

# S RTP Store and Forward

draft-mattsson-srtp-store-and-forward-02

draft-naslund-srtp-saf-00

R. Blom, Y.Cheng, F. Lindholm,  
J. Mattsson, M. Näslund, K. Norrman  
Ericsson Research

IETF 74, March 2009, San Francisco

# Content

- Updates in draft-mattsson-srtp-store-and-forward-02
- Content in draft-naslund-srtp-saf-00
- Request

# Updates

## draft-mattsson-srtp-store-and-forward-02

- New title: SRTP Store-and-Forward Use Cases and Requirements
  - New title due to more restrictive document scope that focus on use cases and requirements. Transform definition moved to draft-naslund-srtp-saf
- Editorial updates
- Store-and-forward e2e sessions
  - Several store-and-forward e2e streams can be protected with a single e2e security context.
  - Introduction of a separate SRTP SaF Source (SSS) parameter, compare SSRC.
- Solution Proposal changed to Solution Outline (Chapter 6)
  - Section 6.3 New Transforms deleted
  - To increase generality, IVSN (counter) is changed into a Packet Unique Value (PUV)
  - Media protection relies on SSS and PUV for crypto synchronisation.
- Appendix on key management

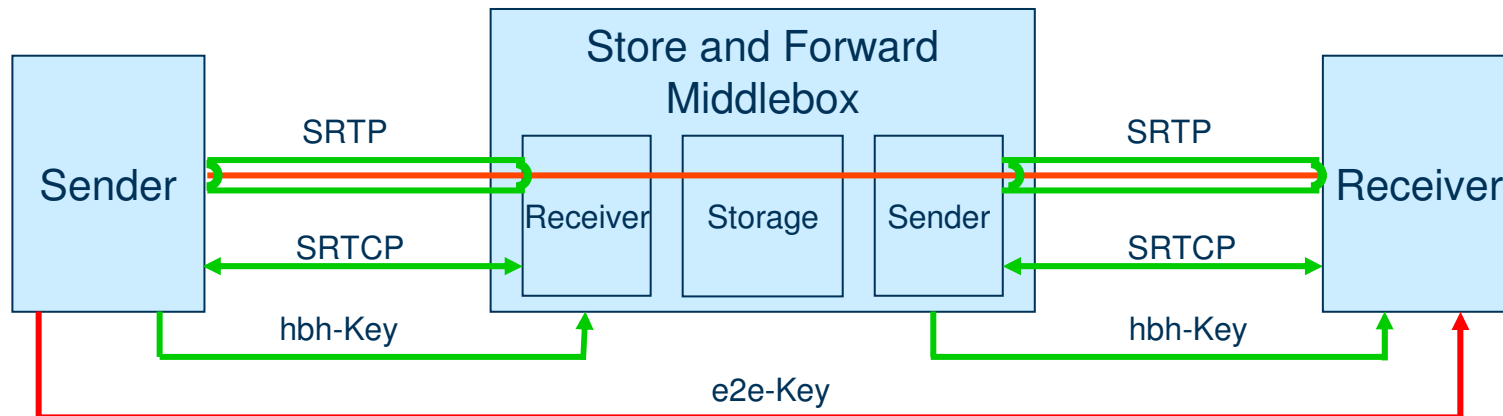
# SRTTP Store & Forward

## Principles

### Combination of

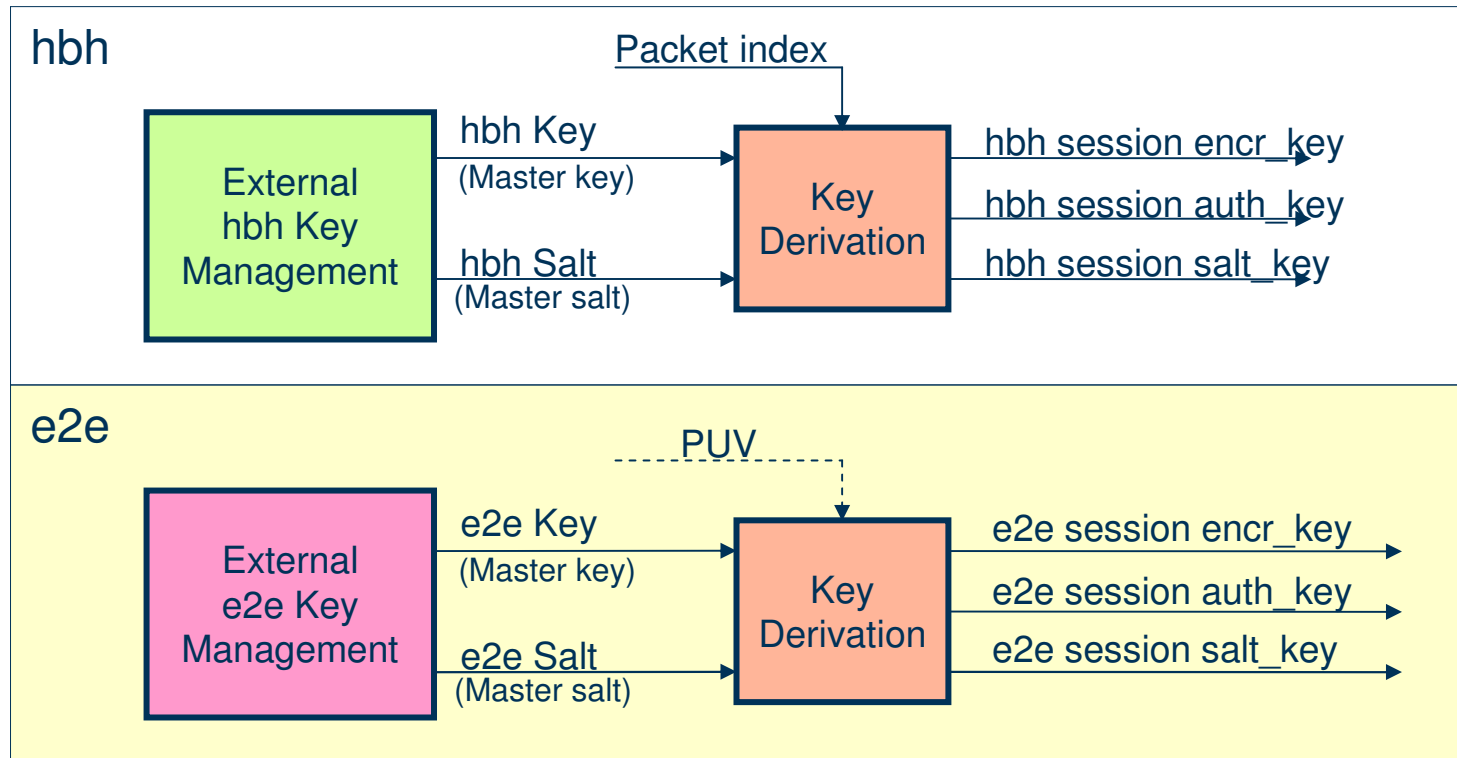
- End-to-end transport independent transform
- Hop-by-hop transport dependent transform

NOTE: The end-to-end transport and hop-by-hop can be used independently of one another (i.e., no requirement that both need to be enabled)

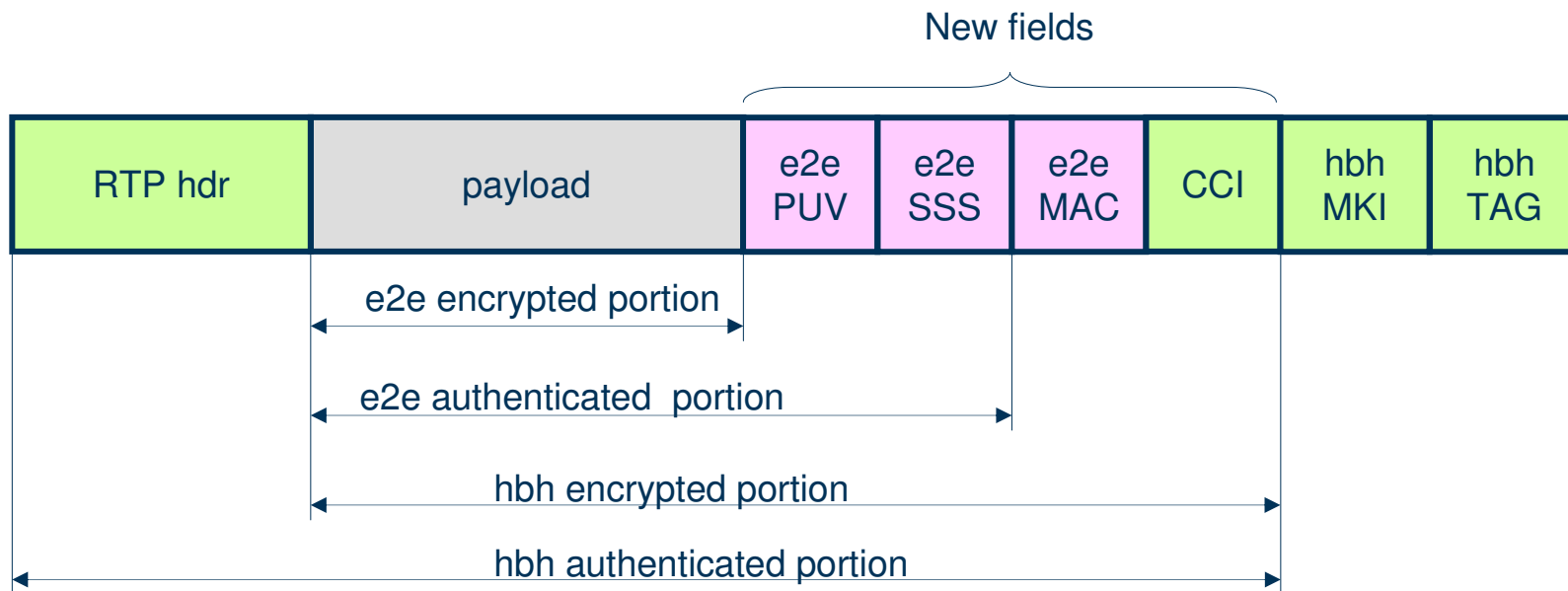


# Two security contexts: e2e and hbh

## Key derivations

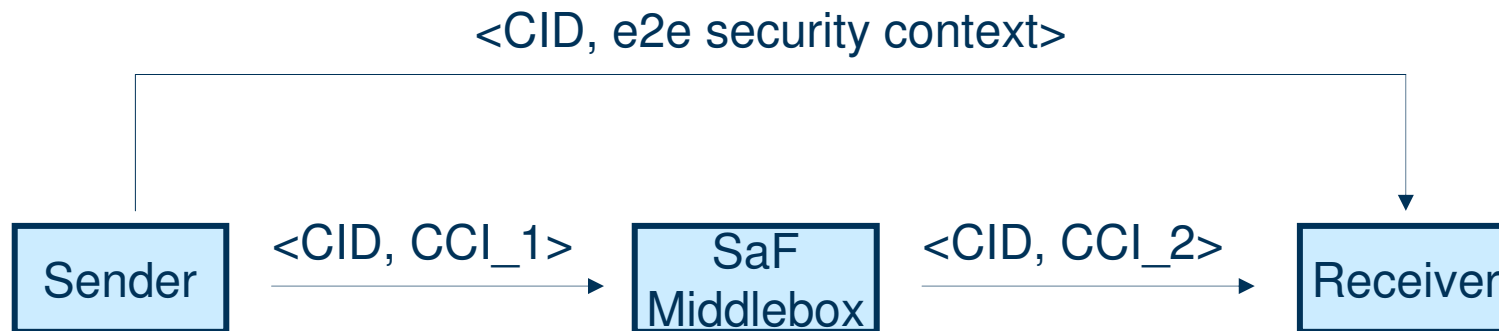
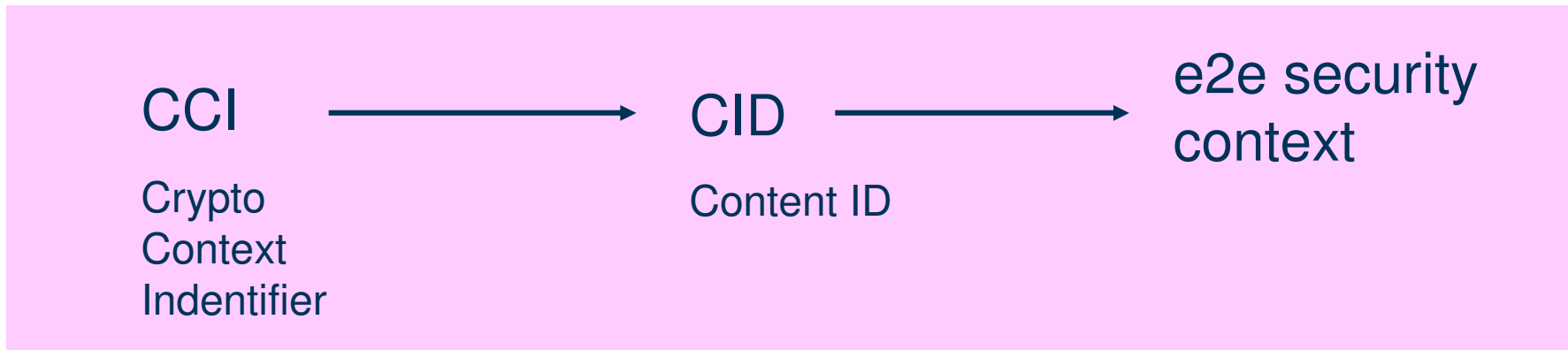


# SRTP SaF Packet format



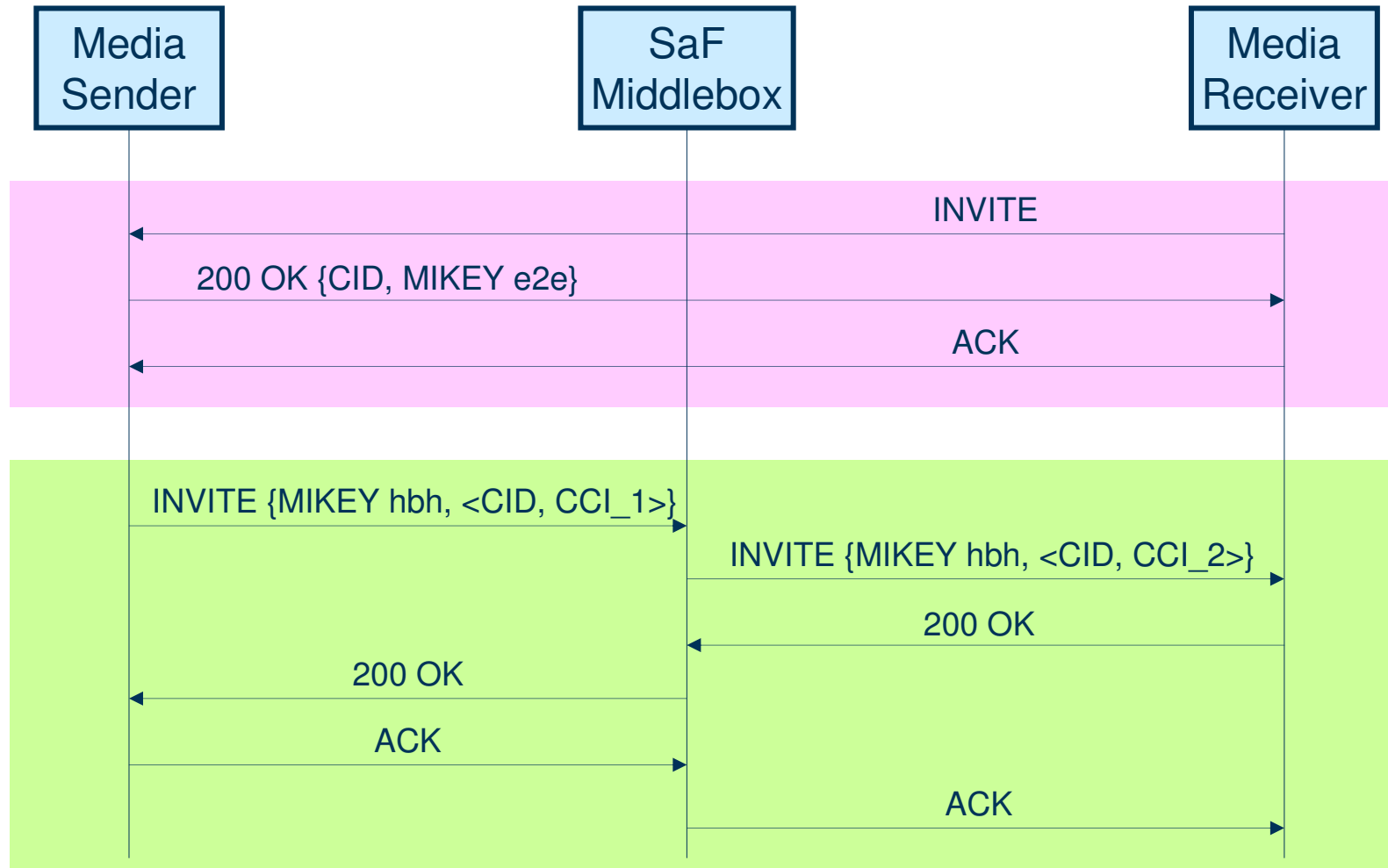
# Key Management

e2e security context identification



# Key Management – Media distr.

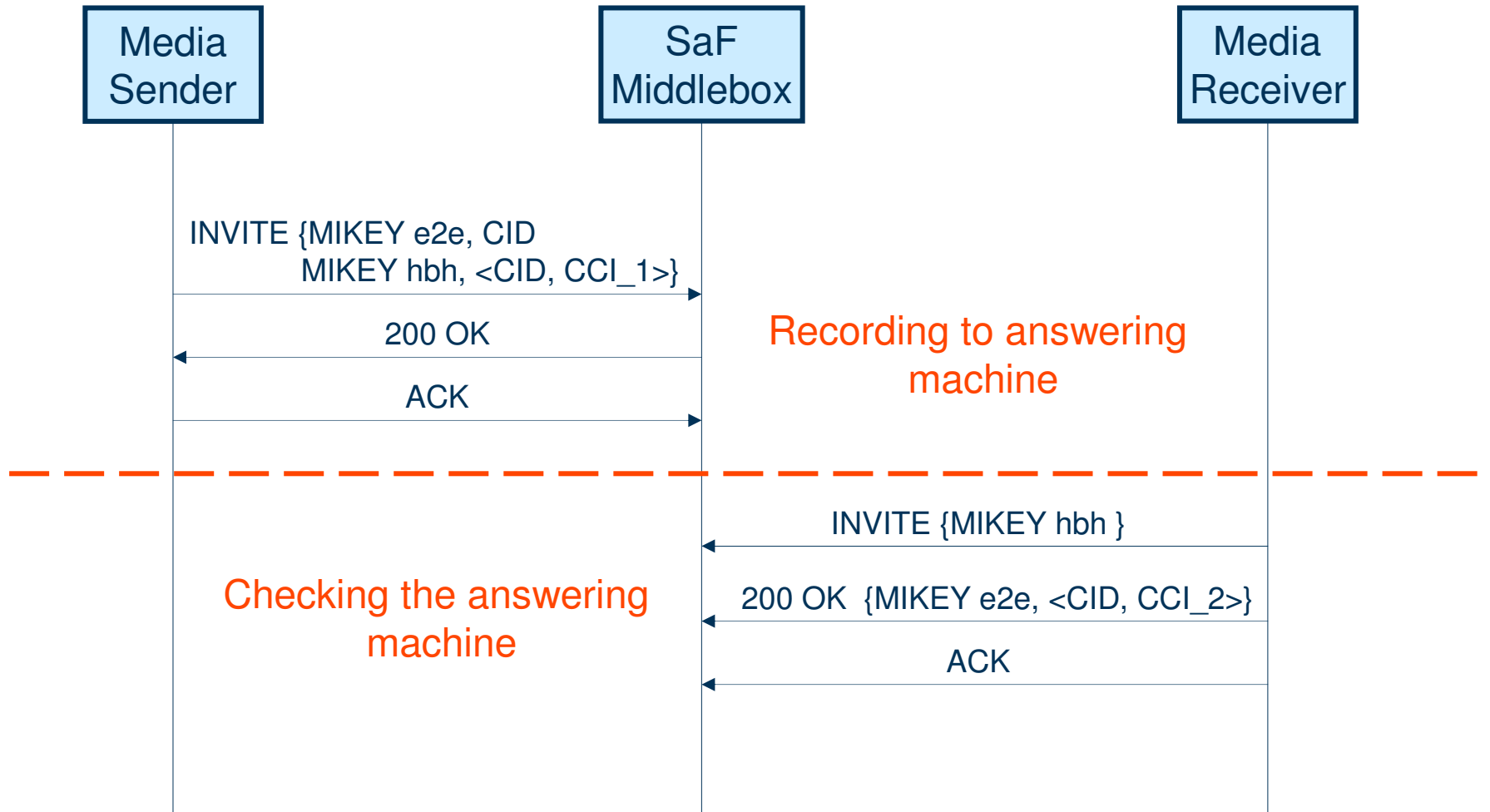
draft-mattsson-srtp-store-and-forward-02





# Key Management – Answering mach.

draft-mattsson-srtp-store-and-forward-02



# SRTP SaF

draft-naslund-srtp-saf-00

## The Use of the Secure Real-time Transport Protocol (SRTP) in Store-and-Forward Applications.

1. Introduction
    - 1.1. Scope of this Document
    - 1.2. Conventions used in this Document
      - 1.2.1. Notation and Definitions
  2. SRTP
  3. **The Store-and-Forward Use Case**
    - 3.1. Problem Statement
    - 3.2. Trust Model and Security Requirements
    - 3.3. Problems with SRTP in SaF Scenarios
  4. **Usage of SaF Security within SRTP**
    - 4.1. **The SaF Extension**
    - 4.2. **SRTP SaF Packet Format**
    - 4.3. **Extension of the SRTP Cryptographic Context**
      - 4.3.1. E2e Context Definition
      - 4.3.2. Identification of e2e Context
    - 4.4. **SRTP SaF Processing**
      - 4.4.1. Sender
      - 4.4.2. SaF Middlebox
      - 4.4.3. Receiver
    - 4.5. **SRTCP SaF**
    - 4.6. **Cryptographic Transforms**
      - 4.6.1. Hbh Transforms
      - 4.6.2. E2e Transforms
      - 4.6.3. Session Key Derivation
  5. **SRTP SaF Default Parameters**
    - 5.1. Adding Future e2e Transforms
  6. Security Considerations
    - 6.1. General
    - 6.2. Keystream Reuse
    - 6.3. Attacks on CCIs
    - 6.4. Authentication and Authorization
    - 6.5. Replay Protection
    - 6.6. Key Management Considerations
    - 6.7. Privacy
    - 6.8. RTCP Considerations
  7. Acknowledgements
  8. **IANA Considerations**
  9. References
    - 9.1. Normative References
    - 9.2. Informative References
- Appendix A. Use Cases
- A.1. Streaming Pre-encrypted Media
  - A.2. Recording Encrypted Media at Home
  - A.3. Answering Machine
  - A.4. Media Rewind
- Authors' Addresses

# SRTP SaF

draft-naslund-srtp-saf-00

- Modeled after RFC 4383
  - The Use of Timed Efficient Stream Loss-Tolerant Authentication (TESLA) in the Secure Real-time Transport Protocol (SRTP)
- E2e protection reuses defined default transform in RFC 3711
  - Key derivation rate = 0
  - GCM AEAD is not included
- hbh protection according to RFC 3711
- RTCP is only protected on hbh basis

# Request

- Request that SRTP SaF is taken on as a WG item

**ERICSSON** 

**TAKING YOU FORWARD**