Private Media Framework

draft-ietf-perc-private-media-framework-04

Paul E. Jones, Cisco
David Benham, Cisco
Christian Groves, Independent

IETF 99 • July 2017

What's New

- Introduced two new appendices
  - Appendix A: PERC Key Inventory
  - Appendix B: PERC Packet Format
- Editorial cleanup

Editorial Cleanup

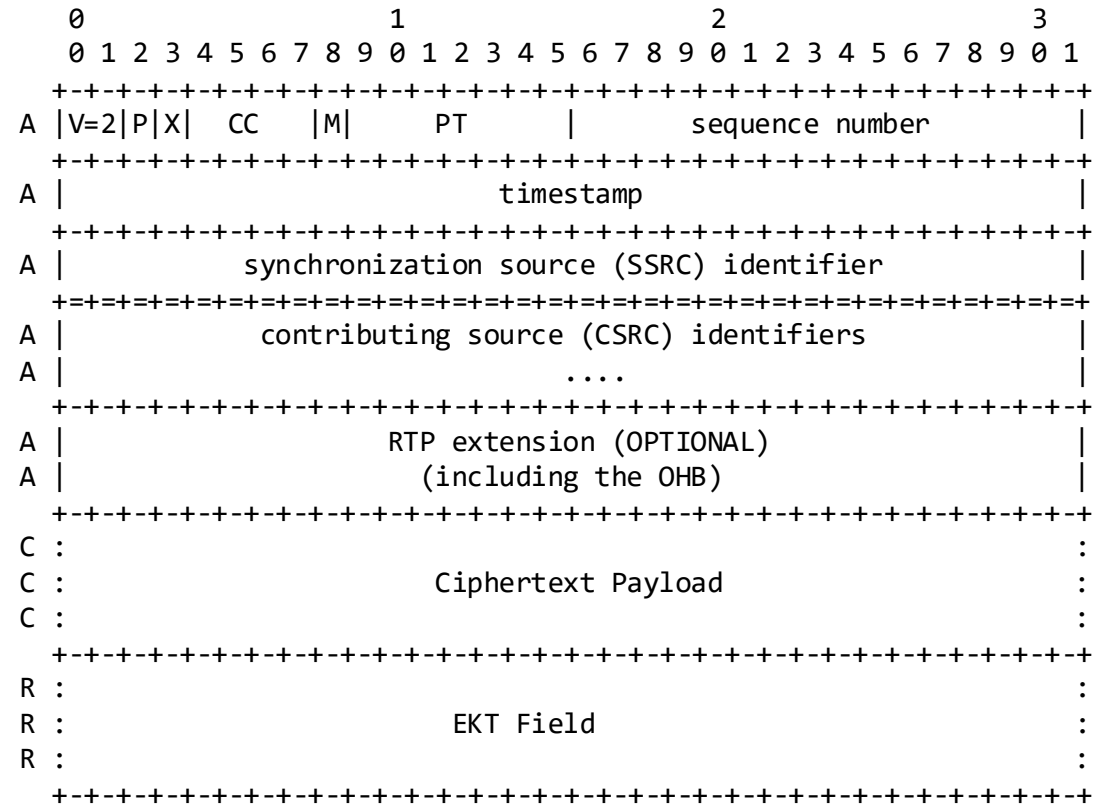
- Removed references to “Key(i)”
  - For any key(i), there might actually be several
  - Changing text to Key[i][j] only made it harder to read
  - The notation was a bit confusing
- Added a little more language to explain key use in 4.2
- “EKT Key” vs “EKTKey”
  - Use “EKT Key” when referring to the EKT Key.
  - Use “EKTKey” when referring to the field in the message
  - Intent was to be consistent with EKT Diet

Appendix A: PERC Key Inventory

- Very high-level, informative overview of PERC keys
  - This is a couple of pages, so a review would be useful
- Moved entity / key table from main text to appendix

Key	Description
KEK (EKT Key)	Key shared by all endpoints and used to encrypt each endpoint's SRTP master key so receiving endpoints can decrypt media.
HBH Key	Key used to encrypt media hop-by-hop.
E2E Key	Key used to encrypt media end-to-end.

Appendix B: PERC Packet Format



C = Ciphertext (encrypted and authenticated)
A = Associated Data (authenticated only)
R = neither encrypted nor authenticated, added
after Authenticated Encryption completed