

SDP Security Descriptions for Media Streams

<draft-ietf-mmusic-sdescriptions-01.txt>

Flemming Andreassen

Mark Baugher

Dan Wing

Cisco Systems

sd descriptions Overview

- WG draft
- SRTP crypto-suites and keys over SDP
 - SIP, SAP, Megaco, MGCP, etc.
- SDP must be protected
 - By encapsulating protocol

Changes from previous draft

- New a=crypto syntax
 - Removed grouping
 - “use” attribute (encrypt, decrypt, both) [comments?]
 - SRC tuple for SSRC, SEQ, and ROC
 - Removed application=srtp|srtcp
- O/A revised; still needs further detail
 - Interoperation with “use” attribute

Example SDP

Offer

```
...  
m=audio 49170 RTP/SAVP 0  
  a=crypto:AES_CM_128_HMAC_SHA1_80  
  inline:d/16/14/...key1.../2^20/  
  FEC_ORDER=FEC_SRTTP SRC=17174//49126  
a=crypto:F8_128_HMAC_SHA1_80  
  inline:d/16/14/...key2.../2^20/  
  FEC_ORDER=FEC_SRTTP SRC=17174//49126
```

...

Answer

```
...  
m=audio 32640 RTP/SAVP 0  
a=crypto:AES_CM_128_HMAC_SHA1_80  
  inline:d/16/14/...key3.../2^20/ SRC=88131/721/13
```

...

Next Steps

- Finish Offer/Answer
- Describe use without Offer/Answer
- -02 will be posted by mid-August