HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

3 Data Link Layer Security

Prof. Dr. Andreas Steffen

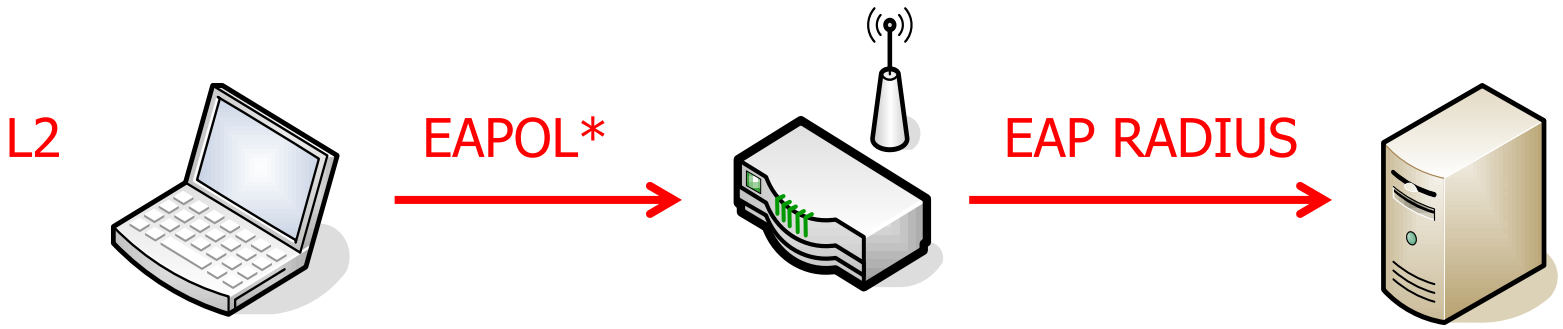
Institute for Internet Technologies and Applications (ITA)

Security Protocols for the OSI Stack

Communication layers	Security protocols
Application layer	Platform Security, Web Application Security, VoIP Security, SW Security
Transport layer	TLS
Network layer	IPsec
Data Link layer	[PPTP, L2TP], IEEE 802.1X, IEEE 802.1AE, IEEE 802.11i (WPA2)
Physical layer	Quantum Cryptography

3.1 Port-Based Network Access Control - IEEE 802.1X

IEEE 802.1X Access Control using EAP Methods



- 802.1X Supplicants and Authenticators are both Port Access Entities (PAEs)

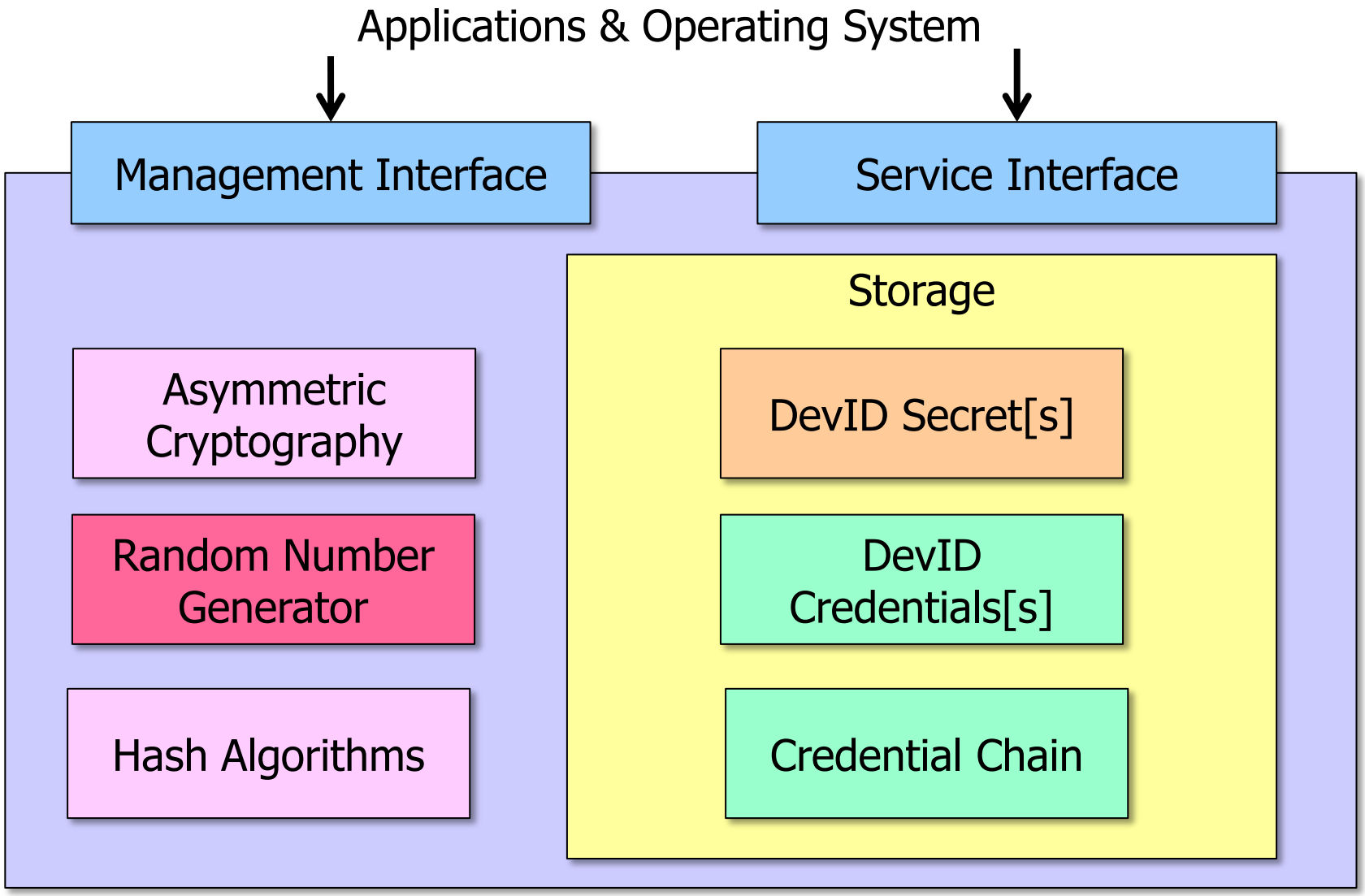
* EAP over LAN (Ethertype 0x888E)

3.2 Secure Device Identity IEEE 802.1AR - DevID

IEEE 802.1AR Secure Device Identifier

- DevID Secure Device Identifier
  - Secure Device Identifier
- IDevID Initial Device Identifier
  - Created during manufacturing and cannot be modified
    Either reaches end of lifetime (certificate) or can be disabled
- LDevID Locally Significant Device Identifier
  - One or several may be created by network administrator
- DevID Module
  - Hardware module which stores the DevID secrets, credentials and the entire credential chain up to the root certificate
  - Contains a strong Random Number Generator (RNG)
  - Implements Asymmetric Algorithms (2048 bit RSA and/or 256 bit ECDSA)
  - Implements SHA-256 Hash Function

IEEE 802.1AR DevID Module

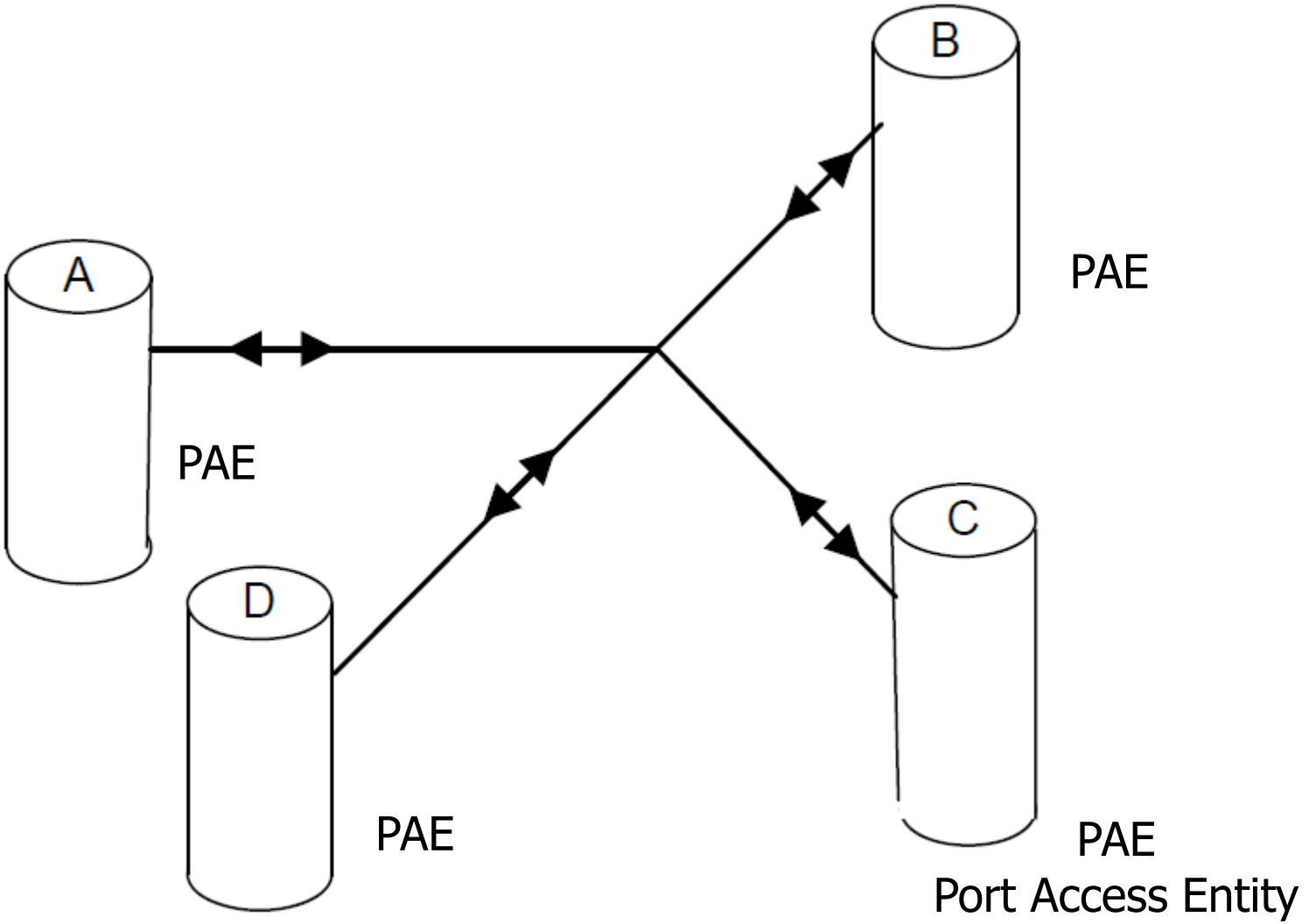


Use of DevIDs

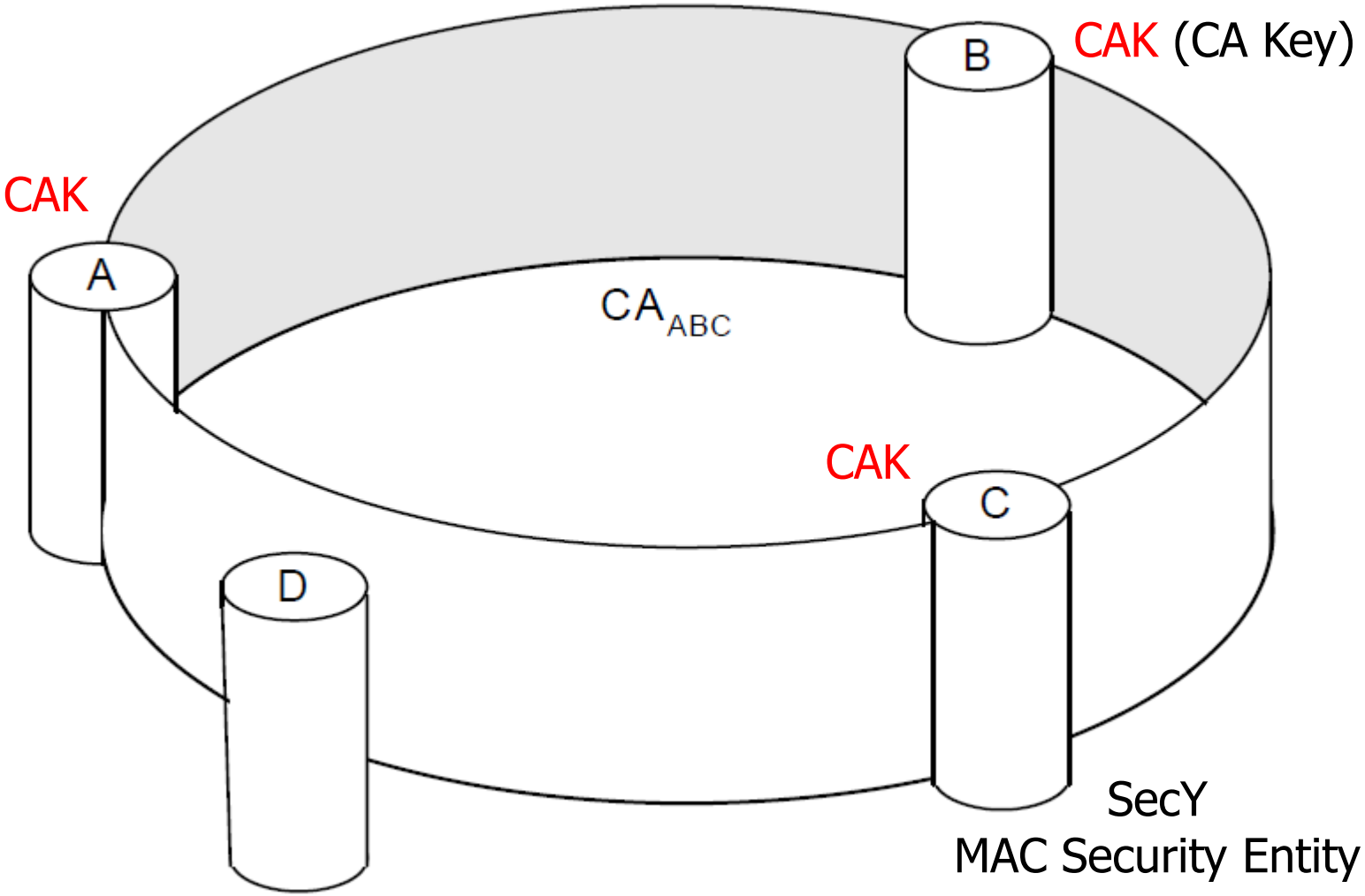
- DevID use EAP-TLS Authentication
  - Device authentication can be based on its DevID certificate.
- DevID use in Consumer Devices
  - Similar but more secure than access control based on a MAC address list which can easily be spoofed, a switch, router or access point can allow access based on a registered commonName (CN), serialNumber (SN) or a subjectAltName contained in the DevID certificate.
- DevID use in Enterprise Devices
  - Similar to the consumer device use case but the DevID is usually registered with a centralAAA server.
- DevID Module based on Trusted Platform Module (TPM)
  - Each TPM has a unique non-erasable Endorsement Key (EK) to which DevID secrets and credentials can be bound.

3.3 Media Access Layer Security IEEE 802.1AE - MACsec

Four Stations Attached to a LAN

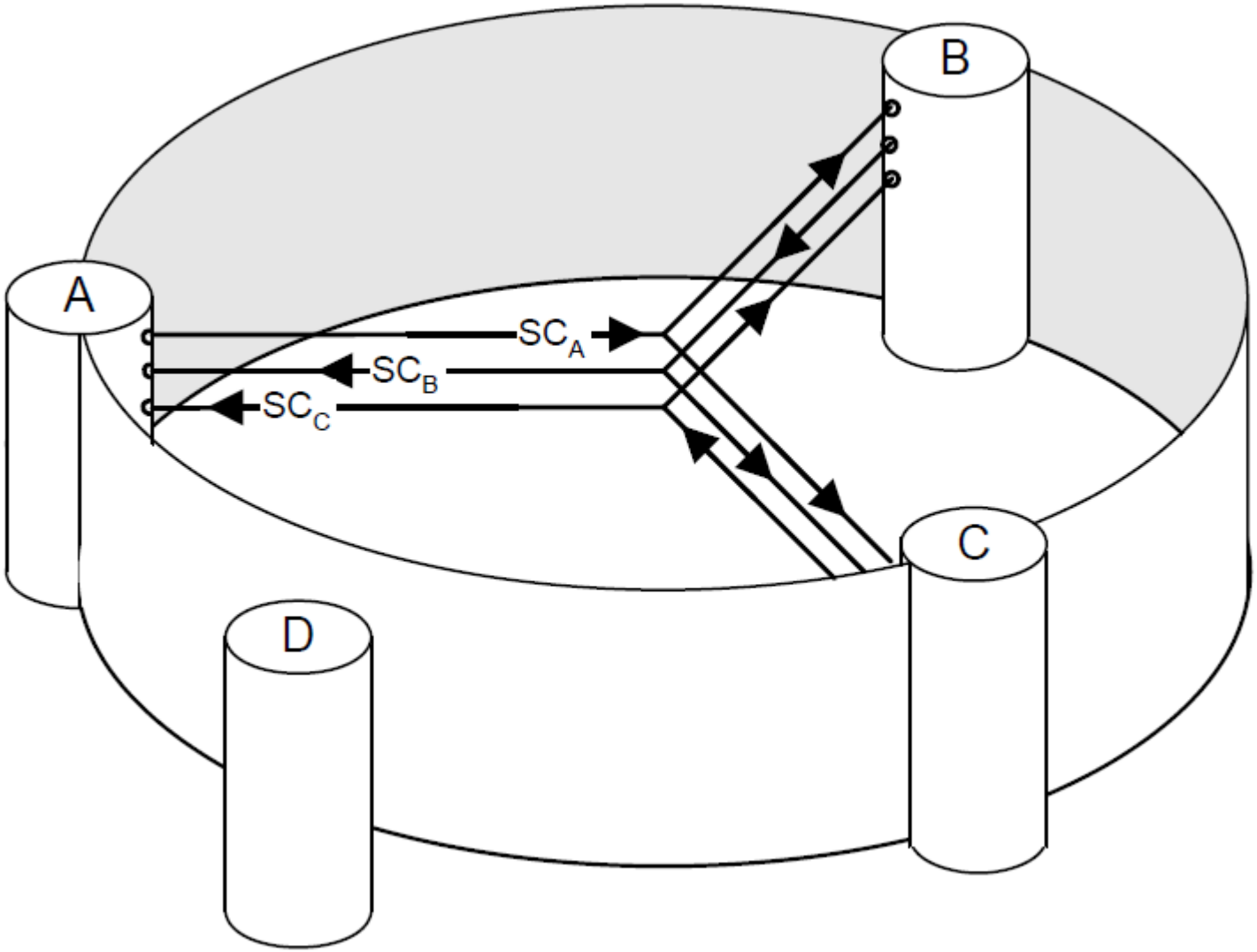


Connectivity Association (CA)



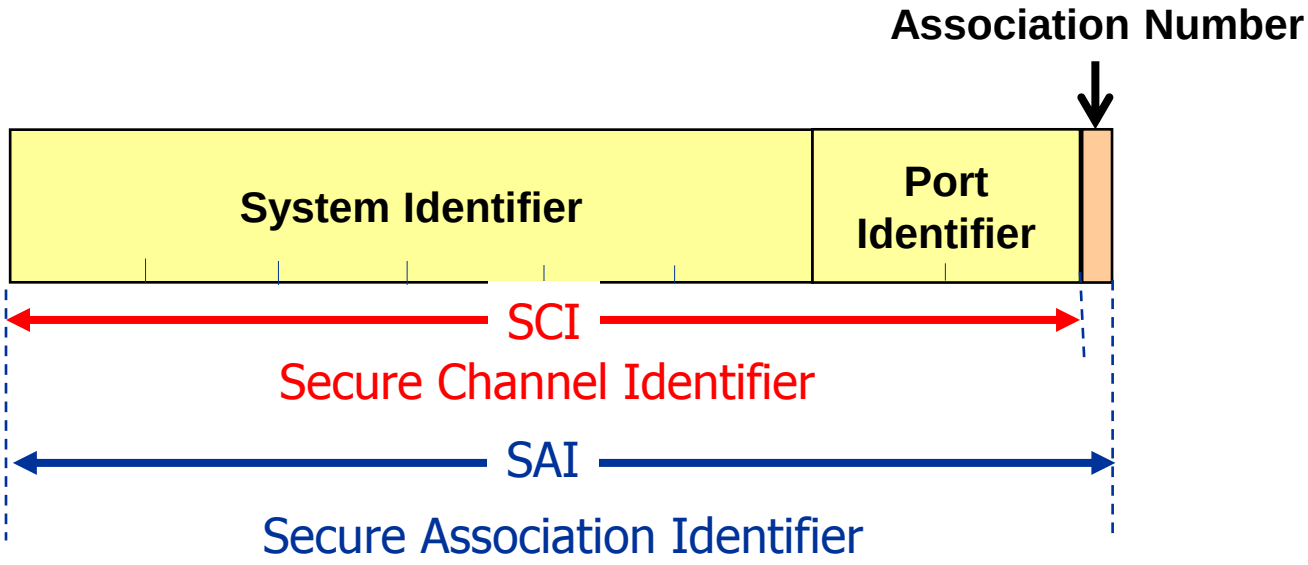
- Station D is not part of the CA

Secure Channel (SC) and Secure Association (SA)



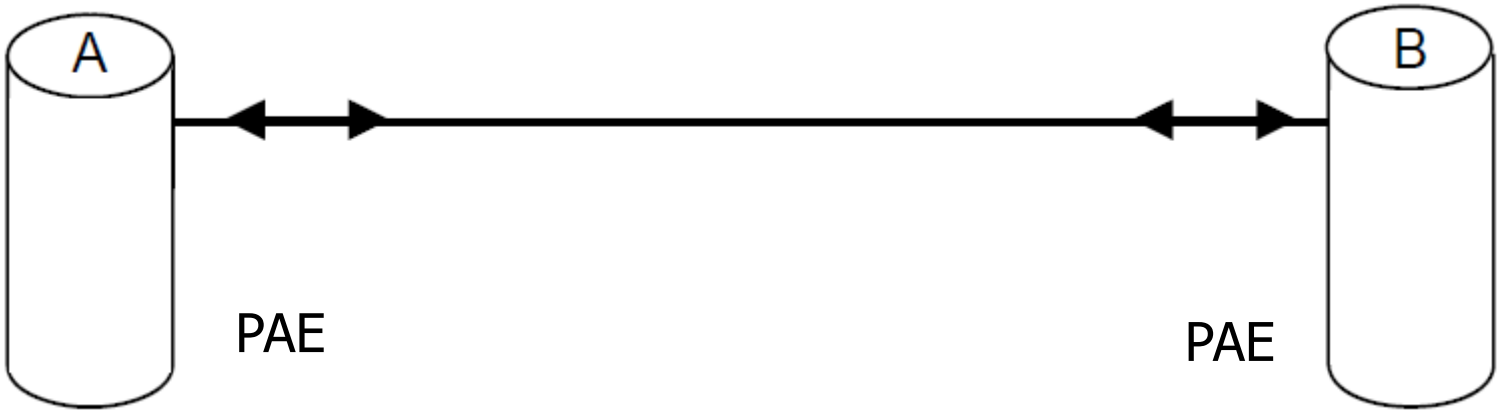
- Each SC comprises a succession of SAs each with a different SAK (SA Key)

Secure Channel and Secure Association Identifiers

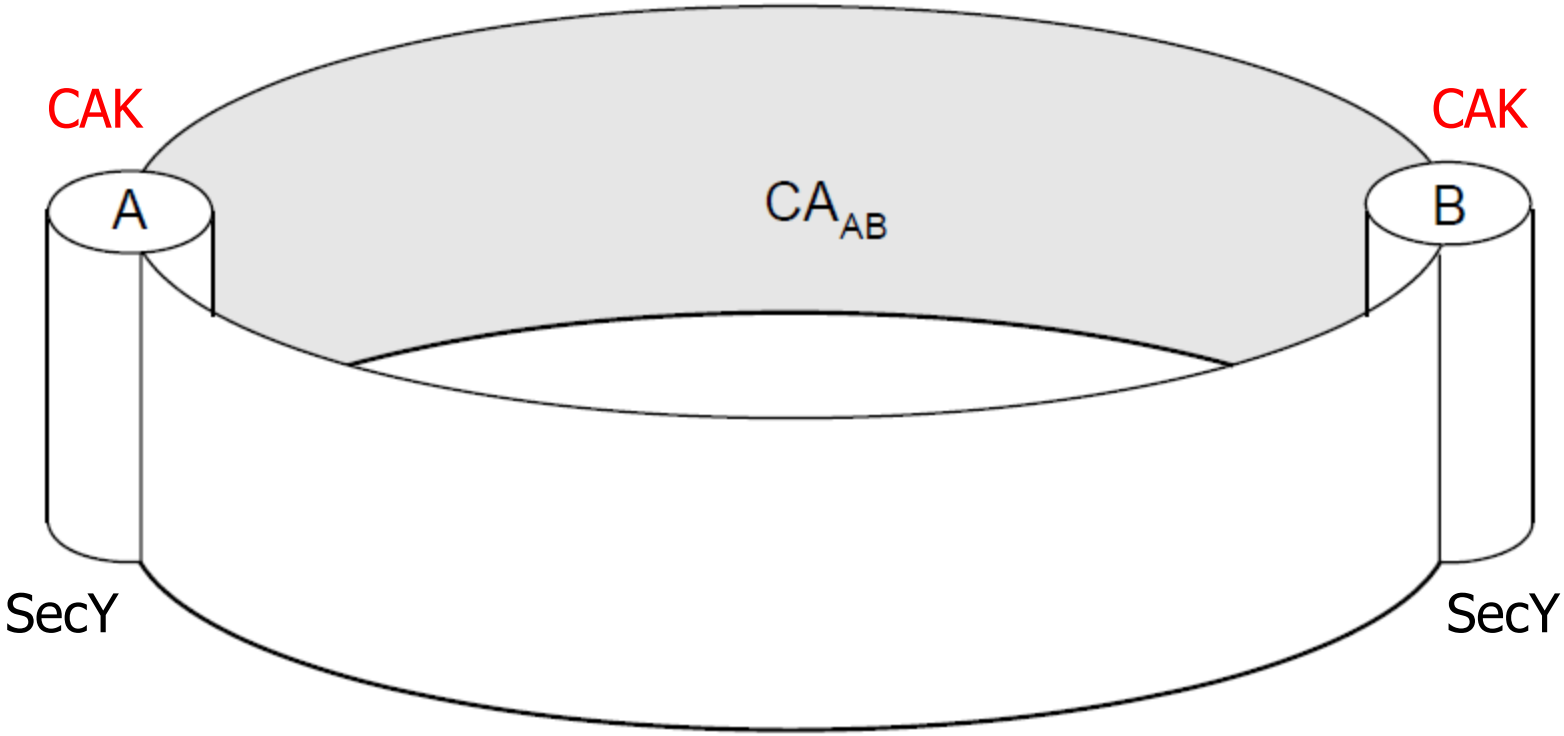


- The Association Number (2 bits) allows the overlapping rekeying of the Secure Association during which two different SAKs co-exist.

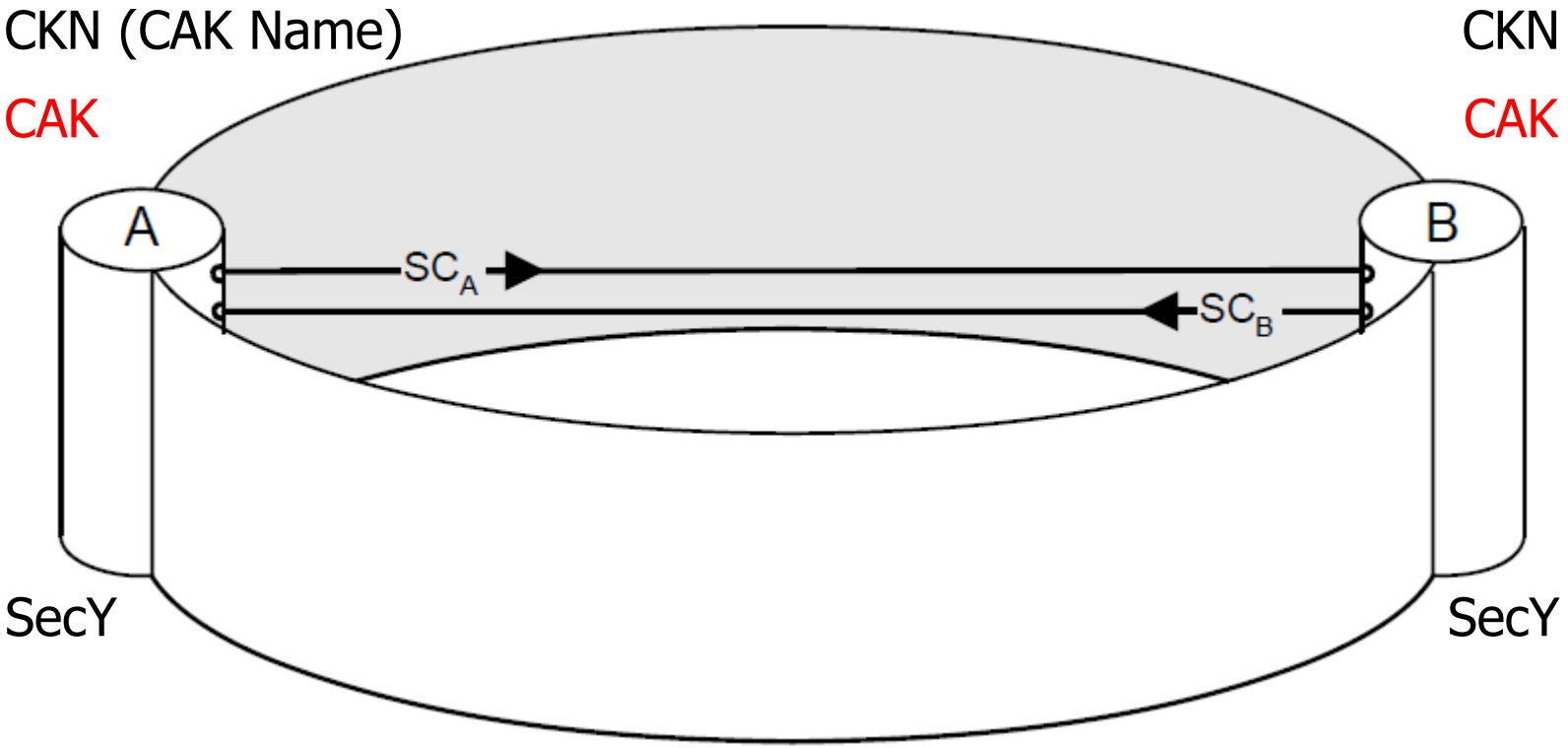
Two Stations in a point-to-point LAN



Connectivity Association (CA)



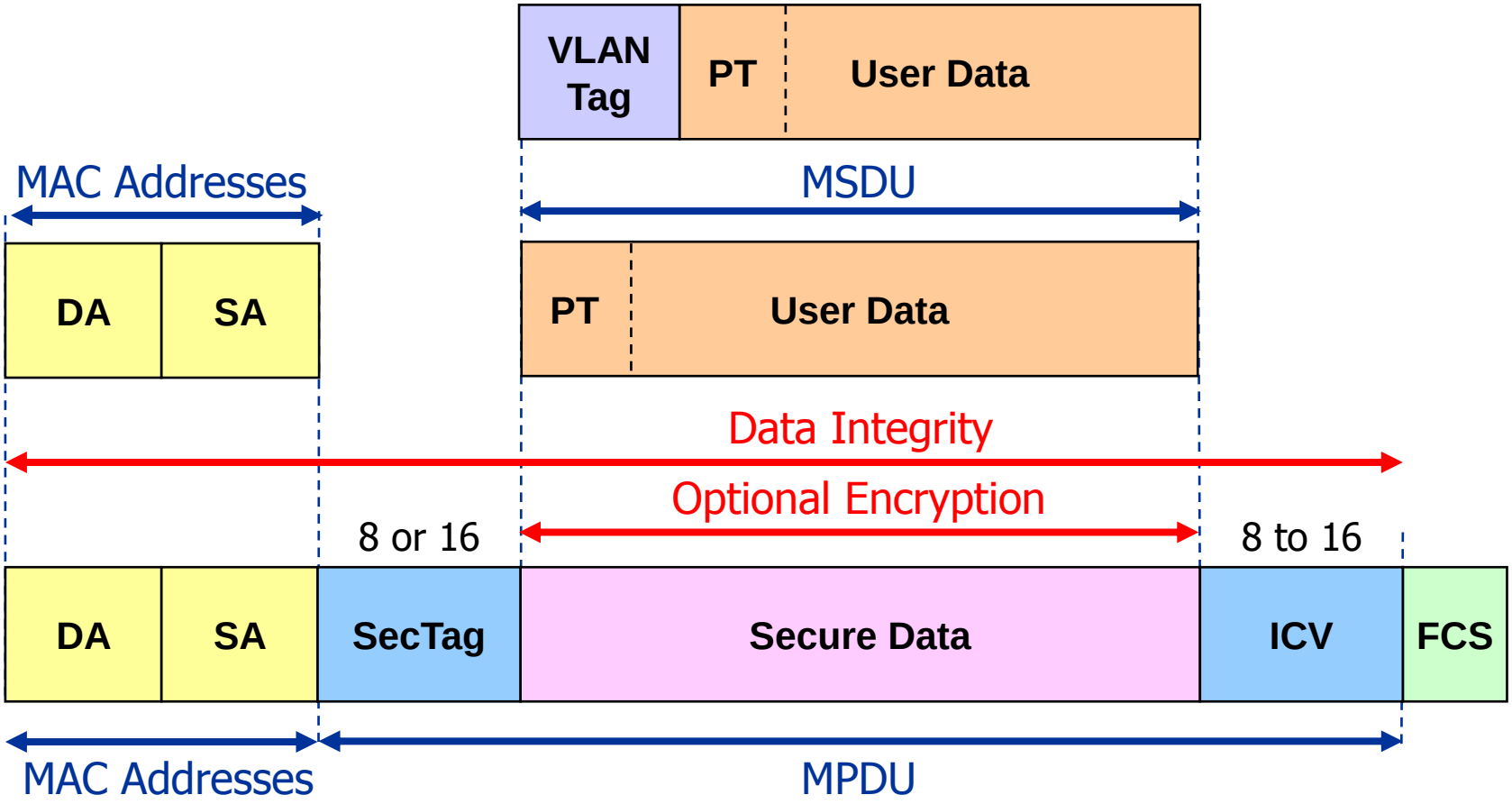
Secure Channel (SC) and Secure Association (SA)



$SA_A \rightarrow SAK_{A0}$, SAK_{A1} , …
$SA_B \rightarrow SAK_{B0}$, SAK_{B1} , …

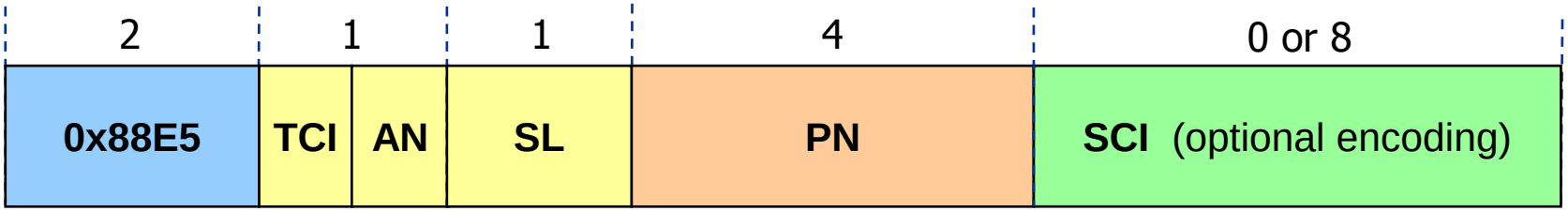
$SA_A \rightarrow SAK_{A0}$, SAK_{A1} , …
$SA_B \rightarrow SAK_{B0}$, SAK_{B1} , …

IEEE 802.1AE MACsec Frame Format



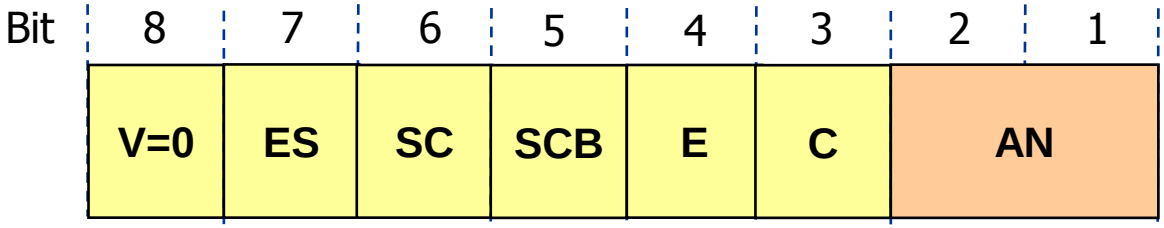
- MSDU – MAC Service Data Unit
- MPDU – MACsec Protocol Data Unit
- ICV – Integrity Check Value

SecTag – Security Tag



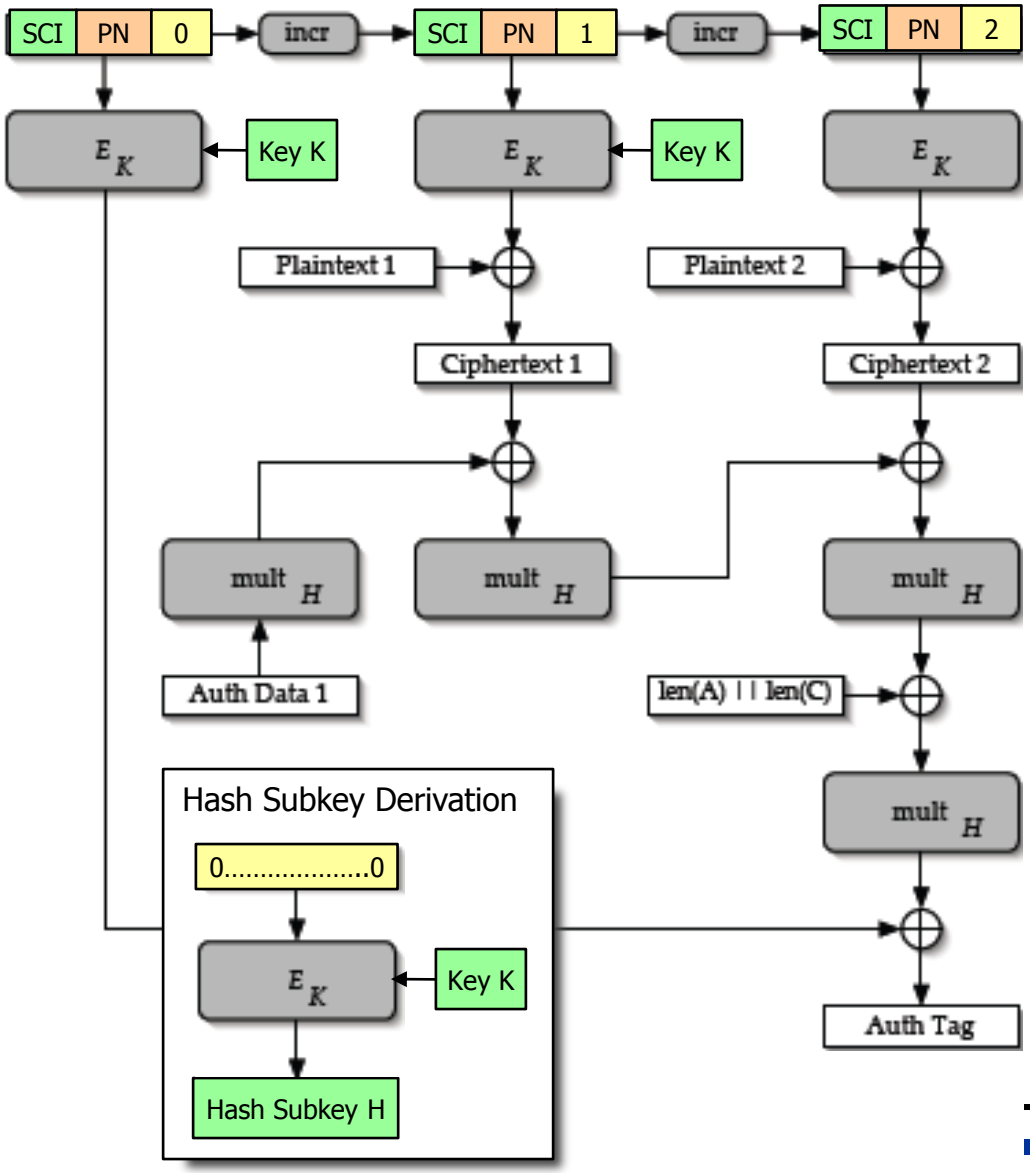
- MACsec Ethertype – is 0x88E5
- TCI – TAG Control Information (6 bits)
- AN – Association Number (2 bits)
- SL – Short Length (6 bits) – length of User Data if < 48 octets, 0 otherwise
- PN – Packet Number – replay protection and IV for encryption
- SCI – Secure Channel Identifier – identifies Secure Association (SA).
  In point-to-point links the SCI consists of the Source MAC Address and the Port Identifier 00-01 and thus the SCI doesn't have to be encoded.

TCI – TAG Control Information Bits



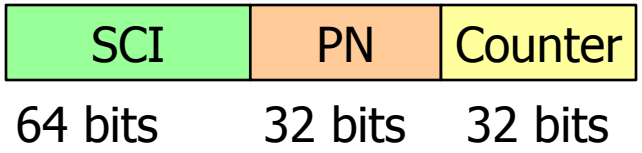
- V – Version (currently 0)
- ES – End Station – if set means that the Source MAC Address is part of the SCI and the SCI shall not be explicitly encoded.
- SC – shall be set only if an explicitly encoded SCI is present
- SCB – Single Copy Broadcast capability – if ES and SCB are set then the implicit SCI comprises a reserved Port Identifier of 00-00.
- E – Encryption – if set encryption is enabled
- C – Changed Text – if clear the Secure Data exactly equals User Data

Authenticated Encryption with Associated Data



ICV

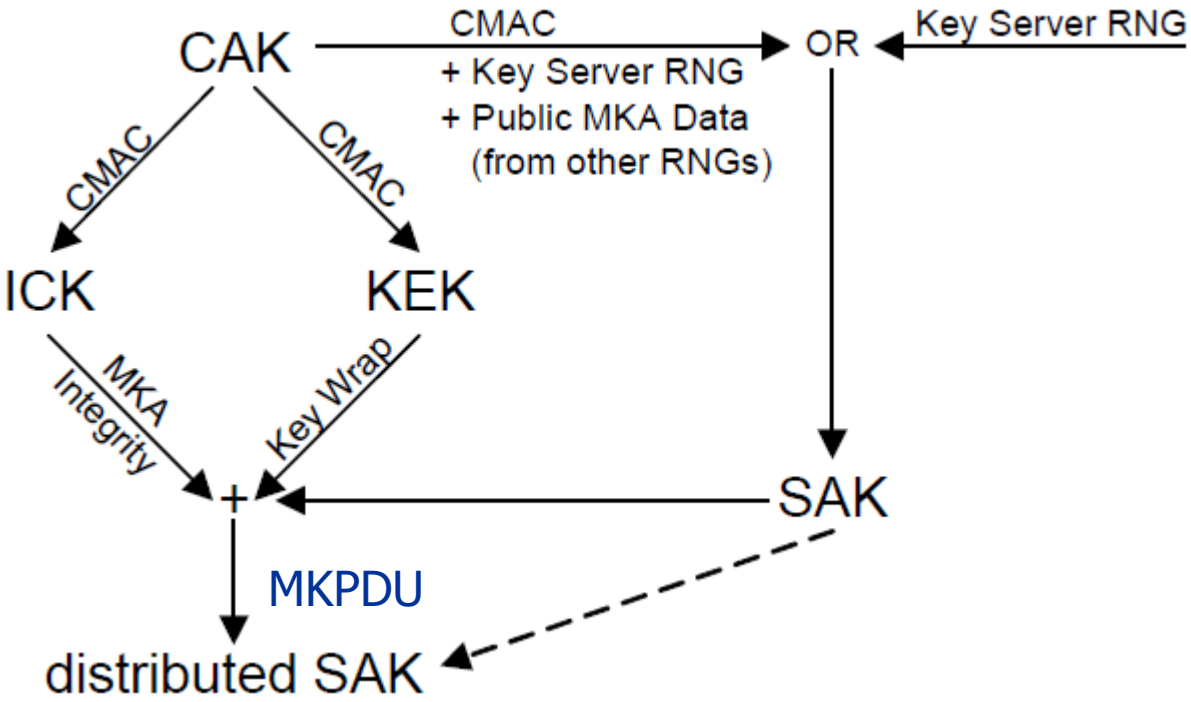
- AEAD is based on special block cipher modes:
- Block size: 128 bits
- Key size: 128/256 bits
- Tag size : 128 bits
- Nonce size: 128 bits



- AES-Galois/Counter Mode AES-GMAC (auth. only)

3.4 MACsec Key Agreement IEEE 802.1X - MKA

MKA distributes random SAK using CAK



- MKPDU – MACsec Key Agreement Protocol Data Unit – carried via EAPOL
- CAK – Connectivity Association Key – pairwise or group root key
- ICK – ICV Key – used for MKPDU Data Integrity
- KEK – Key Encrypting Key – used for AES Key Wrap in MKPDU
- SAK – Secure Association Key

MKA Key Derivation Function - KDF

- The MKA KDF is a Pseudo Random Function (PRF) based on AES-CMAC with a 128 or 256 bit key.

  Output ← KDF(Key, Label, Context, Length)

- KEK ← KDF(CAK, "IEEE8021 KEK", CKN[0..15], 128/256)
- ICK ← KDF(CAK, "IEEE8021 ICK", CKN[0..15], 128/256)
- SAK ← KDF(CAK, "IEEE8021 SAK", KS-nonce | MI-value list | KN, 128/256)
- KS – Key Server – either elected or EAP Authenticator
- MI – Member Identifier – all members of a CA
- KN – Key Number – assigned by Key Server

Connectivity Association Key – CAK

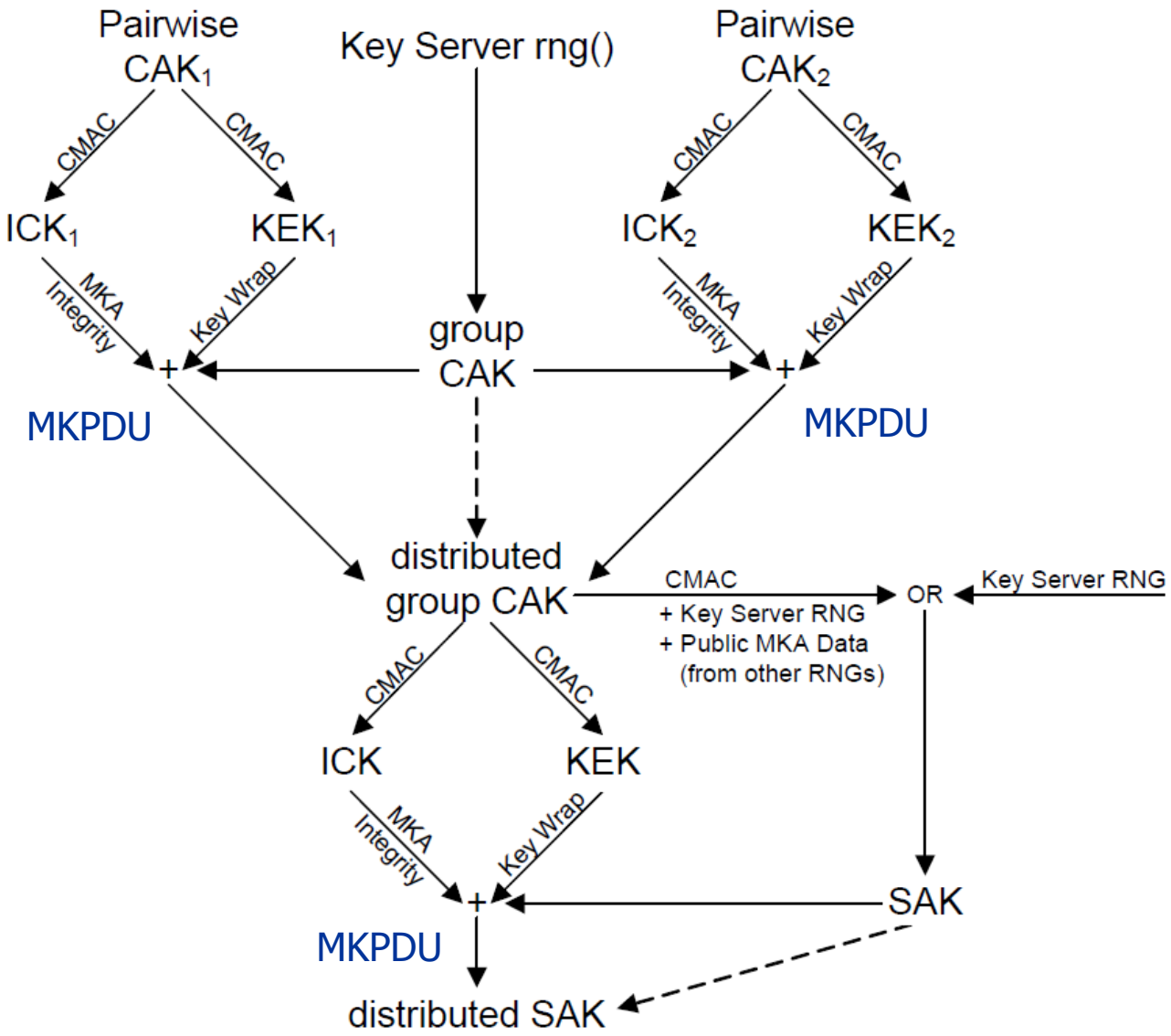
- CAK as a Pre-Shared-Key (PSK)
  - Can be used either as a pairwise CAK or group CAK
  - Statically configured PSK
  - CKN can be chosen arbitrarily with a size of 1..32 octets
- CAK via EAP
  - Can be used as a pairwise CAK.
  - Dynamically derived CAK and CKN between two PAEs via EAP

CAK ← KDF(MSK[0..15]/MSK[0..31], "IEEE8021 EAP CAK",
mac1 | mac2, 128/256)

CKN ← KDF(MSK[0..15]/MSK[0..31], "IEEE8021 EAP CKN" ,
EAP Session-ID | mac1 | mac2, 128/256)

where mac1 < mac2 are the MAC addresses of the PAEs and the Master Session Key (MSK) and Session-ID of the EAP method (EAP-TLS, EAP-PEAP, etc) is included.

Use of Pairwise CAKs to Distribute a Group CAK



IEEE 802.1AE Enabled Products

- Cisco Catalyst 3750-X / 3560-X LAN Access Switch
  - Supports MACsec and MKA on both user/downlink and network/uplink ports

- Juniper EX Series Switches
  - 802.1AE available with the controlled version of Junos OS