SRTP Store-and-Forward

draft-mattsson-srtp-store-and-forward-03
draft-naslund-srtp-saf-02

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

IETF 75, July 2009, Stockholm

Content

- Updates in draft-mattsson-srtp-store-and-forward-03
- Updates in draft-naslund-srtp-saf-02 (and -01)
  - SRTP SaF Packet Format
  - Context Identification
- Request

Updates

draft-mattsson-srtp-store-and-forward-03

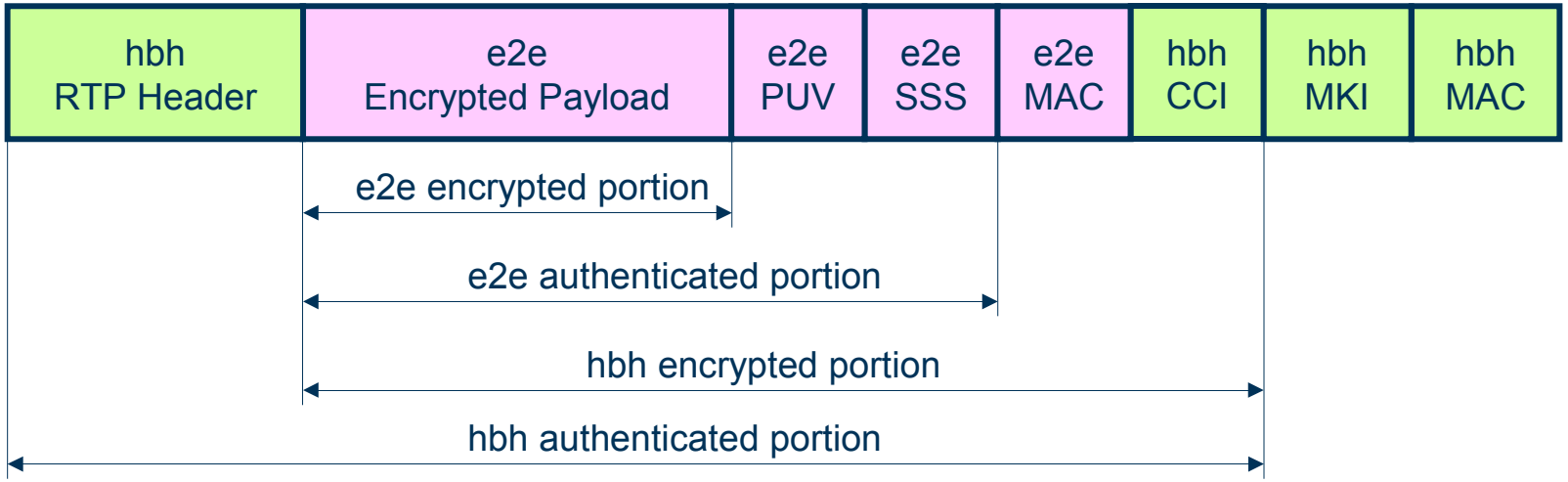
- The key management appendix has been updated to better correspond to real-world applications.
- The appendix on Draft Compound Transform Details has been removed, and part of it has been integrated in a rewritten Section 7 (Commented Example Usage).
- The centralized conferencing use case has been expanded to specifically mention video conferencing applications.
- Editorial updates

Updates

draft-naslund-srtp-saf-02 (and -01)

- The draft has been updated based on the comments received on the avt mailing list. The initial part of the draft has been expanded, a new "Design Rationale" section has been added, and the Security Considerations has been updated.
- The PUV field is now mandatory.
- The use of the CCI field is now optional and the field is strictly hbh.
- The PUV, SSS, and CCI fields now default to 3 bytes in total compared to 10 bytes in the previous (-00) version.
- Minor corrections, rearrangements, and clarifications has been made. Mainly to sections "4.4. Extension of the SRTP Cryptographic Context" and "4.7. Cryptographic Transforms".
- We have implemented SRTP Store-and-Forward according to version-02 and generated a test vector.
- Editorial updates

SRTP SaF Packet Format



- The new fields are of configurable length for maximum data compactness.

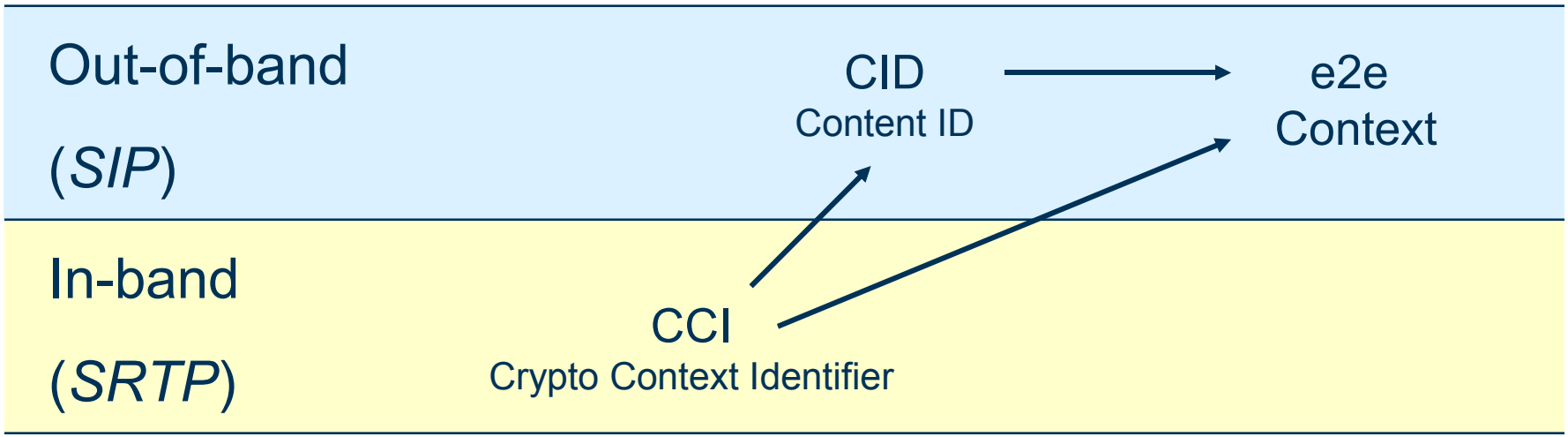
Field	Usage	SRTP Counterpart	Typical Size (bytes)
PUV	MANDATORY	SRTP Index	3
SSS	OPTIONAL	SSRC (IV formation)	0-1
MAC	RECOMMENDED	MAC	4-10
CCI	OPTIONAL	SSRC (context identification)	0-1
TOTAL			**7-15**

- This should not be interpreted as 7-15 added bytes as the hbh MAC might not always be needed.

Context Identification

- **Hop-by-hop**: Any SRTP key management protocol can be used. The hbh context is identified by the triplet context identifier as defined in 3711.
- **End-to-end**: Already defined SRTP key management protocols can be used (dependent on use case). The e2e context is identified by a combination of out-of-band and in-band signaling. The e2e context is uniquely identified with a extended quadruplet context identifier:

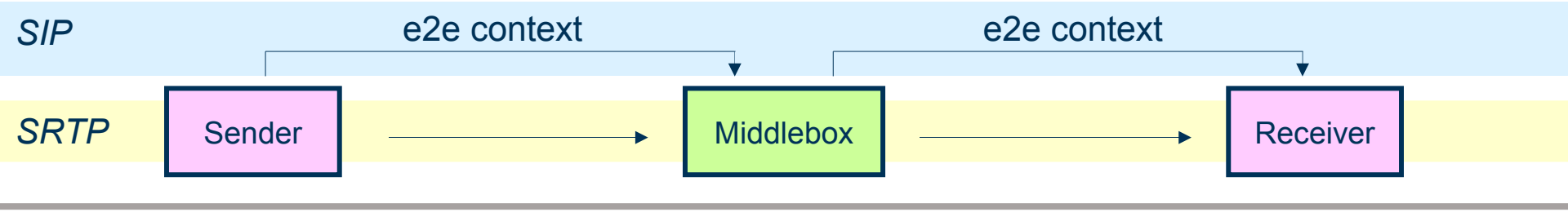
  <**CCI**, SSRC, destination network address, destination port number>



Out-of-band context identification

Transferring the entire e2e context via the middlebox

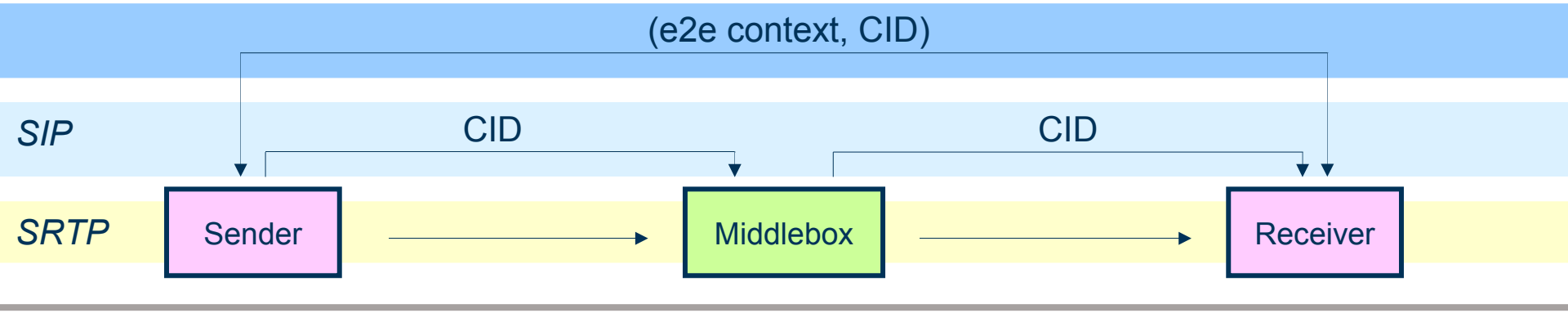
- The e2e context MUST be e2e protected so that middleboxes or other unauthorized entities cannot access or modify it.
- Only half-roundtrip key management protocols can be used.



Out-of-band context identification

Indirection via CID (Content ID)

- The CID must uniquely determine the context between a sender and a receiver.
- Any SRTP key management protocol (e.g. DTLS-SRTP) can be used.
- Sender and receiver must be online at the same time. Works for many use cases (e.g. media distribution).



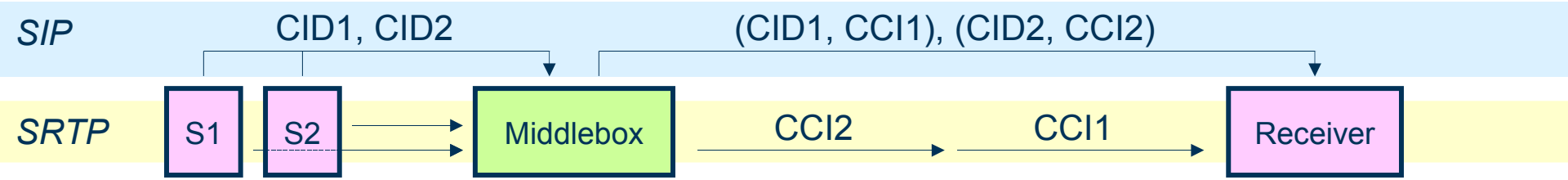
In-band context identification

Switching between e2e contexts

- If the SaF context contains more than one e2e context, the triplet context identifier needs to be extended with the CCI field in the SRTP SaF packet.

  <**CCI**, SSRC, destination network address, destination port number>

- The CCI is a short, in-band alias for the e2e context (or CID) and is only used on hbh basis.
- For each e2e context provided (through direct transfer of the protected context itself or a CID) the middlebox shall assign a unique CCI.



Request

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


ERICSSON