PERC @ IETF95

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.

Milestones

Sep 2016 - Submit architecture or framework specification to IESG

Jan 2017 - Submit documentation of how to integrate solution in SIP, WebRTC and CLUE to IESG

Jun 2017 - Submit SRTP protocol extension specification to IESG

Jun 2017 - Submit Key-management protocol specification to IESG

Milestones & Documents

Architecture / framework	*draft-jones-perc-private-media-framework*
SIP, WebRTC and CLUE	draft-groves-perc-clue [[your draft here]]
SRTP protocol	**draft-jennings-perc-double**
Key-management protocol	**draft-jones-perc-dtls-tunnel** **draft-jennings-perc-srtp-ekt-diet**

Agenda

10m	Chairs	Intro
20m	Adam	Big picture view of PERC
20m	Fluffy	draft-jennings-perc-double
20m	Fluffy	draft-jennings-perc-srtp-ekt-diet
15m	Paul	draft-jones-perc-dtls-tunnel
5m	Chairs	Wrap-up

Recap of the Layers

Signaling	← some today
Key management	← today
SRTP/SRTCP transforms	← focus of interims

An entity with intermediate privilege

Normal SRTP/SRTCP divides the world into two classes:

- In the session: Can encrypt / decrypt payload, MAC/verify headers/payload
- Not in the session: Can observe header fields, encrypted payload

PERC is about creating an entity intermediate between these two

- Not in the session, but gets some capabilities of being in the session
- MDD = Network Attacker + (minimum privilege to do conferencing)

Recap of Interims

Four virtual interims since last IETF

- Three devoted to SRTP requirements
- One for SRTCP

Clear requirements for media protection

See minutes / proceedings for details