IETF 91 AVTCORE

DRAFT-IETF-AVTCORE-SRTP-EKT-03

JOHN MATTSSON (EDITOR)

ERICSSON RESEARCH

UPDATES SINCE -02

- Editorials and general clarifications
  - 128 -> 256, 32 -> 16, “key” -> “SRTP master key”
- Updates and clarifications to the SDESC Section
  - One session parameter “EKT”, not three.
  - “EKT_Cipher”, “EKT_Key”, and “EKT_SPI” is referred to as fields/values in accordance with RFC4568.
- Updates and clarifications to the MIKEY Section
  - -02 required two policy payloads (EKT and SRTP) to be send. But it’s not possible to have two policies associated with the same CS.
  - Include EKT_Cipher and EKT_SPI in SRTP policy.

UPDATES SINCE -02

- The SRTCP compound packet problem is **discussed**
  - "This specification requires the EKT SSRC match the SSRC in the RTCP header, but Section 6.1 of [RFC3550] encourages creating SRTCP compound packets"
  - Potential high-level solution outline given.

COMMENTS SINCE -03

- The SRTCP compound packet problem
  - “The solution outlined for compound packages is clearly not detailed enough for interworking implementations, and it goes against things stated earlier in the draft (EKT placed last in SRTCP packet).”
  - Seems to be a SRTCP problem, not an EKT problem. SRTCP also requires that SRTCP SSRC match the SSRC in the RTCP header
  - Suggestion: Skip the suggested solution and require EKT in both SRTP and SRTCP for these cases:
    - SRTCP and SRTP have different endpoints.
    - SRTCP and SRTP does not share context.

COMMENTS SINCE -03

- SRTP master key lengths and default ciphers.
  - EKT draft makes a one-to-one mapping between EKT cipher and SRTP encryption transform.
    - RFC3711 does not do this for SRTP master key and transform. SRTP PRF derives session keys of the right length.
    - Does not take authentication transform into consideration
  - Suggestion: Simply mandate that EKT Cipher key MUST be at least as long as SRTP master key.

COMMENTS SINCE -03

- SRTP master salt lengths and requirements on ciphersuites.
  - -02 change: Different transforms require different salt lengths -> “Mandate that the same ciphersuite is used”
    - None of the SRTP transforms put requirements on SRTP master salt length.
    - Ciphersuites are SDESC, not SRTP (SRTP has transforms).
    - But a single SRTP parameter set needed to allow EKT to set up new SSRCs.
  - Suggestion: Remove ciphersuite form Section 2. State that a single SRTP parameter set is needed for EKT to set up new SSRCs.

Next steps?