# SDP Security Descriptions for Media Streams

`draft-ietf-mmusic-sdescriptions-03.txt`

March 3, 2004

Flemming Andreasen (fandreas@cisco.com)
Mark Baugher (mbaugher@cisco.com)
Dan Wing (dwing@cisco.com)

# Purpose

- Establish secure media streams by sending security descriptions with ciphers, keys, etc. in SDP
- Divided into core framework and an SRTP-specific part:
  - High-level Operation and parameter definition
  - Use with Offer/Answer
  - Use outside Offer/Answer
  - Grammar

# Overview of Changes

- Removed support for multicast and multipoint SRTP sessions
  - Point-to-point media streams only
  - SIP forking addressed via workaround
    - Turn multipoint into multiple point-to-point instead.
- Removed SRC parameter
  - SSRC, SEQ and ROC no longer signaled
  - ROC must always be zero when joining a session
- Send and receive keys now required to be unique to avoid two-time pad problem during SSRC collissions.

# Overview of Changes, cont.

- Expanded on rules for creating and removing crypto contexts
- Added new “tag” parameter for offer/answer
- Clarified whether each parameter is negotiated or declarative in offer/answer
- Modified IANA registry structure
- Incorporated various other review comments received

# Minor Issue - Address Change

- Scenario:
  - A has performed initial offer/answer exchange
  - Crypto context established
  - A performs a subsequent offer/answer exchange and receives a new media stream destination address
- Issue:
  - Cannot assume new destination address has access to old crypto context ROC value
- Solution:
  - Need to either reset ROC (to zero) or use new SSRC whenever destination address changes (IP or port)
  - Note that ROC is not an issue for all types of ciphers

# Next Steps

- Ready for WGLC