

Network Security: WLAN Security

Mohit Sethi

Ericsson, Finland

Aalto University, Finland

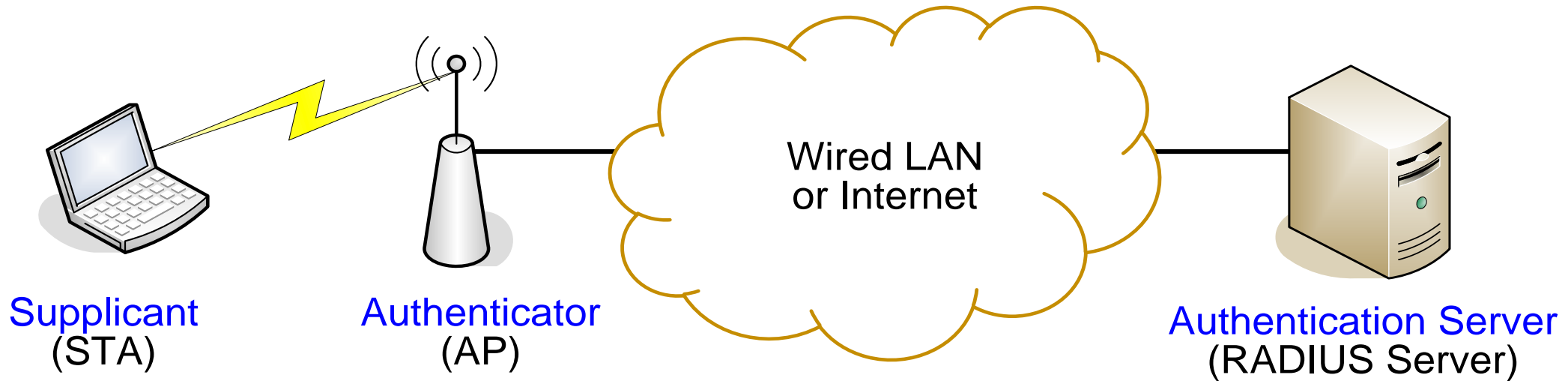
WLAN Security - Outline

- Part 1:
 - WLAN Standards and Components
 - Joining Open WLAN
 - WPA2-PSK and four-way handshake
- Part 2:
 - WPA 3: Opportunistic Wireless Encryption (Enhanced Open)
 - WPA 3: Password Authenticated Key Exchange (PAKE : Dragonfly)
- Part 3:
 - Enterprise security - EAP

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

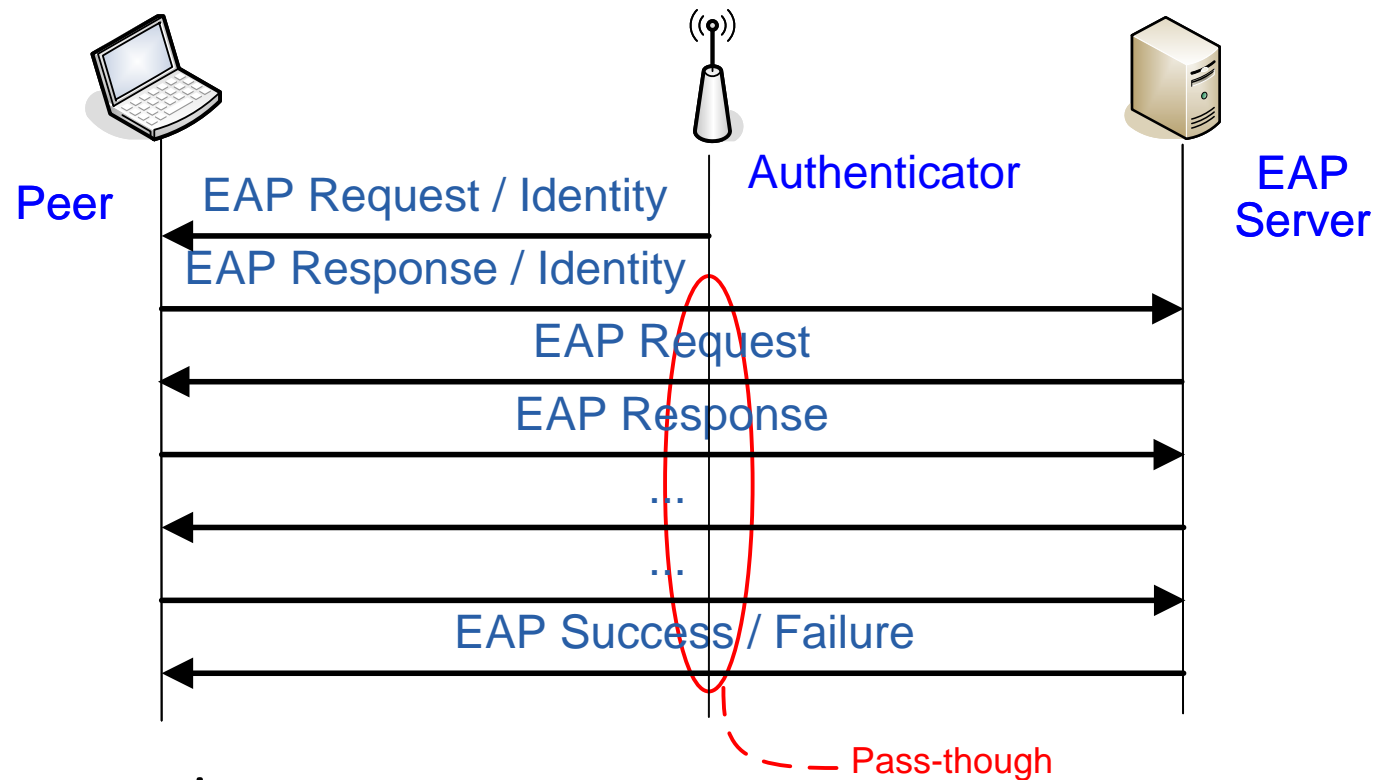


- **Supplicant** wants to access the wired network via the AP
- **Authentication Server (AS)** authenticates the supplicant
- **Authenticator** enables network access for the supplicant after successful authentication

EAP

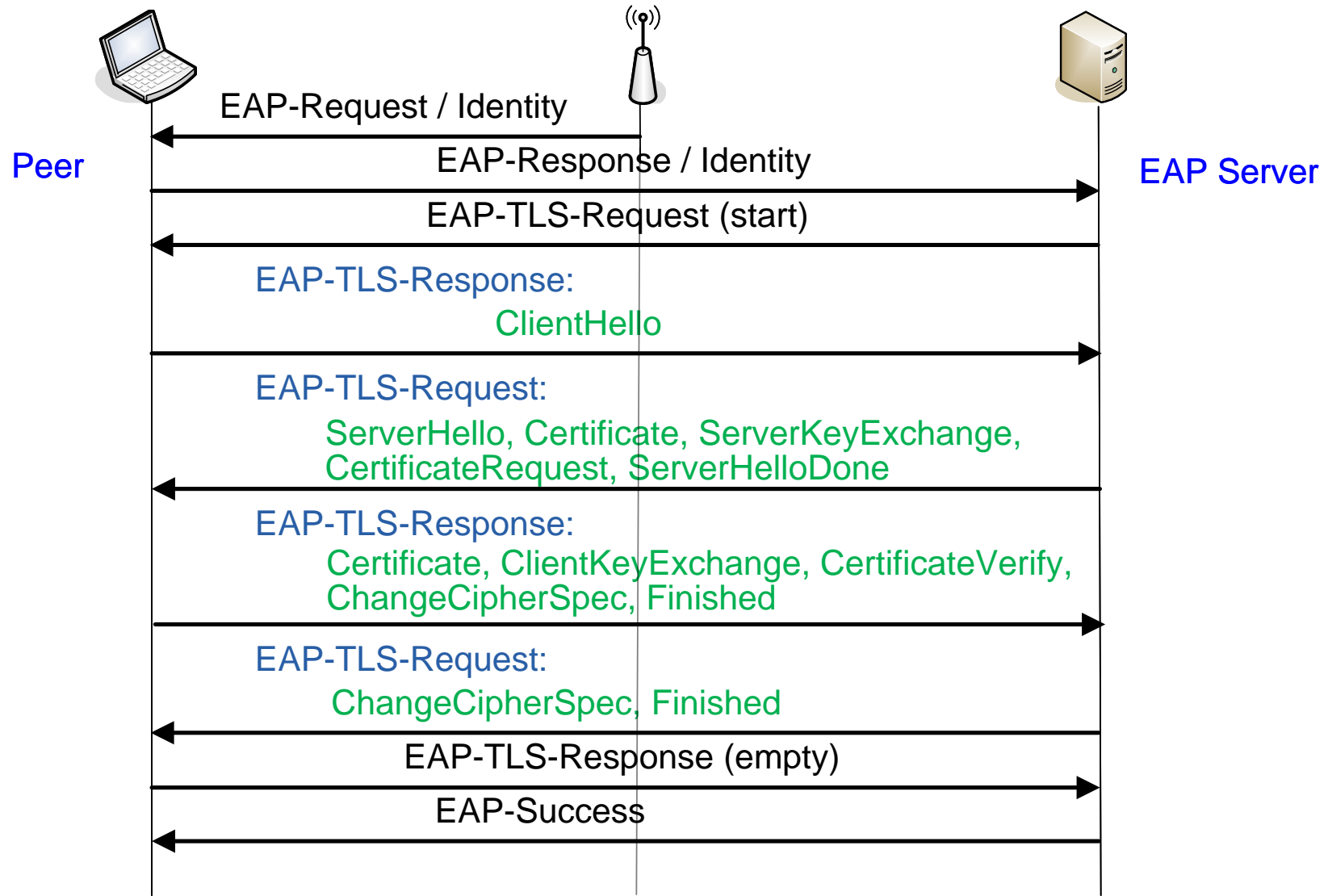
- **Extensible authentication protocol (EAP)** defines generic authentication message formats: **Request, Response, Success, Failure**
- Security is provided by the **authentication protocol** carried inside **EAP, not by EAP itself**
- EAP supports many authentication protocols: EAP-TLS, PEAP, EAP-SIM, ...
- 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

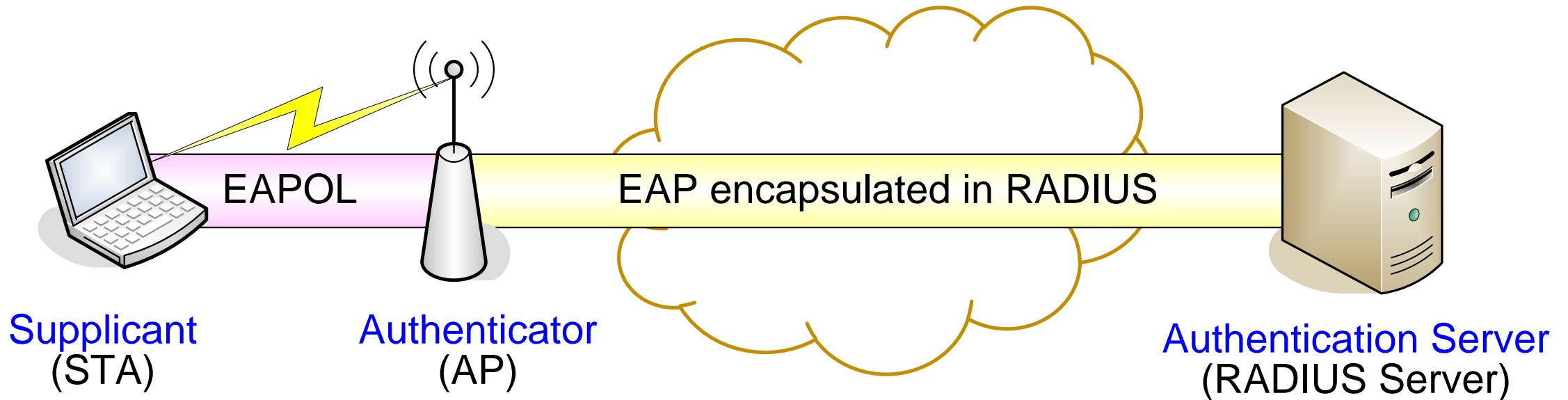
EAP-TLS



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

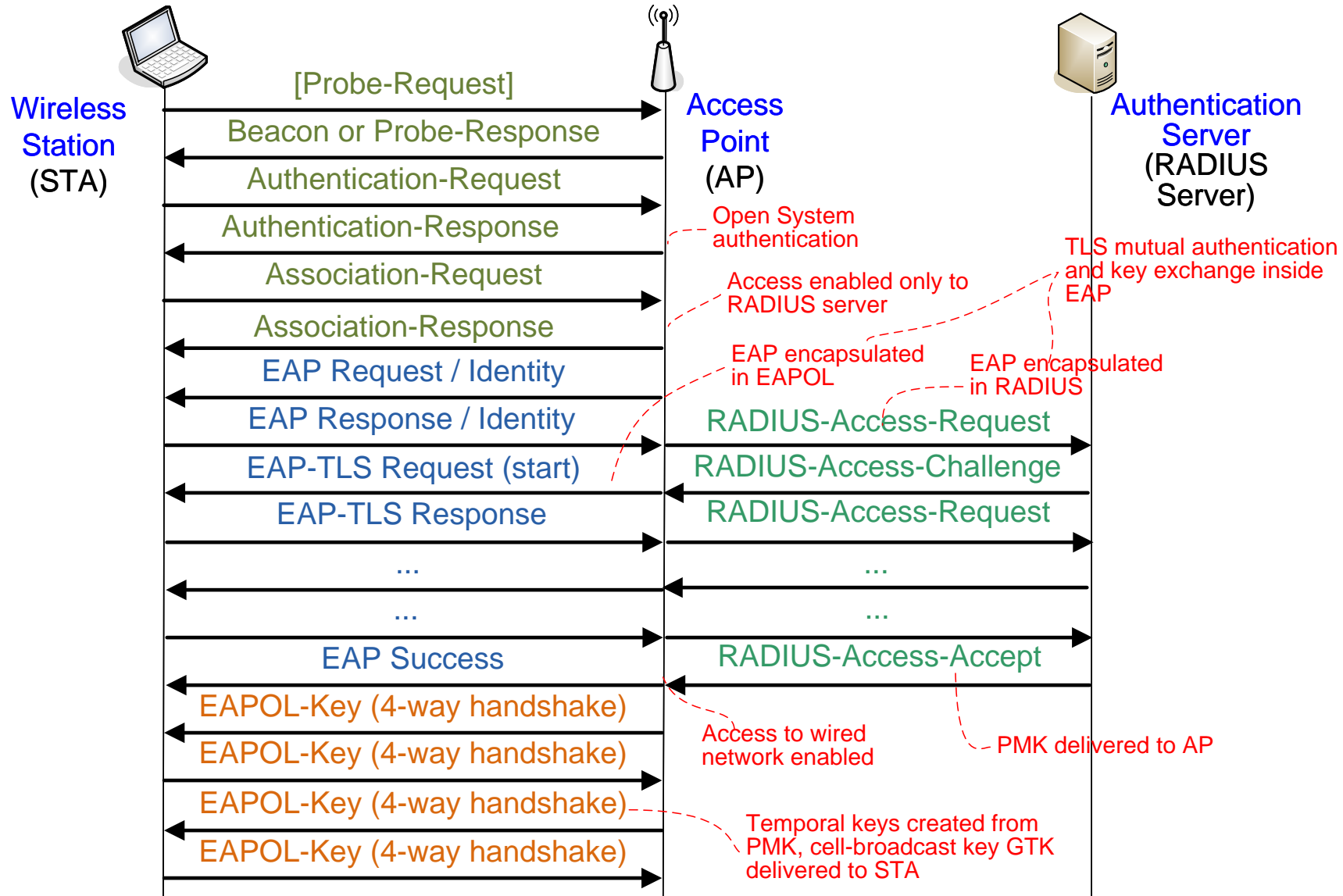


- On the wire network, EAP is encapsulated in **RADIUS** attributes
- On the 802.11 link, EAP is encapsulated in EAP over LAN (**EAPOL**)
- In 802.1X, AP is a **pass-through device**: it copies most EAP messages without reading them

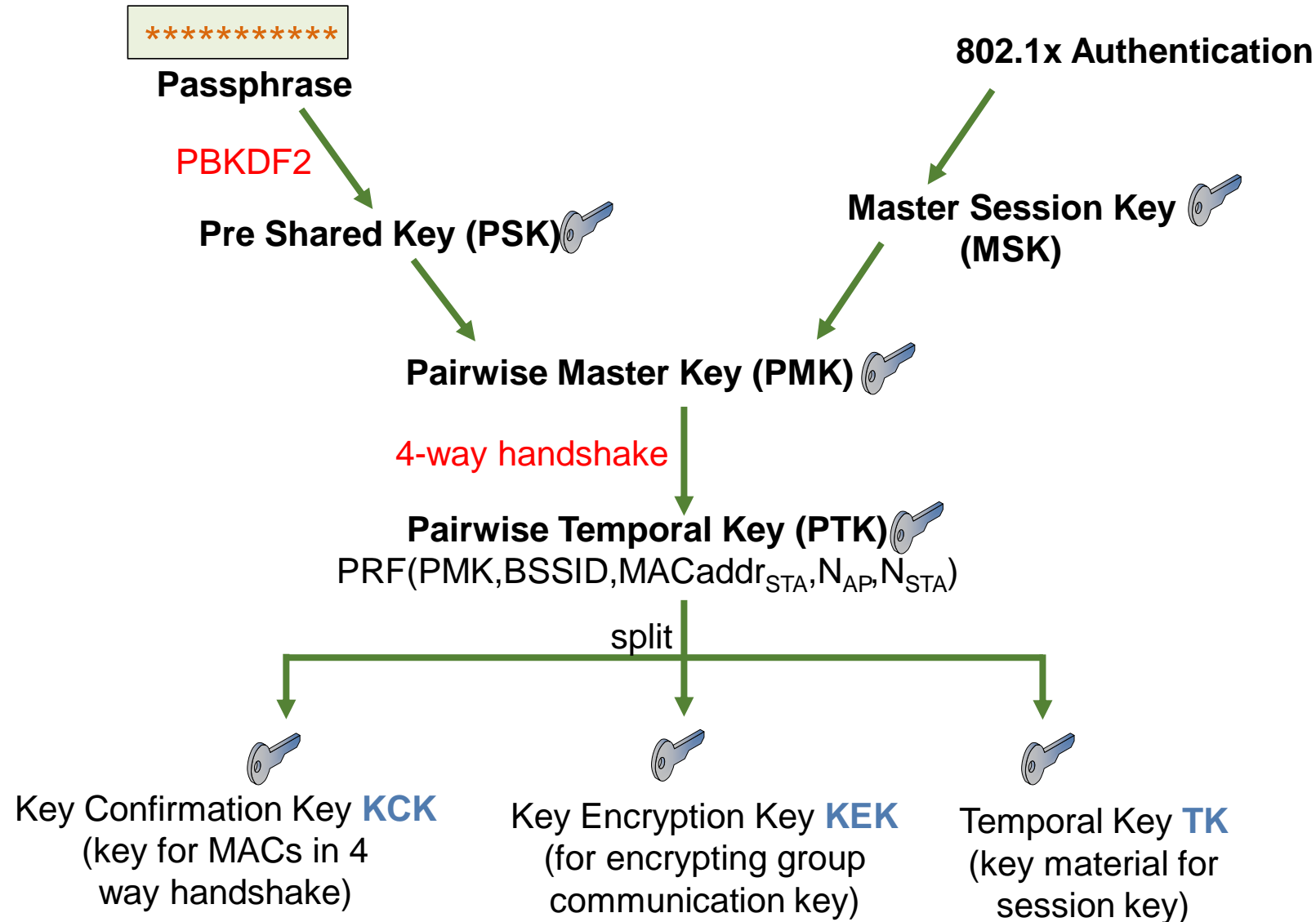
RADIUS

- 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



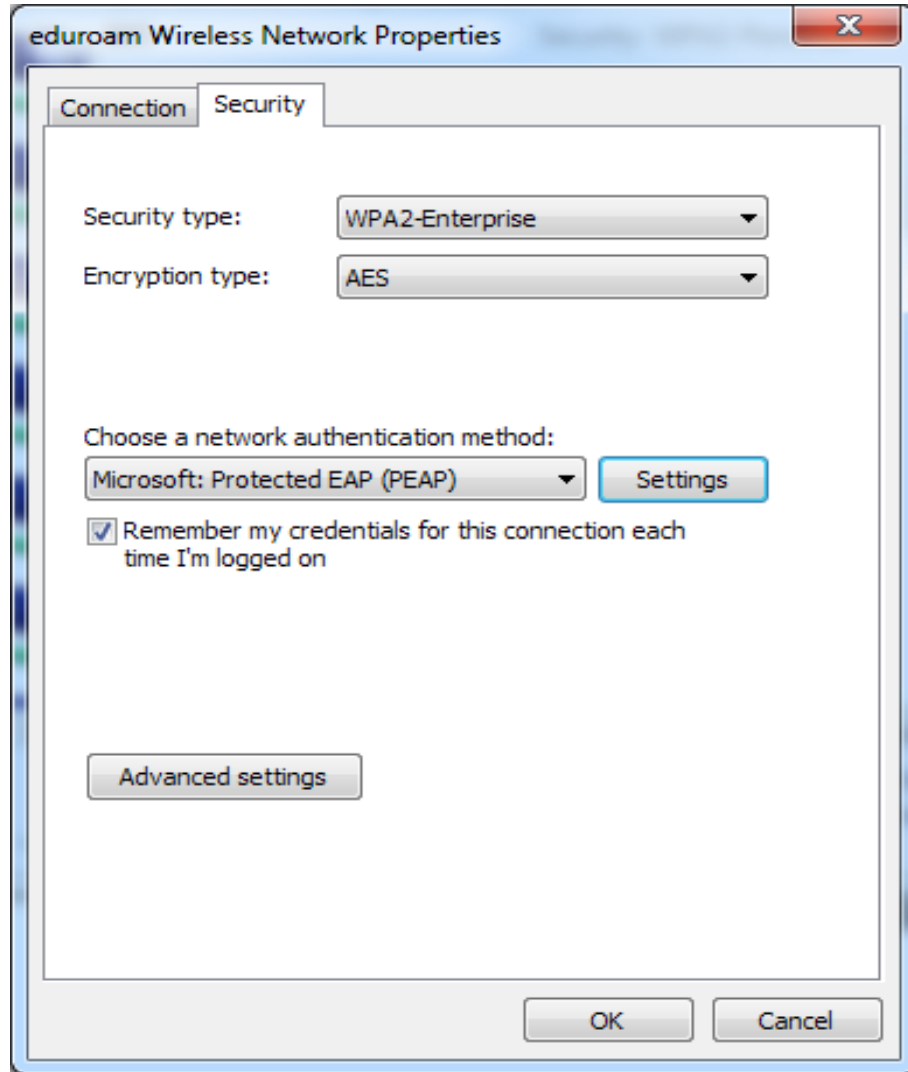
RSN Key Hierarchy



Eduroam

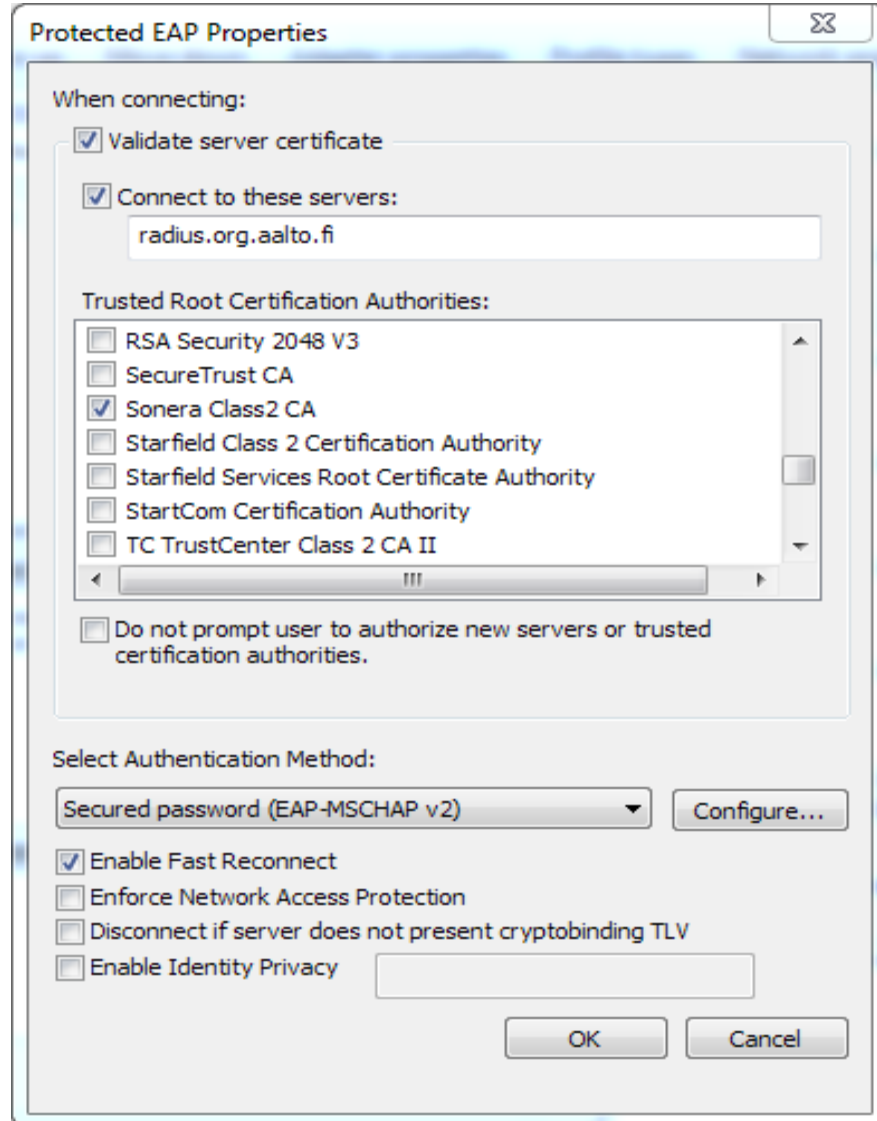
- **Eduroam** is a federation for wireless roaming between educational institutions
 - User is registered at the home university, which has a RADIUS server (AAAA)
 - National educational and research network (NREN), e.g. Funet, operates a national roaming broker
 - National brokers are connected to a 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

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