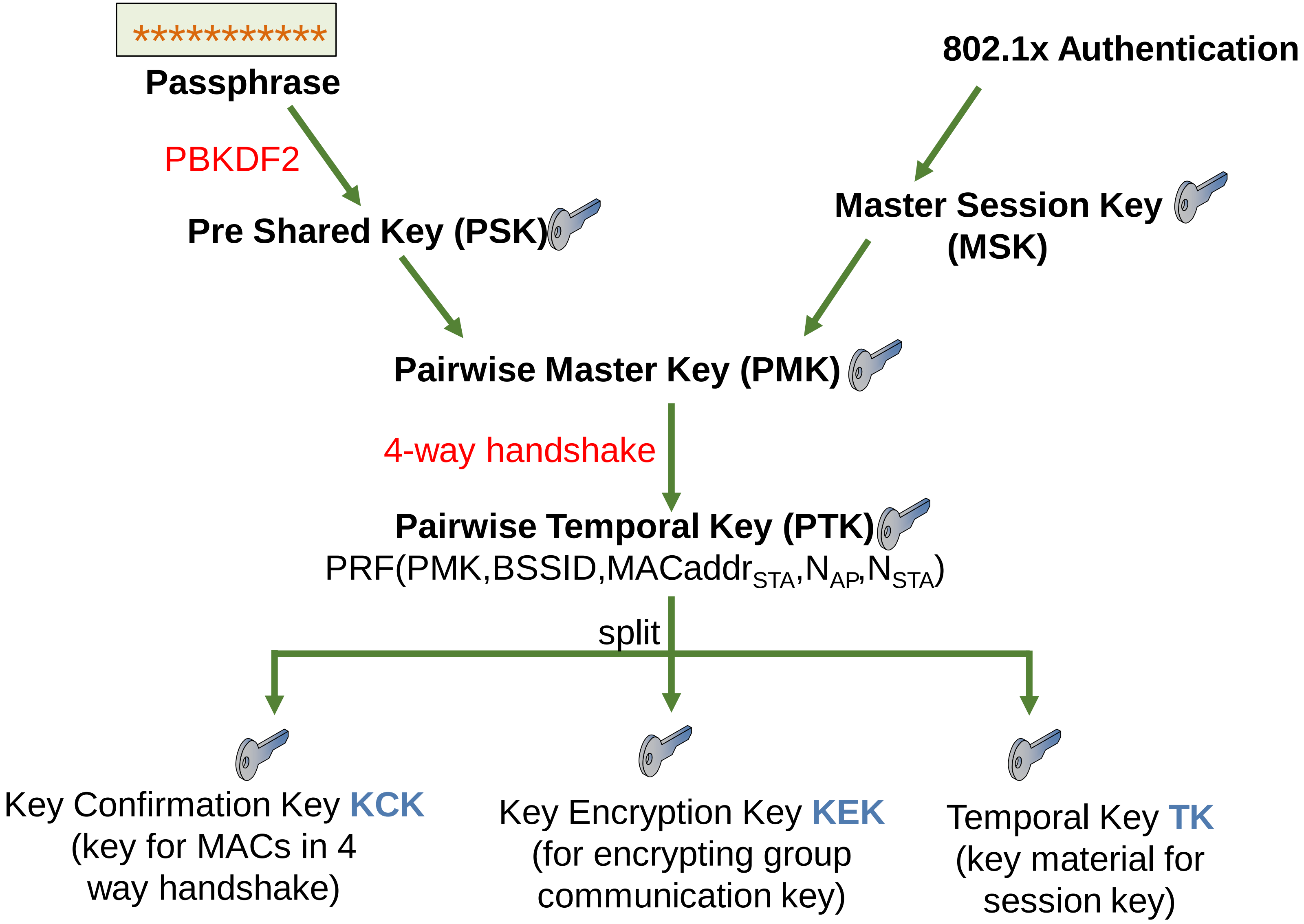
Network Security: WLAN Security: WPA

Mohit Sethi
Ericsson, Finland
Aalto University, Finland

Real WLAN Security

- **Wireless Protected Access 2 (WPA2)**
  - WPA2 is the Wi-Fi alliance name for the 802.11i amendment to the IEEE standard, which is part of 802.11-2020
  - Robust security network (RSN) = name in the IEEE standard
  - Uses 802.1X for access control
  - Uses EAP for authentication and key exchange, eg. EAP-TLS
  - Confidentiality and integrity protocol AES-CCMP

RSN Key Hierarchy



****

Passphrase

PBKDF2

Pre Shared Key (PSK)

802.1x Authentication

Master Session Key (MSK)

Pairwise Master Key (PMK)

4-way handshake

Pairwise Temporal Key (PTK)

PRF(PMK,BSSID,MACaddr$_{STA}$,N$_{AP}$,N$_{STA}$)

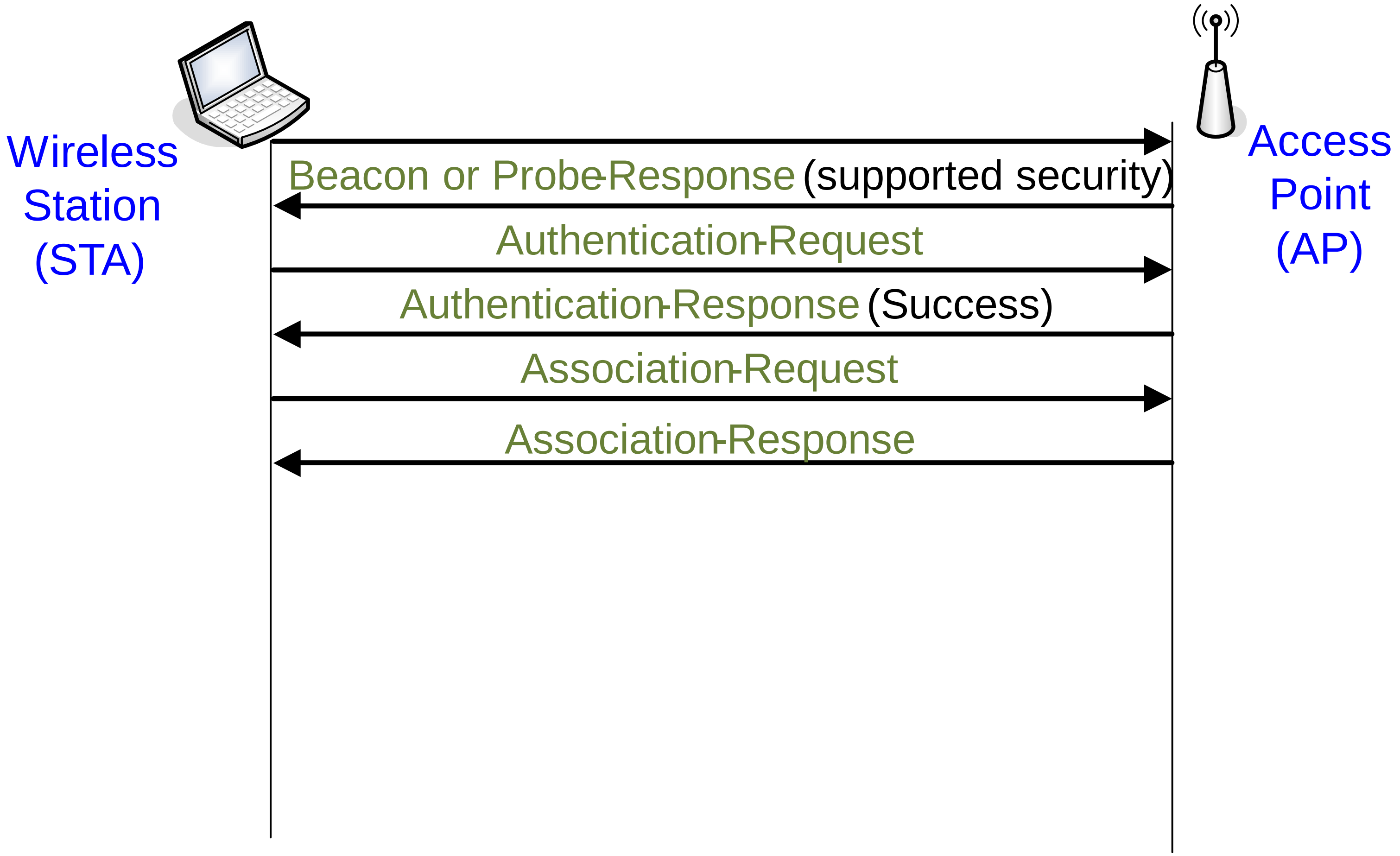
split

Key Confirmation Key **KCK** (key for MACs in 4 way handshake)

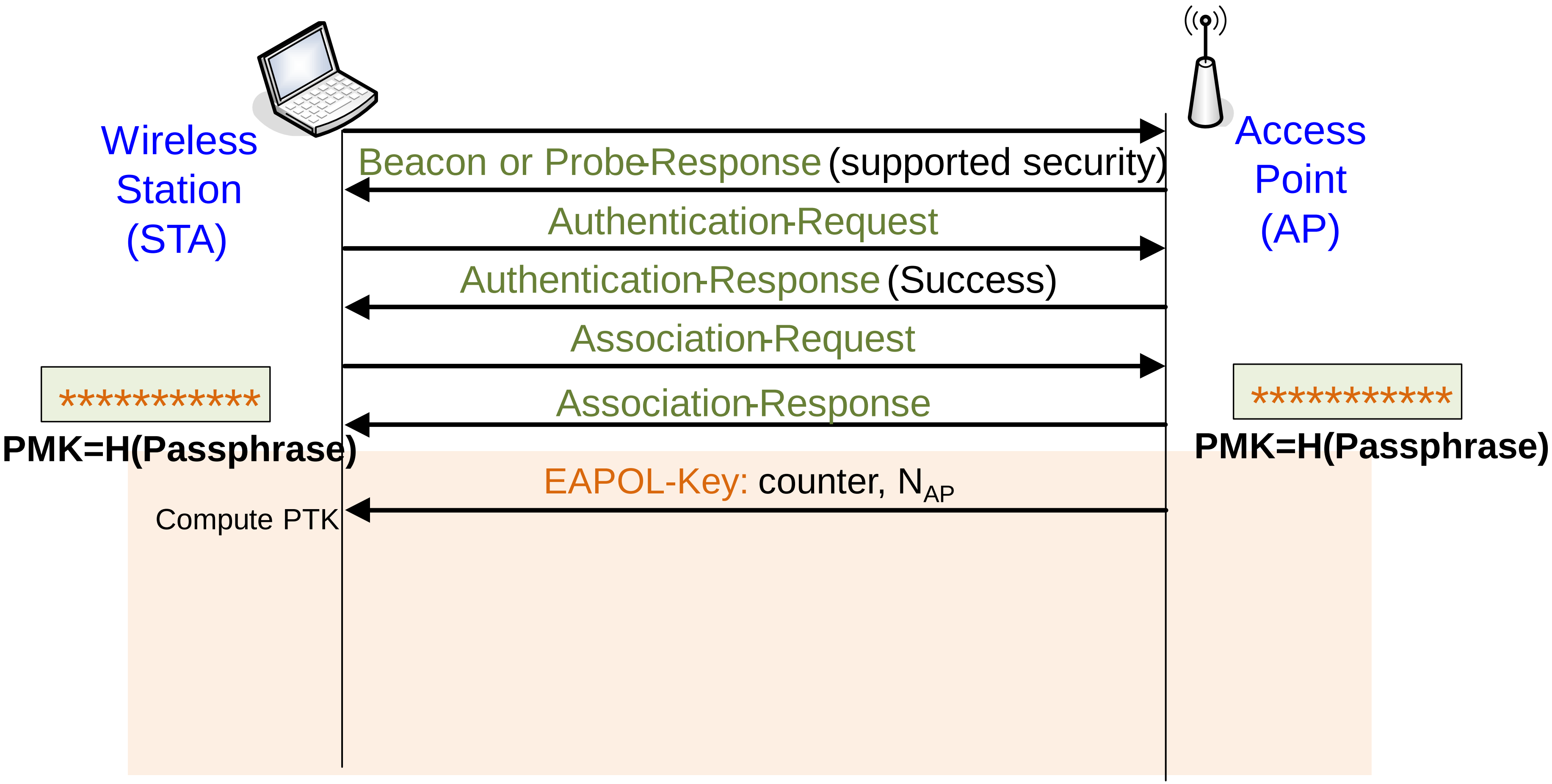
Key Encryption Key **KEK** (for encrypting group communication key)

Temporal Key **TK** (key material for session key)

WPA2 – Four-way handshake

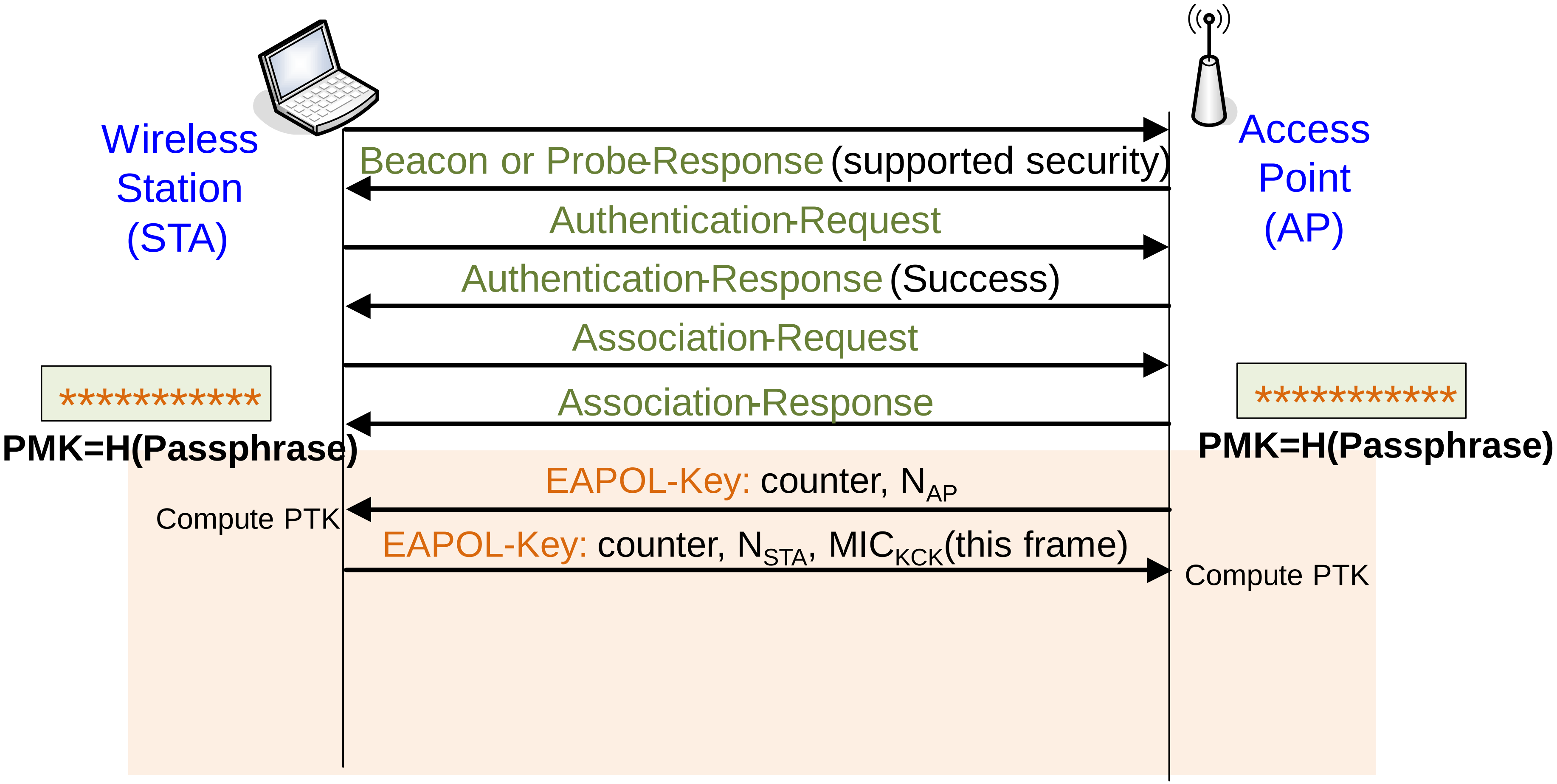


WPA2 – Four-way handshake



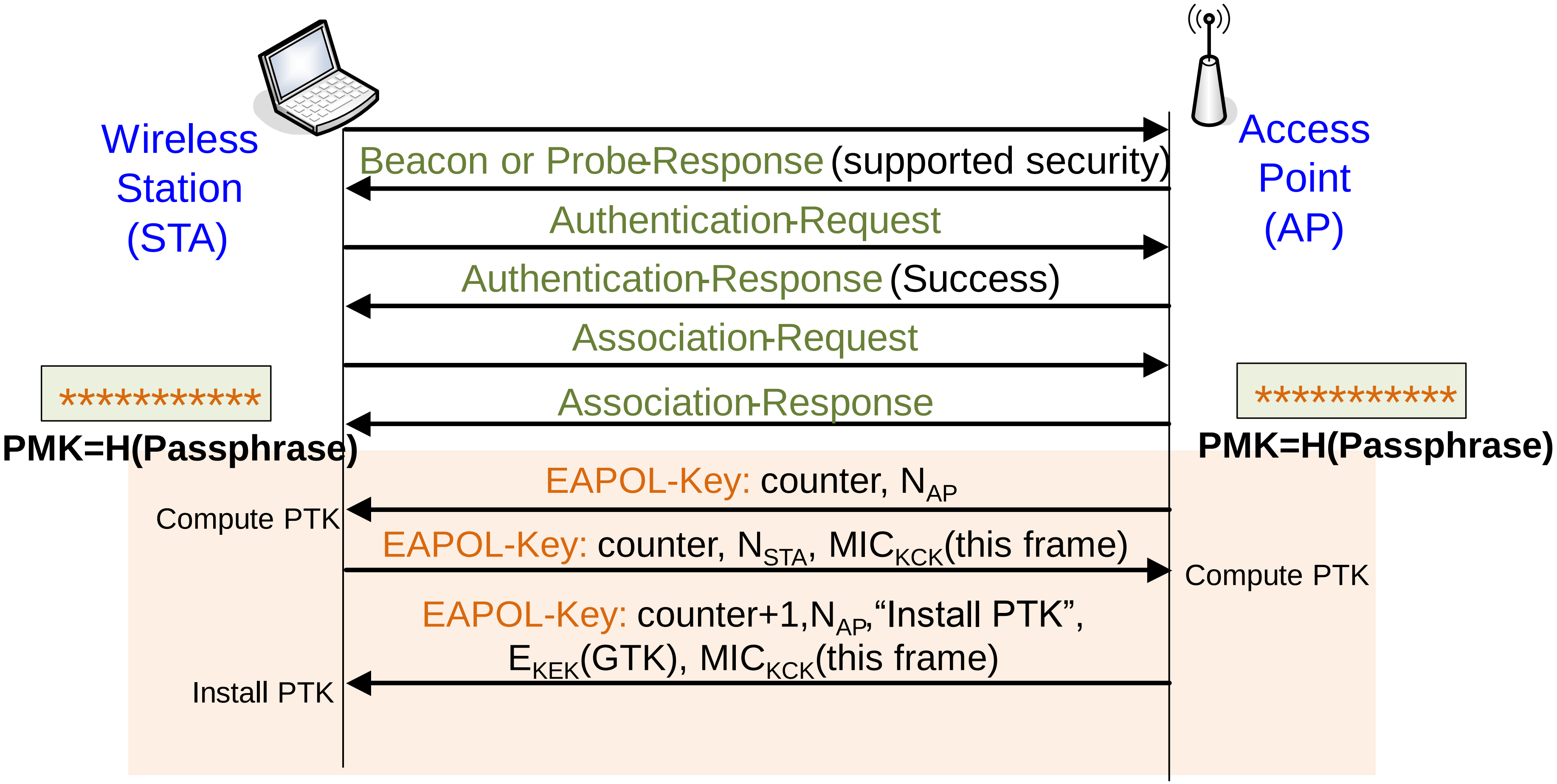
PMK = key derived from Passphrase/802.1x auth
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK,MACaddr$_{AP}$,MACaddr$_{STA}$,N$_{AP}$,N$_{STA}$)
KCK, KEK = parts of PTK
MIC = message integrity check, a MAC

WPA2 – Four-way handshake



PMK = key derived from Passphrase/802.1x auth
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK,$MACaddr_{AP}$,$MACaddr_{STA}$,N_{AP},N_{STA})
KCK, KEK = parts of PTK
MIC = message integrity check, a MAC

WPA2 – Four-way handshake



Wireless Station (STA)

Access Point (AP)

Beacon or Probe Response (supported security)

Authentication Request

Authentication Response (Success)

Association Request

Association Response

****

PMK=H(Passphrase)

****

PMK=H(Passphrase)

EAPOL-Key: counter, N_{AP}

Compute PTK

EAPOL-Key: counter, N_{STA}, MIC_{KCK}(this frame)

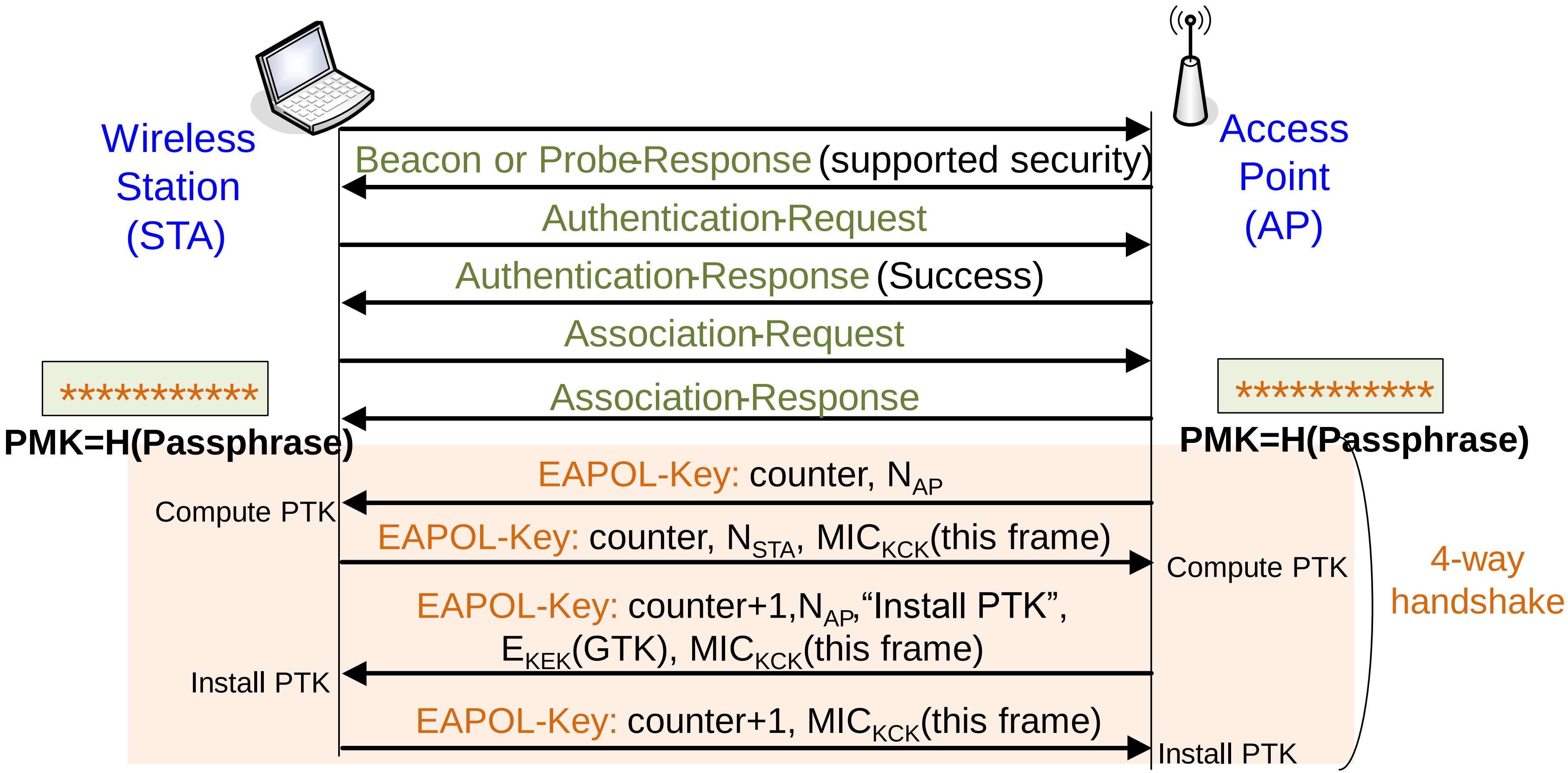
Compute PTK

EAPOL-Key: counter+1, N_{AP}, “Install PTK”, E_{KEK}(GTK), MIC_{KCK}(this frame)

Install PTK

PMK = key derived from Passphrase/802.1x auth
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK, $MACaddr_{AP}$, $MACaddr_{STA}$, N_{AP}, N_{STA})
KCK, KEK = parts of PTK
MIC = message integrity check, a MAC

WPA2 – Four-way handshake



Wireless Station (STA)

Access Point (AP)

Beacon or Probe-Response (supported security)

Authentication-Request

Authentication-Response (Success)

Association-Request

Association-Response

****

PMK=H(Passphrase)

****

PMK=H(Passphrase)

EAPOL-Key: counter, N_{AP}

Compute PTK

EAPOL-Key: counter, N_{STA}, MIC_{KCK}(this frame)

Compute PTK

EAPOL-Key: counter+1,N_{AP},“Install PTK”, E_{KEK}(GTK), MIC_{KCK}(this frame)

Install PTK

EAPOL-Key: counter+1, MIC_{KCK}(this frame)

Install PTK

4-way handshake

PMK = key derived from Passphrase /802.1x auth
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK,$MACaddr_{AP}$,$MACaddr_{STA}$,N_{AP},N_{STA})
KCK, KEK = parts of PTK
MIC = message integrity check, a MAC