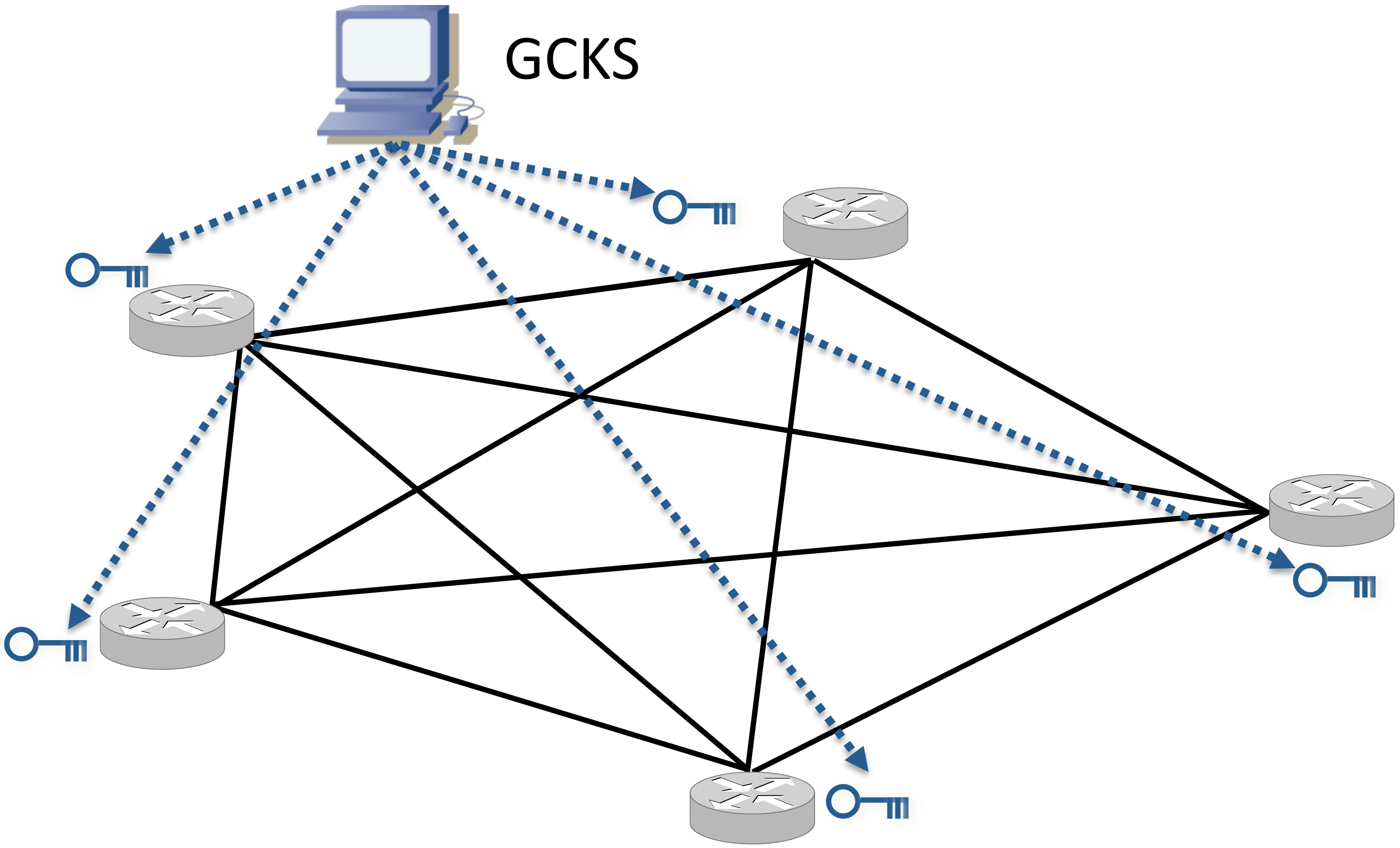
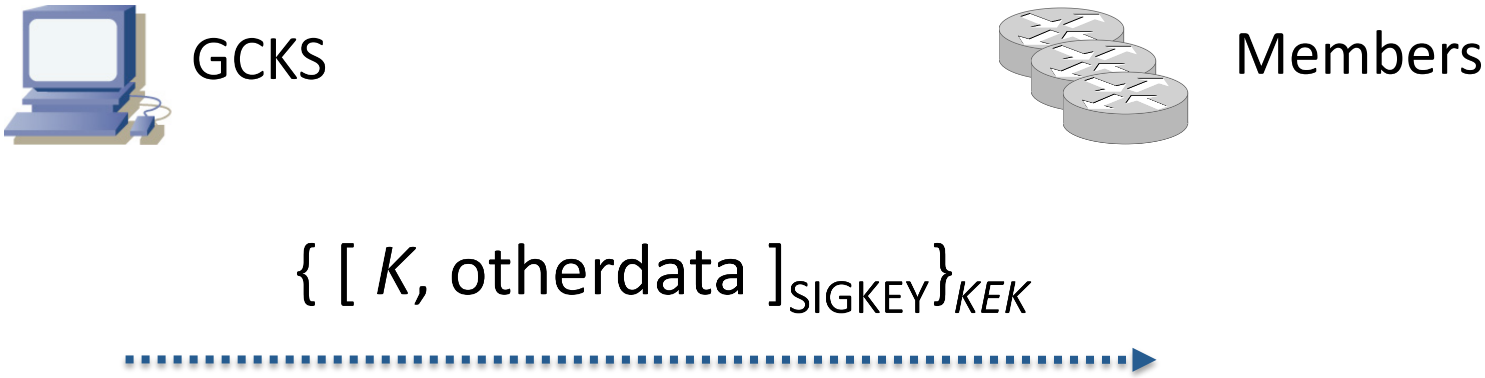
Symmetric Key Transport and Group Key Management

mcgrew@cisco.com

Multicast and Group Keying



Groupkey Push



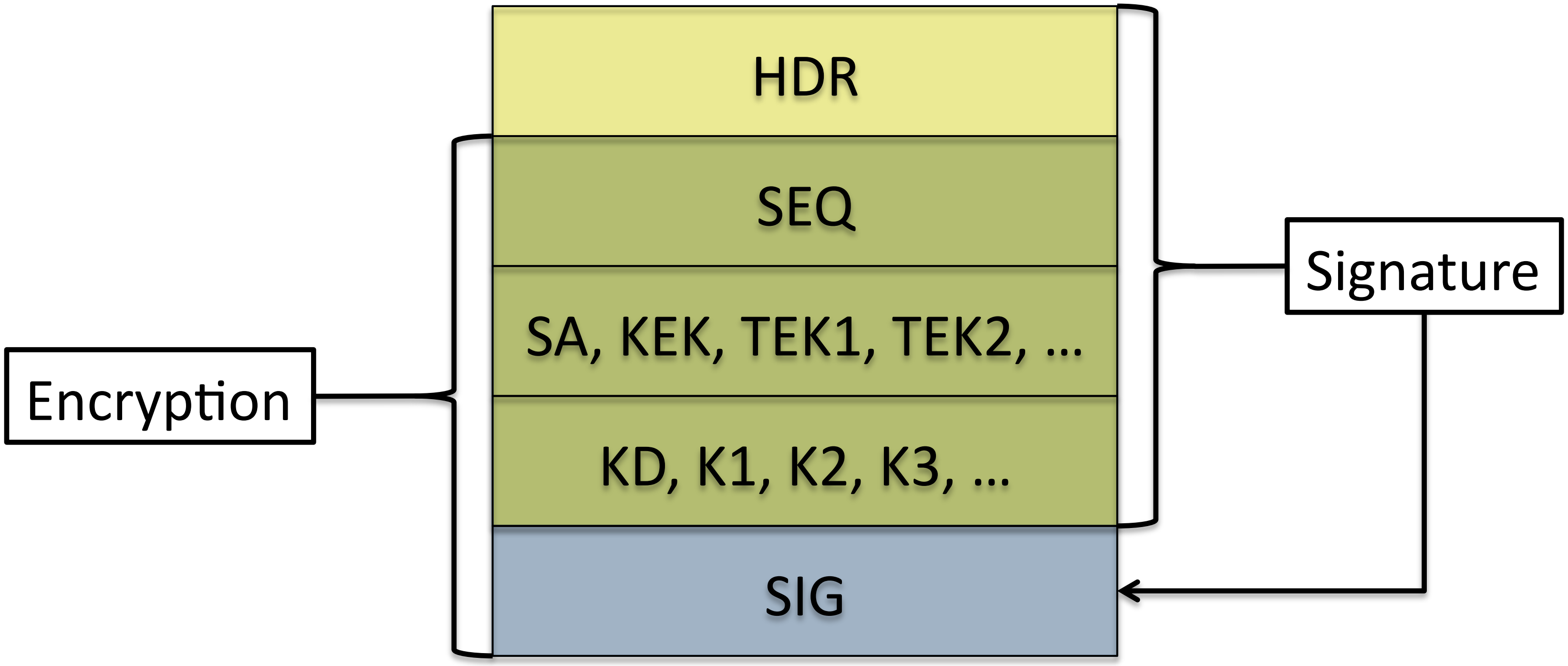
GCKS

Members

$\{ [\, K, \text{otherdata}\,]_{\text{SIGKEY}} \}_{KEK}$

- Protection of group key
  - – Symmetric confidentiality
    - Encryption with group key
  - – Asymmetric authentication
    - Signature with GKCS public/private keypair

GDOI GROUPKEY_PUSH



GROUPKEY_PULL similar, uses HMAC

Key Wrap *Service*

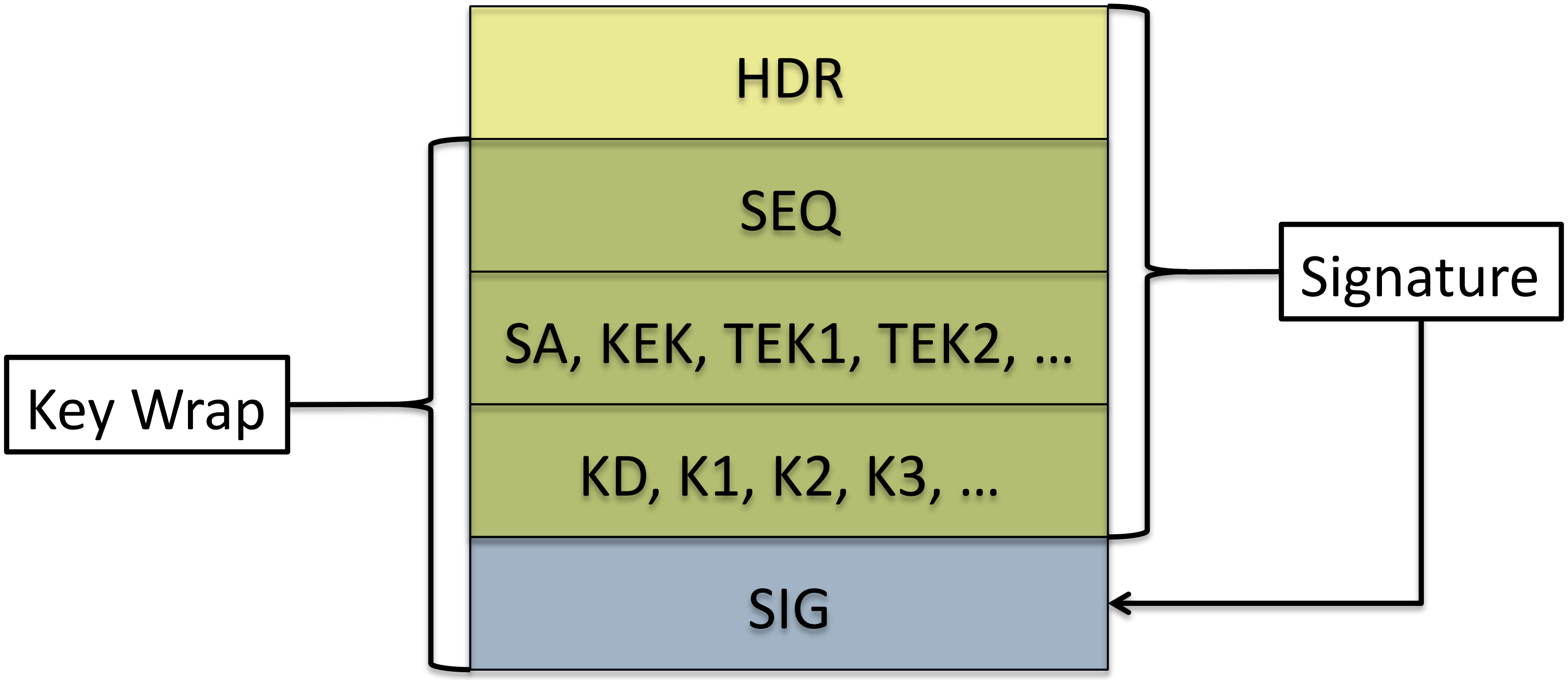
- Confidentiality
- Symmetric Authentication
- Does not require nonce/IV

- *Implied: Robust against implementation error*

Key Wrap *Algorithm*

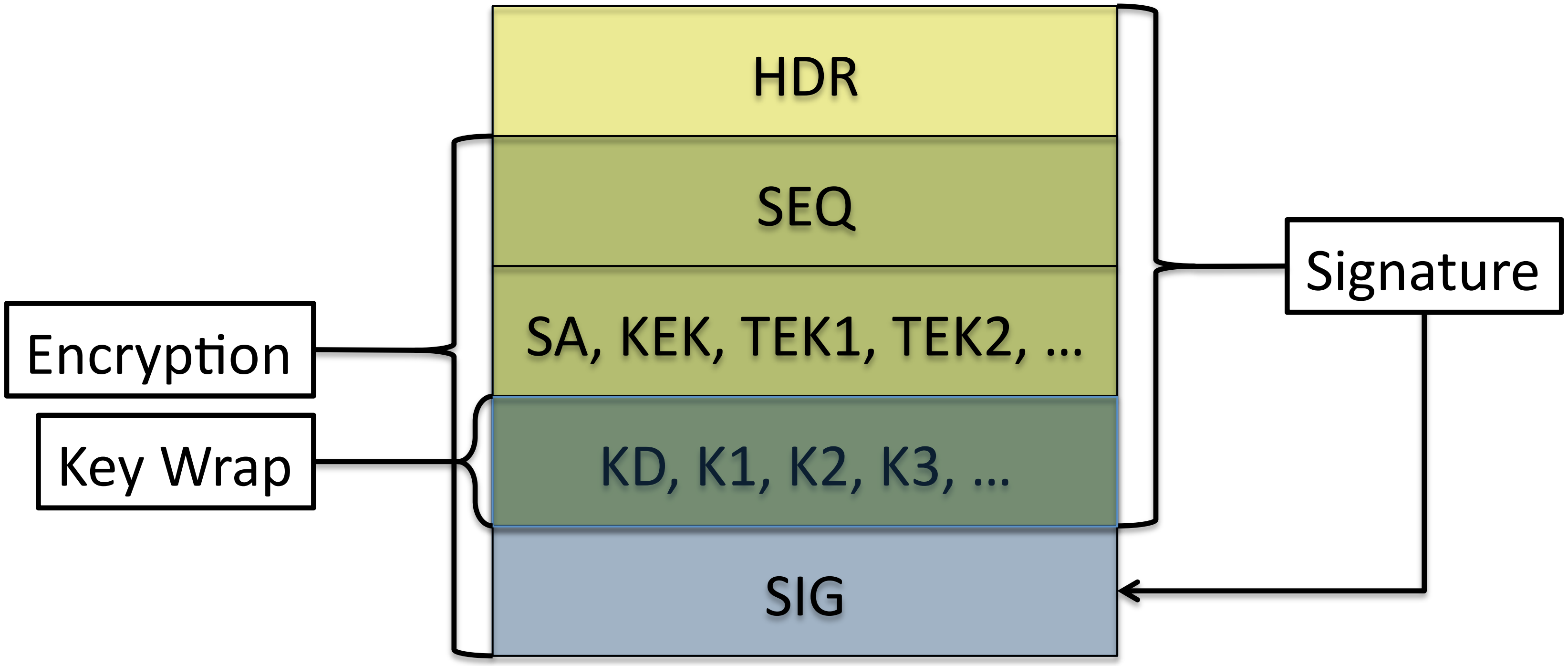
- NIST Draft 2001
- RFC 3394 *Advanced Encryption Standard (AES) Key Wrap Algorithm*
- RFC 5649 *Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm*
- Symmetric Encryption (128, 192, 256 bits)
- Symmetric Authentication (64-bit checksum)
- **Six** passes of AES

Option 1: KW replaces Encryption



Question: KW appropriate for GDOI/IKE packet protection?

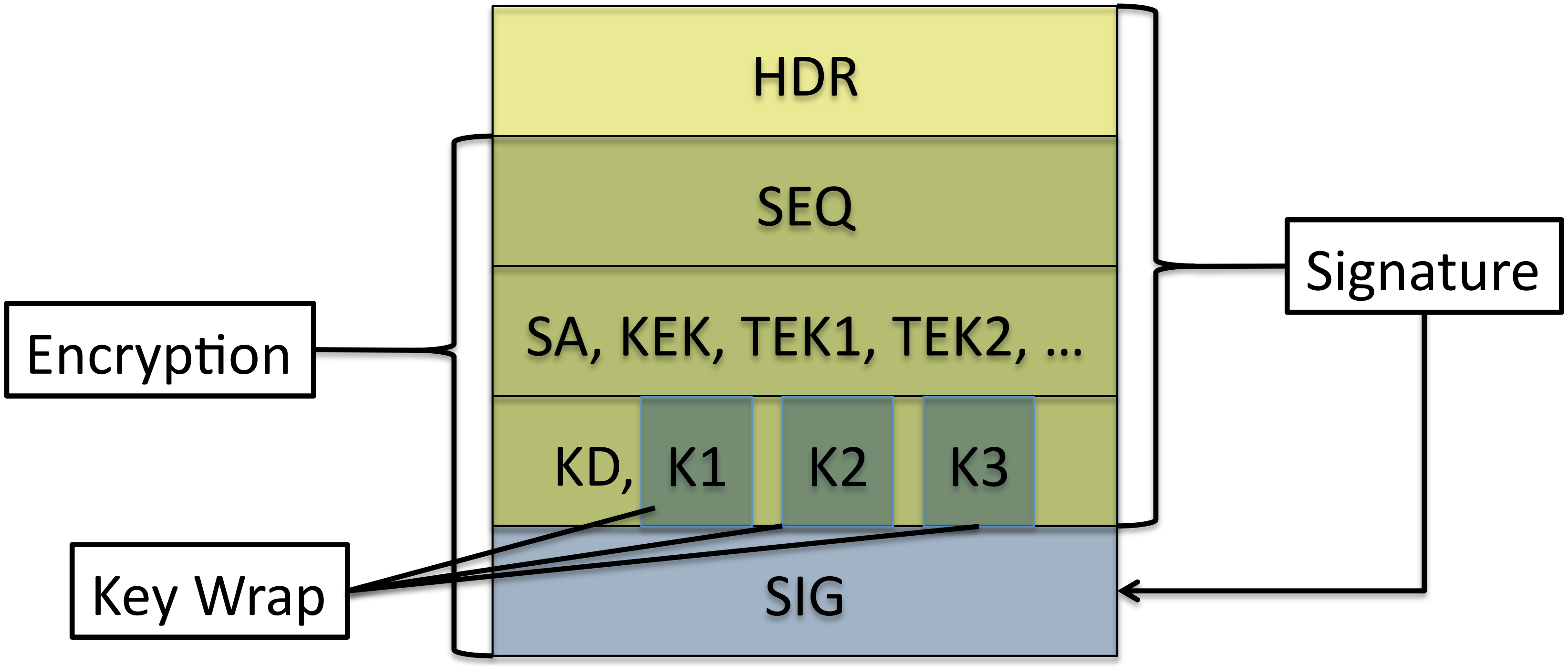
Option 2: KW Superencryption



Question: what key used in KW?

Question: OK to not wrap KEK, TEKs?

Option 3: Multi-Superencryption



Question: what key used in KW?

Question: OK to not wrap KEK, TEKs?

Other Issues

- Groupkey-push and pull need packet processing rates
  - KW *algorithm* has > 6x computational cost
- Groupkey-push *can* use IV/nonce
- Use a keywrap algorithm based on AES-CBC and HMAC-SHA1? Other algorithm?