# IETF93 AVTCORE WG minutes

IETF 93 - CLUE WG meeting minutes

Monday July 22, 2015 13:00-15:30

Chairs: Roni Even, Magnus Westerlund

Note takers: Bo Burman, Emil Ivov

## Status Update

Chairs

No RFC was published since last meeting.

RTP topologies draft went to RFC editor's queue.

Draft-ietf-avtcore-srtp-aes-gcm-17 is in IESG processing and will most likely be approved.

Drfat-ietf–aria-srtp-08 registers for DTLS and MIKEY, can progress it is Informational;  was split to draft-ietf –aria-sdes-00 as standard track for the SDES registration, however there has been opposition to a standard track document.

Authors will work more on draft-ietf-avtcore-rfc5764-mux-fixes-02. Marc Petit-Huguenin as editor, should publish an update in the next two weeks and ready for WGLC after that.


Draft-ietf-topologies-update milestone is done.

RTCP in overlay multicast milestone was deleted. Other milestone dates will be reviewed.

New errata: RFC 4867: 4347, 4348, and 4349 (all technical) requiring clarification now when AMR-NB and AMR-WB payload format is being deployed. Please review. There is also an editorial errata on RFC 3611; minor error in one of the examples, which will need a bit further review.

Magnus gave a RMCAT status update, since the RMCAT chairs were not able to attend AVTCORE.

## Circuit Breakers for Unicast RTP Sessions

Colin Perkins

Draft-ietf-avtcore-rtp-circuit-breakers-10

There have been comments from Simon Perreault based on early experimentation experience, all of which seem reasonable and will be included in the next version. Magnus Westerlund provided comments regarding mismatch between RTT, RTCP reporting interval, and inter-packet interval, which will require a bit more discussion before they can be resolved.

Updates to the draft based on received comments will be made as quickly as possible. The authors are aware that there are other documents waiting for this one.

## Sending Multiple Media Streams in a Single RTP Session

Magnus Westerlund

Draft-ietf-avtcore-rtp-multi-stream-08, -rtp-multi-stream-optimization-06,  -multi-media-rtp-session-09

slides-93-avtcore-0.pdf

The authors think that all three documents are ready for WGLC. –multi-media-rtp-session has undergone a major, but editorial, re-write.

Roni: The WGLC will be a little longer than usual since it is summer vacations.

Varun, Suhas, and Cullen volunteer to review.


## Multipath RTP

Varun Singh

Draft-ietf-avtcore-mprtp-00

Varun: Hope to be able to test the (upcoming) open source implementation with OpenWebRTC.

Justin: can you consider decreasing the subflow ID in the RTP header extension from two bytes to one byte to make it fit in one 32-bit word?

Varun: Yes, we can do that. (action item for Varun)

Varun: should we include MPRTCP count (MRC) in the RTCP header? <No response from room>.

Varun: Should we wait for continuous nomination and passive-aggressive nomination to finish and replace MPRTCP extension for interface advertisement?

 Justin: propose taking this to the new ICE WG, since it needs to understand this.

Regarding security, how do you envision this to work with DTLS-SRTP? We need to work on that too. Varun: in this document, or in another document? Cullen: agree this need to be closely coordinated with ICE. Justin: having a few words on that in the security section would be useful.

Action for Varun to clarify this behavior in the security section

Varun: remove section 9.3 for now, saying that this is one of the requirements MPRTP has on ICE version 2? Justin: Describe how to work without ICE in this document, and leave how to work with ice for discussion in new ICE WG. Emil: Do we want to describe how to work without ice? Varun: yes, for example inside an ISP's network for RTSP streaming. Reviews are appreciated.

Chairs asked the WG who read the draft, and only a few did (only one, Colin?).

Varun: Also please let me if you know of any implementations, including proprietary

## Codec-Independent Selective Forwarding

Bernard Aboba

Draft-aboba-avtcore-sfu-rtp-00

Bernard: Draft describes issues that could require new work in AVTCORE. Suggest starting with a type of roadmap before detailing work.

Mo: The layer drop functionality is not only useful with SVC, but also with other codecs.

Bernard: Don't know if RPSI or SLI is ever used by SFU's. Stephan Wenger: RPSI has been used in non-IETF systems. Mo: I'm aware of RPSI-like semantics in messages, without actually using RTCP RPSI, for both point-to-point and in conferencing.

CALL TO ACTION: let's define a complete problem statement so that we can also start thinking about a solution

Mo: This is a useful document, but not sure what the eventual goal is? Is it an updated topology, clarifying the working of an SFU? Bernard: The goal is to have a problem statement, describing all of these things, as a basis to lead separate discussions leading to a decision to do work or not.

Mo: Do you think there need to be more than already ongoing in AVTEXT? Bernard: Yes, but we haven't had a full discussion yet.

Harald: Is this related to PERC and encryption? Bernard: The thing described here is unrelated to PERC. There's a difference between not wanting to look at the codec data and not being able to. Harald: If you solved this for the encrypted domain, would it not be solved also here? It would be a pity to have two solutions. Bernard: Don't think that we can put that entire load of this to

PERC. Stephen: I don't know how it relates to PERC, maybe it relates, maybe it doesn't, but we need to take a look at this in a better way. Magnus: If you solve it in PERC, it will not be exactly the same set of issues, but I think that we should look at this. Emil: Agree with Magnus; PERC will need to look at it in an encrypted environment, but this just makes such work doubly useful. Randell Jessup (via Jabber): Like that this is worked on here. Cullen: Some problems described in this draft are specific to SVC, while some are the same for simulcast, and in that case we want a single solution for it.

Magnus (as chair): Propose to keep this draft it as individual and get some discussion started on the mailing list. Bernard: Yes, we can add more information to the draft from such discussion.

## Encrypted Key Transport for Secure RTP
John Mattsson

Draft-ietf-avtcore-srtp-ekt-03

Roni (from floor): There is interest in EKT not only for PERC, but whenever you don't trust a middleman with the keys.

 John: Yes. Next version of EKT will not include any PERC-specific things.

Mo: Keep next version in AVTCORE and include both PERC and non-PERC things?

John: Yes, plan to include PERC EKT functionality in the version after next. Mo: People in AVTCORE should be aware of a SRTP and EKT design team in PERC that will define what to do with that.

Suhas as PERC co-chair: Contact me if you want to participate in that design team.

Cullen: leaving this draft in AVTCORE and not move it to PERC will be a surprise for some parties. Magnus: PERC charter clearly allows doing it there. Ben: AD has no opinion on where EKT work is done, here or in PERC. Magnus (as chair): Conclusion is to wait with decision to move the draft or not until EKT requirements from PERC become clearer.

Mo: GCM modes proposed now are a bit heavy for audio conferencing; would it be worth keeping also modes that are appropriate for audio? John: Yes.

This is an additional **action item** to be taken to mailing list, (in addition to the issues to include in -04 that are listed in the presentation).

Paul Jones explained some details on changes to this document proposed by draft-jones-perc-private-media-framework.

Cullen: Want to think about security for key distribution a bit more.

Session closed 14:28