SRTP 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

ERICSSON
TAKING YOU FORWARD

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 synch.
- Appendix on key management

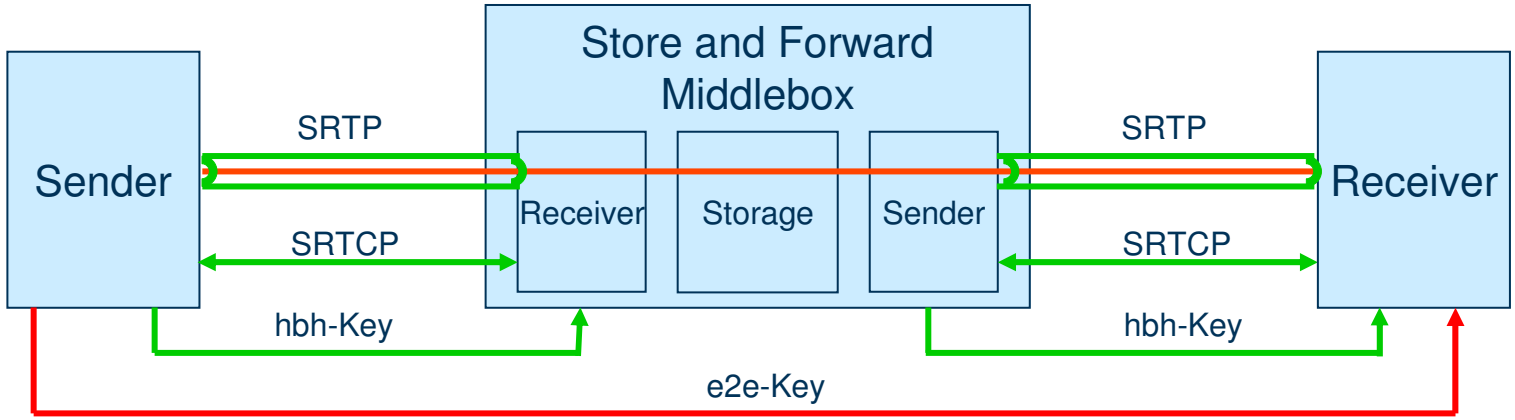
SRTP Store & Forward

Principles

Combination of

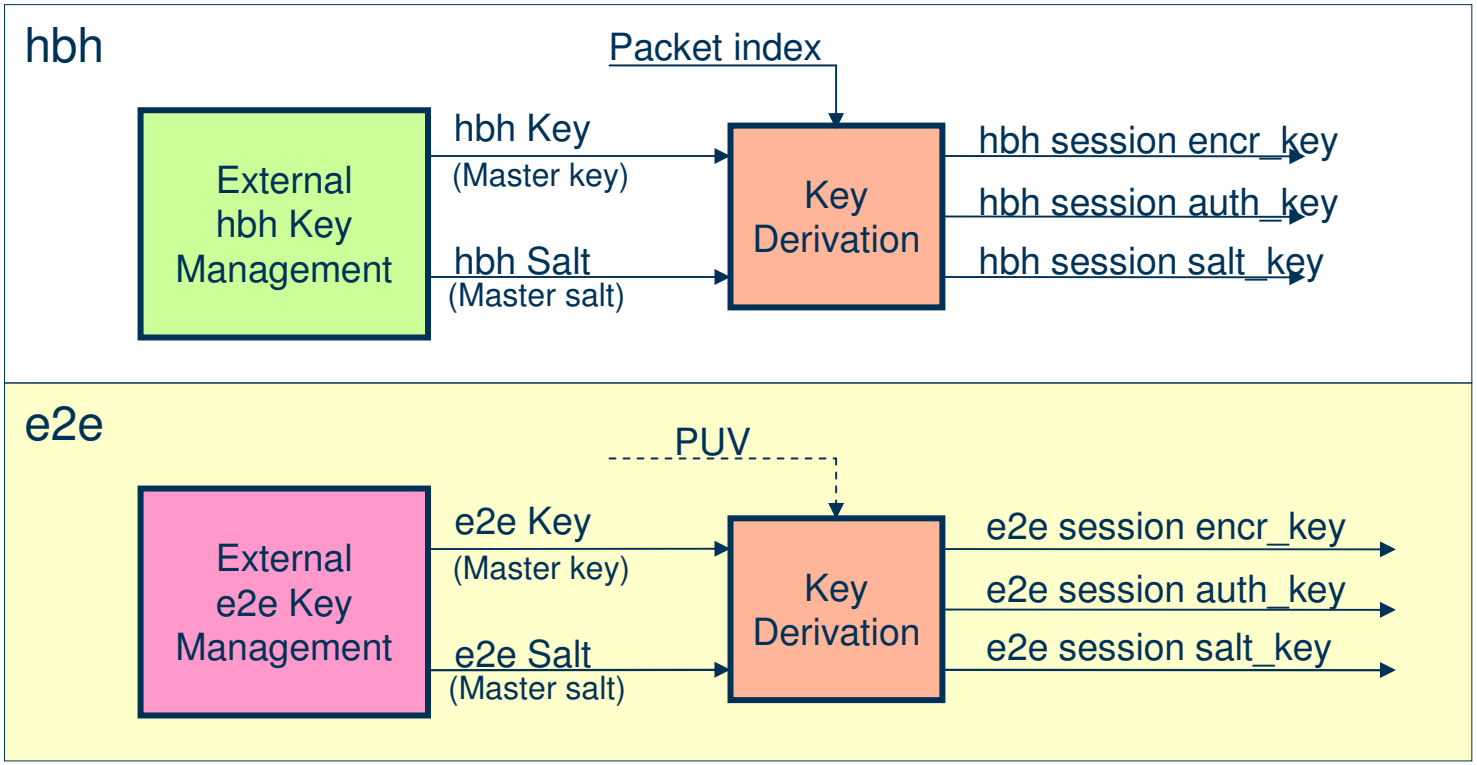
- End-to-end transport independent transform
- Hop-by-hop transport dependent transform

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)

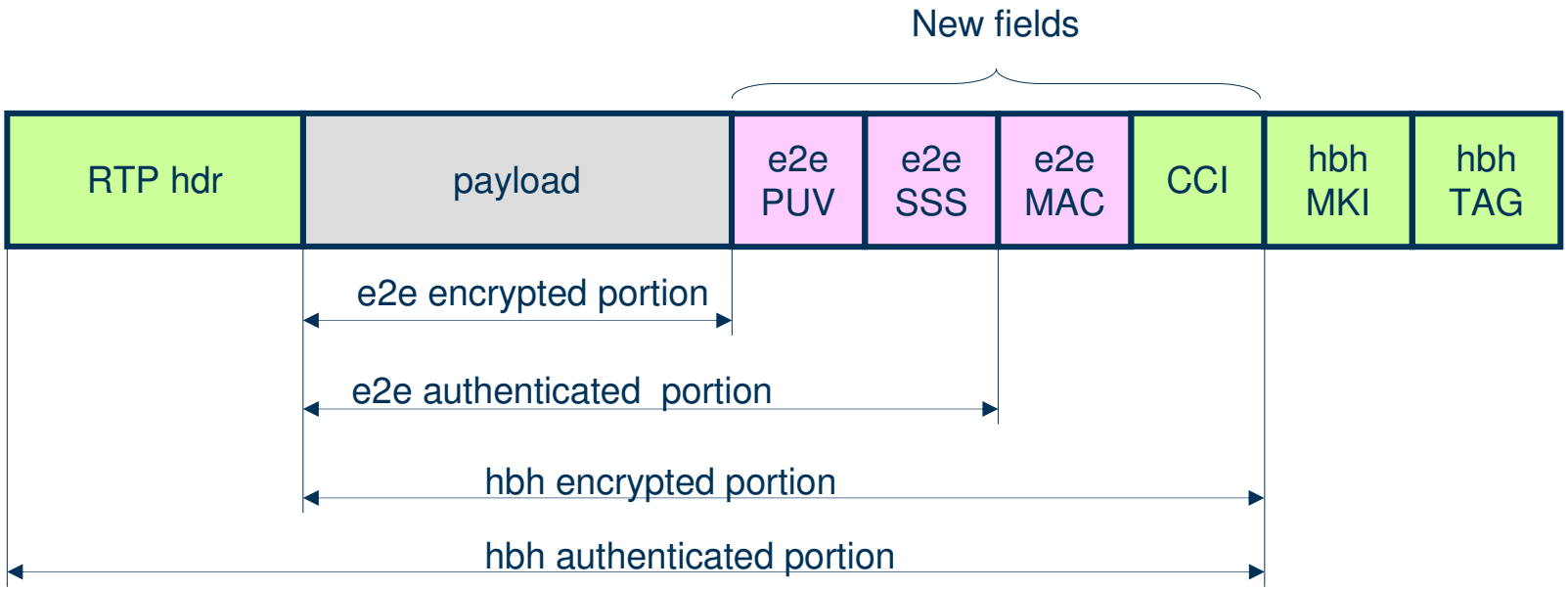


Two security contexts: e2e and hbh

Key derivations



SRTP SaF Packet format



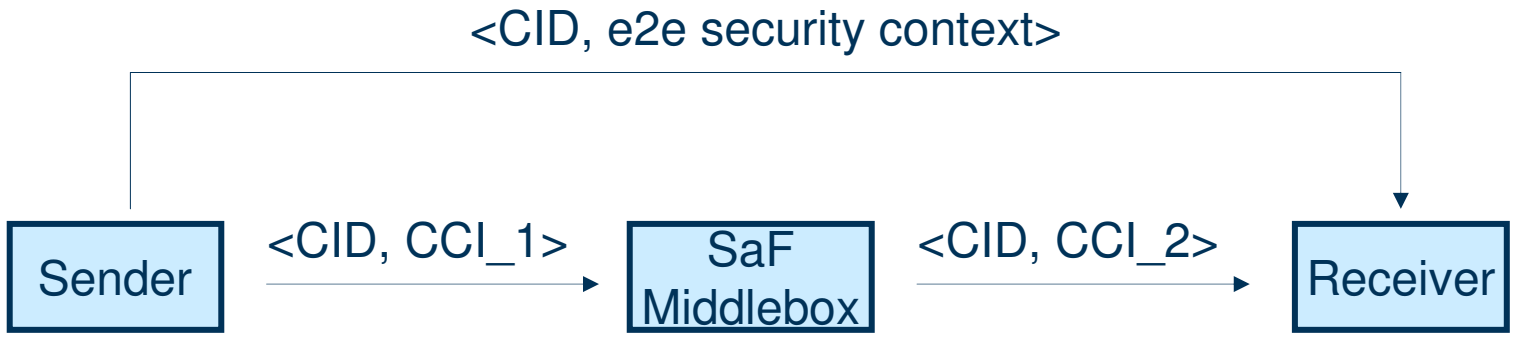
Key Management

e2e security context identification

CCI → CID → e2e security context

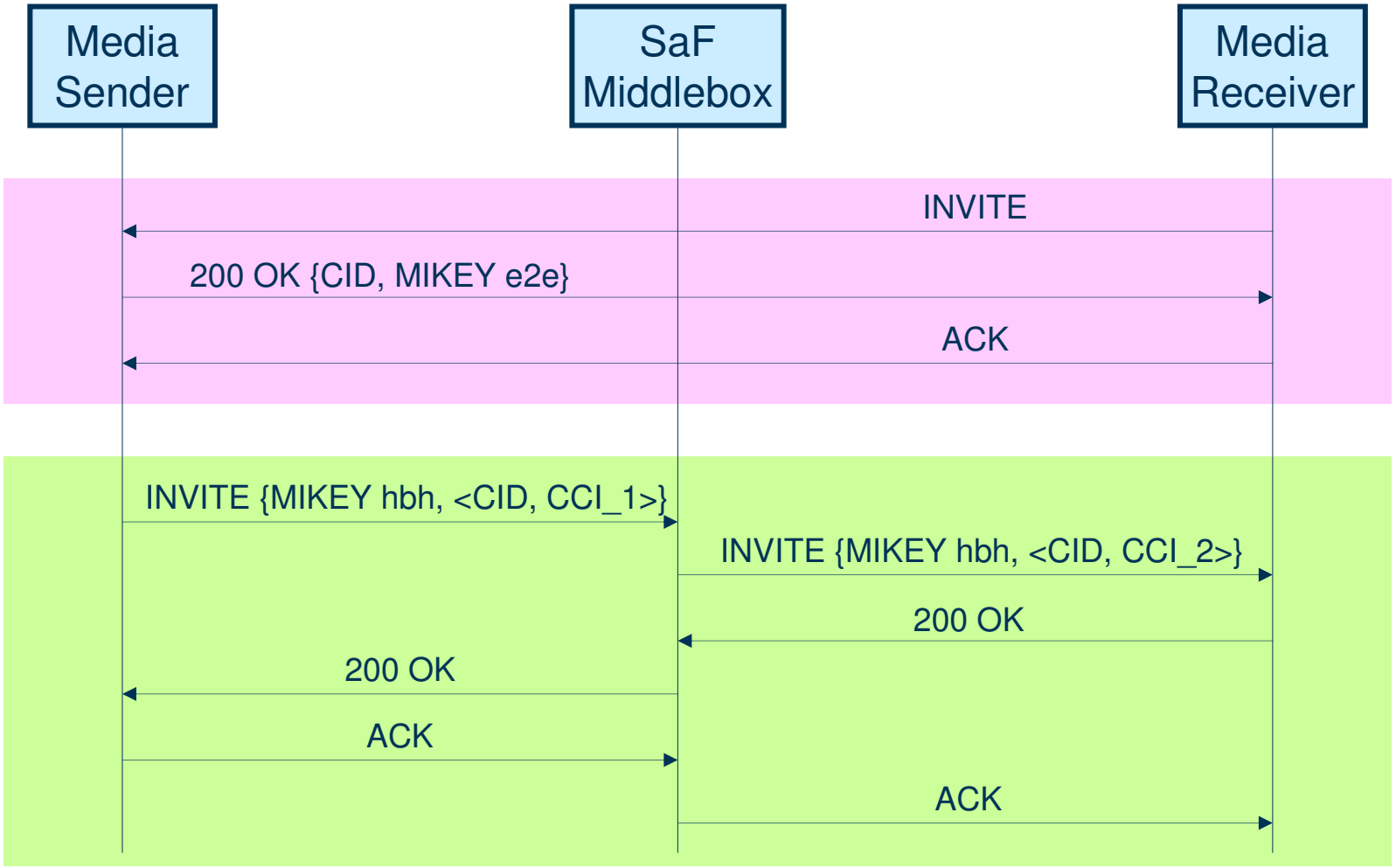
Crypto Context Indentifier

Content ID



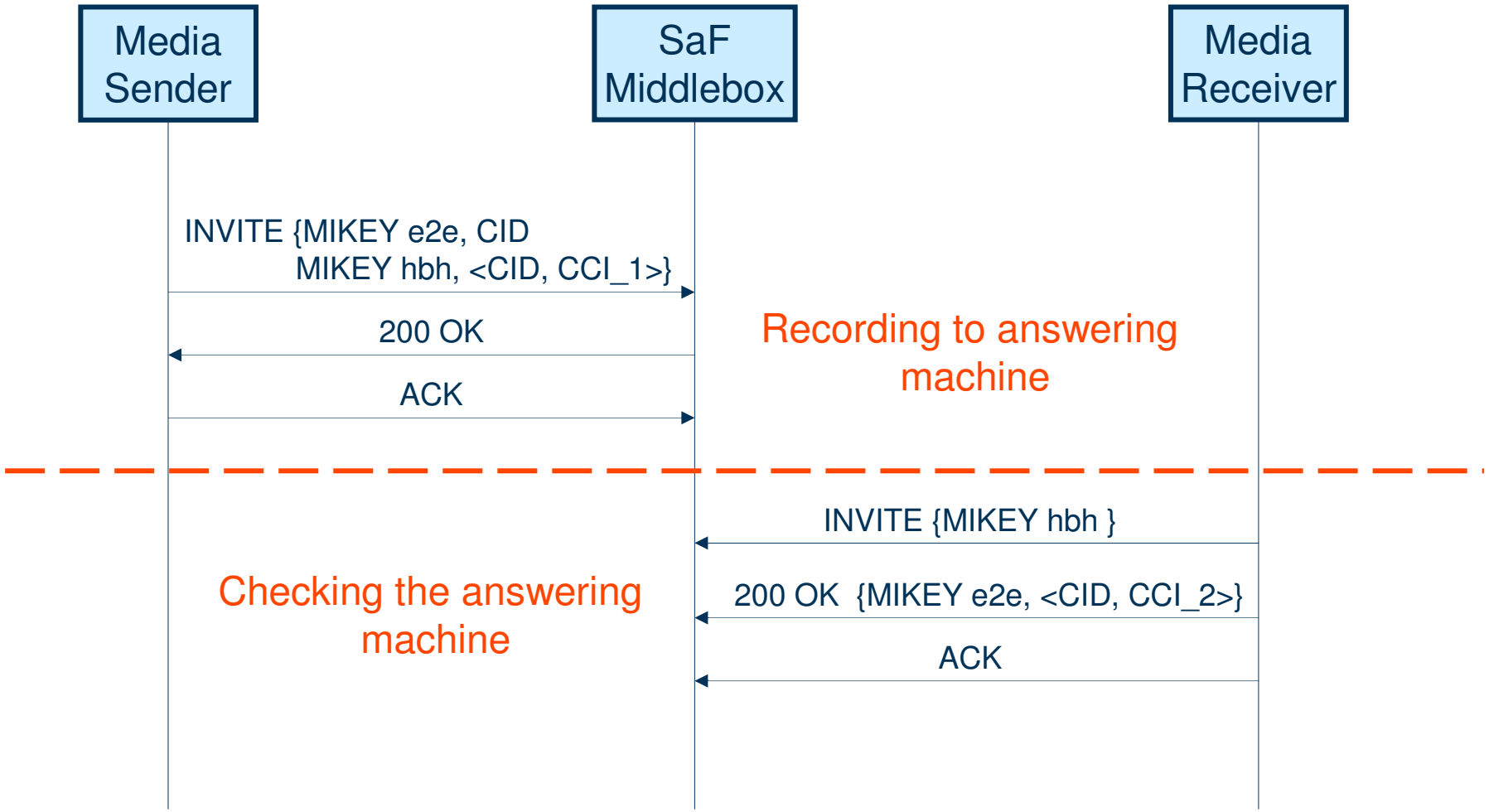
Key Management – Media distr.

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.

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