Network Security: WLAN Security

Mohit Sethi

Ericsson, Finland

Aalto University, Finland

WLAN Security - Outline

- Part 1:
  - WLAN Standards and Components
  - Joining Open WLAN
  - WPA2-PSK and four-way handshake
  - WPA 3: Opportunistic Wireless Encryption (Enhanced Open)
  - WPA 3: Password Authenticated Key Exchange (PAKE : Dragonfly)
  - Enterprise wireless security - EAP

WLAN Standards

- IEEE 802.11 standard defines physical and link-layer for wireless Ethernet
- Wi-Fi is an industry alliance to promote 802.11 interoperability
- Original 802.11-1997, latest 802.11-2020, many amendments
- Physical layer:
  - Uses unlicensed bands at 2.4 GHz (microwave ovens, Bluetooth) and 5 GHz
  - Up to 14 radio channels in the 2.4 GHz band, but only about 3 non-overlapping ones
- Link layer
  - Looks like Ethernet (802.3) to layers above
  - MAC protocol differs from 802.3 because one antenna cannot detect collisions while transmitting
    → explicit ACKs needed

WLAN Components

- Access point (AP) = bridge between wireless (802.11) and wired (802.3) networks
- Wireless station (STA) = PC or other device with a wireless network interface card (NIC)
  - To be precise, AP is also a STA
- Stations are identified by globally unique 48-bit MAC address
  - MAC = Medium Access Control, don’t confuse with message authentication code
  - MAC address is assigned to each network interface card (NIC) by the manufacturer, which gets them from IEEE
- Infrastructure mode = wireless stations communicate only with AP
- Ad-hoc mode = no AP; wireless stations communicate directly with each other
- We will focus on infrastructure-mode WLANs

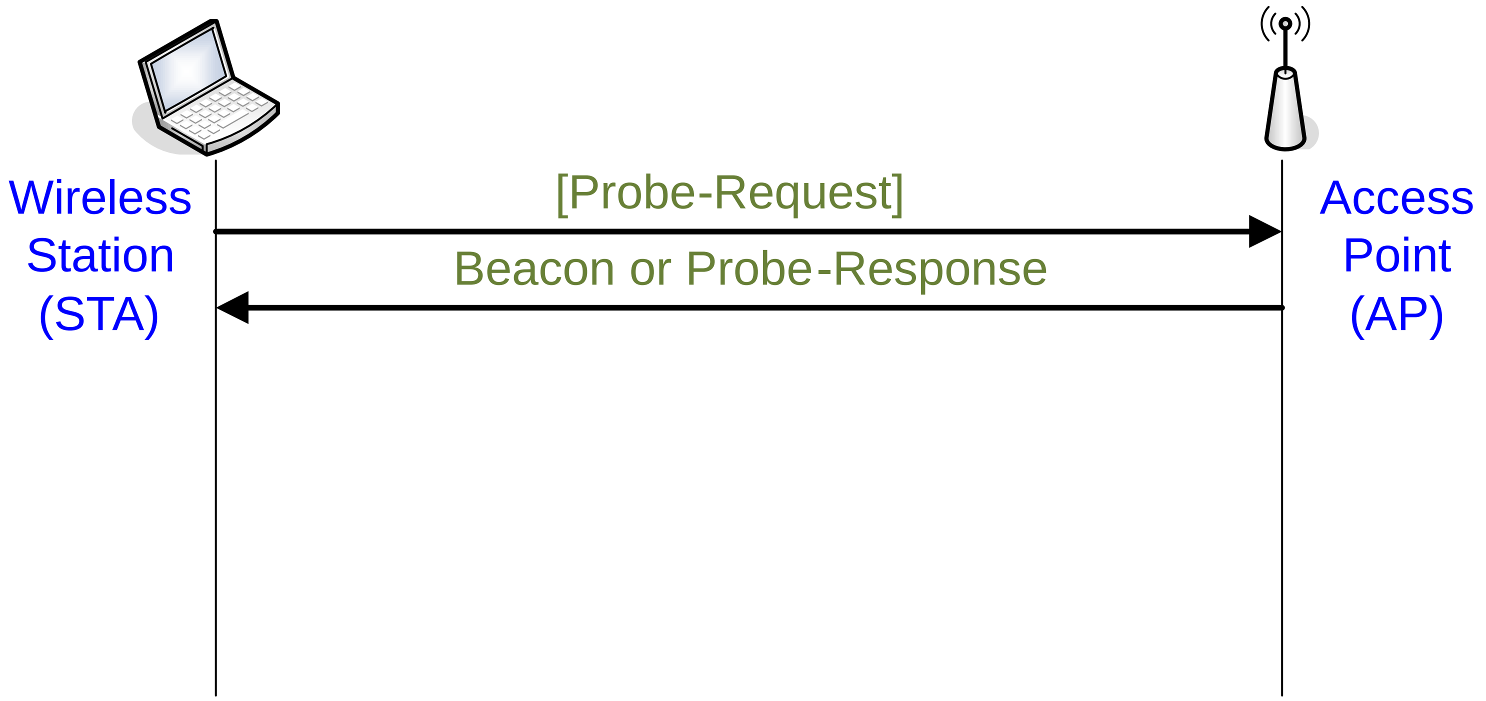
WLAN Structure

- Basic service set (BSS) = one WLAN cell (one AP + other wireless stations)
- The basic service set is identified by basic service set identifier (BSSID) = AP MAC address
- Extended service set (ESS) = multiple cells where the APs have the same service set identifier (SSID)
- The wired network is called distribution network in the standard; typically it is wired Ethernet
- APs in the same ESS can belong to the same IP network segment, or to different ones

Joining an open WLAN

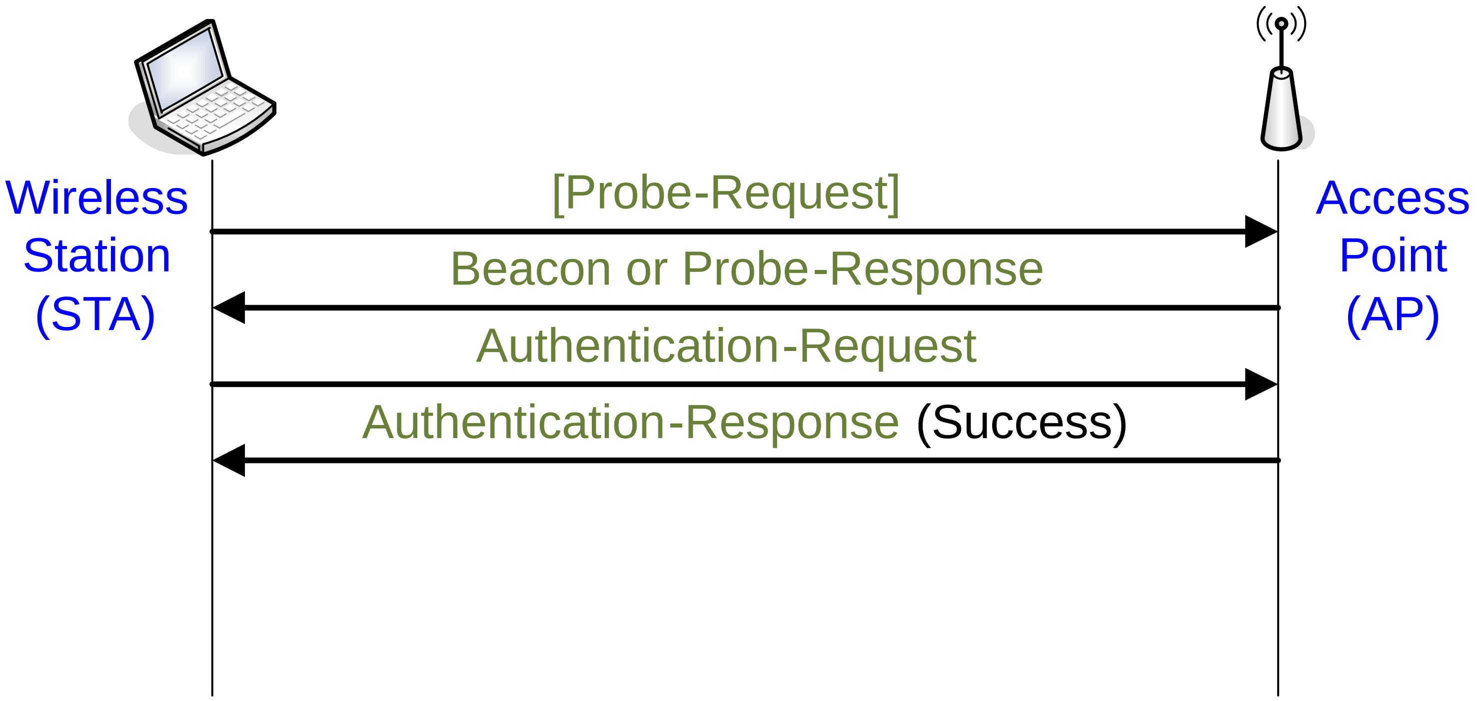
Joining an open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off



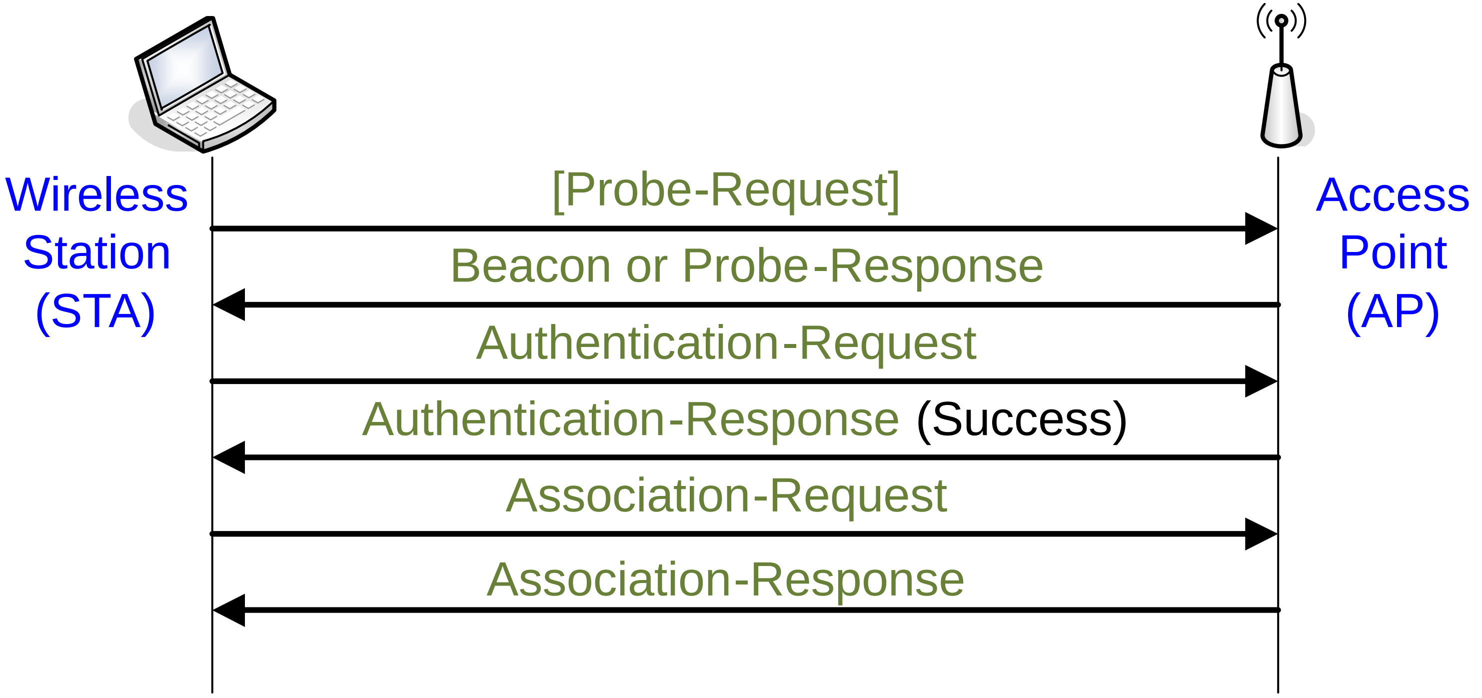
Joining an open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off



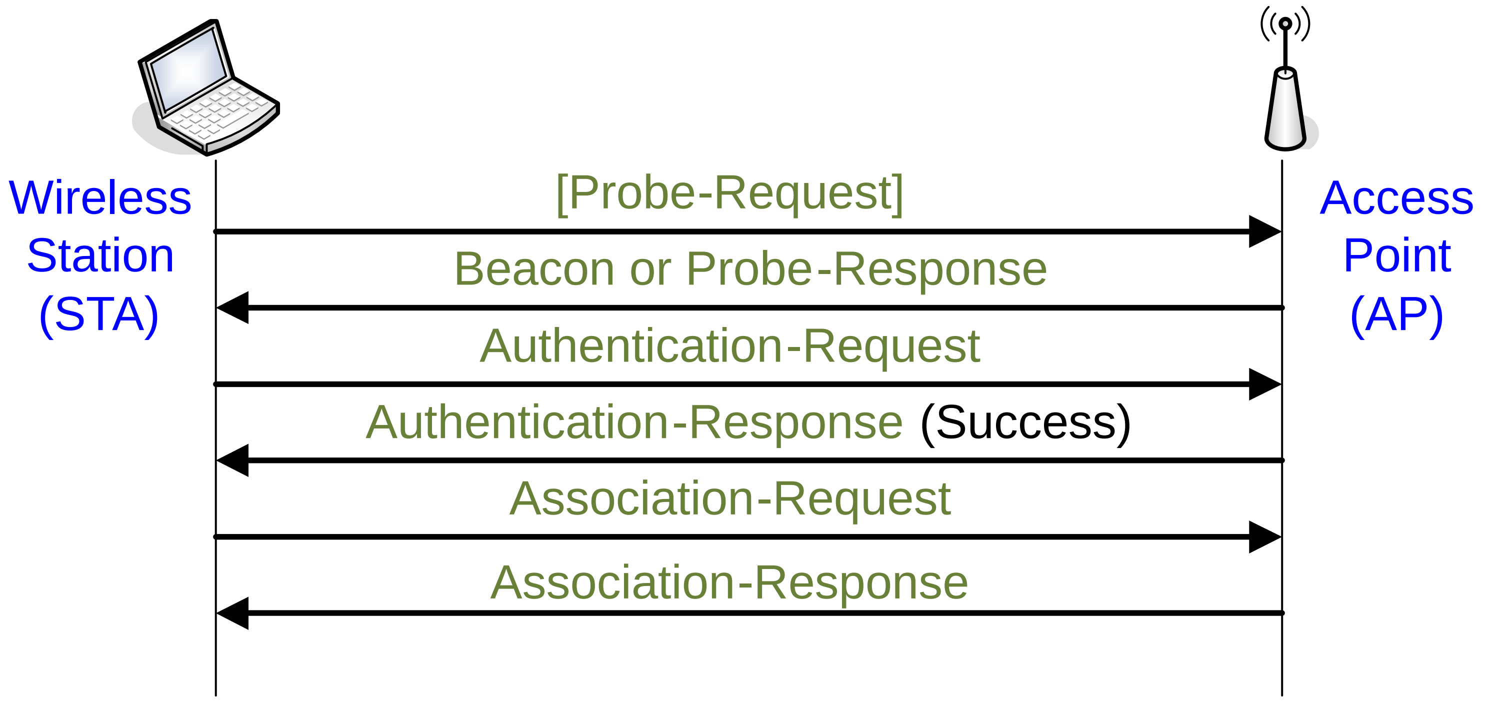
Joining an open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off



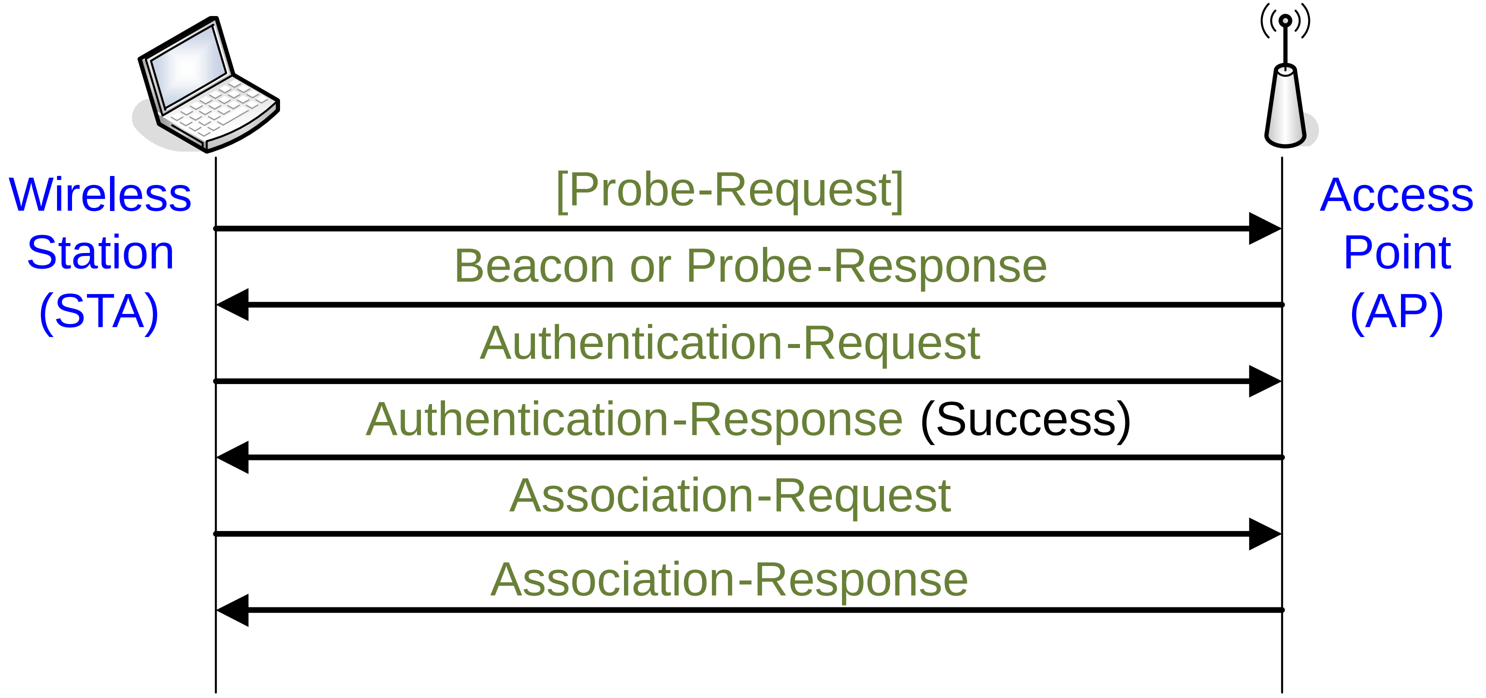
Joining an open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off
- STA must specify SSID to the AP in association request



Joining an open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off
- STA must specify SSID to the AP in association request



- Open system authentication = **no authentication**, empty authentication messages

Leaving a WLAN

- Both STA and AP can send a Disassociation Notification or Deauthentication Notification
- Include reason codes
  - station inactivity
  - station leaving

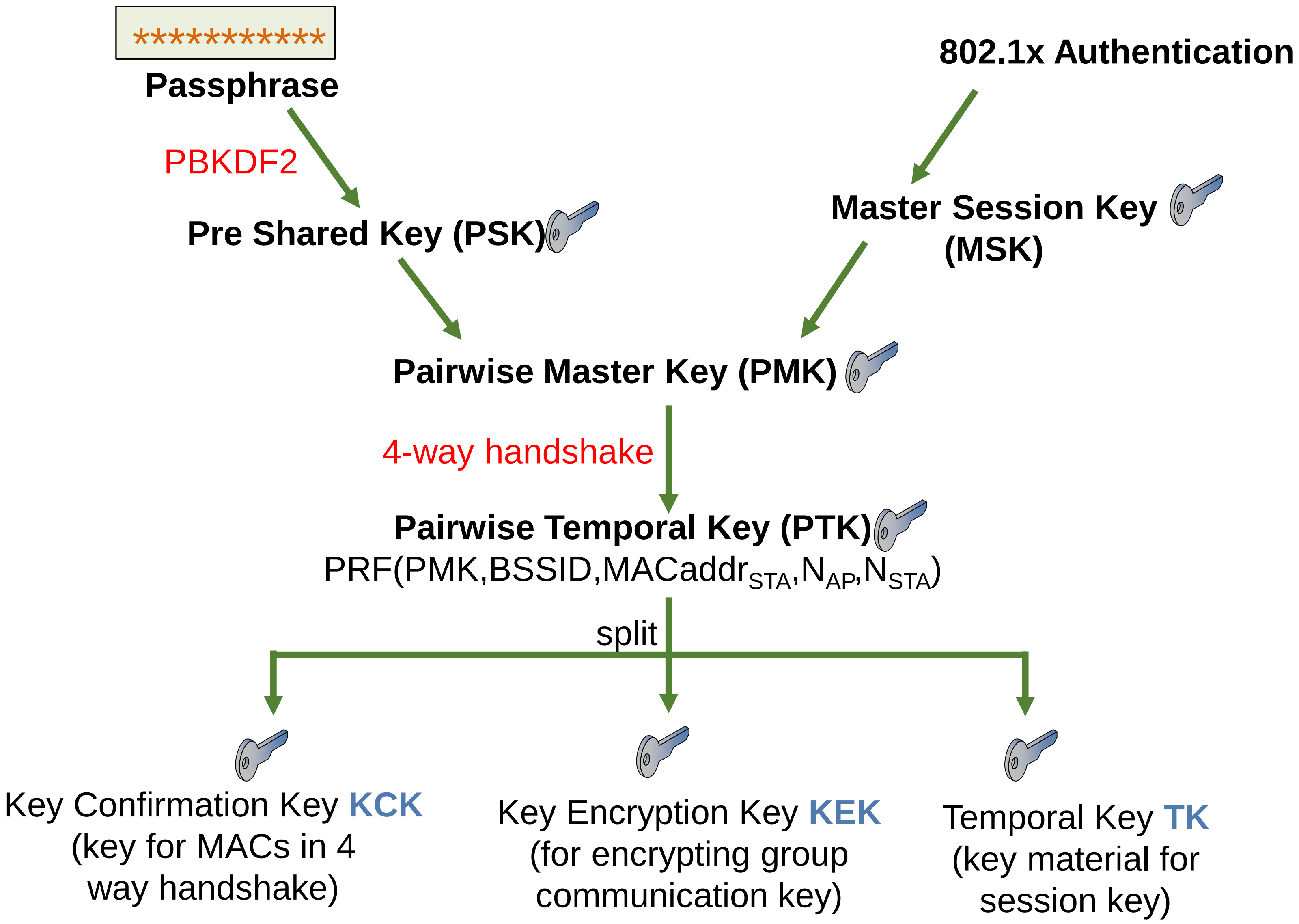
Network Security: WLAN Security: WPA

Mohit Sethi
Ericsson, Finland
Aalto University, Finland

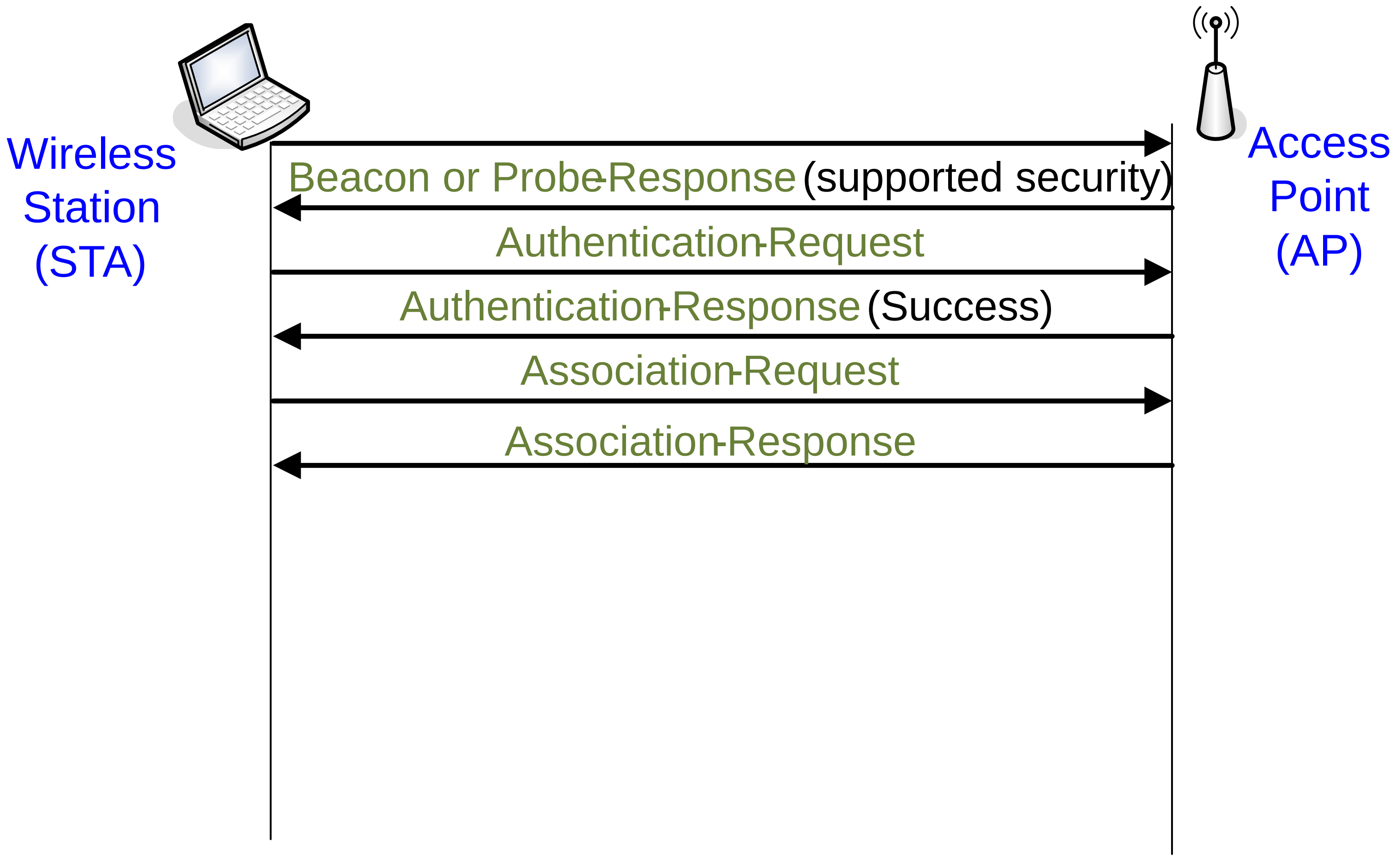
Real WLAN Security

- **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

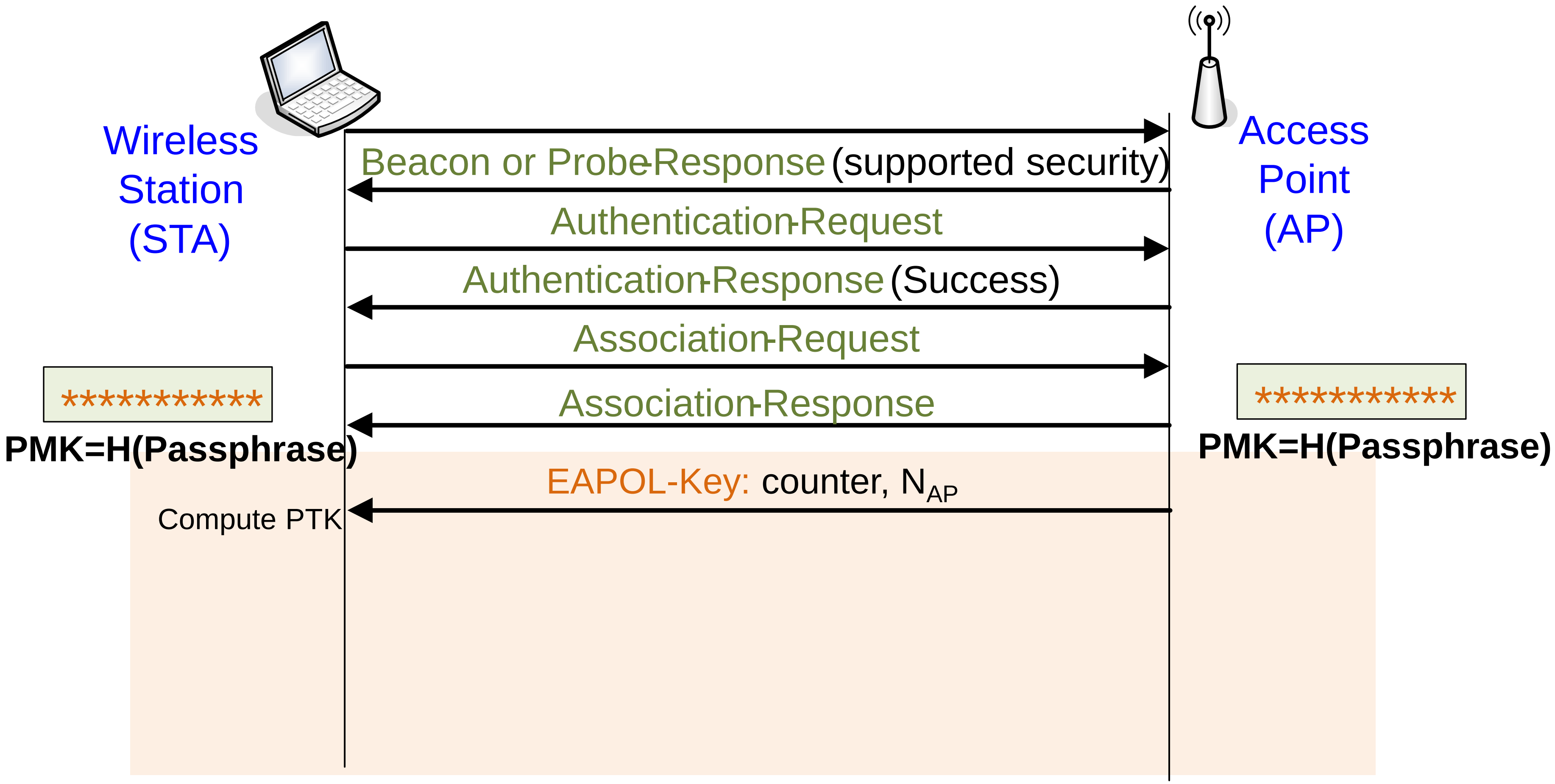
RSN Key Hierarchy



WPA2 – Four-way handshake

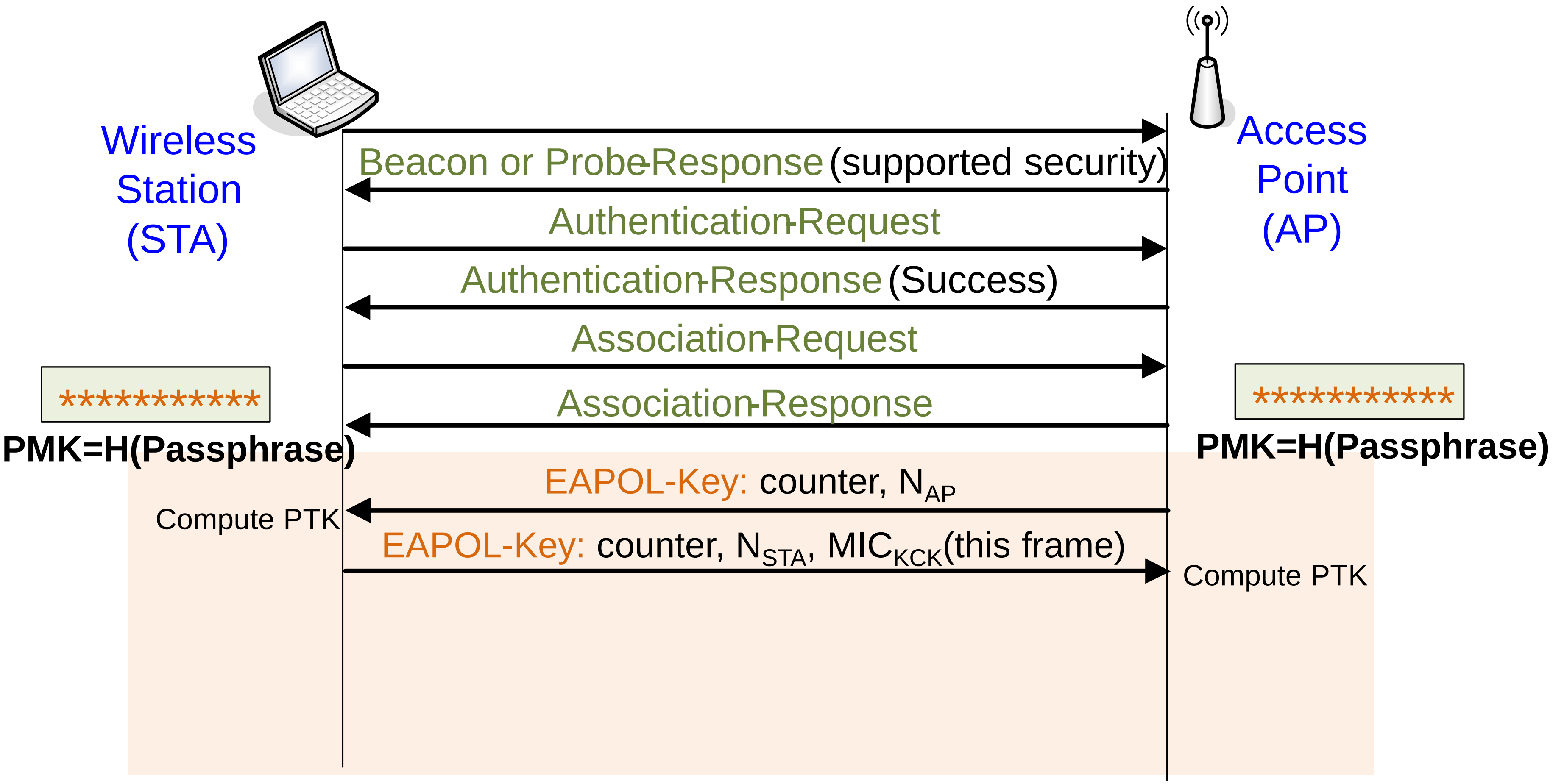


WPA2 – Four-way handshake



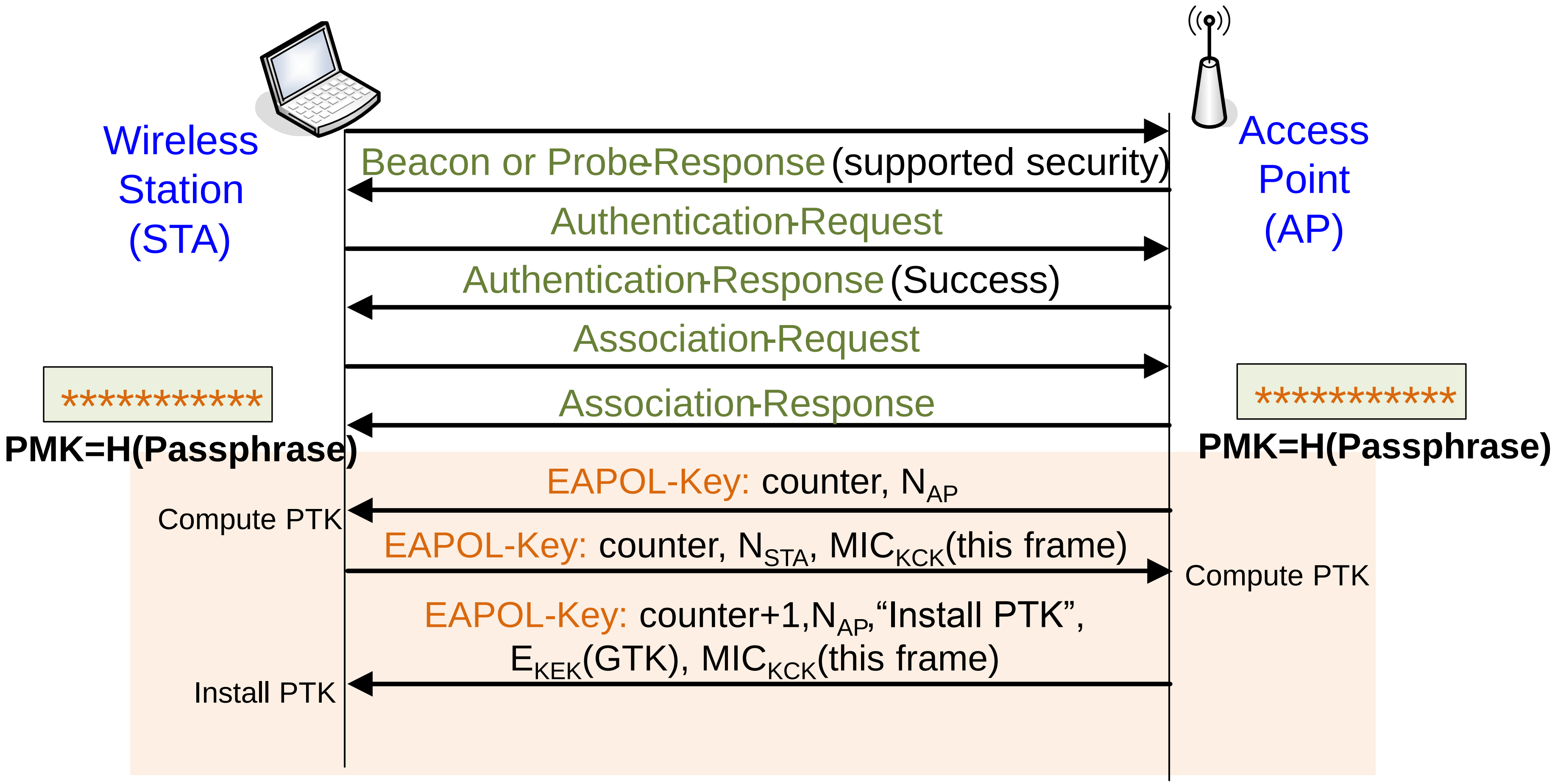
PMK = key derived from Passphrase/802.1x auth
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK,$MACaddr_{AP}$,$MACaddr_{STA}$,N_{AP},N_{STA})
KCK, KEK = parts of PTK
MIC = message integrity check, a MAC

WPA2 – Four-way handshake



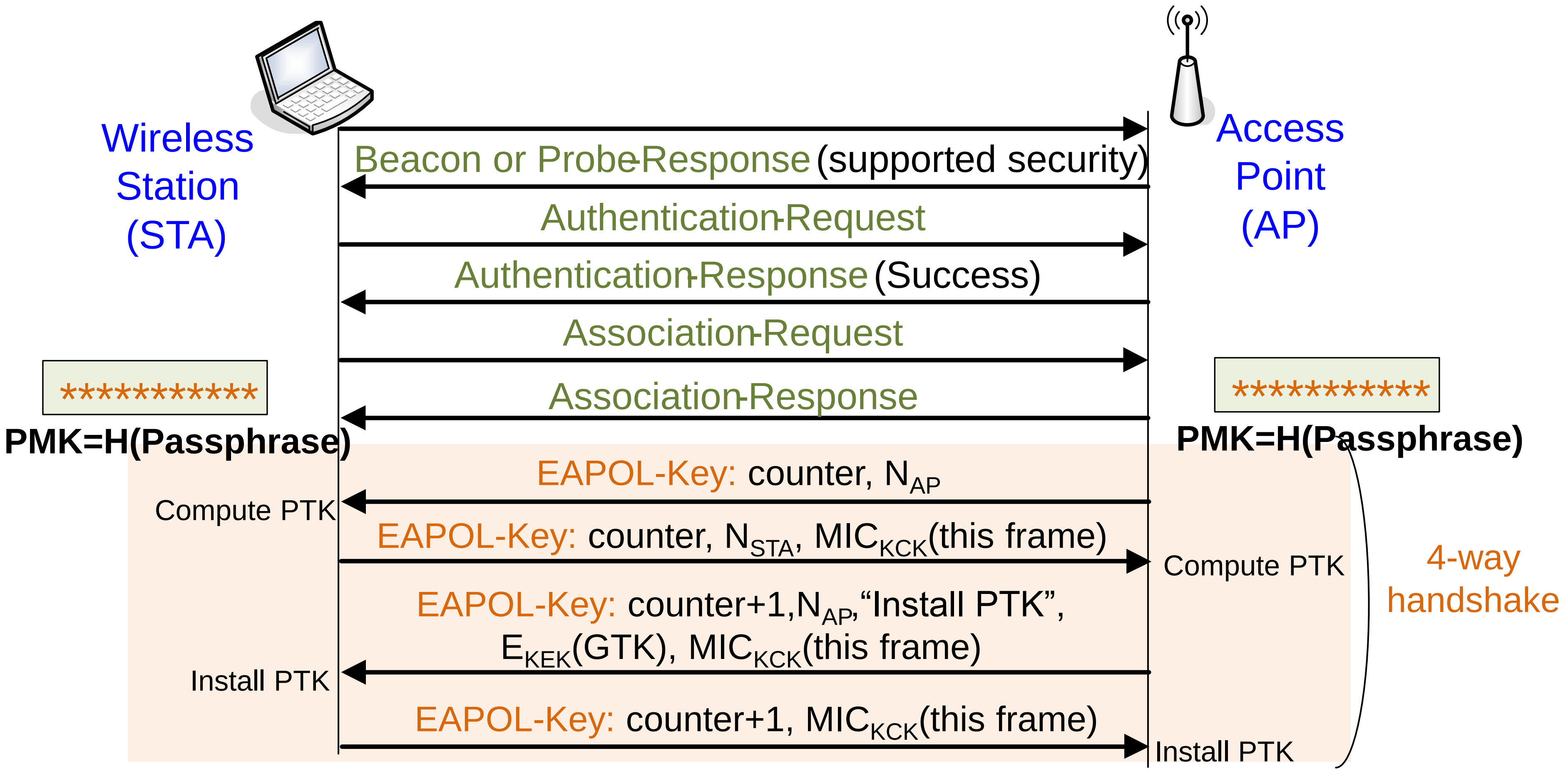
PMK = key derived from Passphrase/802.1x auth
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK,$MACaddr_{AP}$,$MACaddr_{STA}$,N_{AP},N_{STA})
KCK, KEK = parts of PTK
MIC = message integrity check, a MAC

WPA2 – Four-way handshake



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

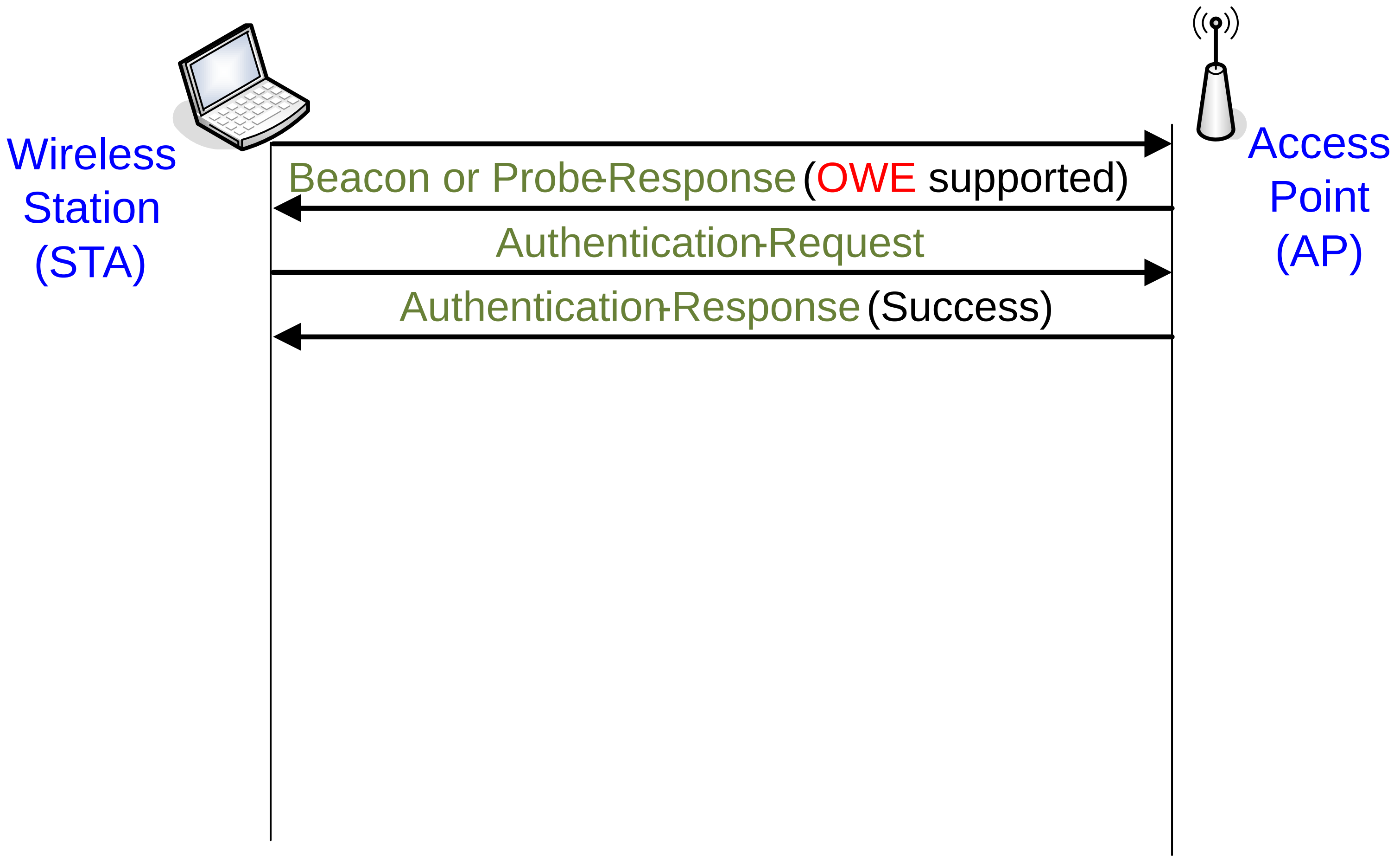
Network Security: WLAN Security: WPA3

Mohit Sethi
Ericsson, Finland
Aalto University, Finland

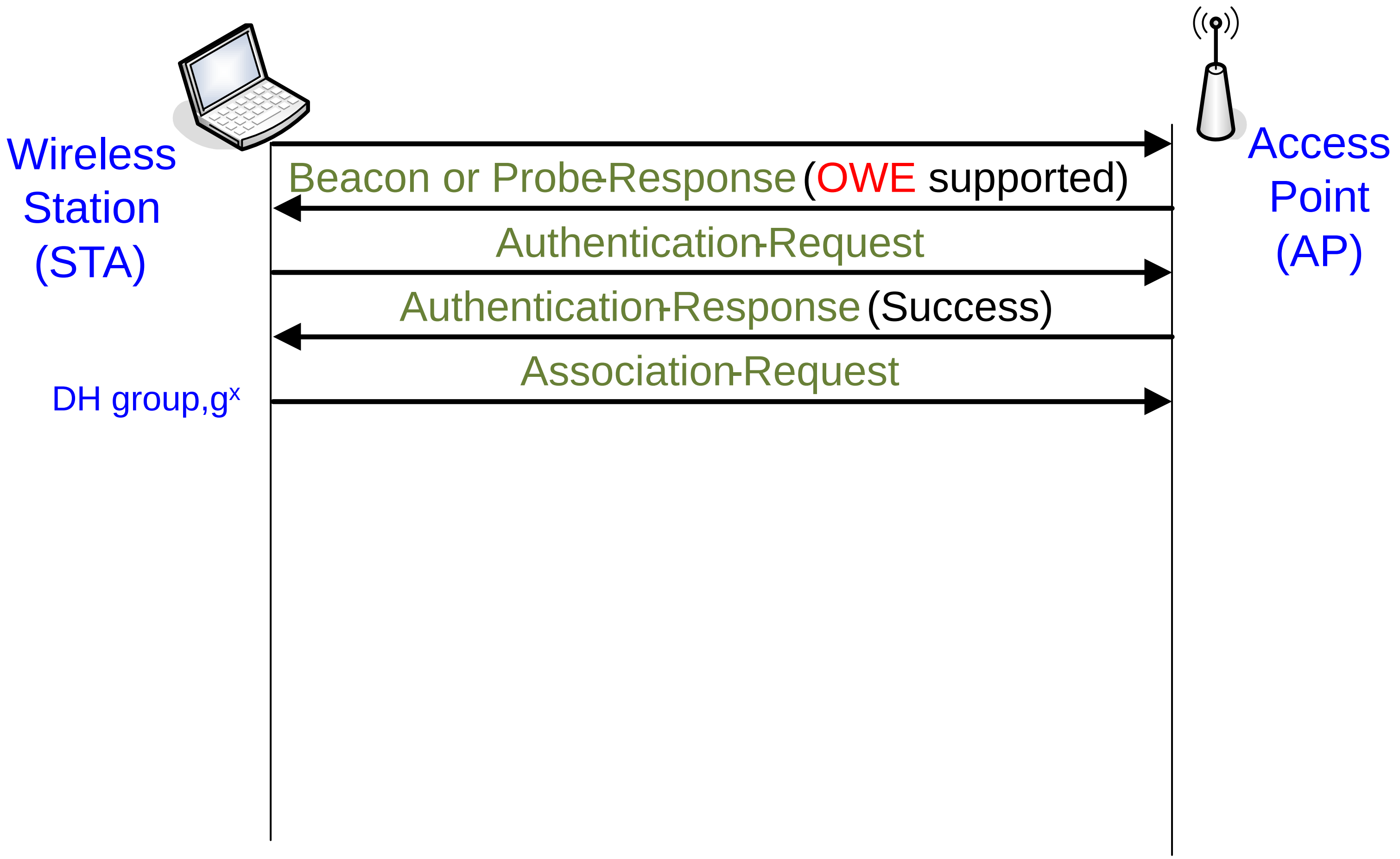
WPA3 Enhanced Open

- Open networks used in cafes and airports
  - Better user experience than asking for passphrase
- WPA3 Enhanced Open provides Opportunistic Wireless Encryption (OWE) for open networks – RFC 8110
- Station and AP perform Diffie-Hellman (DH) exchange during association
- A PMK is derived from DH shared secret
- PMK is used in 4 – way handshake as before

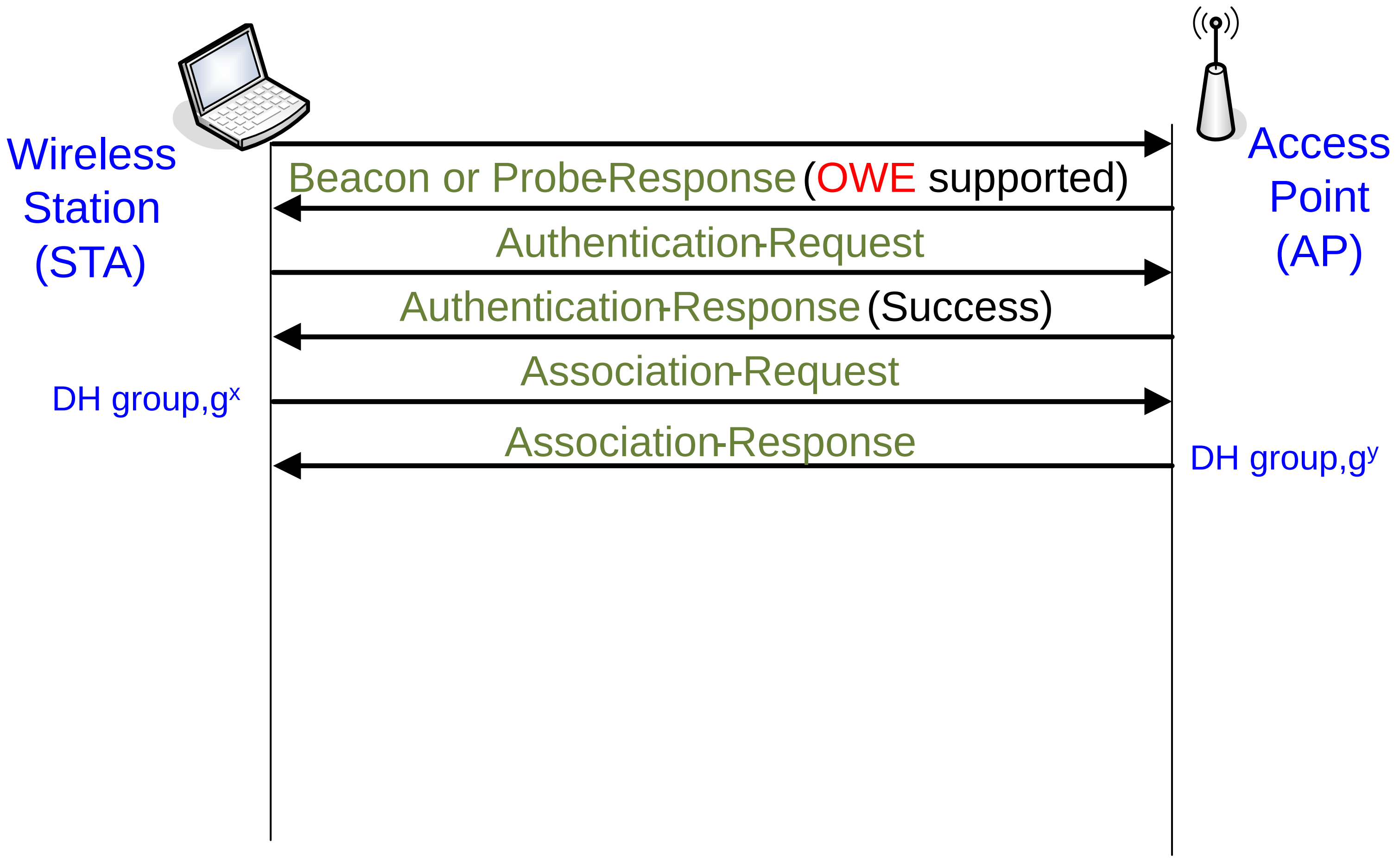
WPA3 Enhanced Open



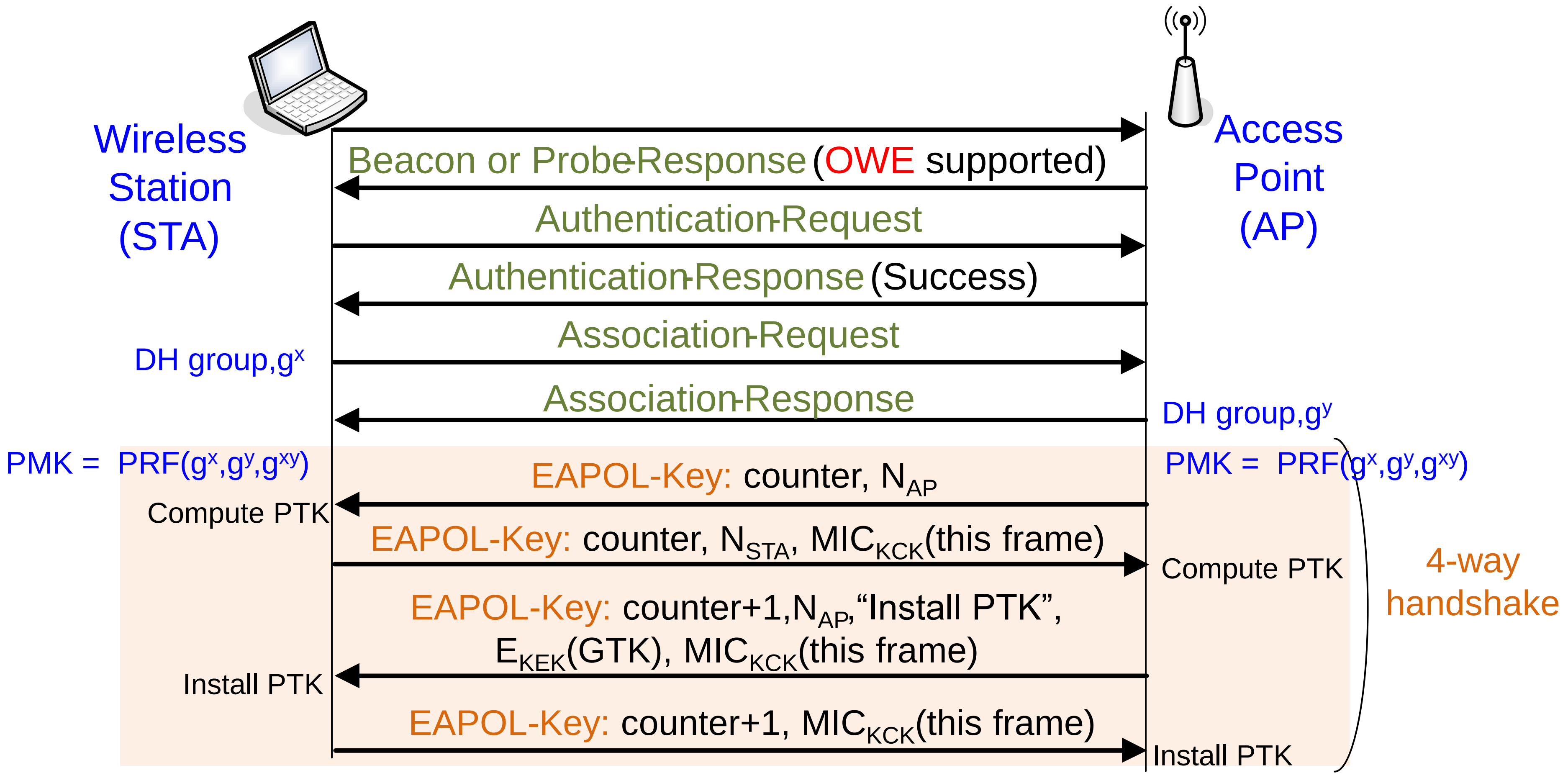
WPA3 Enhanced Open



WPA3 Enhanced Open



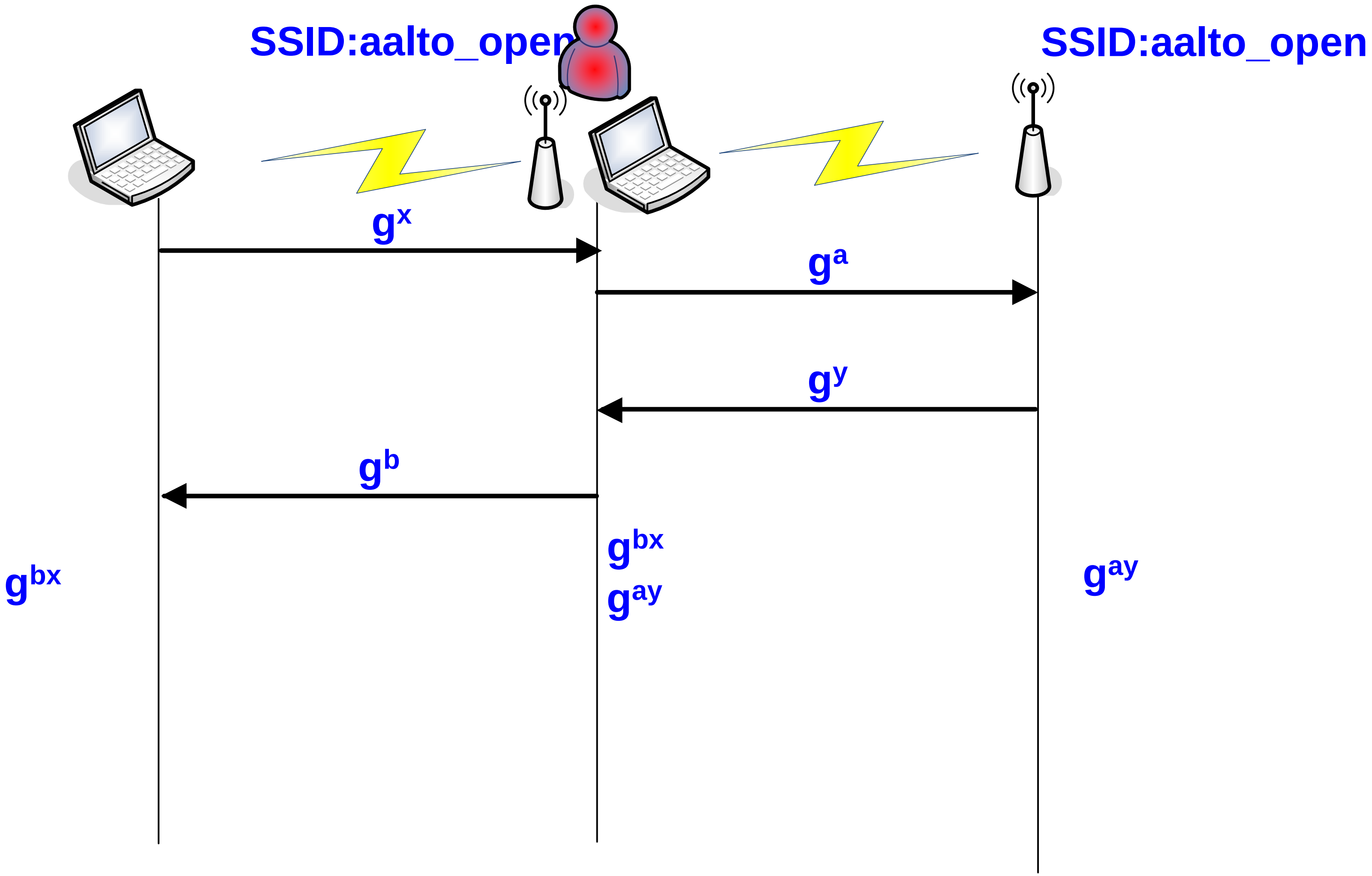
WPA3 Enhanced Open



WPA3 Enhanced Open

- OWE is encryption NOT authentication
  - Susceptible to active MiTM attack
  - Does NOT prevent evil twin APs

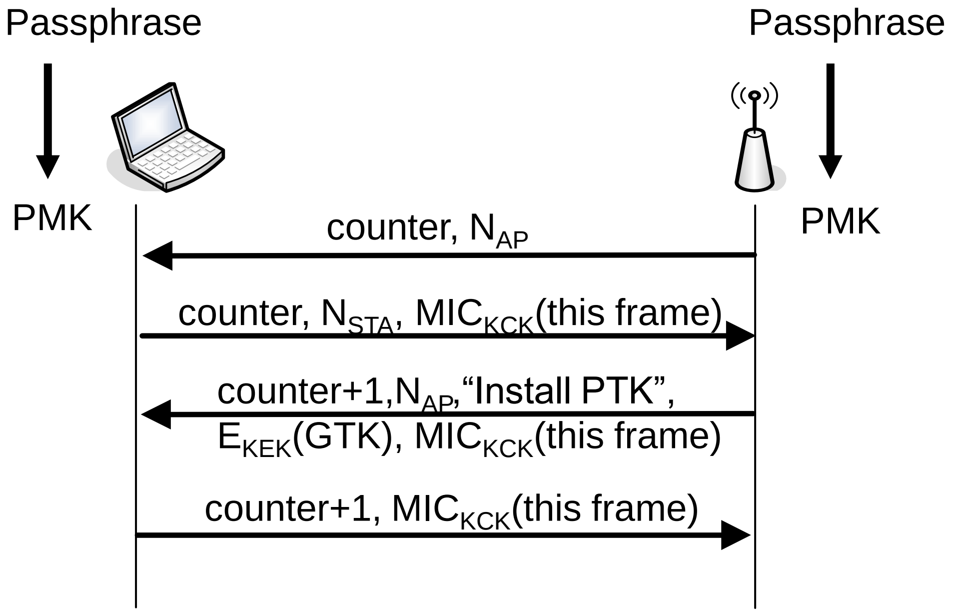
WPA3 Enhanced Open



WPA3 Enhanced Open

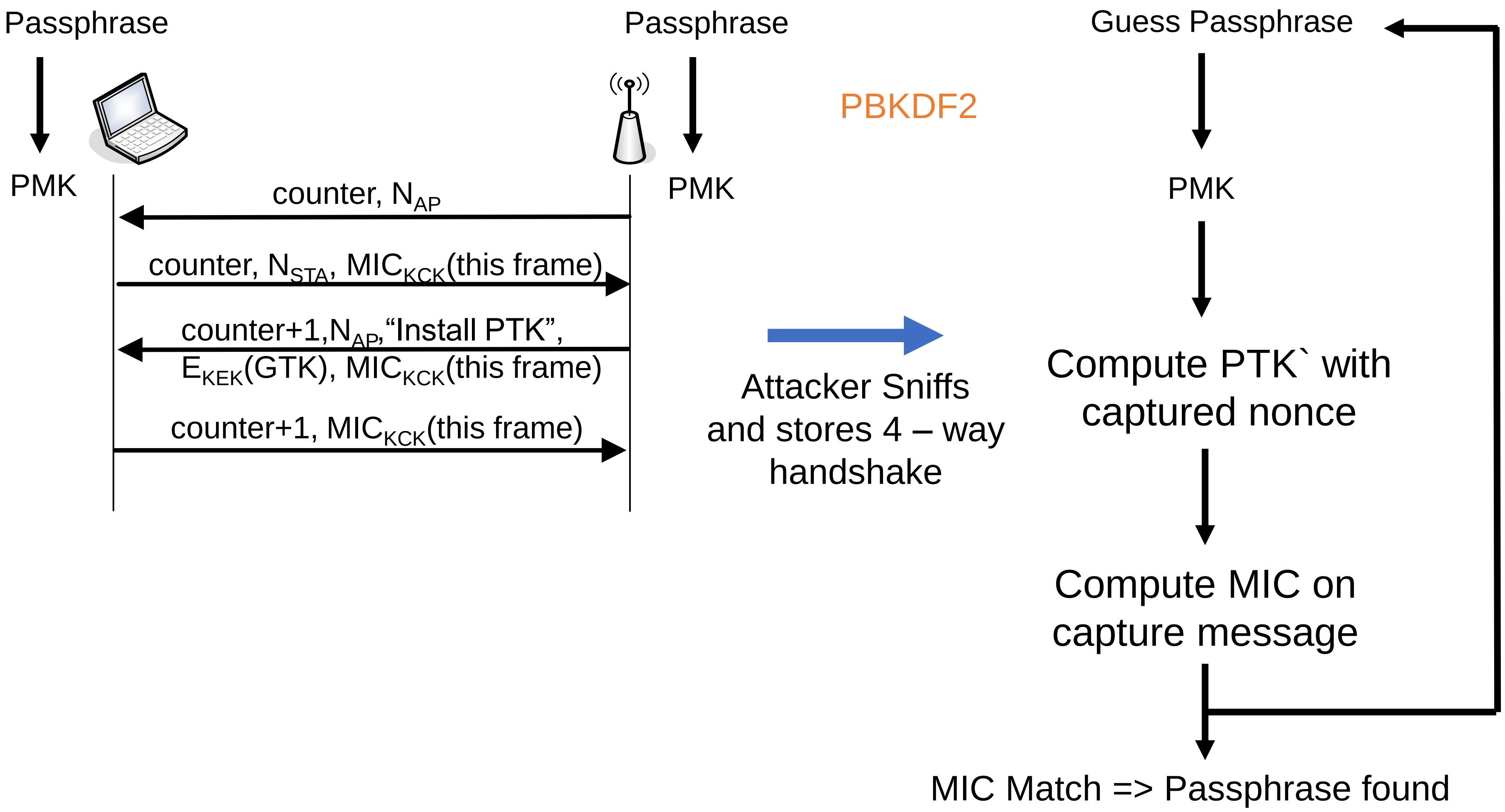
- Both ECC and FFC based Diffie-Hellman supported
- OWE is encryption NOT authentication
  - Susceptible to active MiTM attack
  - Does NOT prevent evil twin Aps
- No prior contact between Station and AP for PMK (= no shared knowledge of passphrase)
- Better than open authentication:
  - Passive attacker now needs to be active
  - Attacker cannot inject packets without active MiTM first
  - Forward secrecy when private keys are deleted
- Can do client authentication later with captive portal

WPA2 – Personal: Weakness

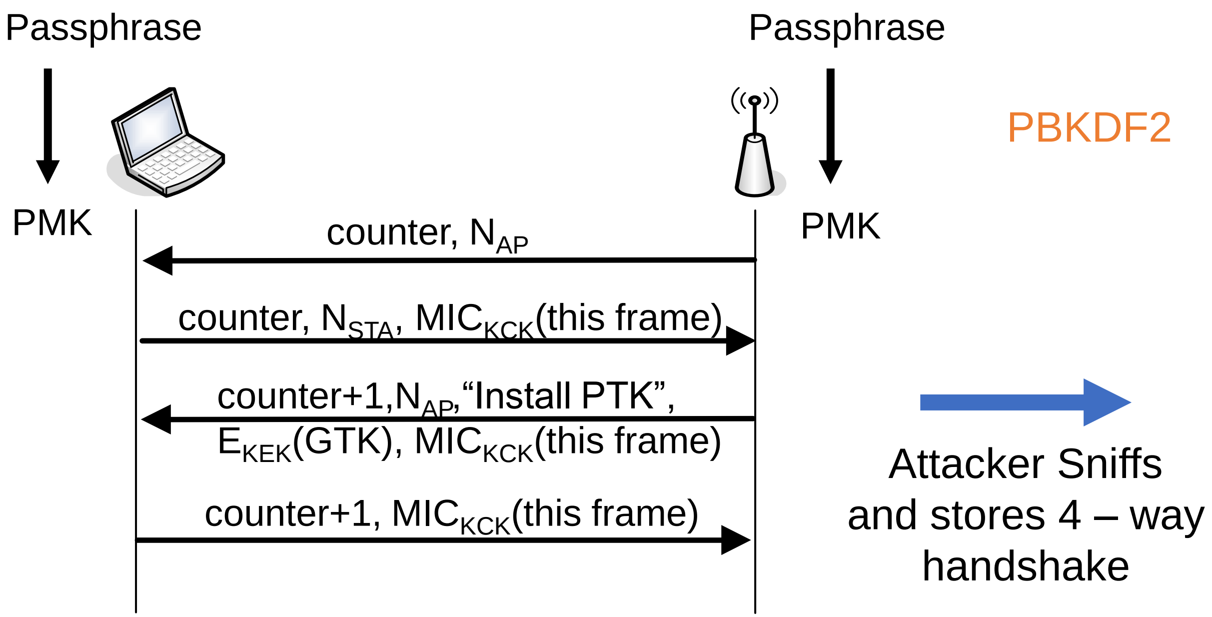


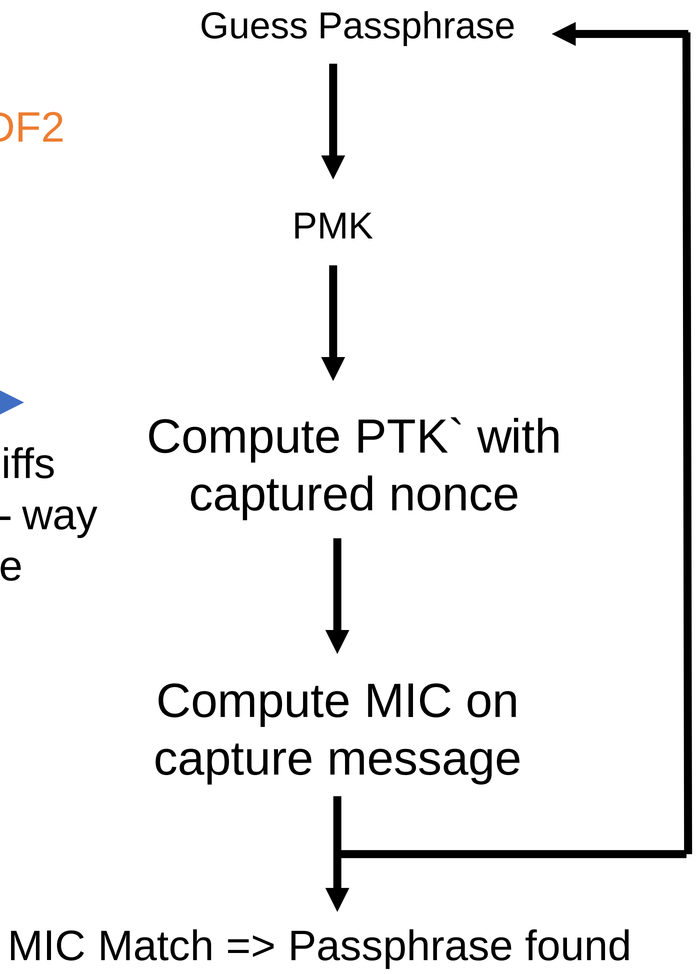
PBKDF2

WPA2 – Personal: Weakness



WPA2 – Personal: Weakness



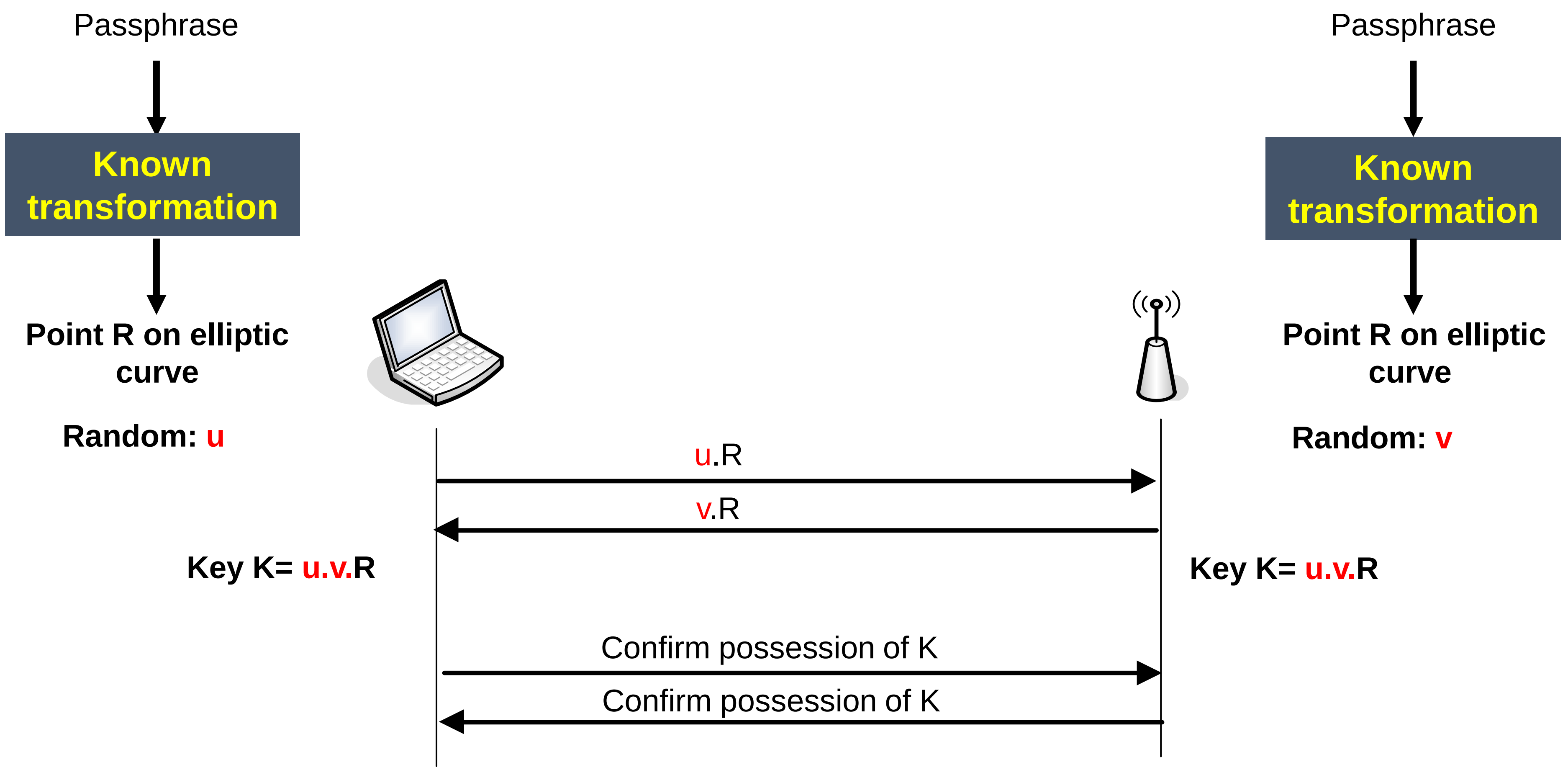


- Unlimited offline guessing
- Capture today – decrypt later

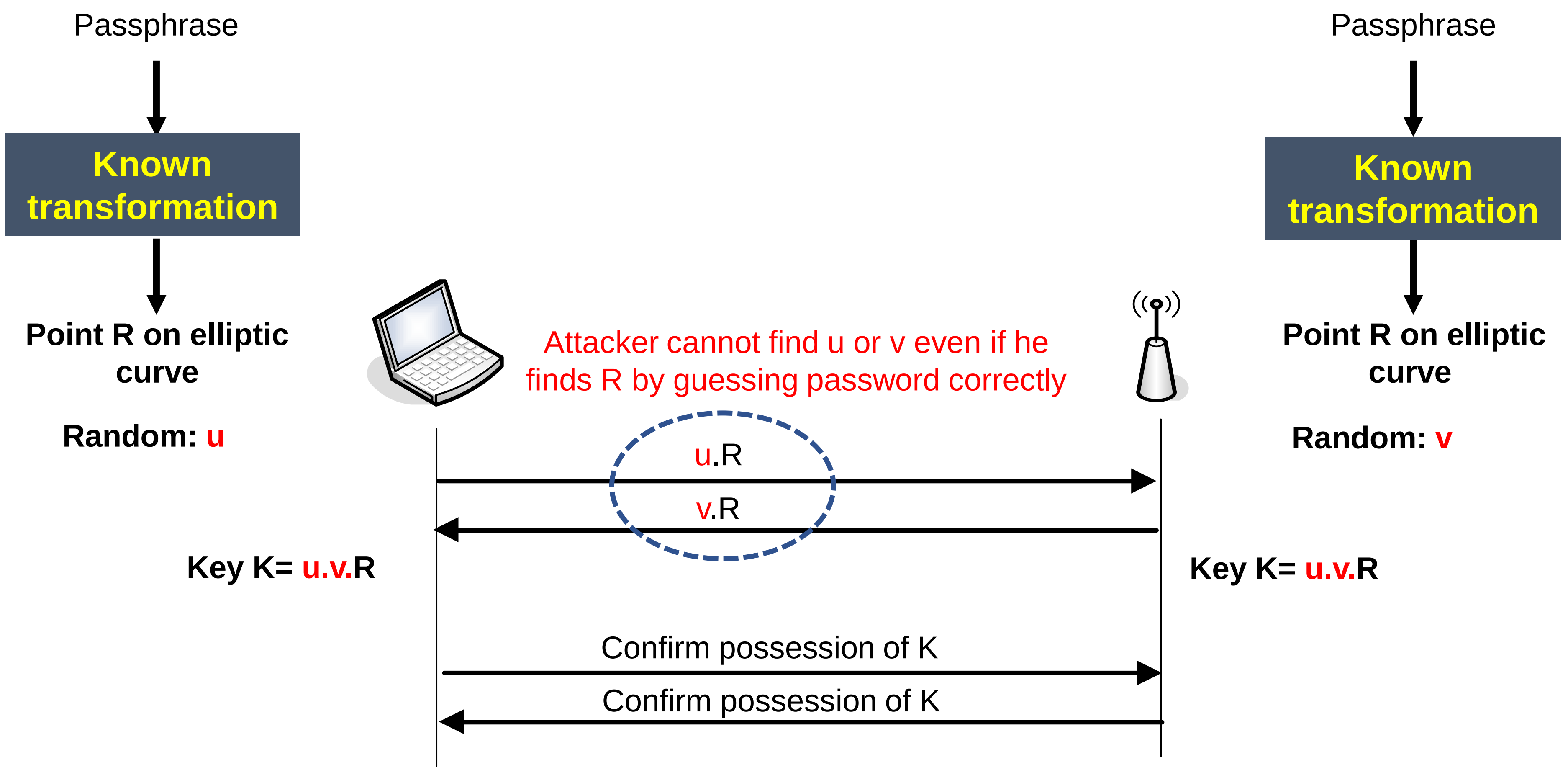
WPA3 PAKE : Dragonfly

- WPA3 uses Password Authenticated Key Exchange (PAKE) for preventing password guessing
  - WPA3 uses a variant of Dragonfly – RFC 7664 as PAKE
  - Original protocol called Simultaneous Authentication of Equals (SAE) defined in 802.11s in 2016
  - Standard for security in mesh networks
- Offline attacker cannot perform password guessing
- A live attacker physically present in the network can keep guessing but devices can setup protection against such repeated guessing - denial of service (DoS)

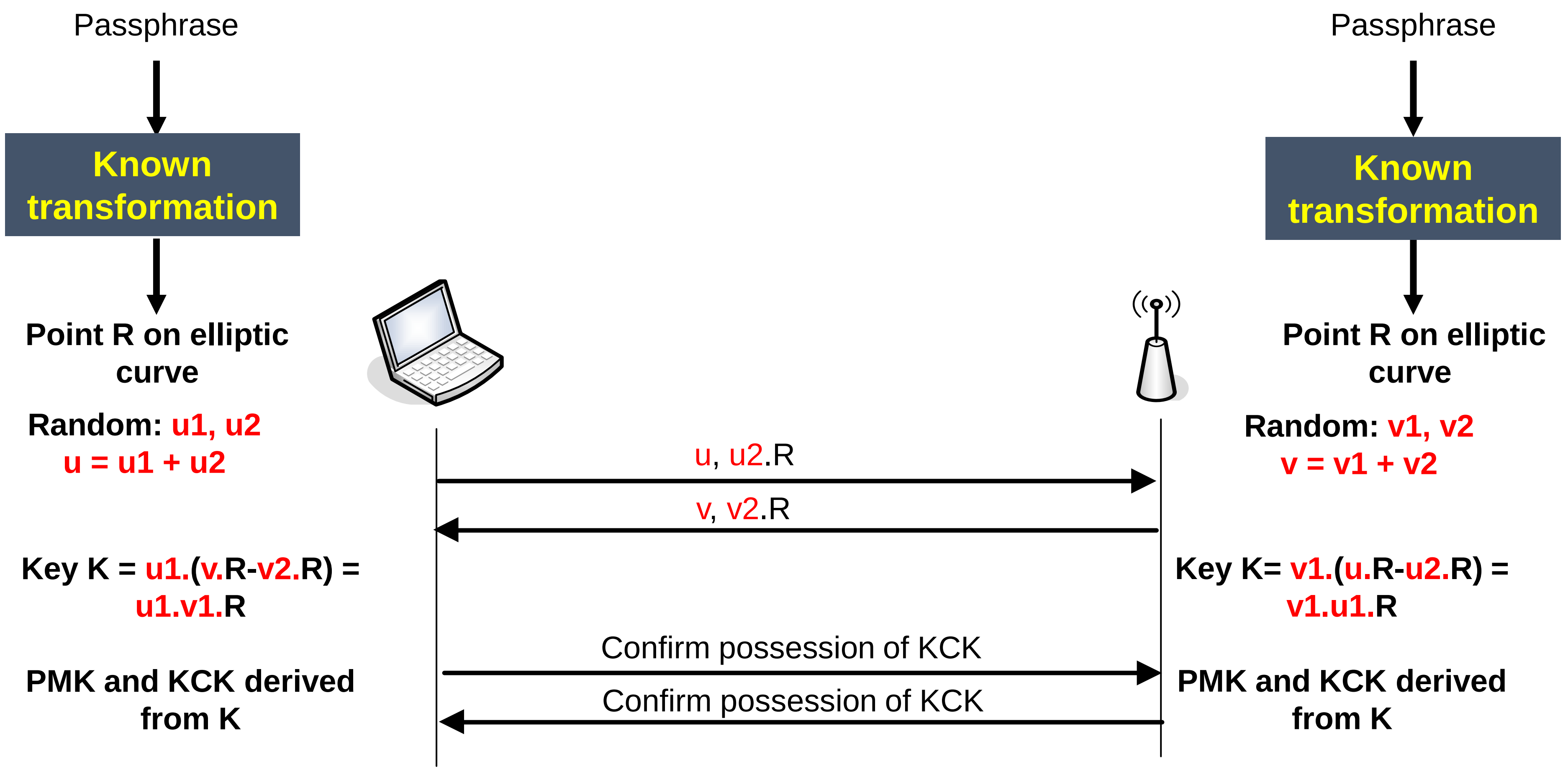
PAKE example



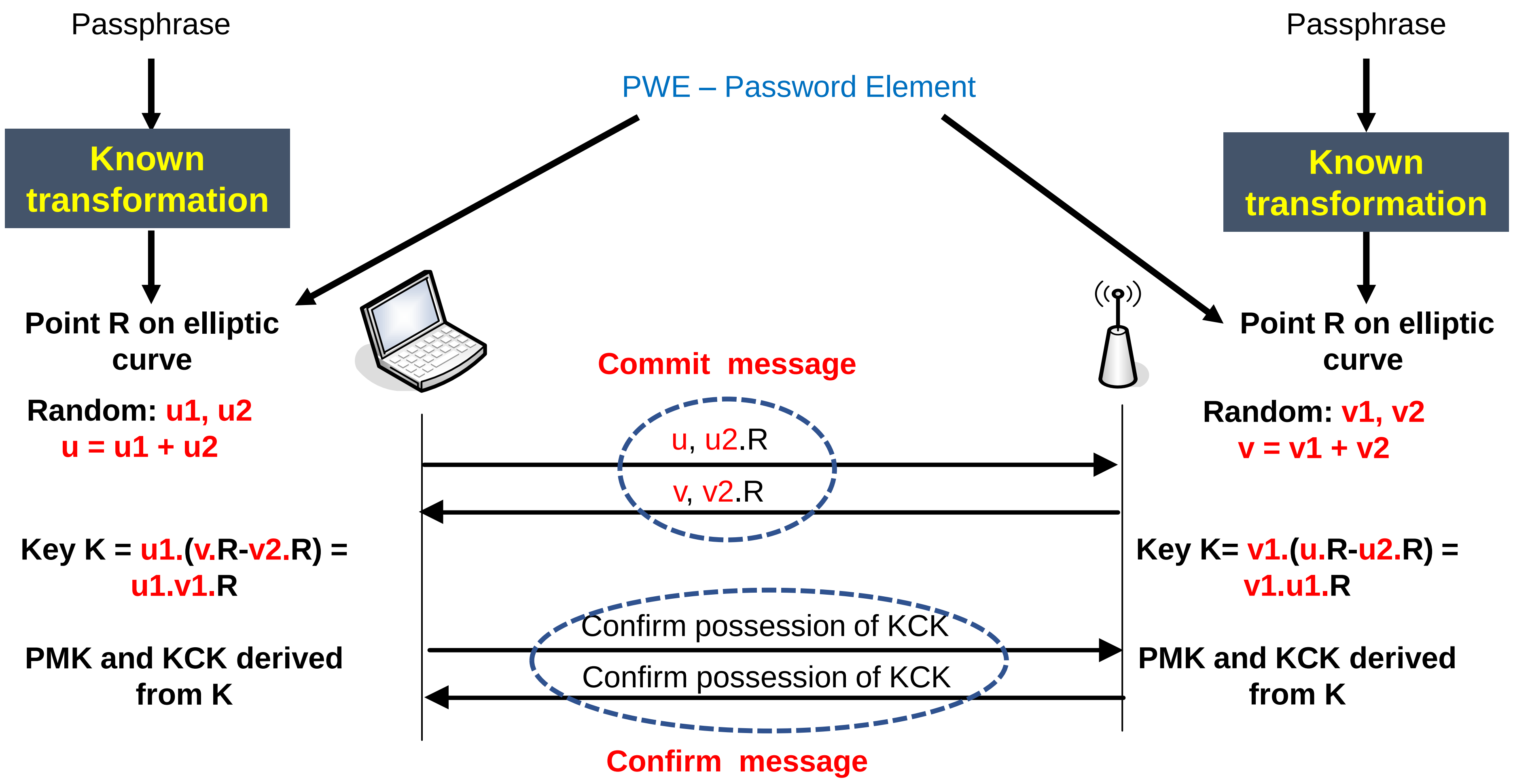
PAKE example



Dragonfly


Passphrase
Known transformation
Point R on elliptic curve
Random: u1, u2
u = u1 + u2
Key K = u1.(v.R-v2.R) = u1.v1.R
PMK and KCK derived from K
u, u2.R
v, v2.R
Confirm possession of KCK
Confirm possession of KCK
Passphrase
Known transformation
Point R on elliptic curve
Random: v1, v2
v = v1 + v2
Key K= v1.(u.R-u2.R) = v1.u1.R
PMK and KCK derived from K

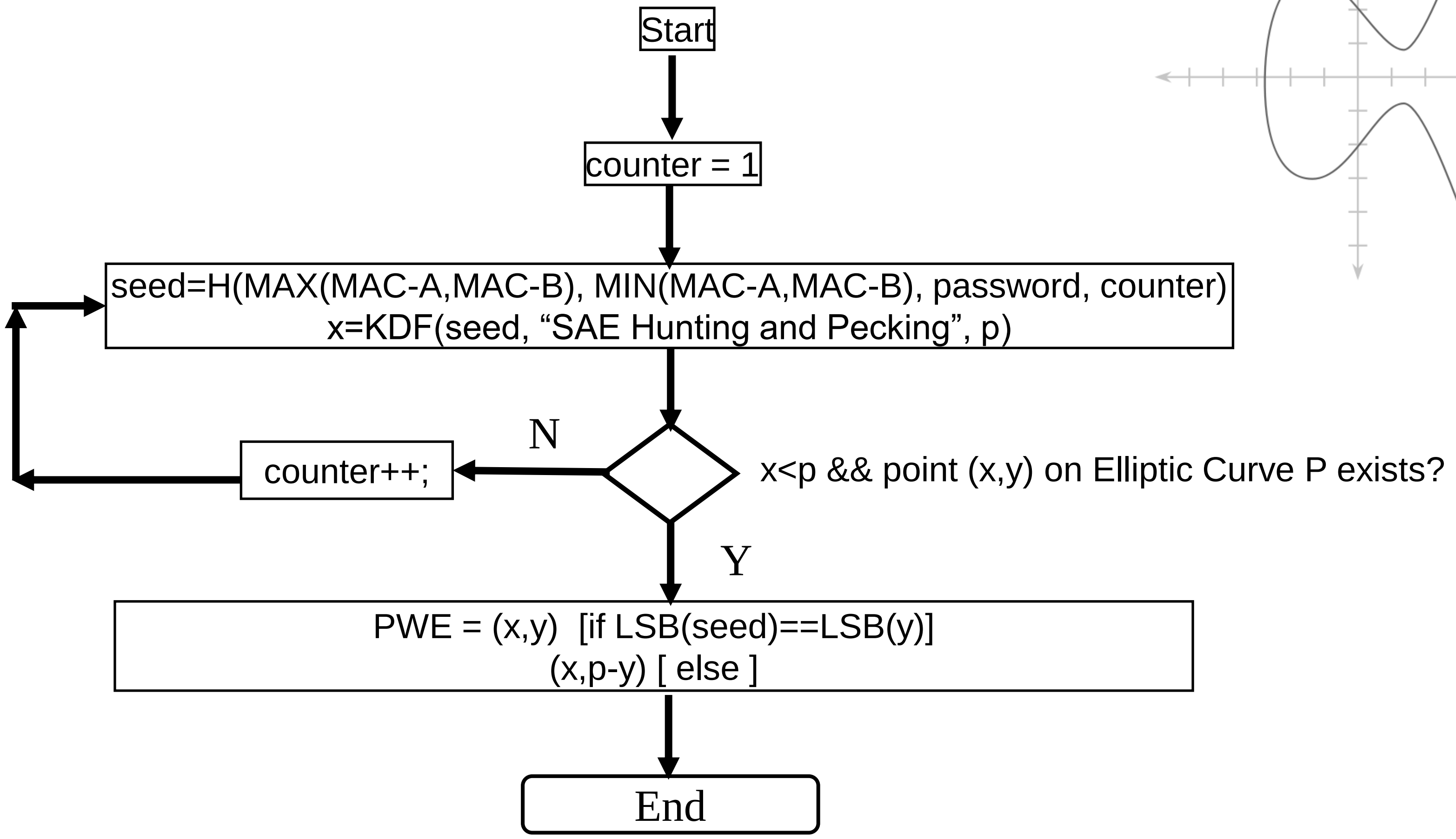
Dragonfly

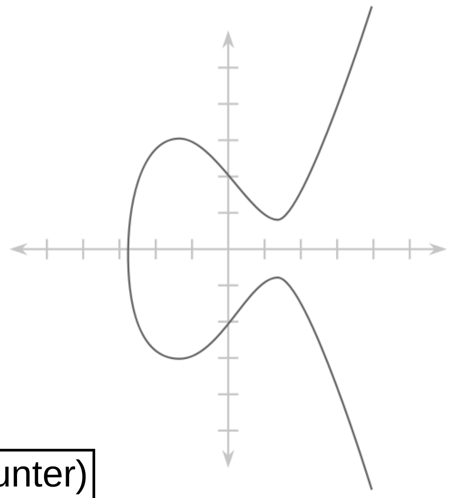

Passphrase
Known transformation
Point R on elliptic curve
Random: u1, u2
u = u1 + u2
Key K = u1.(v.R-v2.R) = u1.v1.R
PMK and KCK derived from K
PWE – Password Element
Commit message
u, u2.R
v, v2.R
Confirm possession of KCK
Confirm possession of KCK
Confirm message
Passphrase
Known transformation
Point R on elliptic curve
Random: v1, v2
v = v1 + v2
Key K= v1.(u.R-u2.R) = v1.u1.R
PMK and KCK derived from K

WPA3 PAKE : Dragonfly

- Dragonfly supports ECC and FFC group
- If not carefully implemented, side channel attacks are very possible
- Designed as a balanced PAKE – both sides know passphrase in plain
- Fresh PMK negotiated each time. This PMK is used in 4 – way handshake as before.
- PMK cannot be recovered even if passphrase is revealed later => forward secrecy after deleting u and v.

Example of PWE selection





WPA3 PAKE : Dragonfly

- Lot of controversy in IETF/IRTF when publishing
  - Trevor Perrin (well-known and respected cryptographer):
  - Questioned CFRG process: https://mailarchive.ietf.org/arch/msg/cfrg/0mnqMOmLy2N2H2K_F93MdUN_G28
  - Provided a critical review of Dragonfly: https://mailarchive.ietf.org/arch/msg/cfrg/YE4eKgOE9LTGbYd_hzN-nGDN-No
  - Asked for removal of CFRG chair: https://mailarchive.ietf.org/arch/msg/cfrg/scLoq7DvtXzo9Jl9AG9fQOcSGsM
- Many attacks in published in April 2019
  - https://papers.mathyvanhoef.com/dragonblood.pdf

Aalto University

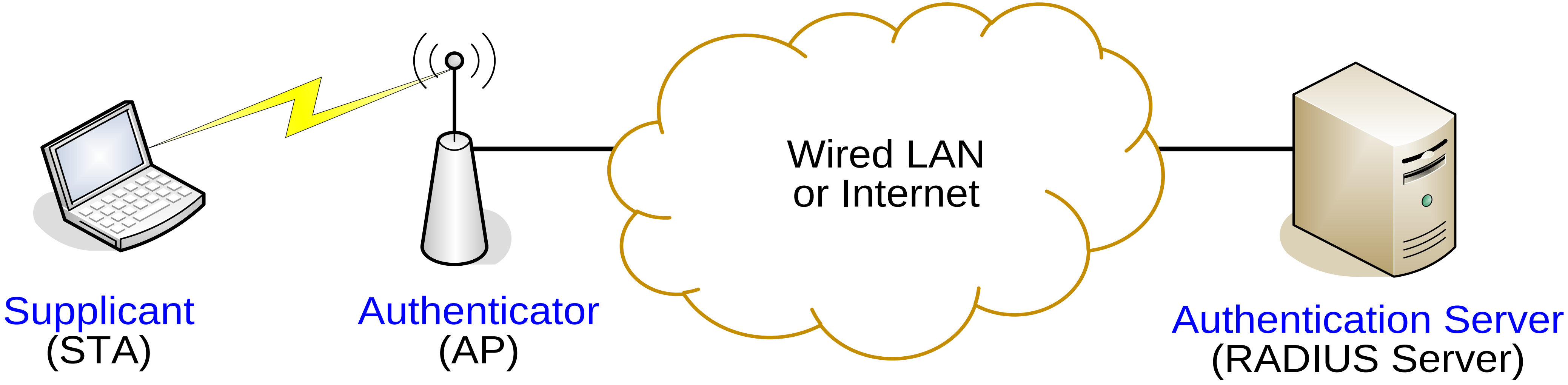
Network Security: WLAN Security: 802.1X and EAP

Mohit Sethi
Ericsson, Finland
Aalto University, Finland

IEEE 802.1X

- **Port-based access control** — originally intended for enabling and disabling physical ports on switches and modem banks
- Conceptual controlled port at WLAN AP
- Uses Extensible Authentication Protocol (EAP) to support many authentication methods

802.11/802.1X architecture

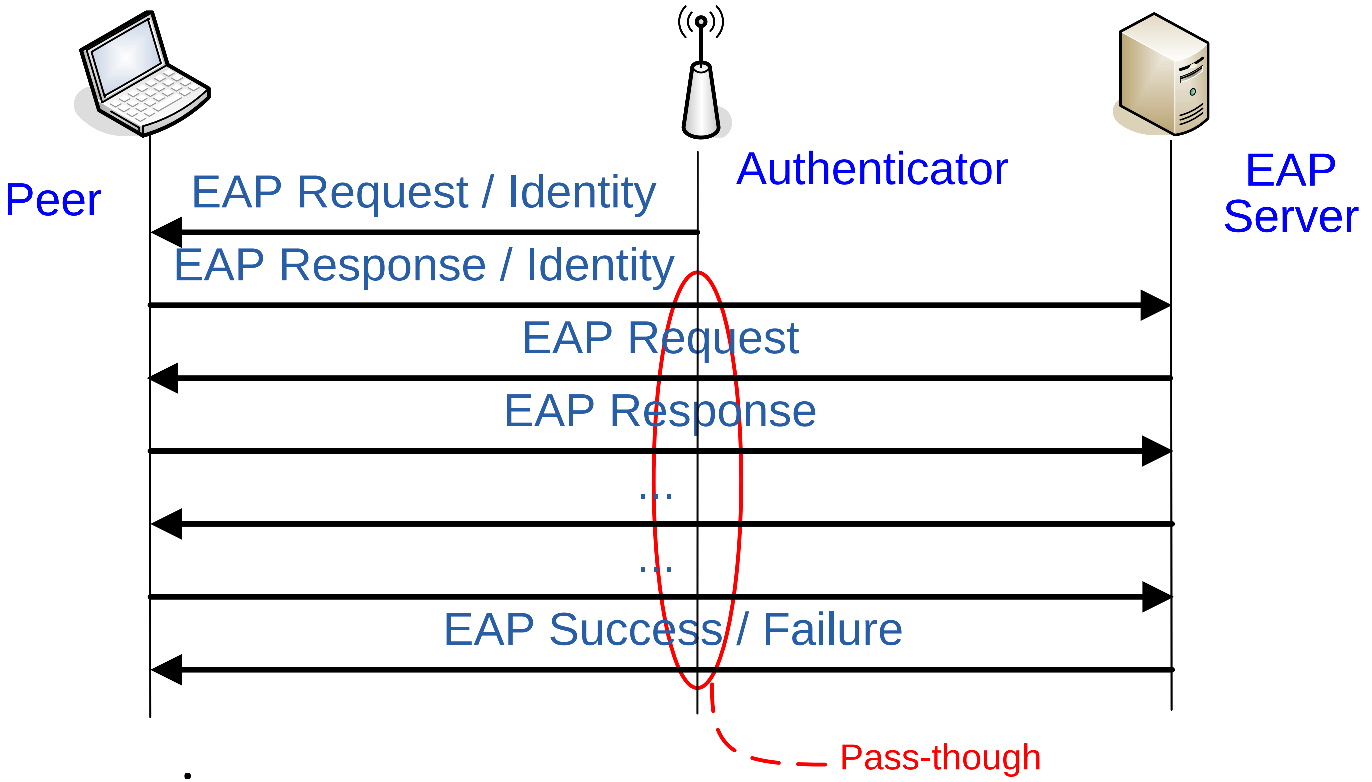


- Supplicant wants to access the wired network via the AP
- Authentication Server (AS) authenticates the supplicant
- Authenticator enables network access for the supplicant after successful authentication

EAP

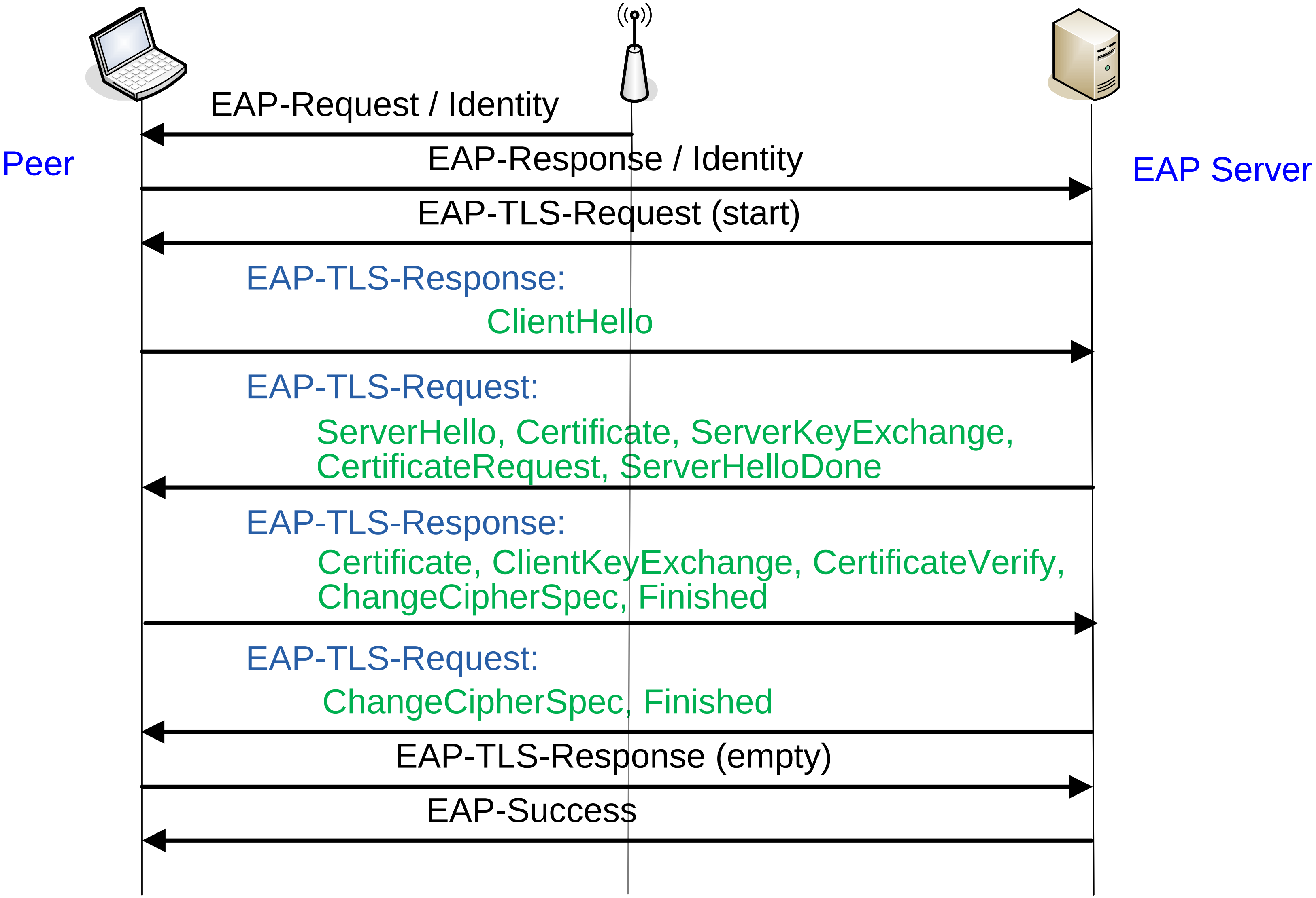
- **Extensible authentication protocol (EAP)** defines generic authentication message formats: Request, Response, Success, Failure
- Security is provided by the authentication protocol carried inside EAP, not by EAP itself
- EAP supports many authentication protocols: EAP-TLS, PEAP, EAP-SIM, ...
- Used in 802.1X between supplicant and authentication server
- EAP term for supplicant is peer, reflecting the original idea that EAP could be used for mutual authentication between equal entities

EAP Protocol

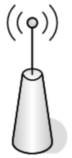


- Request-response pairs
- User identified by **network access identifier (NAI)**: username@realm
- Allows multiple rounds of request-response, originally for mistyped passwords
- Additionally, the EAP server will tell Authenticator to open the port

EAP-TLS

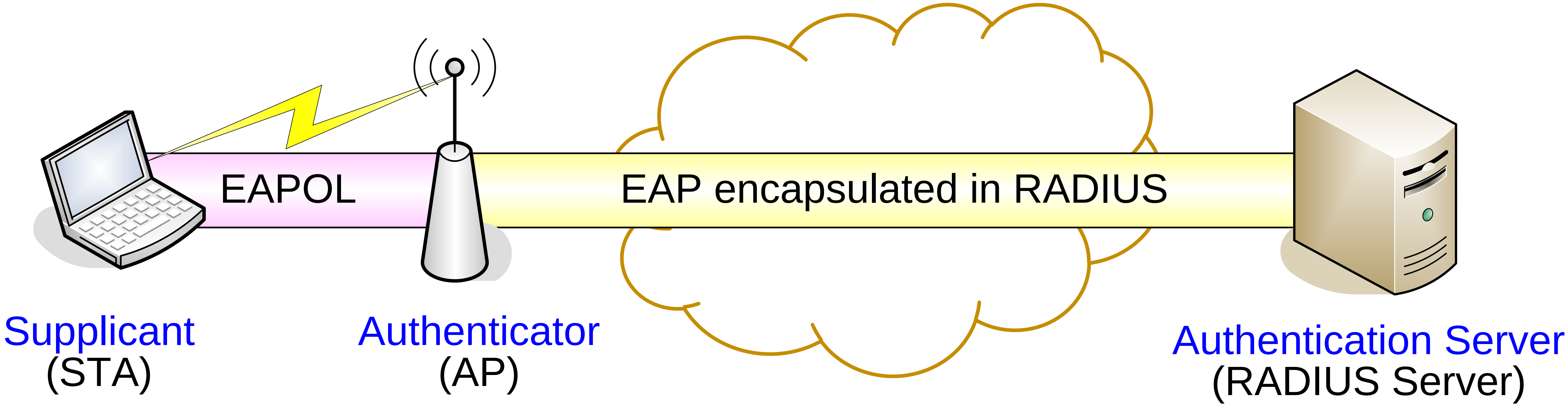

EAP-Request / Identity
Peer
EAP-Response / Identity
EAP Server
EAP-TLS-Request (start)
EAP-TLS-Response:
ClientHello
EAP-TLS-Request:
ServerHello, Certificate, ServerKeyExchange,
CertificateRequest, ServerHelloDone
EAP-TLS-Response:
Certificate, ClientKeyExchange, CertificateVerify,
ChangeCipherSpec, Finished
EAP-TLS-Request:
ChangeCipherSpec, Finished
EAP-TLS-Response (empty)
EAP-Success

Terminology

			
TLS	Client		Server
EAP/AAA	Peer	Authenticator	EAP server / Backend authentication server
802.1X	Supplicant	Authenticator	Authentication server (AS)
RADIUS		Network access server (NAS)	RADIUS server
802.11	STA	Access point (AP)	

Confused yet?

EAP encapsulation

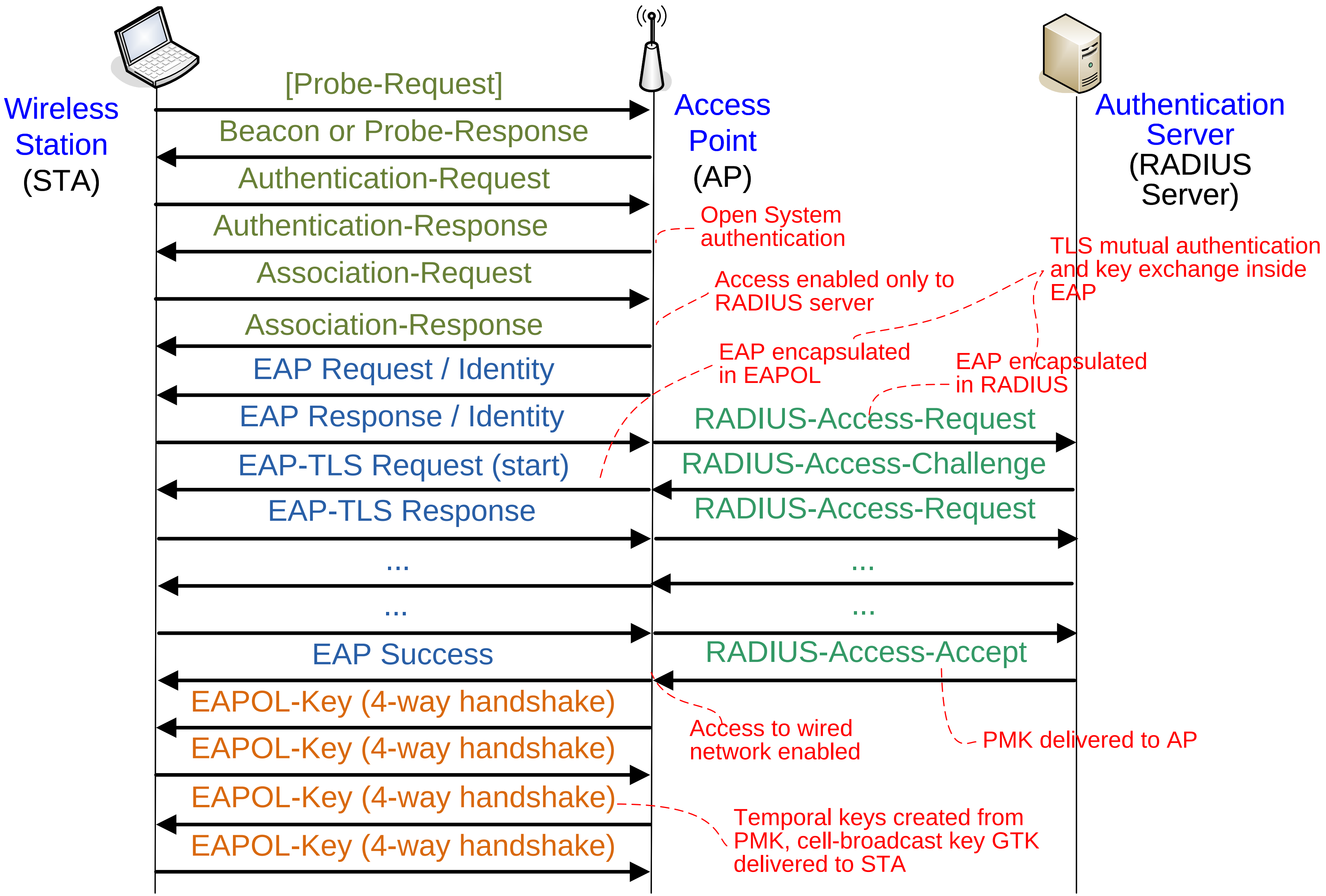


- On the wire network, EAP is encapsulated in RADIUS attributes
- On the 802.11 link, EAP is encapsulated in EAP over LAN (EAPOL)
- In 802.1X, AP is a pass-through device: it copies most EAP messages without reading them

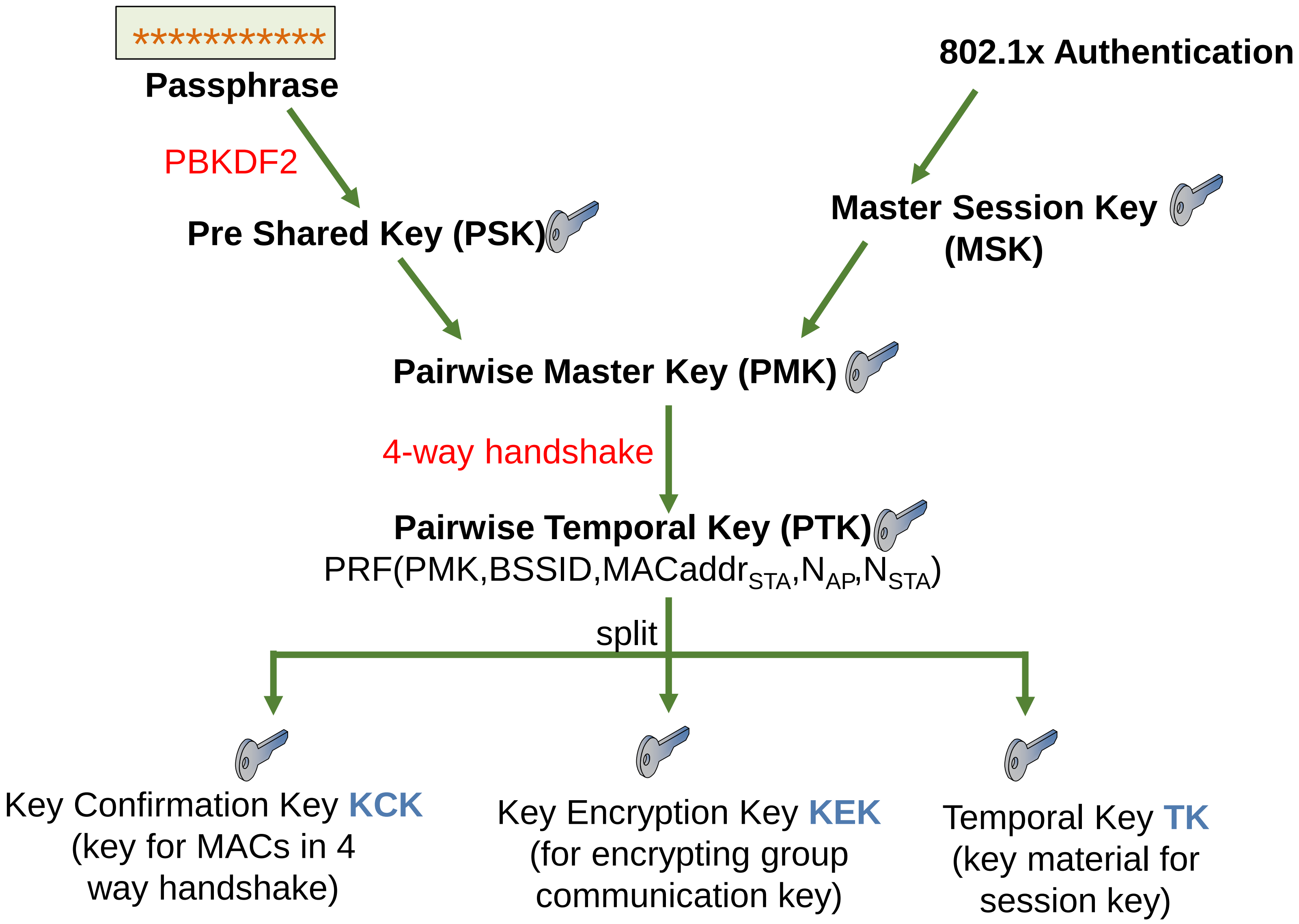
RADIUS

- Remote access dial-in user service (RADIUS)
  - Originally for centralized authentication of dial-in users in distributed modem pools
- Defines messages between the network access server (NAS) and authentication server:
  - NAS sends Access-Request
  - Authentication server responds with Access-Challenge, Access-Accept or Access-Reject
- In WLAN, AP is the NAS
- EAP is encapsulated in RADIUS Access-Request and Access-Challenge; as many rounds as necessary
- RADIUS has its own security protocol based on shared keys between the endpoints (AP and server)

EAP Protocol in action



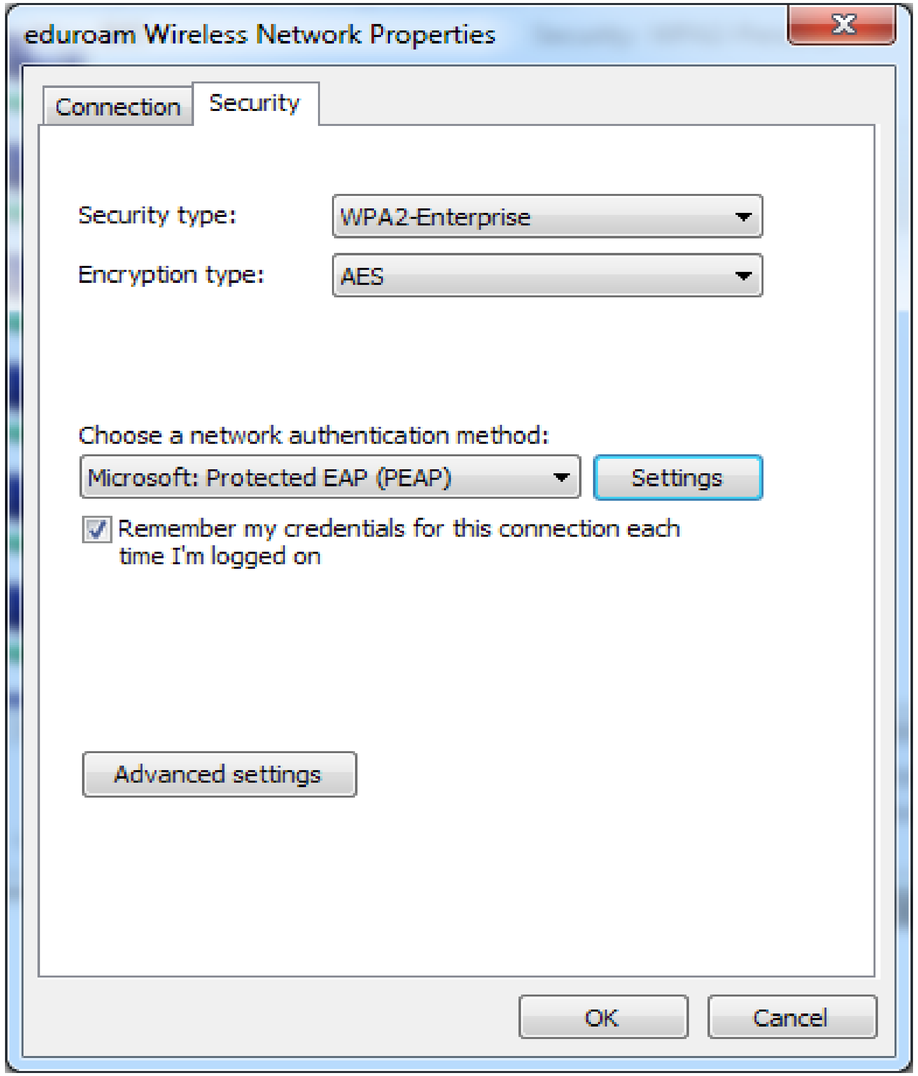
RSN Key Hierarchy



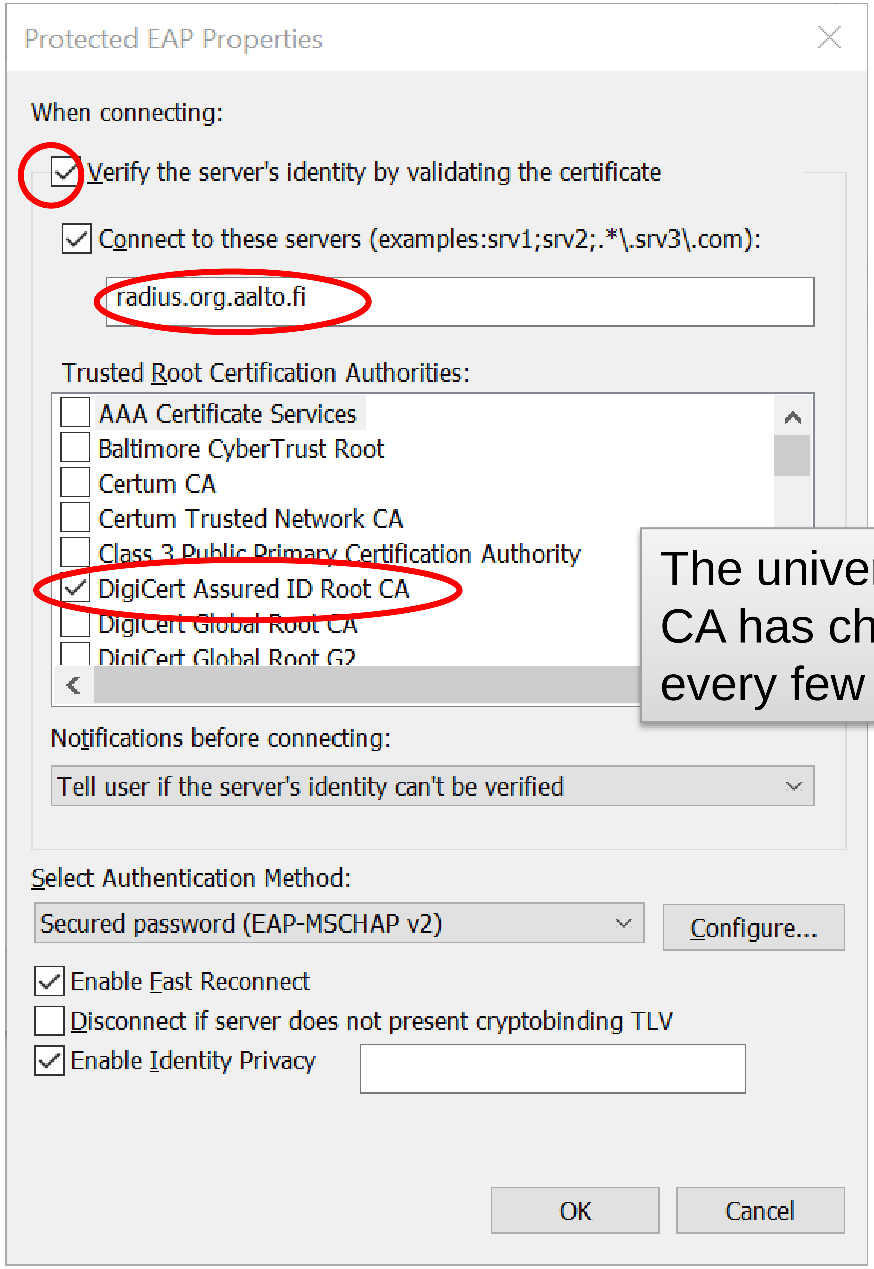
Eduroam

- Eduroam is a federation for wireless roaming between educational institutions
  - User is registered at the home university, which has a RADIUS server (AAA)
  - National educational and research network (NREN), e.g. Funet, operates a national roaming broker
  - National brokers are connected to a regional broker for international roaming
- EAP authentication: user's home institution determines the EAP authentication method
  - Aalto uses PEAP
- Users identified by NAI: username@realm
  - NAI for Aalto users: firstname.lastname@aalto.fi (earlier also username@aalto.fi, seems to be no longer in use)
  - In PEAP, the outer NAI only needs to have only correct realm, but Aalto seems to require the username to be correct as well (should test if this is still the case)

Eduroam



- Eduroam uses WPA2 with AES encryption
- Aalto RADIUS server is radius.org.aalto.fi
- Aalto user's NAI looks like the email address, e.g. first.last@aalto.fi
- Aalto users are authenticated with EAP-PEAP —Microsoft's proprietary EAP method with TLS for the server authentication and password for the client
- Roaming between universities enabled by federation between RADIUS servers



The university CA has changed every few years

Eduroam

- IN EAP-TLS and PEAP, the client authenticates the RADIUS server based on a certificate
- To verify the certificate, the client needs to know:
  - trusted CAs
  - name of the RADIUS server
- On many clients, any commercial CA and any name in the certificate is accepted → anyone with any commercial certificate can set up a fake AP and pretend to be the RADIUS server