SRTP Store and Forward

draft-mattsson-srtp-store-and-forward-01

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

ERICSSON

TAKING YOU FORWARD

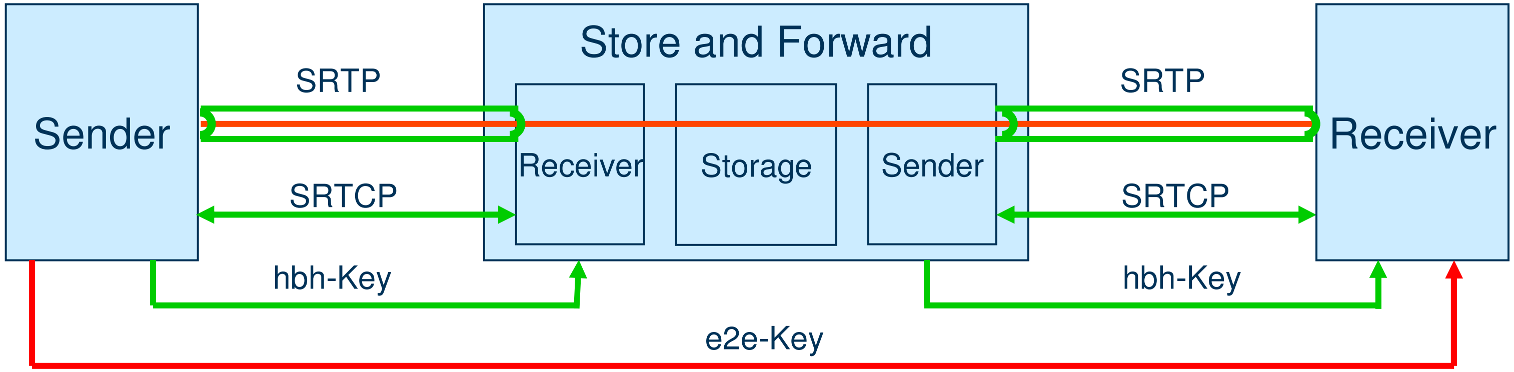
Content

- SRTP Store and Forward
- Updates in -01
  - Introduction
  - Use cases
  - Solution details
    - e2e transform
    - SRTP framework
- An example
- Check outstanding issues from -00
- Request

SRTP Store & Forward

Combination of

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



Updates

Introduction

- Clearer problem statement
- Not possible to directly store RTP/SRTP.
  - Media and additional information needed, hint tracks.
  - Storage of media streams will not be handled in the draft

Updates

Added use cases

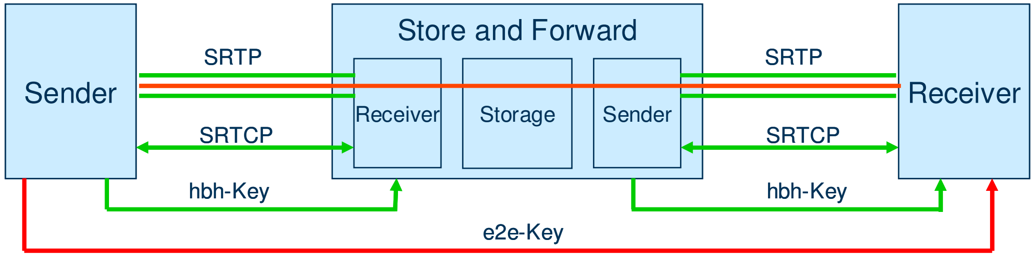
4.2. Media Distribution Use Cases

- **4.2.1. Streaming Pre-encrypted Media**
- **4.2.2. Video on Demand**
- **4.2.3. Caching Protected Media in the Network**
- **4.2.4. Recording Encrypted Media at Home**

4.3. Answering Machine use case

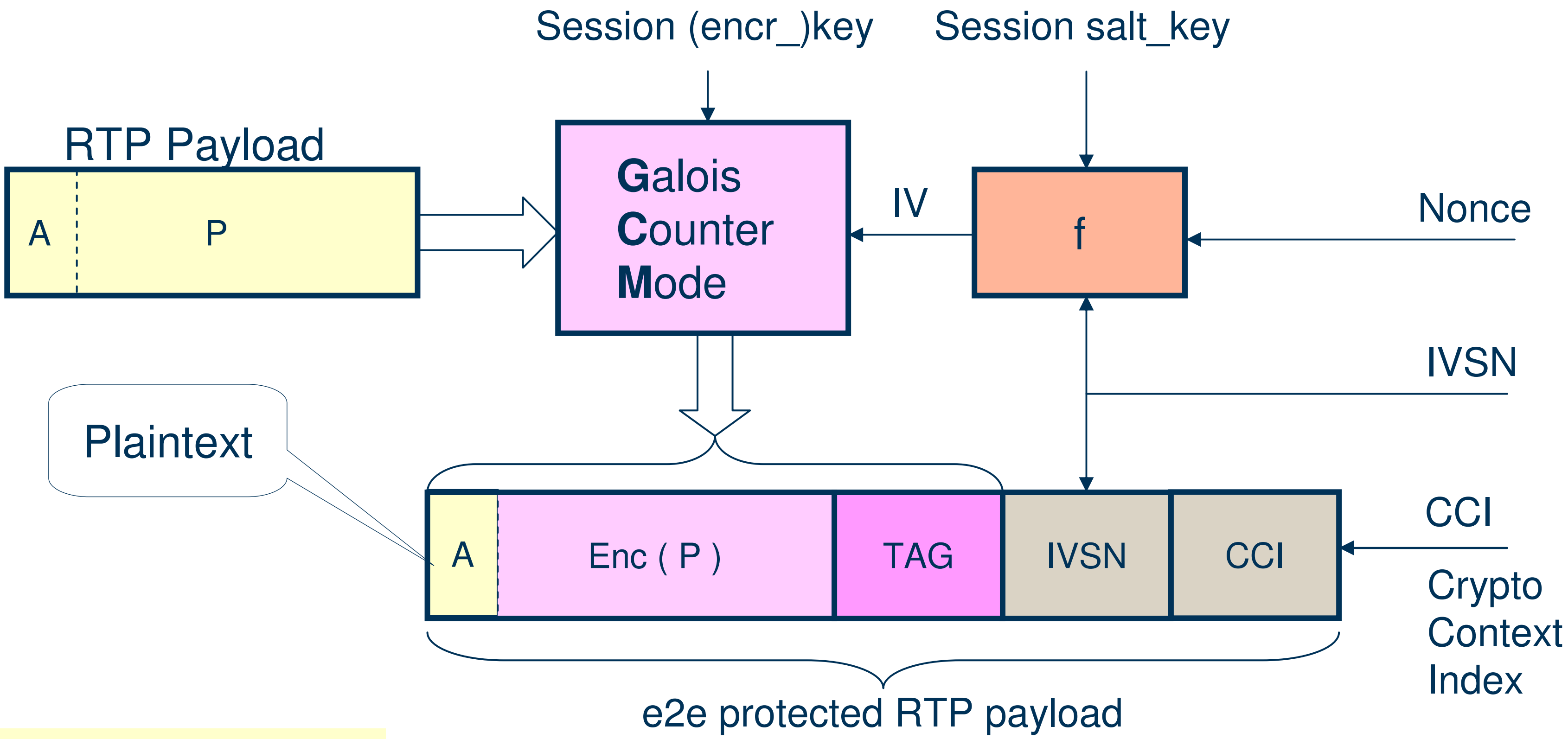
- 4.3.1. Storing/Caching Encrypted Media
- 4.3.2. Transport Protection
- 4.3.3. Playback of Media Stream
- 4.3.4. Multiple Callers

4.4. Use Case: Centralized Conferencing



Update

Media protection transform – GCM – AEAD

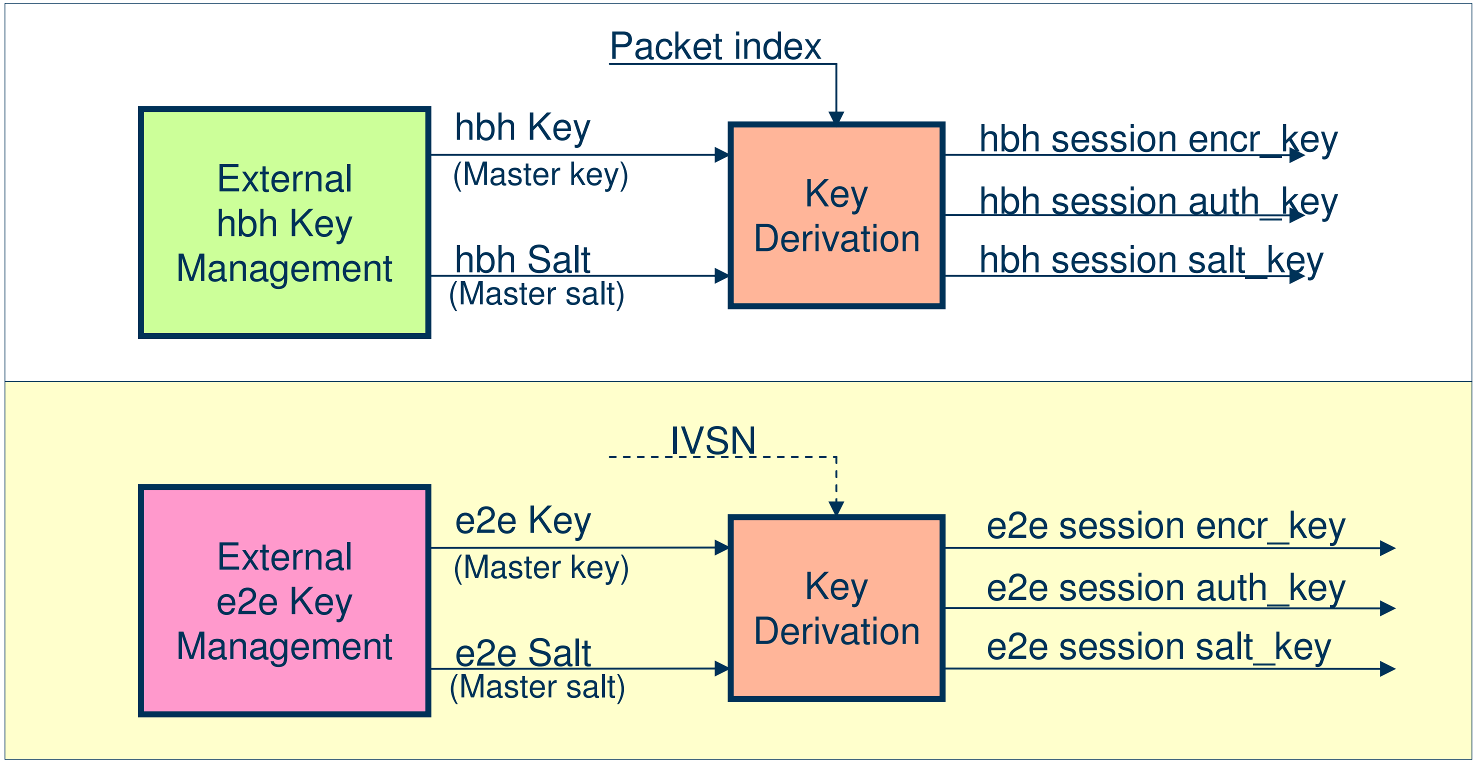


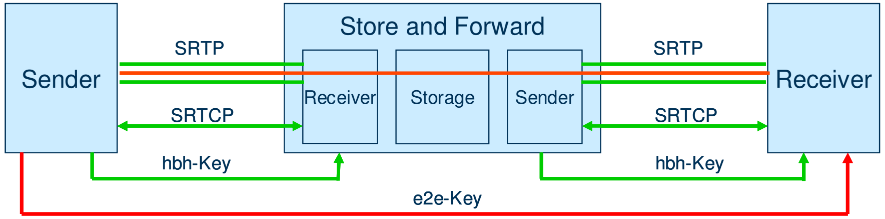
IVSN ~ SRTP index
Nonce ~ SSRC
CCI ~ extended MKI

AEAD == Authenticated Encryption with Associated Data

Updates

SRTP framework extension; Two security contexts

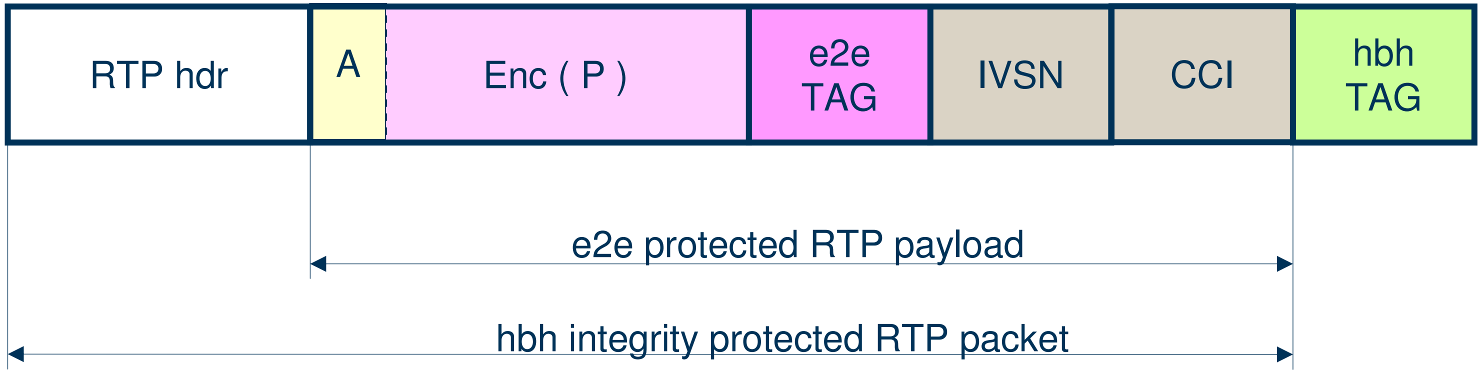




An example

e2e encryption and authentication; hbh authentication

Step	SRTP S & F		RFC 3711
1	Do e2e transform	~	Do encryption
2	Do hbh transform	~	Do authentication



Outstanding issues -00

- Combined inner and outer transforms
  - Minimal impact on SRTP framework
    - Only introducing handling of two security contexts
  - Handling of independent inner and outer protection transforms
    - Defining combined e2e and hbh transforms. New transforms can be added within current framework
  - Keying and handling of independent security contexts
    - Same key mgmt for e2e and hbh equalling key mgmt in RFC3711
  - Switching between security contexts
    - Introduction of CCI in e2e transform

Request

- Request that SRTP Store and Forward is taken on as a WG item

ERICSSON

TAKING YOU FORWARD