication tag)

- Waiting for Authors to submit revised ID

Current Milestone Review

- Feb 2015 - Submit in band keying mechanism for SRTP draft for Proposed Standard
- Feb 2015 - Submit Update to RTP Topologies (RFC 5117) for Informational
- Mar 2015 - Submit Real-Time Transport Control Protocol (RTCP) in Overlay Multicast for Proposed Standard
- Apr 2015 - Submit Multiple Media Types in an RTP Session for publication as proposed standard
- Apr 2015 - Submit Update to the RTP Specification (RFC3550) regarding Sending Multiple Media Streams in a Single RTP Session: Grouping RTCP Reception Statistics and Other Feedback as proposed standard
- Apr 2015 - Multiplexing Scheme Updates for SRTP for DTLS
- May 2015 - Submit Guidelines for using the Multiplexing Features of RTP for Informational
- May 2015 - Submit Update to the RTP Specification (RFC3550) regarding Sending Multiple Media Streams in a Single RTP Session as proposed standard
- Jun 2015 - Submit RTP Congestion Control: Circuit Breakers for Unicast Sessions for publication as proposed standard
- Nov 2015 - Submit Multipath RTP as experimental RFC