**Key Management for Multimedia Sessions**
<draft-carrara-mm-kmgt-sol-00.txt>
<draft-blom-mm-kmgt-00.txt>

# MIKEY: Multimedia Internet KEYing

<draft-ietf-msec-mikey-00.txt>

# Outline

- Background
- Scenarios and goals
- Overview and Changes

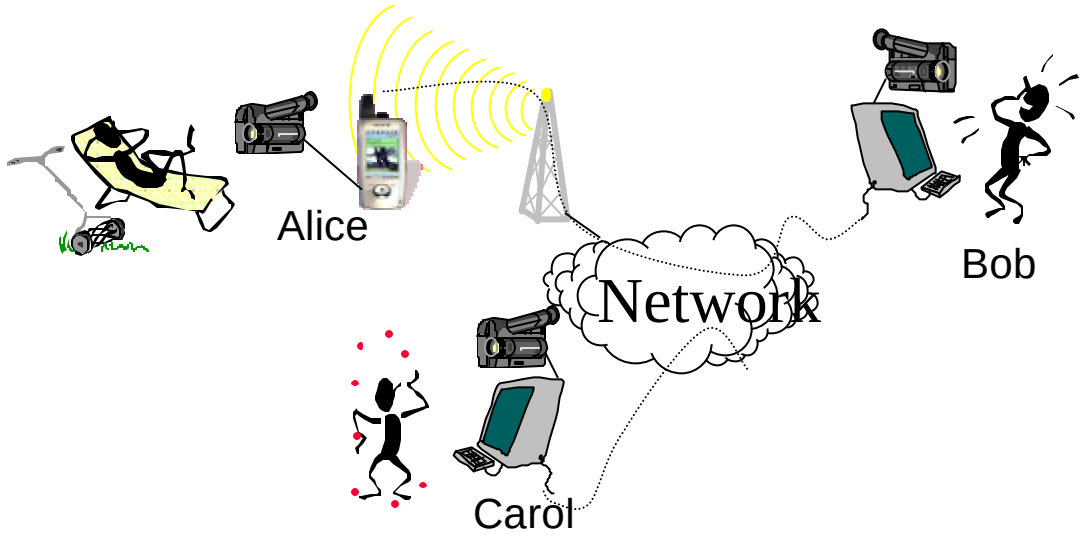
# Background

Work split between MSEC WG an MMUSIC WG

- Security part in MSEC WG (i.e. MIKEY)
- Extensions to SDP and RTSP in MMUSIC WG (draft-ietf-mmusic-kmgmt-ext-00.txt)

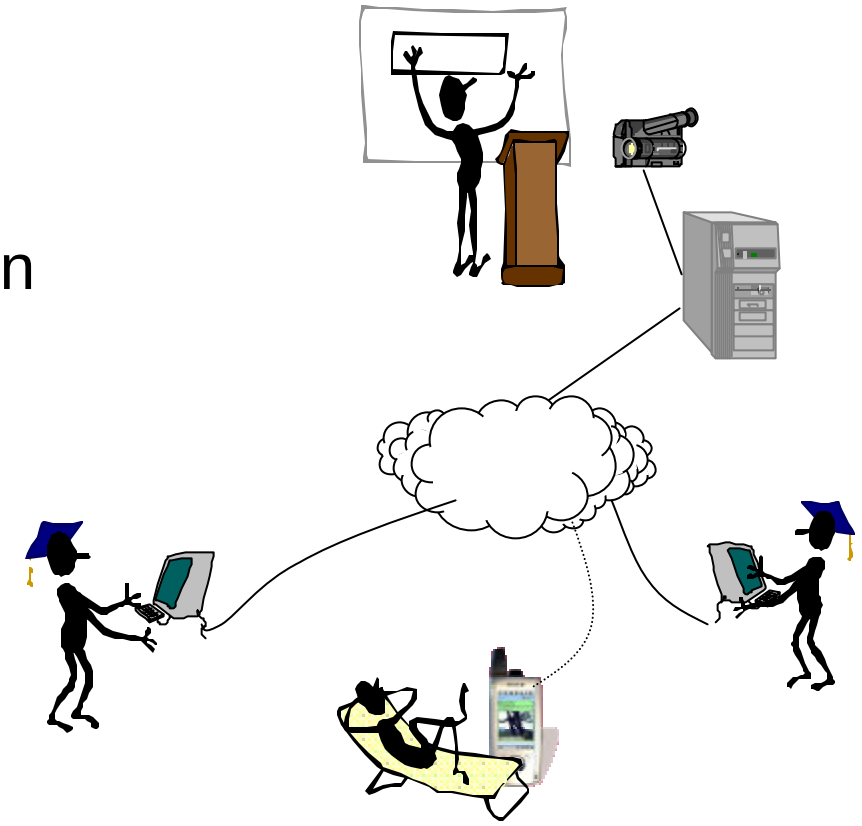
# Scenarios (1)

- SIP call with small interactive “ad-hoc” groups
- Heterogeneous environment
- SRTP for media protection



# Scenarios (2)

- One-to-“a few”
- Limited size of group
- RTSP for set up
- SRTP for media protection



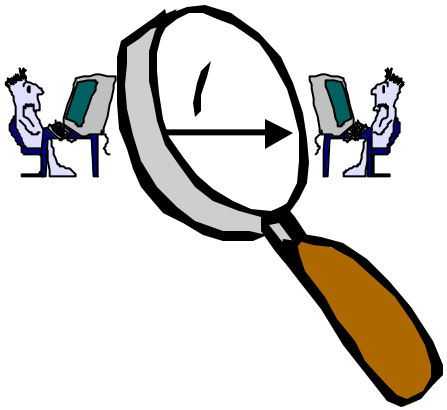
# Design goals and requirements

- End-to-end security of the key exchange
- Suitable for unicast and small groups
- Simplicity
- Efficiency
  - low extra bandwidth consumption,
  - low computational workload,
  - small code size
  - time efficient

# Changes

- Protocol remains fairly unchanged
- Different terminology (more aligned with the other MSEC WG drafts)
- Clarifications of
  - goals,
  - scenarios,
  - message processing,
  - replay protection.
- New definitions of payload formats

# Specific Terminology



Multimedia Crypto Session 1

Audio stream 1 (SRTP) → Crypto Session A

Video stream 1 (SRTP) → Crypto Session B

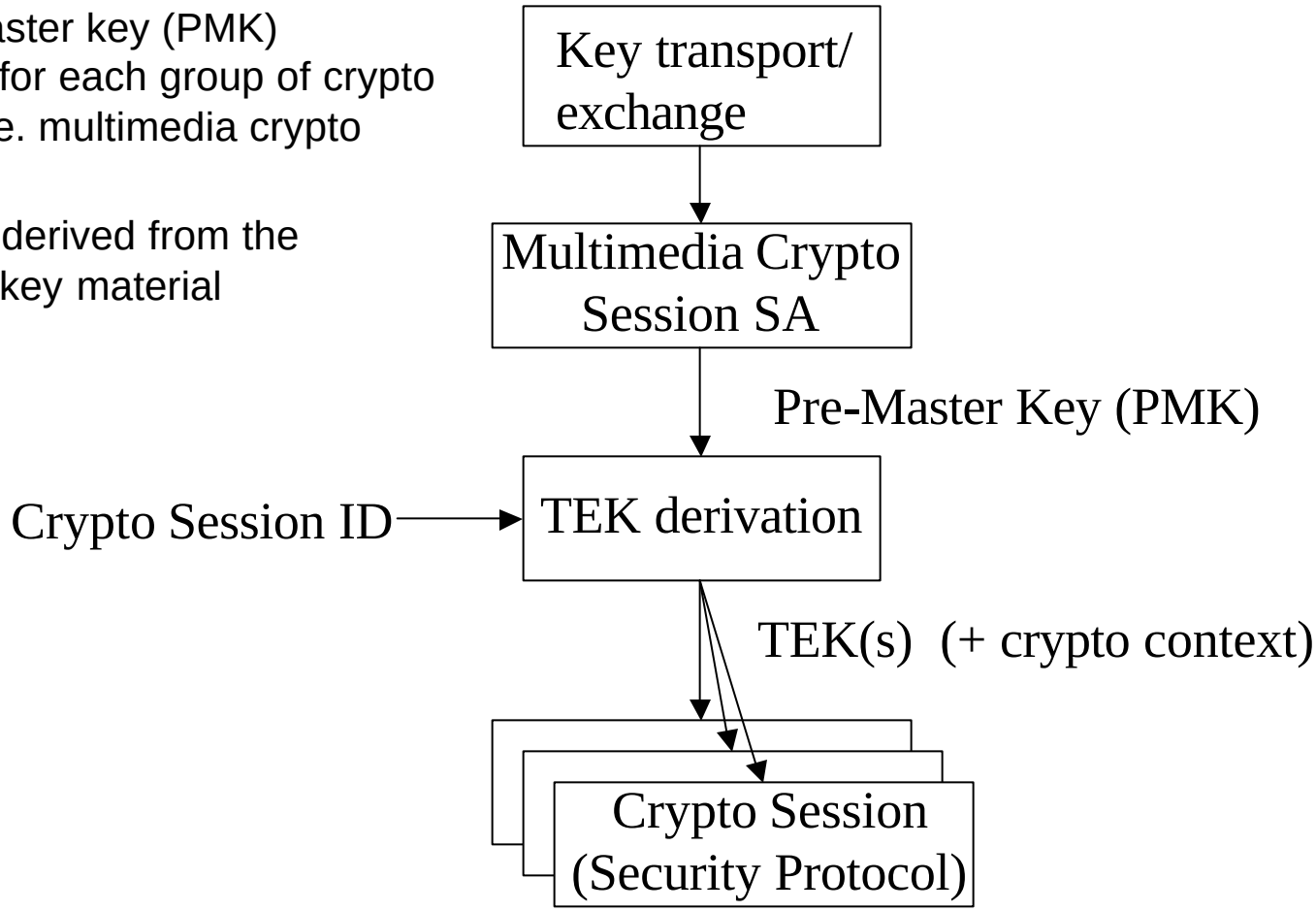
Multimedia Crypto Session 2

Audio stream 2 (SRTP) ← Crypto Session C

Video stream 2 (SRTP) ← Crypto Session D

# Overview

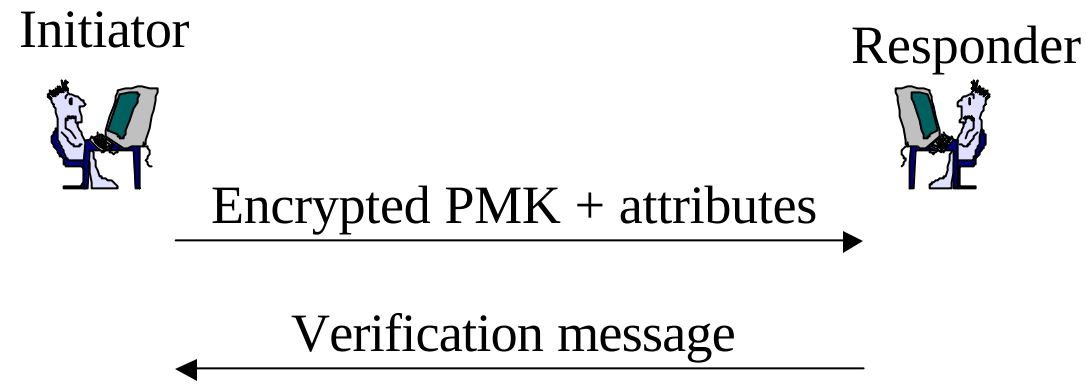
- One pre-master key (PMK) exchanged for each group of crypto sessions (i.e. multimedia crypto session)
- The TEK is derived from the exchanged key material



# Key transport and exchange mechanisms

- Pre-shared key based
- Public key based
- Diffie-Hellman based

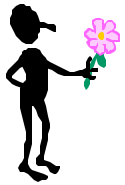
Example: Key transport

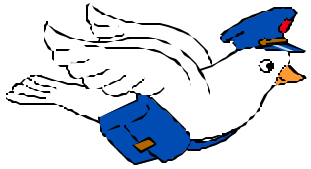



**Note**: max 1 roundtrip

# Transporting MIKEY

- Extension proposed to the Session Description Protocol (SDP) and the Real Time Streaming Protocol (RTSP)
- Can also be used in SIP (as SIP carries SDP)
- MMUSIC work in progress





(MIKEY over home-pigeon?)

# Replay protection

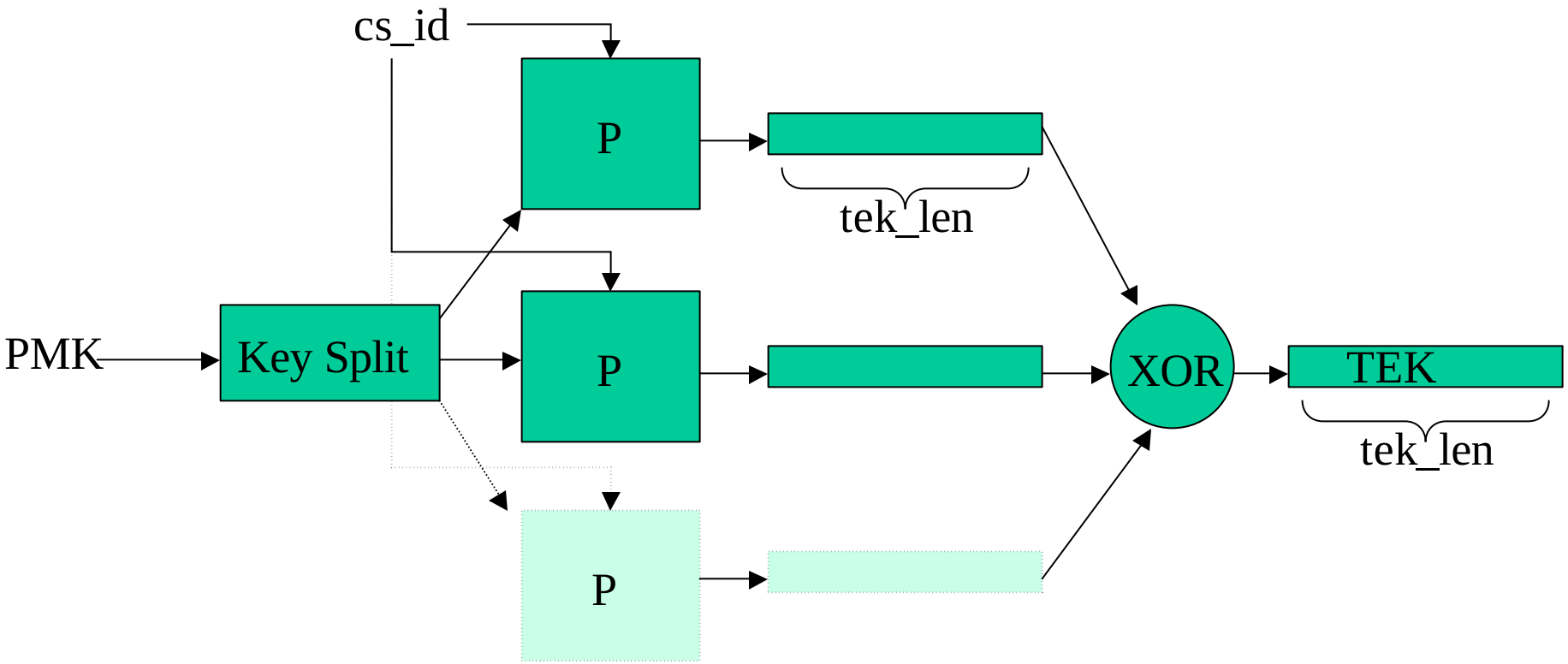
- Timestamps prevent against replay attacks assuming that:
  - Each host has a clock which is at least "loosely synchronized" to the time of the other hosts.
  - If the clocks are to be synchronized over the network, a secure network clock synchronization protocol is be used.

# Replay cache

- tradeoff between storage and time synchronization (hash of msg + timestamp ≈ 40 bytes)

- Client-Server: The client needs the cache, not the server
- Client-Client: both need a replay cache (however, the workload could be assumed to be quite small)

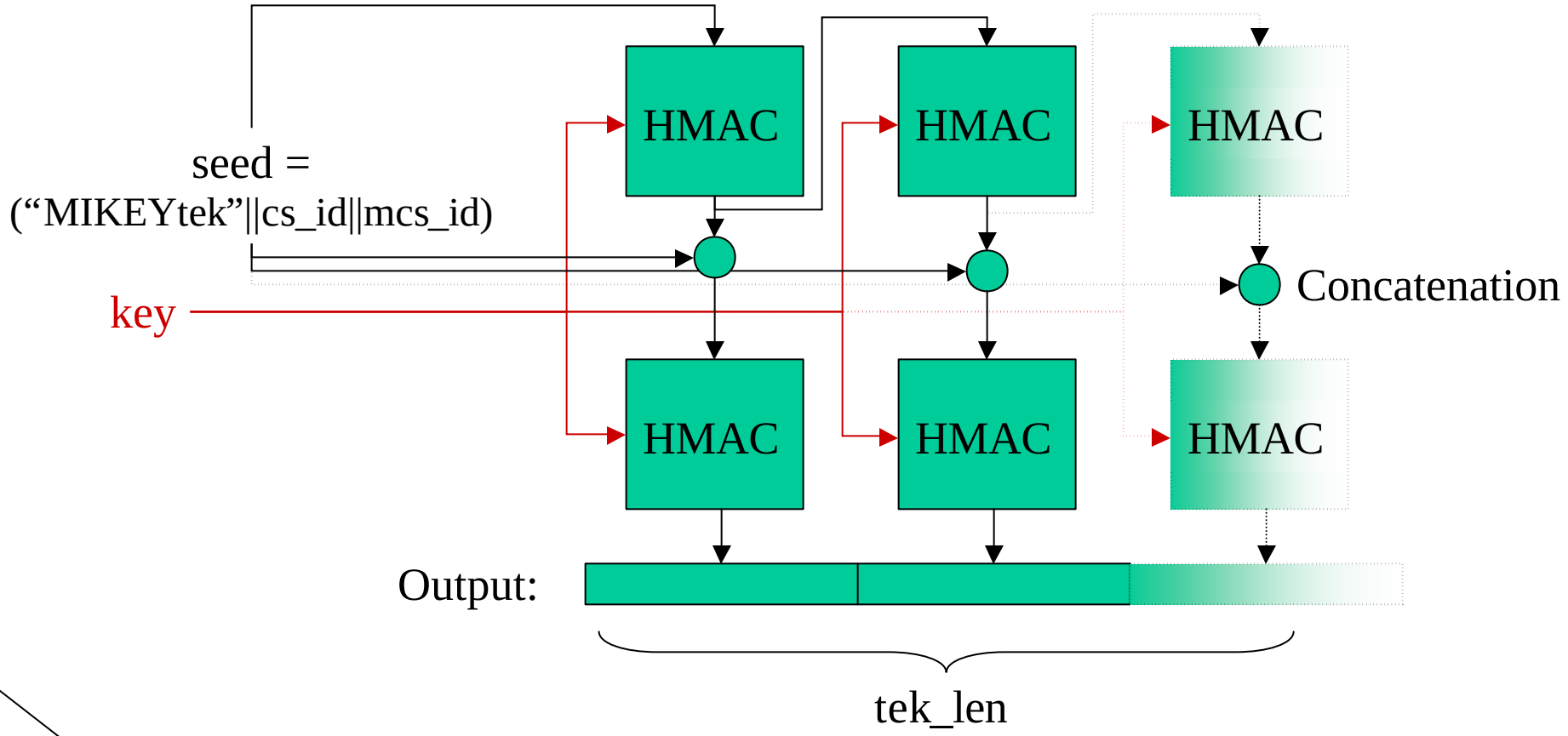
# TEK derivation




**Input:** PMK - Pre-Master Key of length pmk_len,
cs_id - crypto session id

**Output:** TEK of desired length, tek_len (<= pmk_len)

# The P function



# Final slide

- Milestone
- How to proceed?
- Questions and Comments?