SRTP Store and Forward

draft-mattsson-srtp-store-and-forward-00

R. Blom, Y. Chen, F. Lindholm, J. Mattsson, M. Näslund, K. Norrmann
Ericsson Research
Trust Model and Assumption

Store and forward

Sender ➔ Store & Forward ➔ Receiver

- e2e context; Payload protection
- Honest but curious
- hbh context_1 ➔ Store & Forward ➔ hbh context_2
- Transport protection
Use cases

Examples

- **Answering machine**
  - Storing/cashing encrypted media
  - Transport protection
  - Playback of encrypted media; Random seek
  - Multiple callers

- **Centralized conferencing**
  - Non trusted conference bridge
  - Push-to-talk

- **Pre-encrypted media distribution**
Requirements

Inner protection transform (~ new SRTP transform)
- Transport independent media protection
- Playback of protected media

Outer protection transform (~ current SRTP)
- Transport protection

Combined inner and outer transforms
- Separation of security contexts
- Switching between different media security context
Inner protection transform

- RTP Payload
- AES-CTR
- f
- Encrypted Payload
- IVSN
- HMAC-SHA1
- Encrypted portion of SRTP packet

Session encr_key → AES-CTR → f → Encrypted Payload → IVSN → HMAC-SHA1

Session salt_key

IVSN ~ SRTP index
Outstanding issues

- Combined inner and outer transforms
  - Minimal impact on SRTP framework
  - Handling of independent inner and outer protection transforms
  - Keying and handling of independent security contexts
  - Switching between security contexts