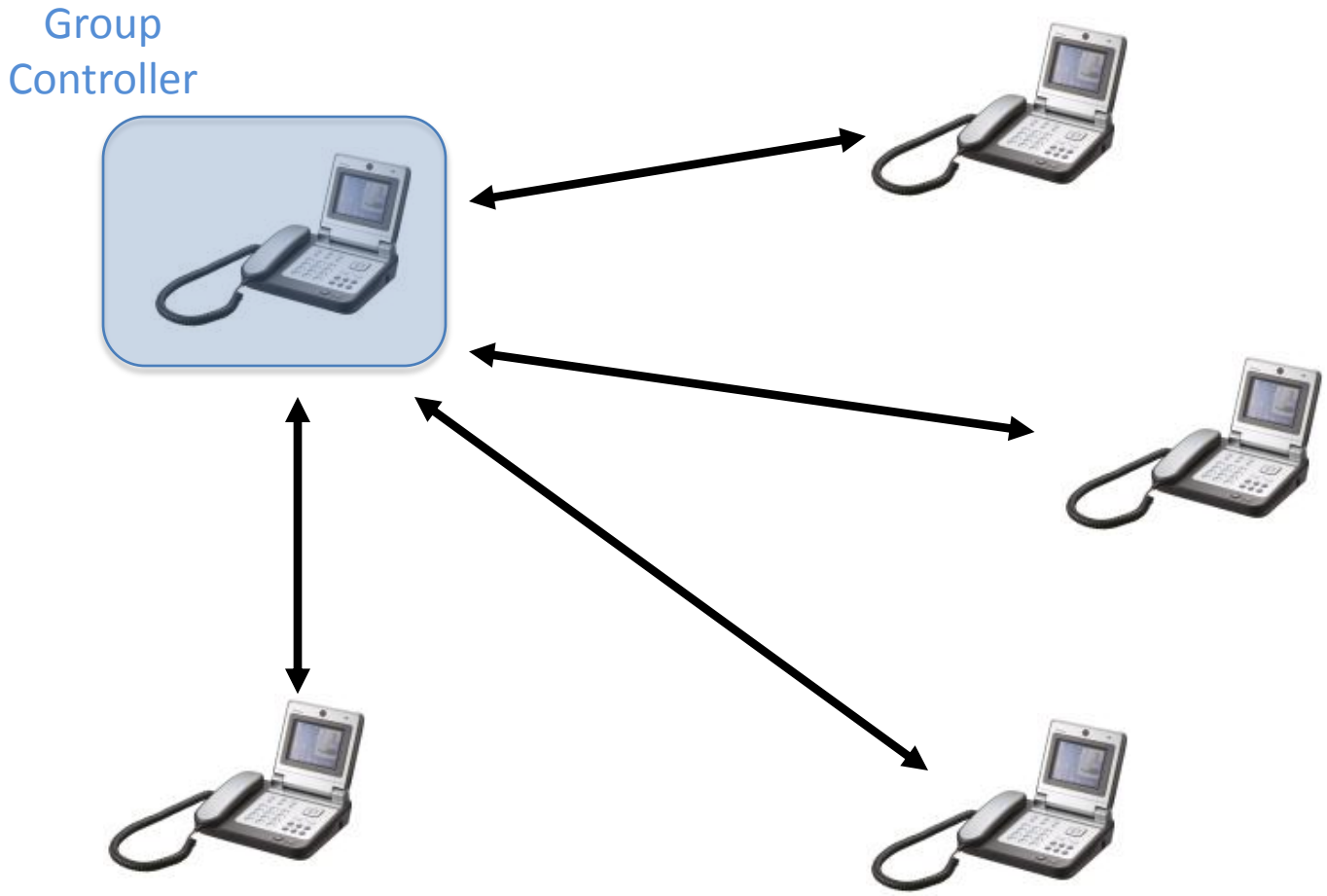
draft-mcgrew-srtp-ekt-04
draft-mcgrew-srtp-big-aes-01
draft-mcgrew-srtp-aes-gcm-01

mcgrew@cisco.com

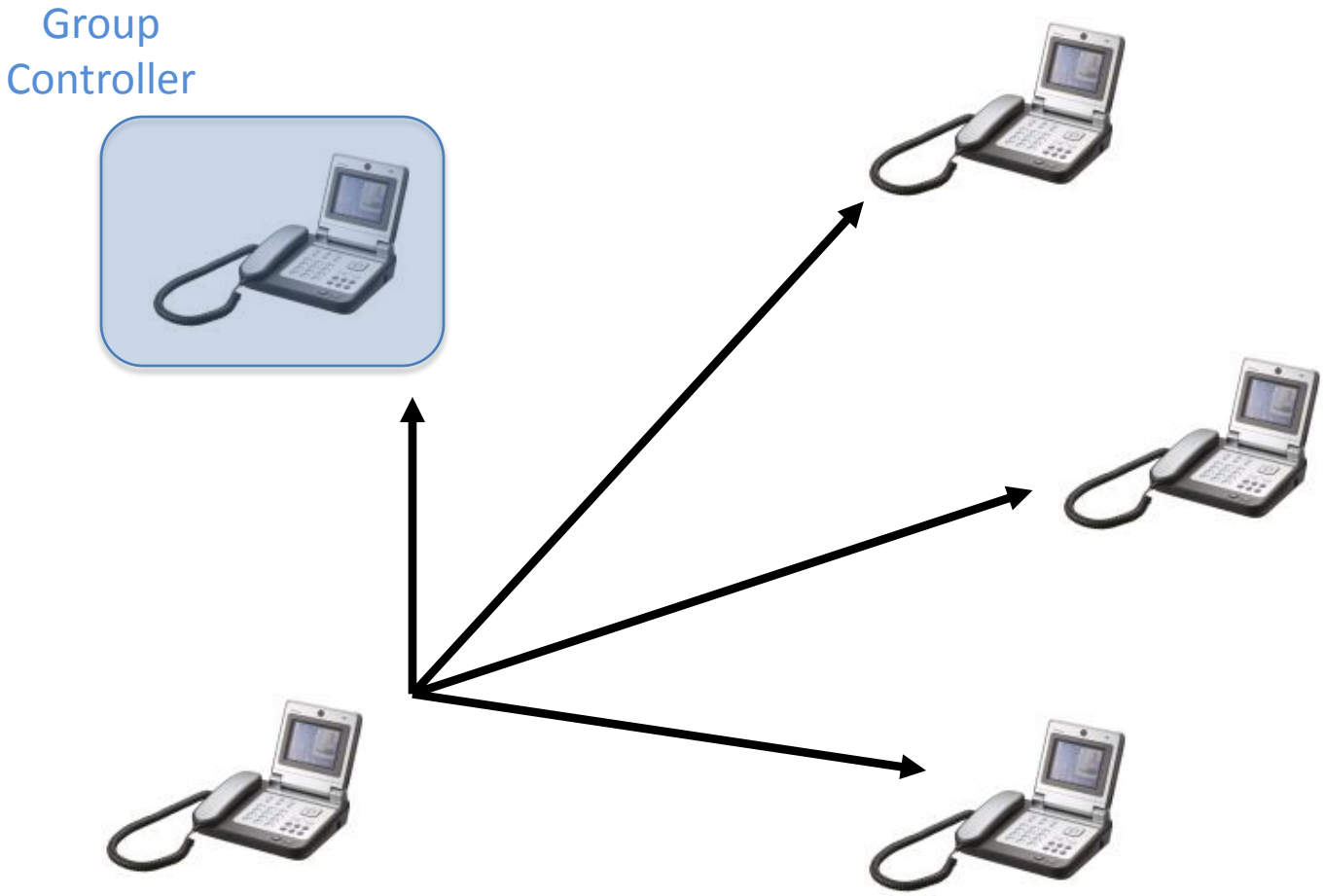
draft-mcgrew-srtp-ekt-04 Encrypted Key Transport for SRTP

- In-band key transport protected by separate RTP session-level key
  - Conveys SRTP master key and ROC
- Layer of indirection between Key Management and SRTP
  - Avoids layer violation
  - Key management should be oblivious to RTP Sources, SSRCs, Seq Nums, Rollover Counter
  - Indirection is important for large groups

1. DTLS-SRTP-KTR (1:1)



2. EKT (1:Many)



Looking back and forward

- EKT defined 2006-2007
  - Expired pending implementation and interest
  - We now have both!
- EKT is only way to avoid layer violations
  - Essential for scalability to large groups
- EKT currently defined to use SDP Security Descriptions
  - DTLS-SRTP-KTR has much better security
  - DTLS-SRTP is IETF standard for SRTP keying

draft-mcgrew-srtp-big-aes-01 The use of AES-192 and AES-256 in Secure RTP

- RFC 3711 used only the Advanced Encryption Standard (AES) with 128-bit keys
  - Motivation: compactness, simplicity
  - 128-bit keys are more than adequately secure
- This draft adds AES-192 and AES-256 to SRTP
  - RTP Payload encryption
  - Key Derivation

Motivations for larger keys

- Confidentiality resistant to possible future advances in cryptanalysis
  - New mathematical ideas (DC, LC, XLS)
  - Construction of a practical quantum computer
- Fallback plan in case of advances
- Suite B conformance
- Interoperability
  - ZRTP, non-standard SRTP uses of AES-256

What's in the draft

- AES-192, AES-256 encryption transform
- AES-192, AES-256 key derivation function
  - Usage requirements
- Crypto Suites
  - RFC 4568 (SDP Security Descriptions)

Questions

- Should we make AES-192 optional?
- Should we add DTLS-SRTP bindings?
- Should we make this work standards track?

draft-mcgrew-srtp-aes-gcm-01 AES-GCM and AES-CCM Authenticated Encryption in Secure RTP

- Adds to SRTP:
  - AES Galois/Counter Mode (GCM)
  - AES Counter and CBC-MAC Mode (CCM)
  - Interface to other Authenticated Encryption algorithms

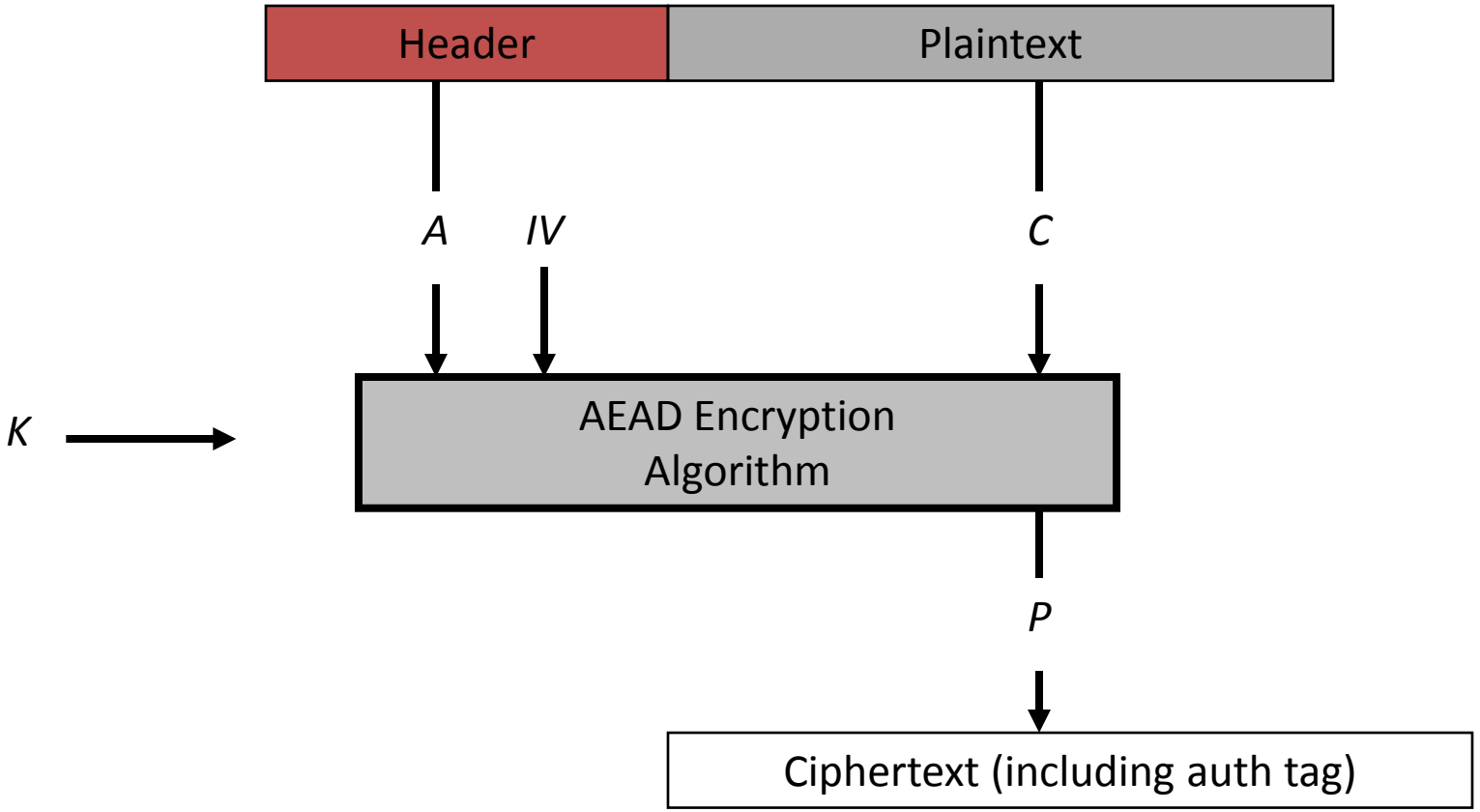
AES GCM

- Provides encryption and authentication
- Best mode for performance and efficiency
  - Especially suitable for hardware
  - Especially suitable for short packets
- For compact software, use CCM

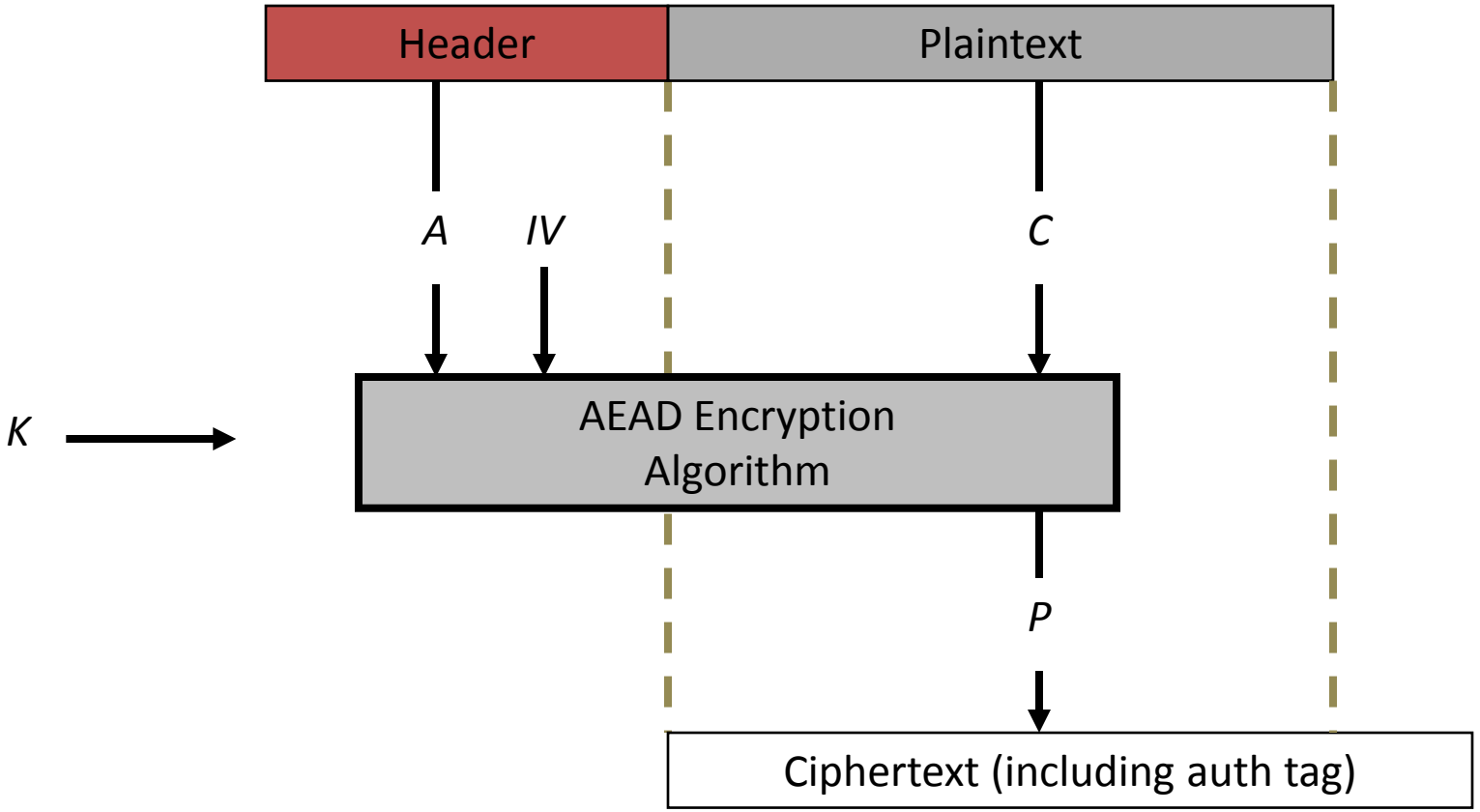
Authenticated Encryption with Associated Data (AEAD)

- Provides encryption *and* authentication
  - Obviates Message Authentication Code like HMAC
- RFC 5116 defines AEAD interface
- This draft uses that interface
  - Simplifies definition
  - Promotes crypto agility and implementation reuse

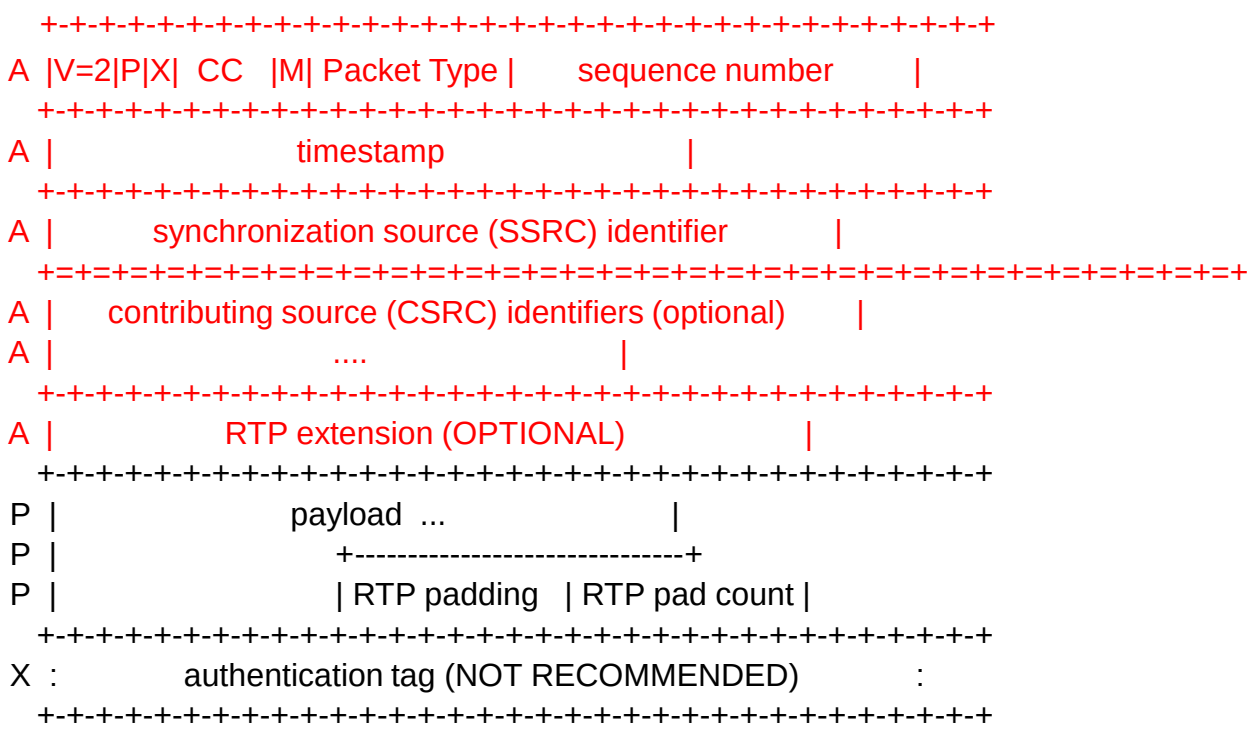
AEAD encryption



AEAD encryption



AEAD use in SRTP



P = Plaintext (to be encrypted and authenticated)

A = Associated Data (to be authenticated only)