heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

서울대학교 컴퓨터공학부
Seoul National University
Dept. of Computer Science and Engineering

Wireless Security (SWI)

abraham.rubinstein@heig-vd.ch

Chapter IV and V

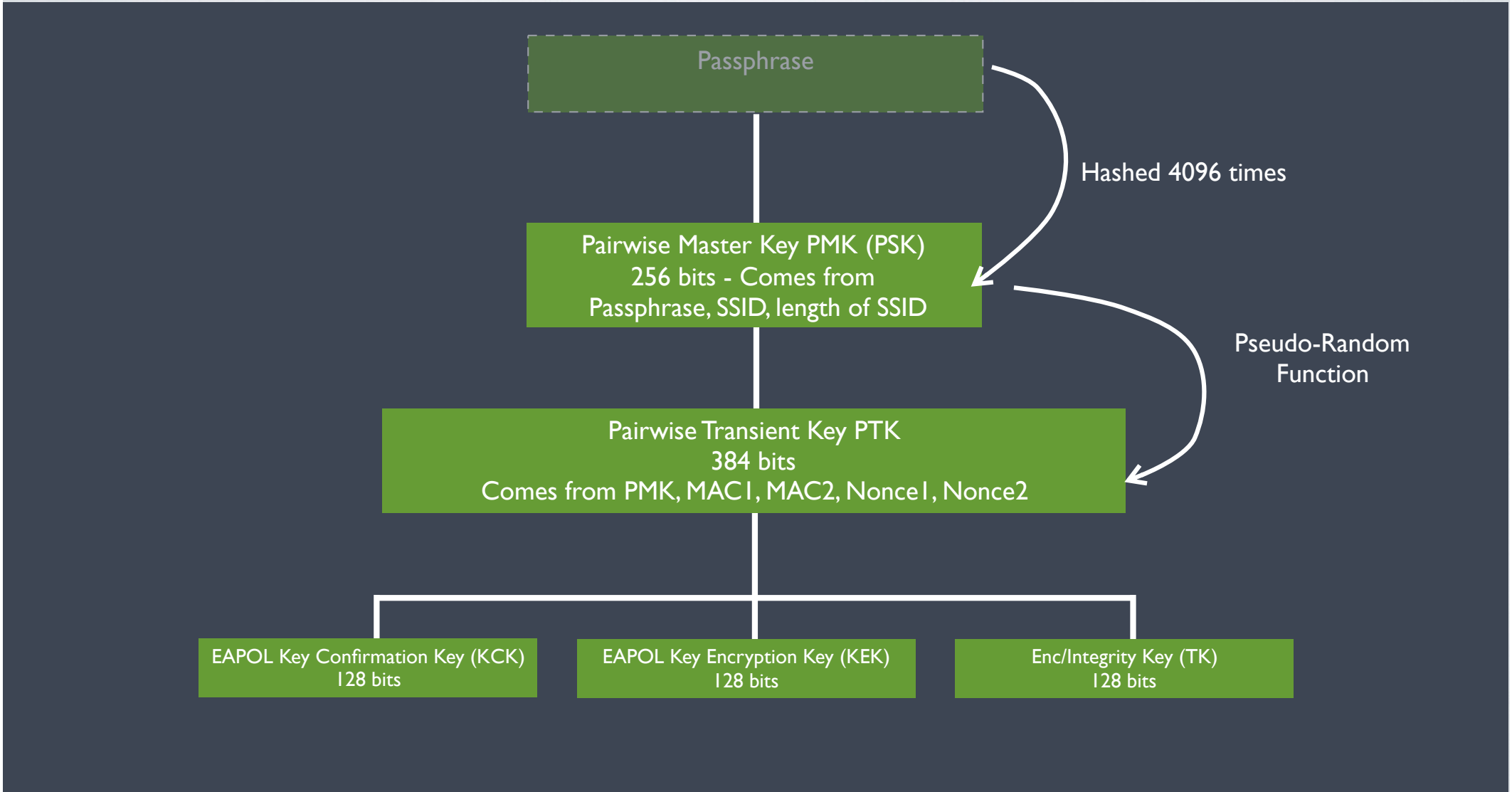
WPA2 and Enterprise Security

WPA2

- New security system. It does **not use WEP** and it does **not use RC4**
- Based on AES (Advanced Encryption Standard)
- Introduces the **CCMP** (**C**ounter Mode with **C**BC-**M**AC) **P**rotocol
  - Uses AES CTR (Counter mode) for confidentiality
  - Uses AES CBC-MAC (Cipher Block Chaining Message Authentication Code) for integrity and authentication

WPA2-PSK

Key Derivation



4-Way Handshake

Pairwise Transient Key PTK
Comes from PMK, MAC1, MAC2, Nonce1, No

Group Master Key GMK
(Randomly Generated by the AP)

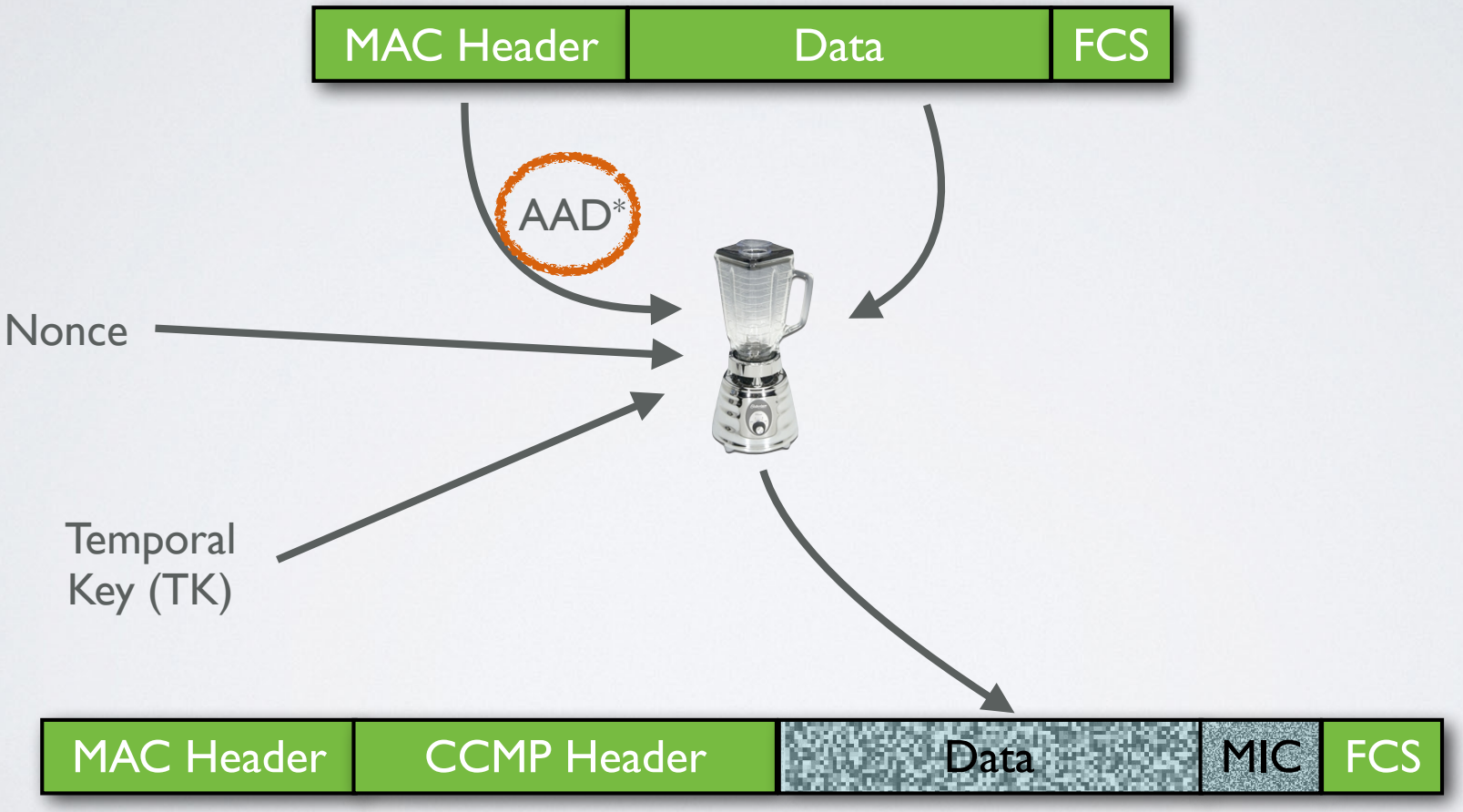
Authenticator Nonce

Supplicant Nonce authenticated with the KCK

ACK + GTK encrypted with KEK and authenticated with KCK

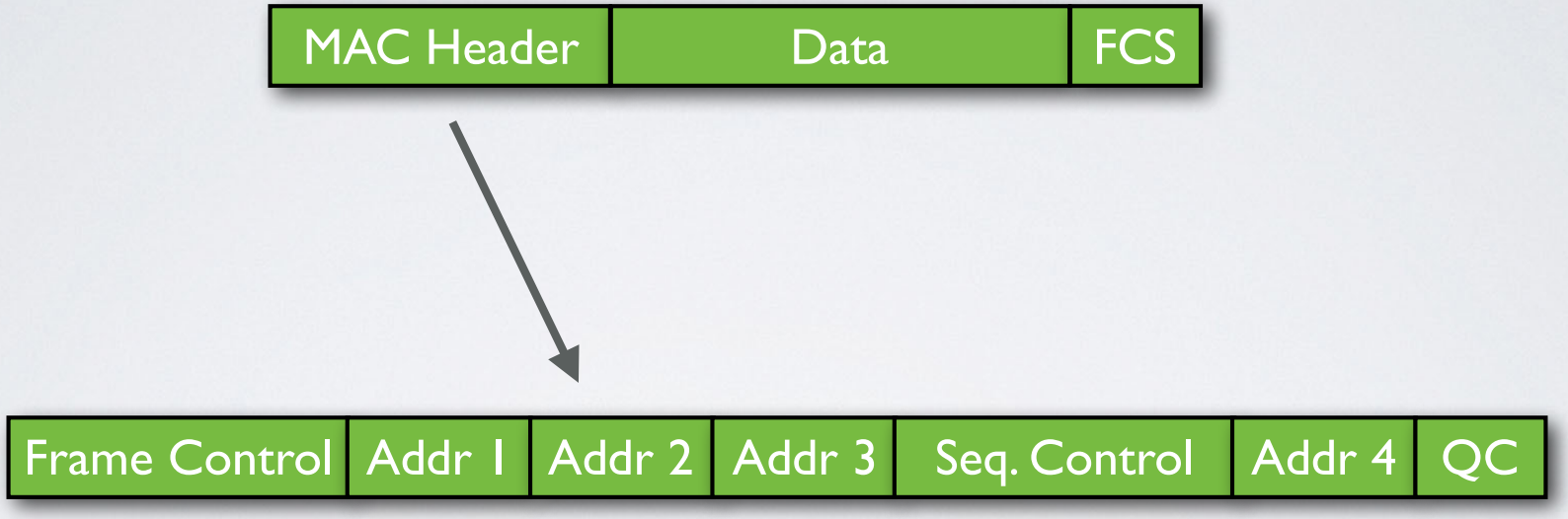
ACK authenticated with KCK

General View



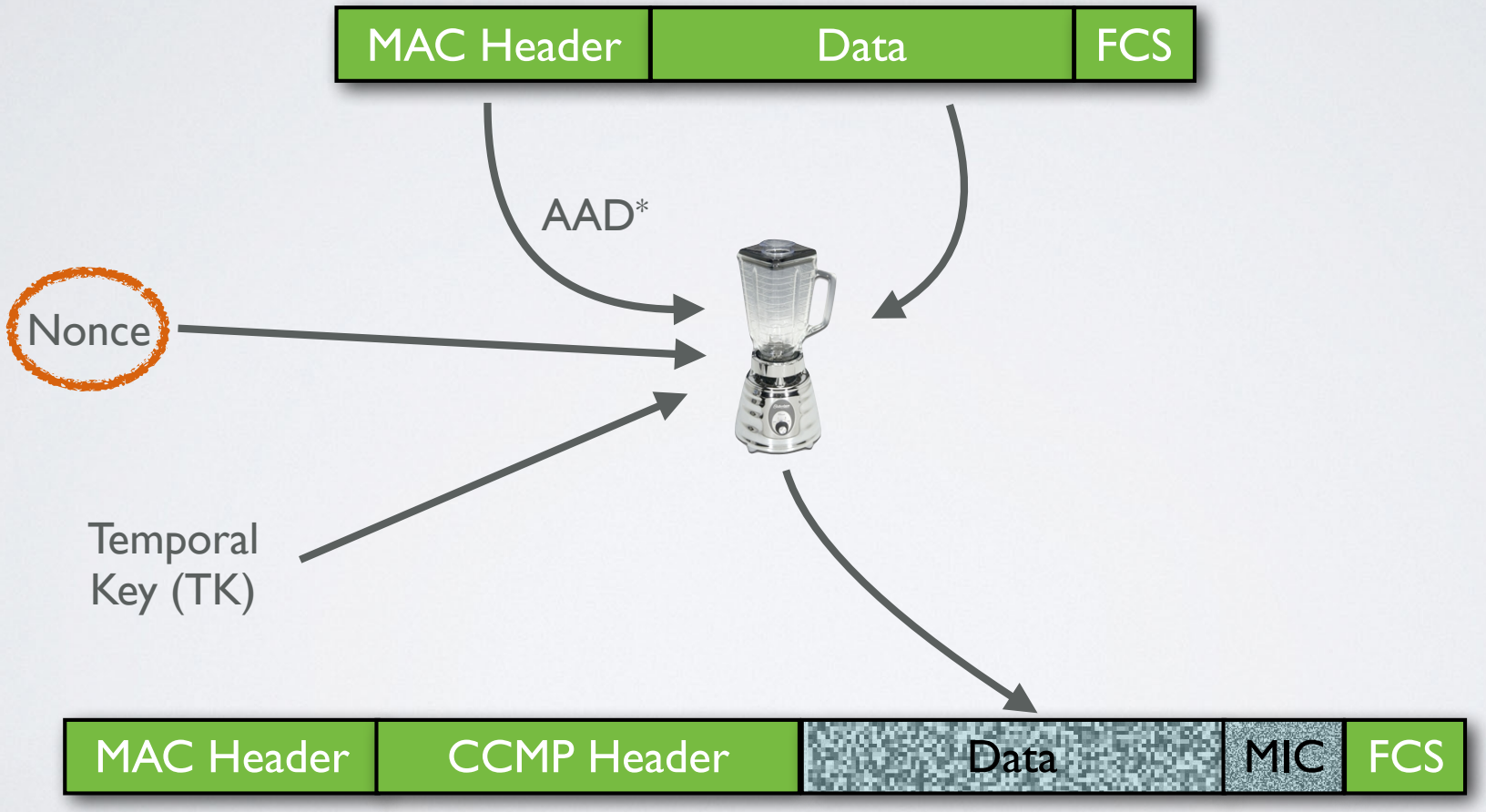
*Additional Authentication Data

Additional Authentication Data (AAD)



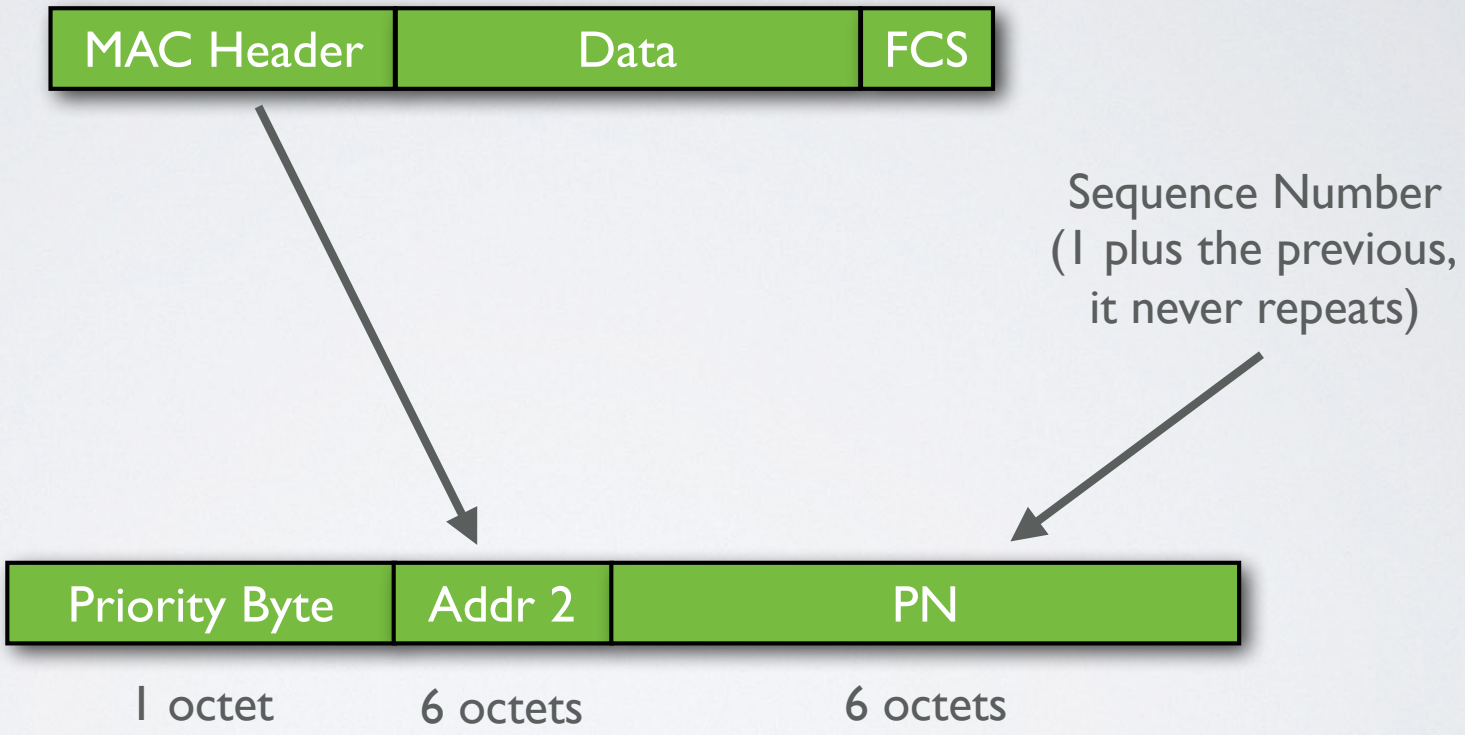
*Fields that would change with a retransmission are set to 0

General View



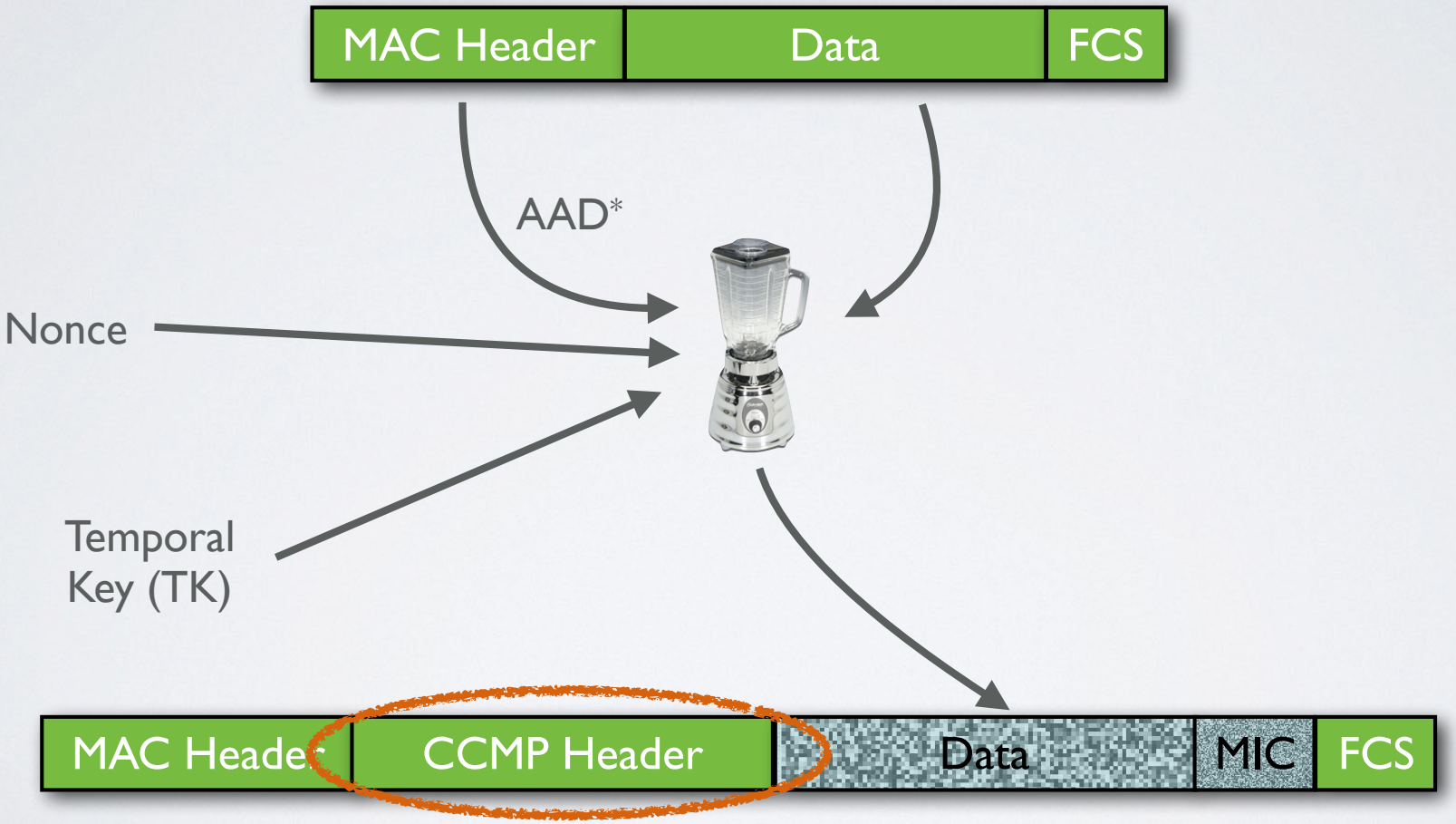
*Additional Authentication Data

Nonce



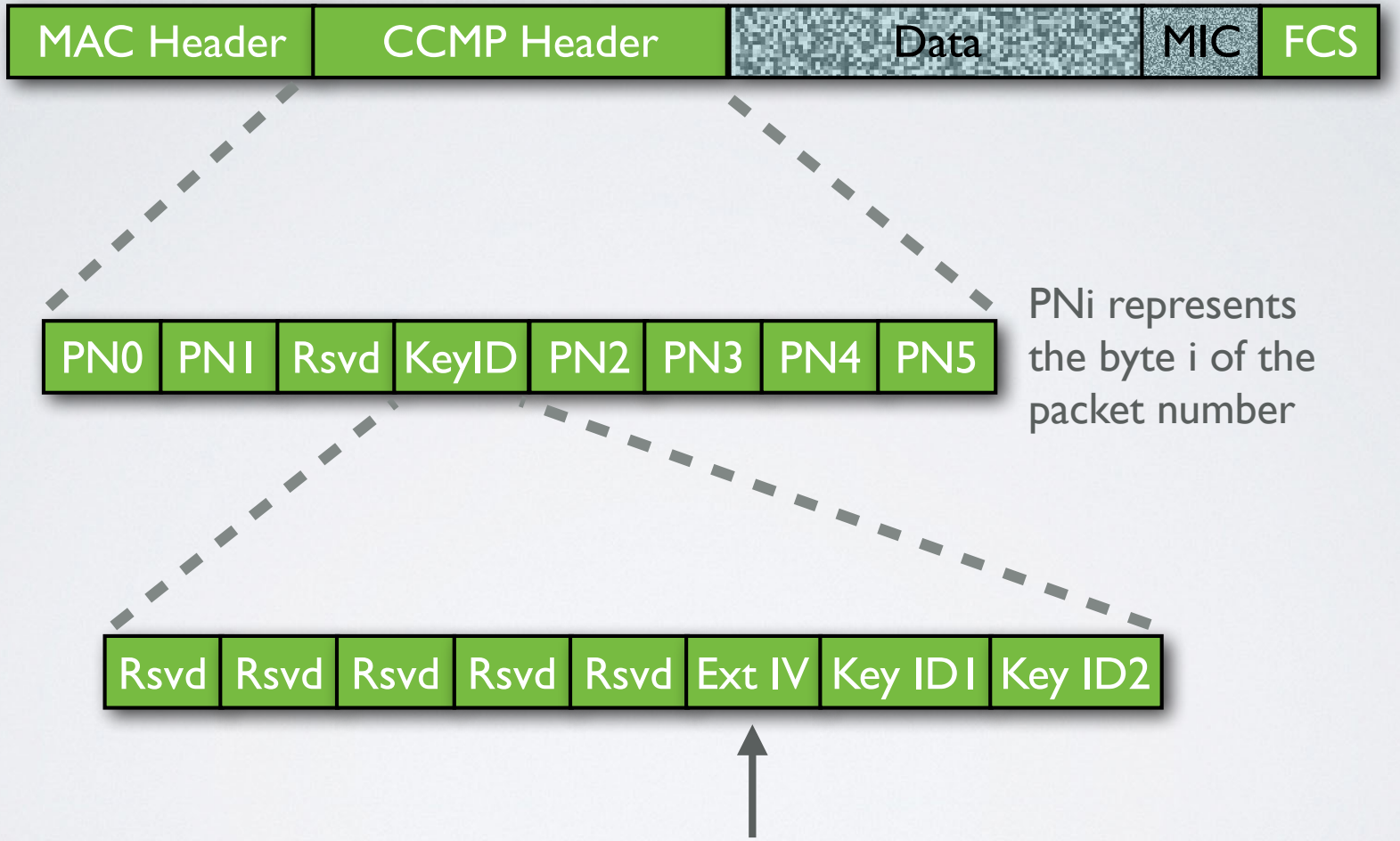
- Addr 2 is the Source address
- In practice, as of today, Priority Byte always is set to 0

General View



*Additional Authentication Data

CCMP Header

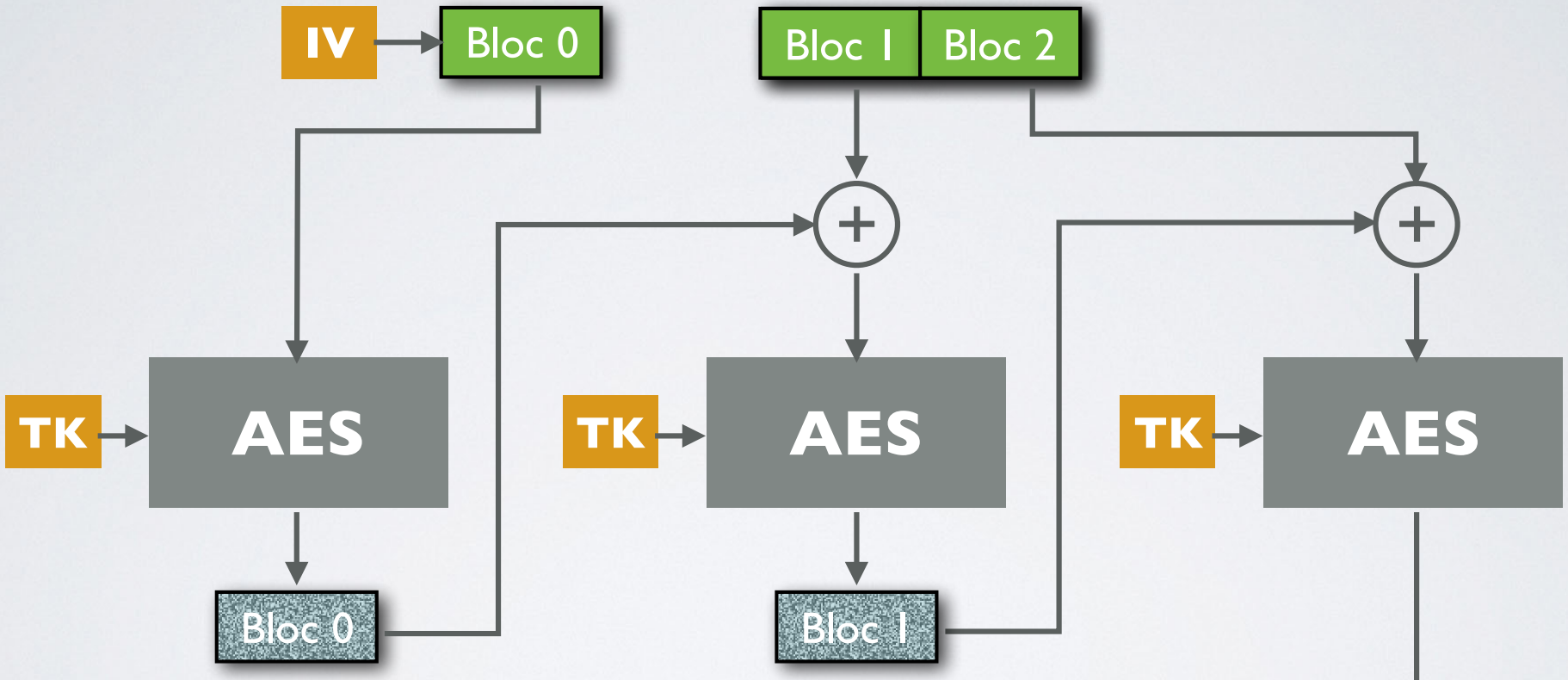


All Rsvd = 0

Cipher Block Chaining Message Authentication Code (CBC-MAC)

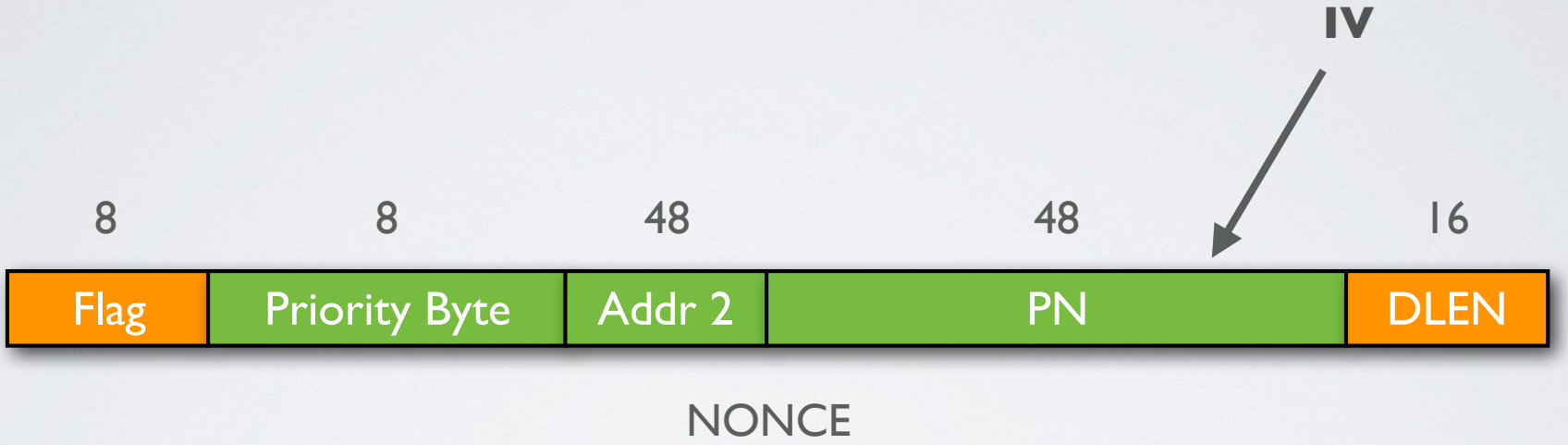
The MIC is calculated on:

Cipher Block Chaining Message Authentication Code (CBC-MAC)



Le MIC est calculé sur :

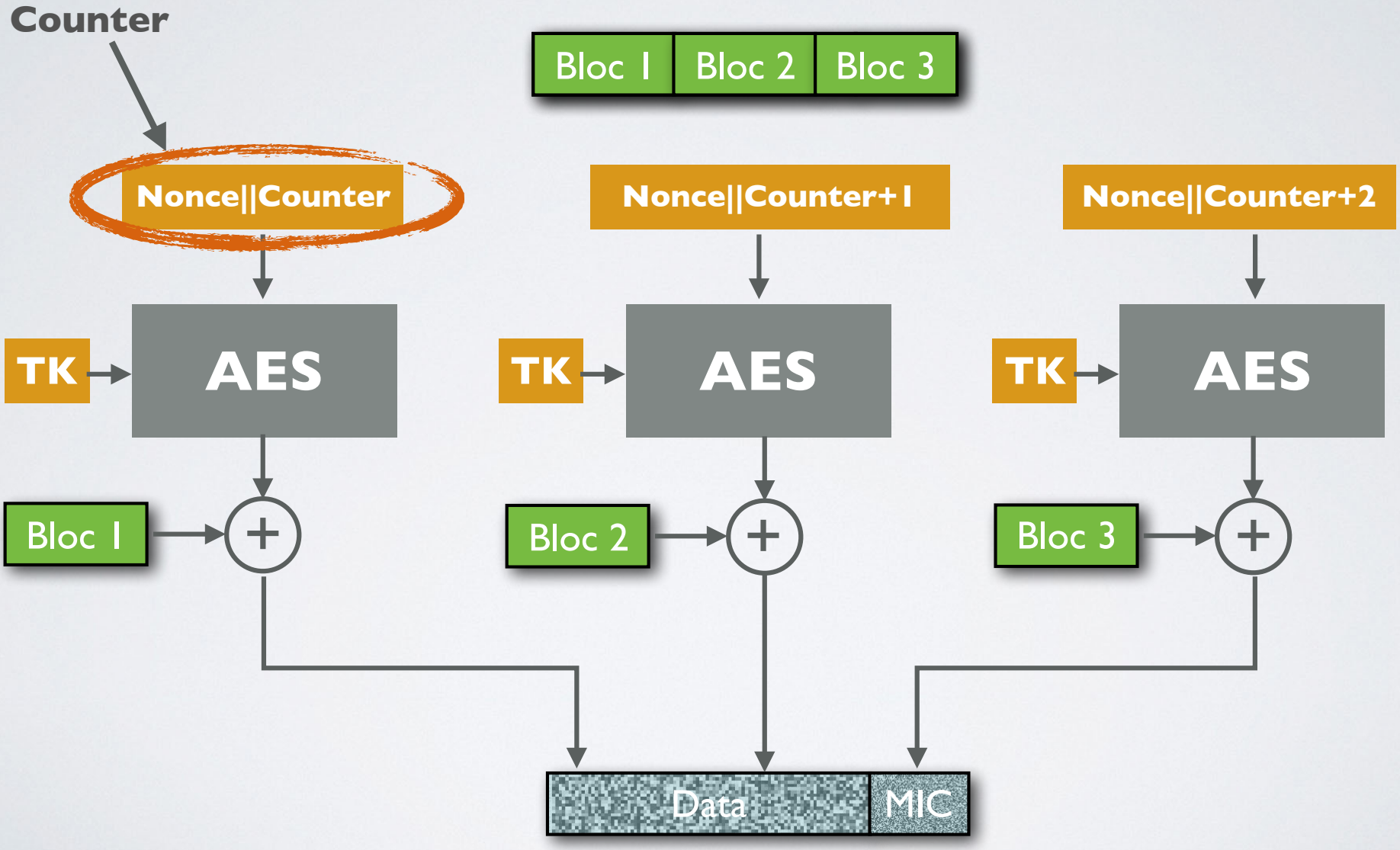
Bloc 0



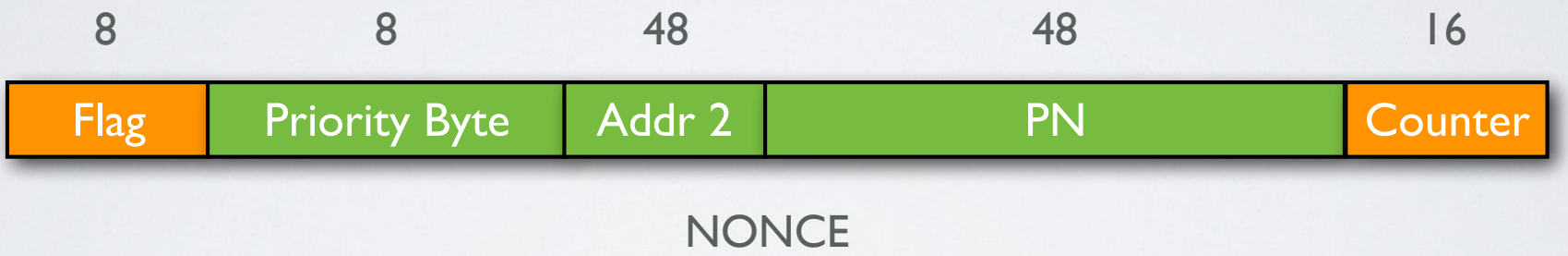
FLAG = 01011001

DLEN = Length of the data field

Encryption "Counter Mode"



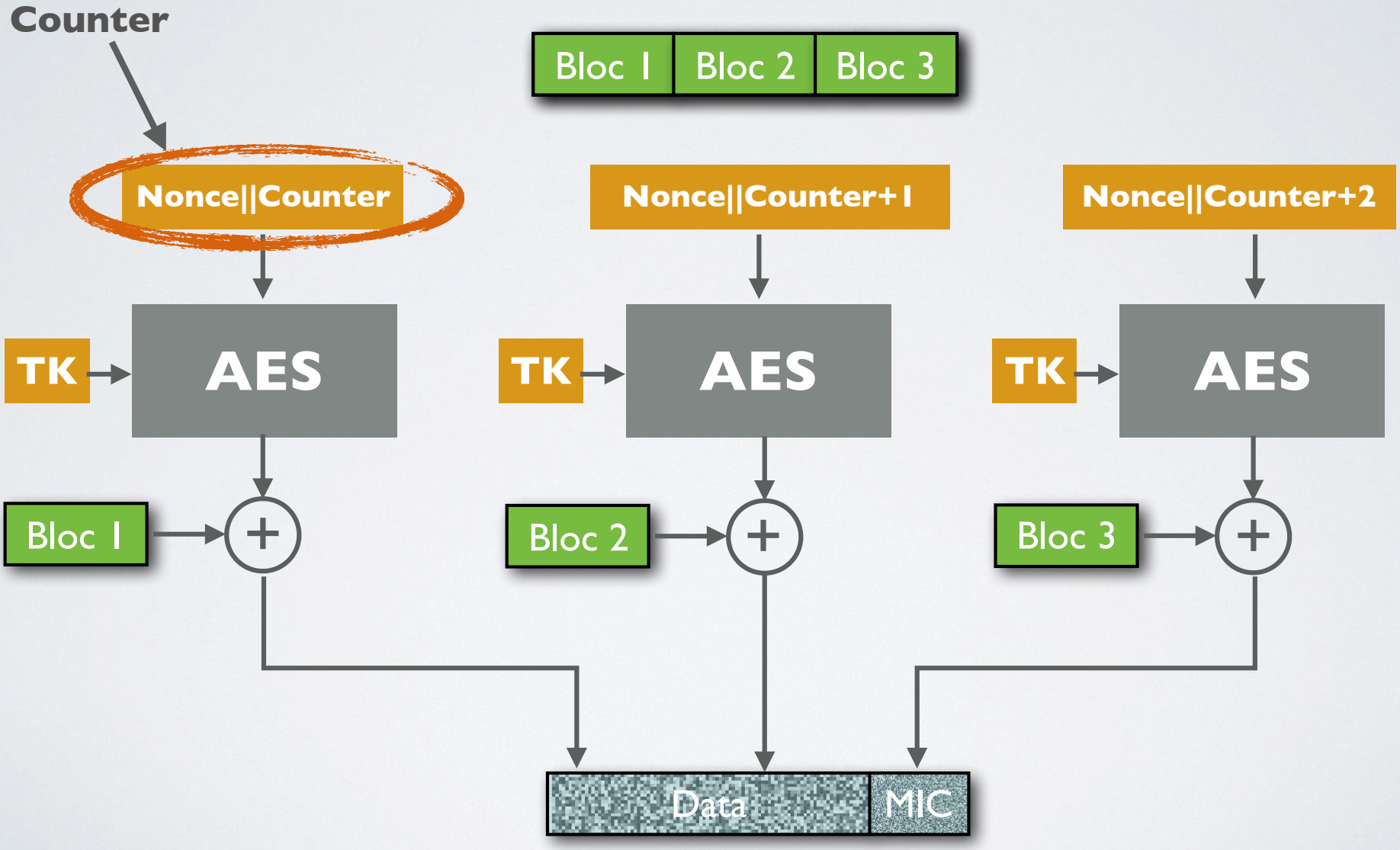
COUNTER



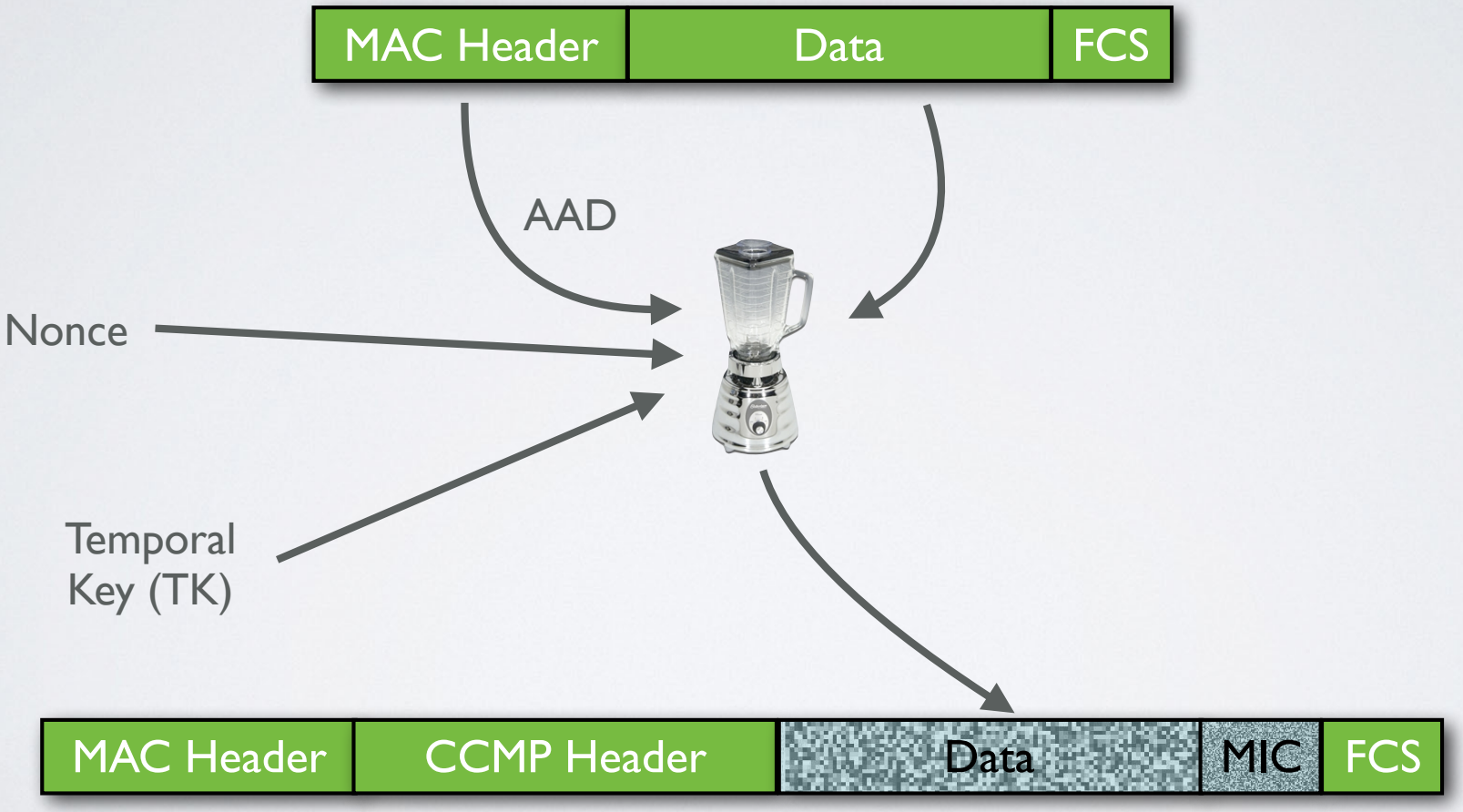
FLAG = 01011001

Counter = 0, 1, 2, …

Encryption "Counter Mode"



General View

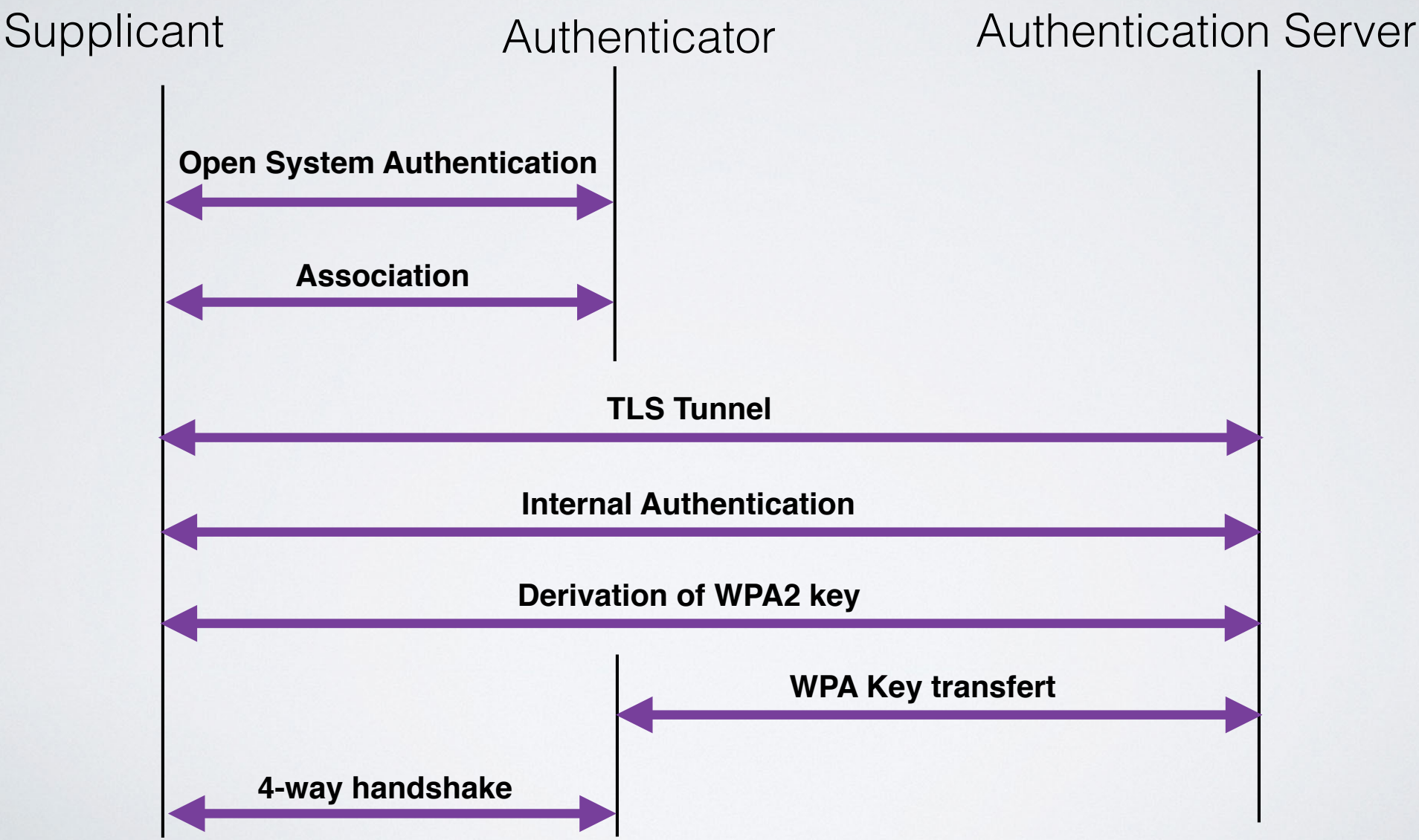


WPA2-Entreprise

EAP-TLS

EAP-PEAP

Enterprise Authentication



Authentication Methods

- Extensible Authentication Protocol - Transport Security Layer (EAP-TLS)
- Extensible Authentication Protocol - Tunneled Transport Security Layer (EAP-TTLS)
- Protected Extensible Authentication Protocol (PEAP)

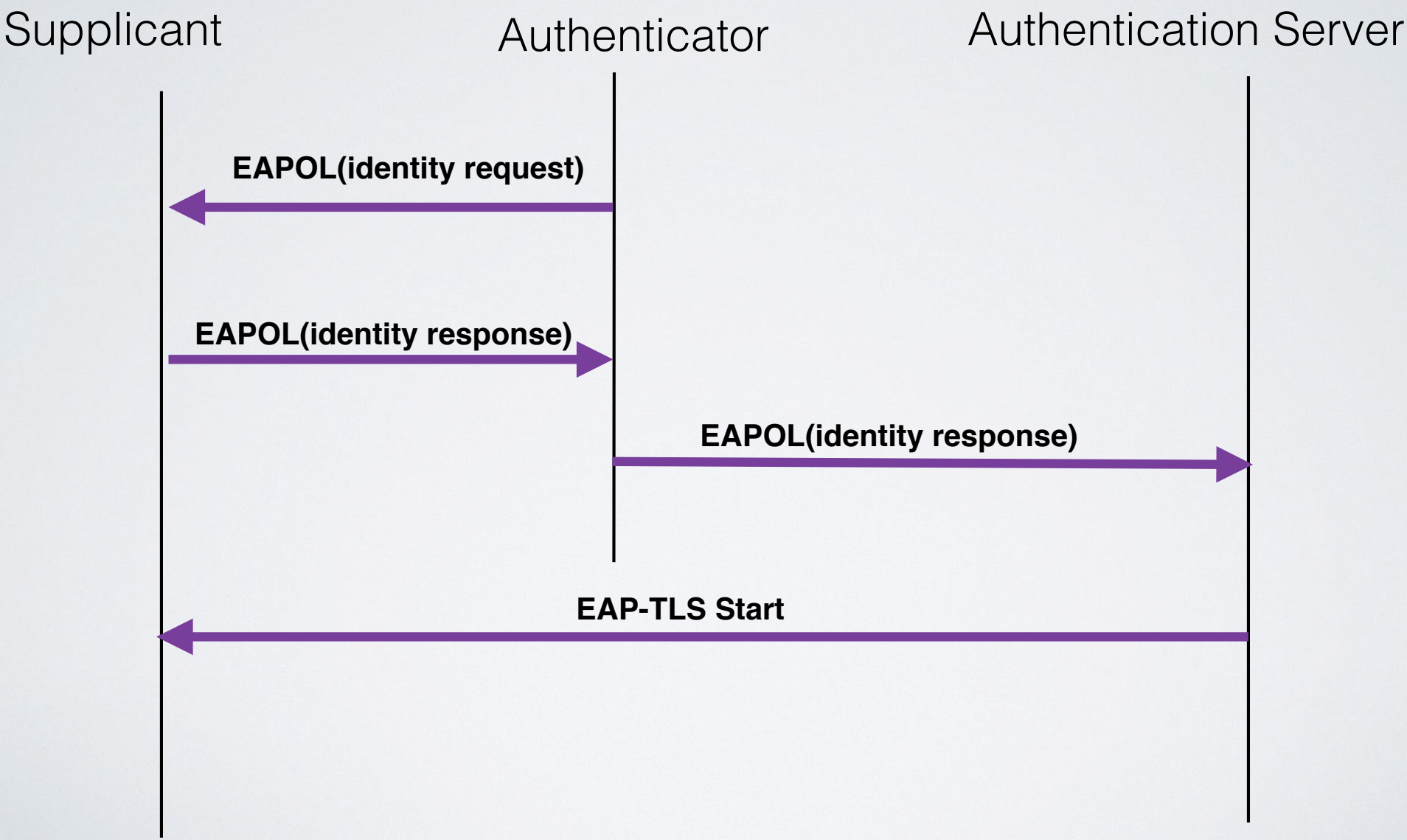
Authentication Methods

- EAP-TLS
- EAP-TTLS
- PEAP

EAP-TLS Phases

1. Initialisation
2. Hello Phase
    - Nonce exchange (ClientHello.random and ServerHello.random),
    - Agree on algorithms
3. Certificate exchange phase
    - Certificat transmission
    - Pre Master Secret transmission
4. Generate Master secret from Pre Master Secret and Nonces
5. Confirmation and conformity phase and end of authentication

Initialisation Phase



The Random Numbers

- Composed by concatenating the time in seconds from January 1st 1970 (4 bytes) and 28 random numbers
- We still have about 100 years with those 4 bytes

At the End of the Handshake

- The Supplicant and the Authentication Server are in possession of the Pre Master Secret
- The Master Secret is calculated using the function :

master_secret = TLS-PRF-48(pre_master_secret, "master secret", client.random || server.random)

At the End of the Handshake

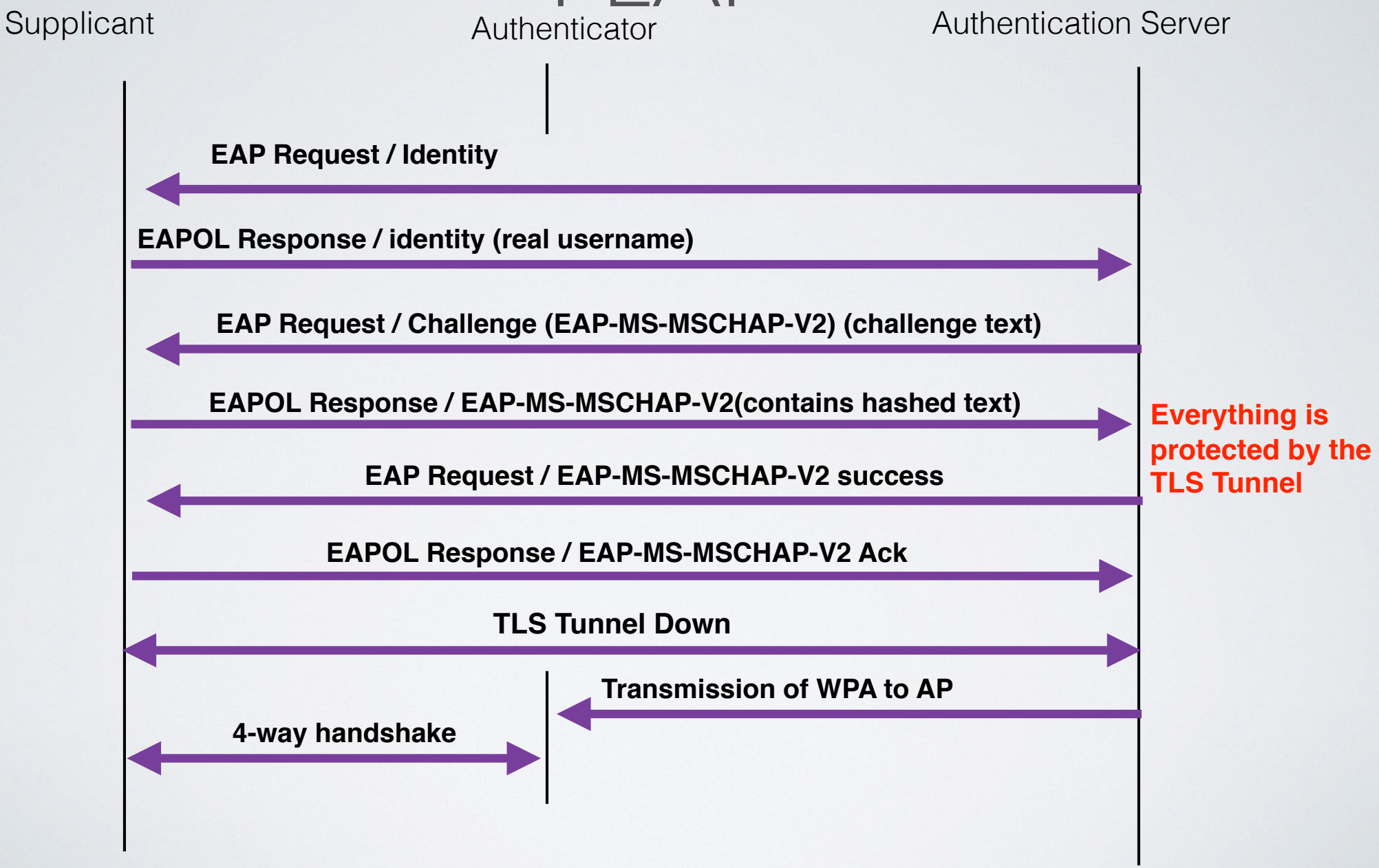
- The Key_Material is calculated using function:

Key_Material = TLS-PRF-128(master_secret, "client EAP encyption", client.random || server.random)

MSK : Master Session Key = Key_Material(0,63)

PMK = Key_Material(0, 31)

PEAP


Supplicant
Authenticator
Authentication Server
EAP Request / Identity
EAPOL Response / identity (real username)
EAP Request / Challenge (EAP-MS-MSCHAP-V2) (challenge text)
EAPOL Response / EAP-MS-MSCHAP-V2(contains hashed text)
EAP Request / EAP-MS-MSCHAP-V2 success
EAPOL Response / EAP-MS-MSCHAP-V2 Ack
TLS Tunnel Down
Transmission of WPA to AP
4-way handshake
Everything is protected by the TLS Tunnel

PEAP

- The client authentifies the server using the certificate in the TLS tunnel setup phase
- The internal authentication only concerns the client
- Some Operating Systems allow not to verify the server certificate
    - Possibility of attack !