PERC

draft-ietf-perc-double-02
draft-ietf-perc-srtp-ekt-diet-02

IETF 97

fluffy@cisco.com

DOUBLE Changes since IETF 96

- Very few changes
- Update for changes decided at last meeting
  - Added list of what RTP header extensions an endpoint can use if they come from the MD (not other end)
    - This list currently consists of only the mixer to client audio level
- Fixed a few typos

- No open issues on Double

EKT Changes

- Huge thanks to Russ Housley for a really great review
  - Have made all changes suggested in that review and added text to draft to try and address all questions raised

EKT Changes

- Moved TTL to correct message
- Text to say truncate trailing octets after the master SRTP salt
- Moved implicit sizes to explicit
  - Used to derive sizes of things from knowing what crypto was used
  - Problem with future extensions where two things might have sizes that were not uniquely computable from just from knowing signalling info
  - Solved by including explicit size in message
- Added IANA table for messages types
- Fixed up the DTLS extension and negotiation
  - Only on wire change was including supported EKT ciphers in negotiation
  - This needs review by someone that knows TLS

Open Issues

Implicit vs Explicit Sizes

- The length of the SRTP master key is known from which SRTP crypto profile was negotiated by the DTLS
- The size of the EKT_Plaintext would be computed from variable size SRTP_Master_Key plus fixed sizes of SSRC and ROC
- The cipher used to encrypt the EKT_Plaintext would be known by looking at the SPI
- Given both of these, then the length of the EKT_Ciphertext can be computed instead of carried in the message
- This would allow removing SRTPMasterKeyLength (1 byte)
- This 1 byte shows up in occasional SRTP packet that has the long EKT field

Moving Forward

- I would like to see us to a WGLC so we can get some comments and decide if we are done or now