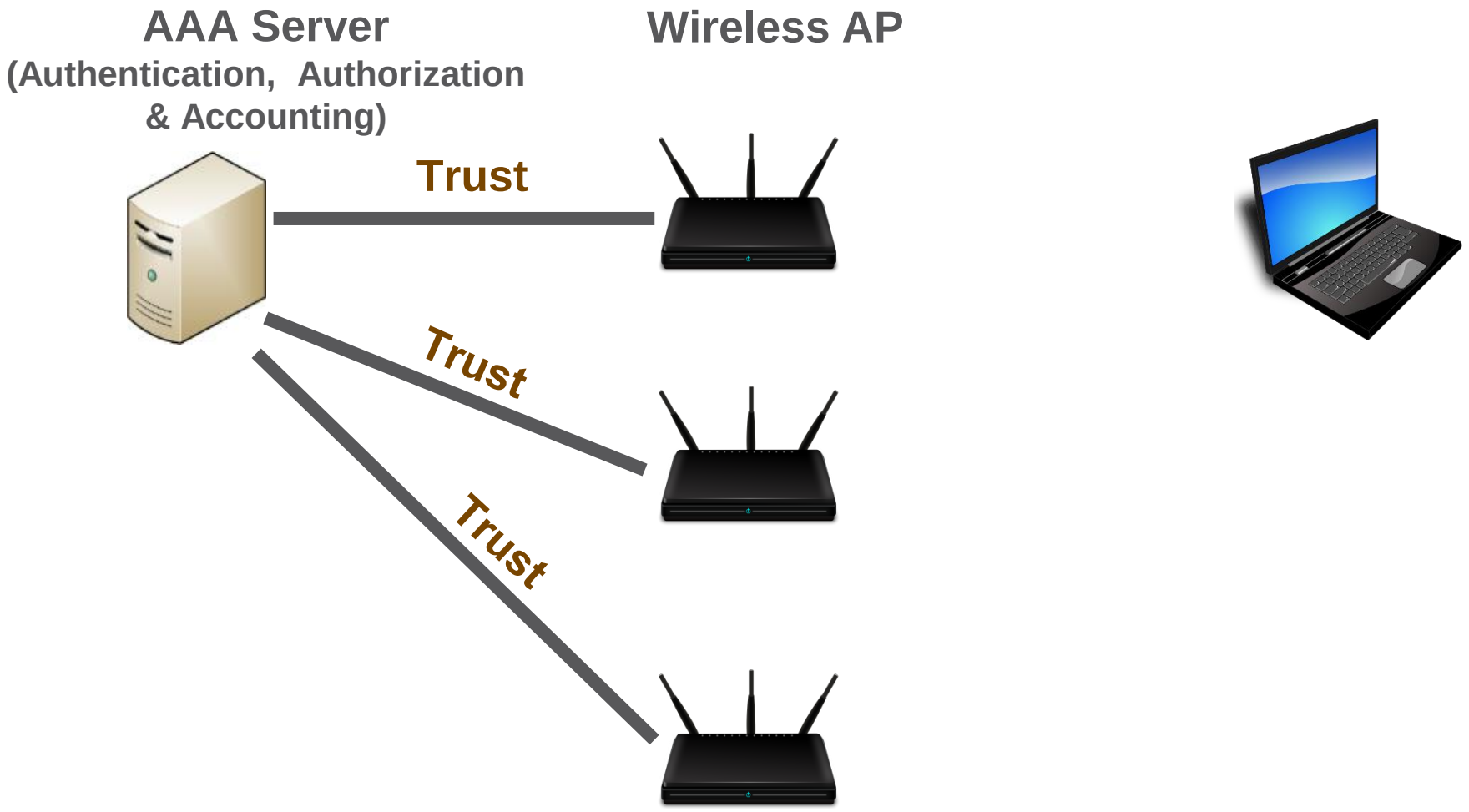
Aalto University

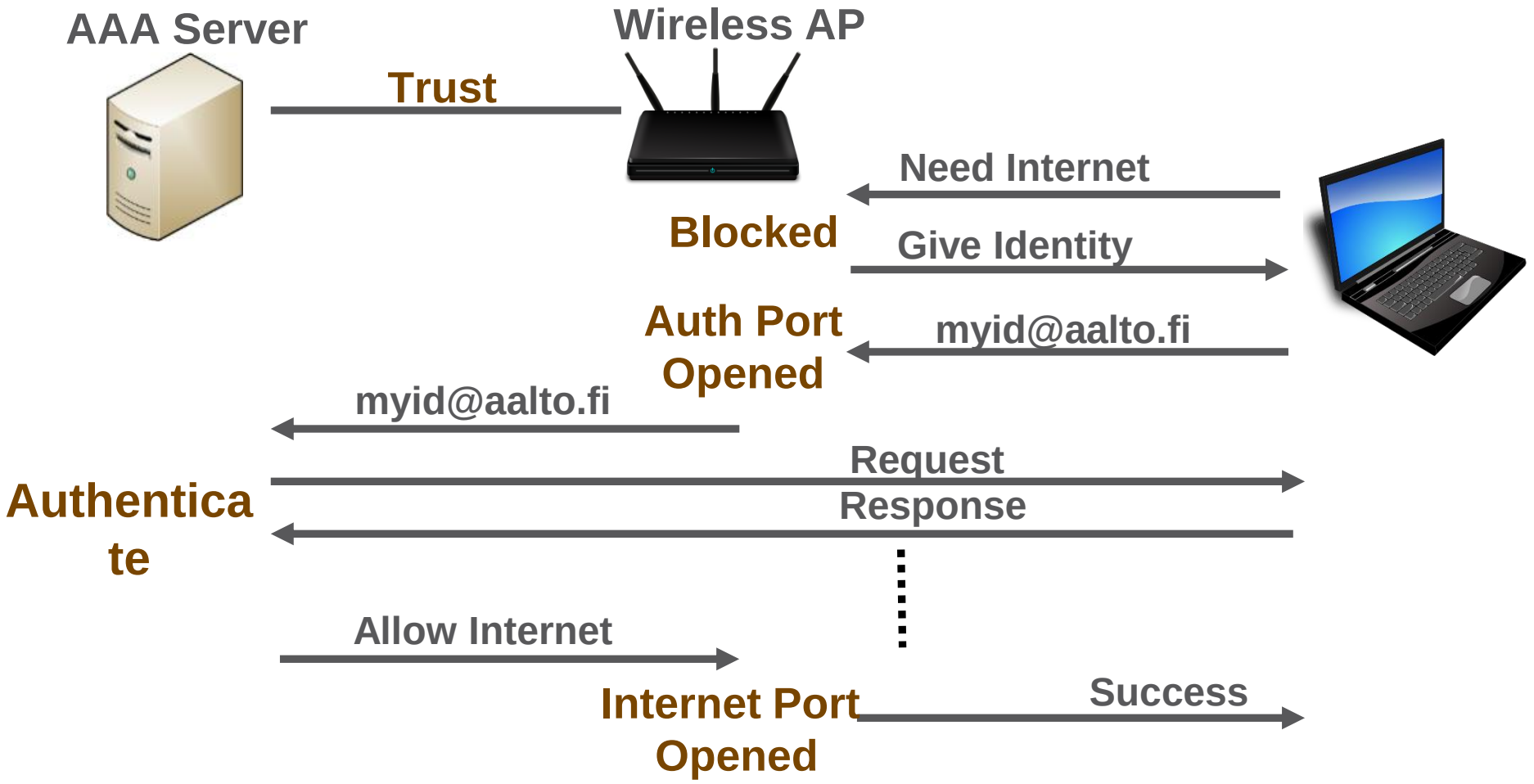
Network Security: WLAN Security: EAP-NOOB

Mohit Sethi
Ericsson, Finland
Aalto University, Finland

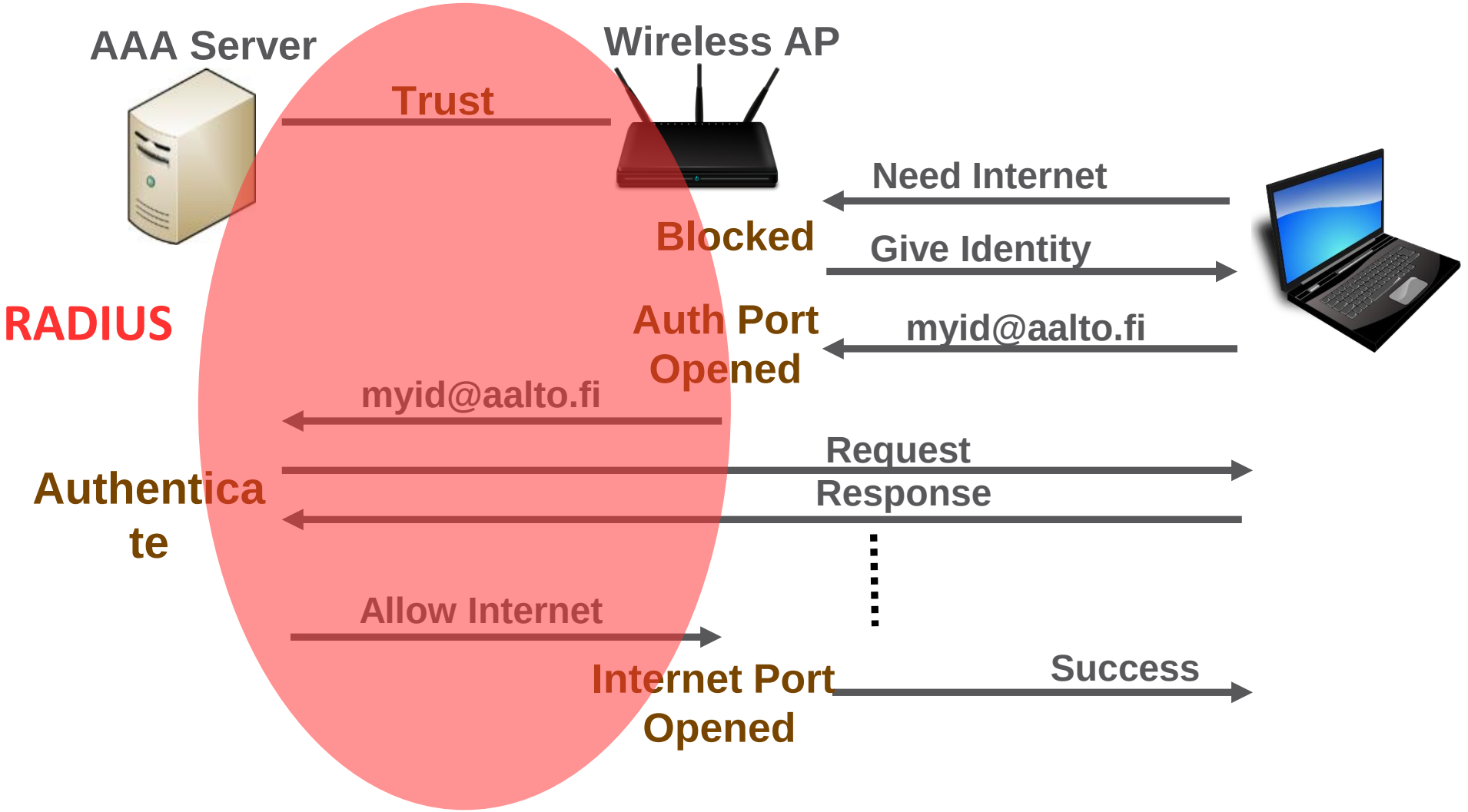
EAP recap


AAA Server
(Authentication, Authorization
& Accounting)
Wireless AP
Trust
Trust
Trust

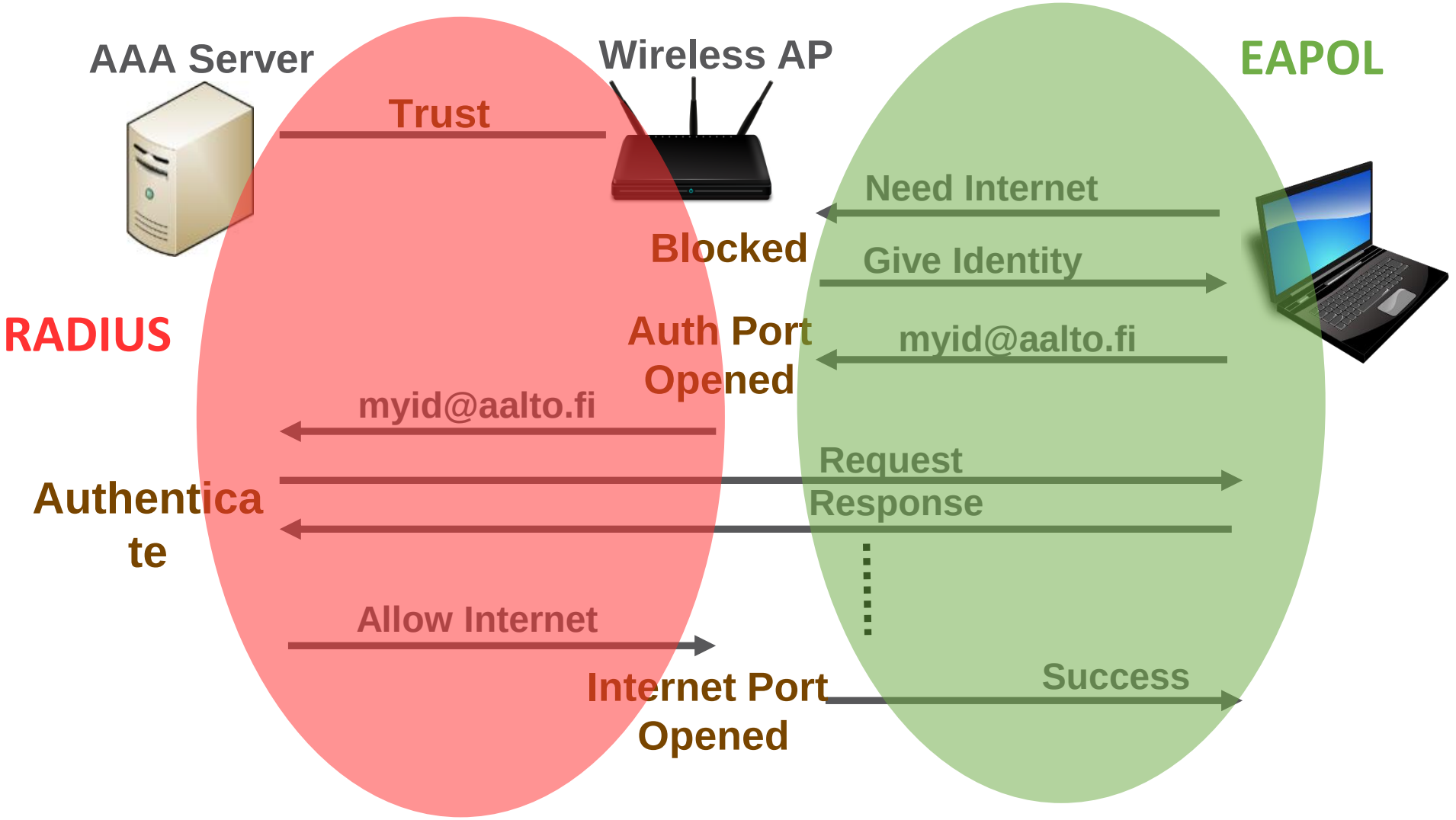
EAP recap


AAA Server
Wireless AP
Trust
Need Internet
Blocked
Give Identity
Auth Port Opened
myid@aalto.fi
myid@aalto.fi
Request
Authenticate
Response
Allow Internet
Internet Port Opened
Success

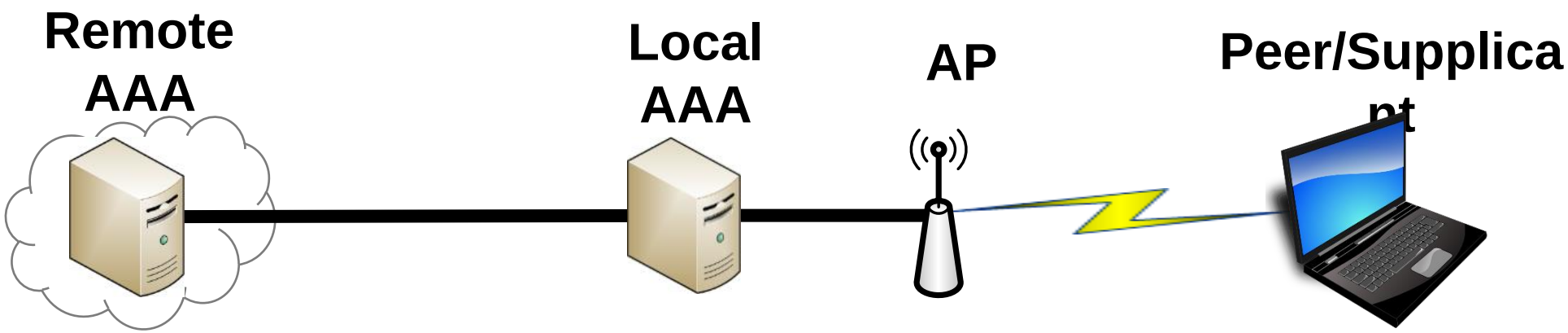
EAP recap


AAA Server
Wireless AP
Trust
Need Internet
Blocked
Give Identity
RADIUS
Auth Port Opened
myid@aalto.fi
myid@aalto.fi
Request
Authentica te
Response
Allow Internet
Internet Port Opened
Success

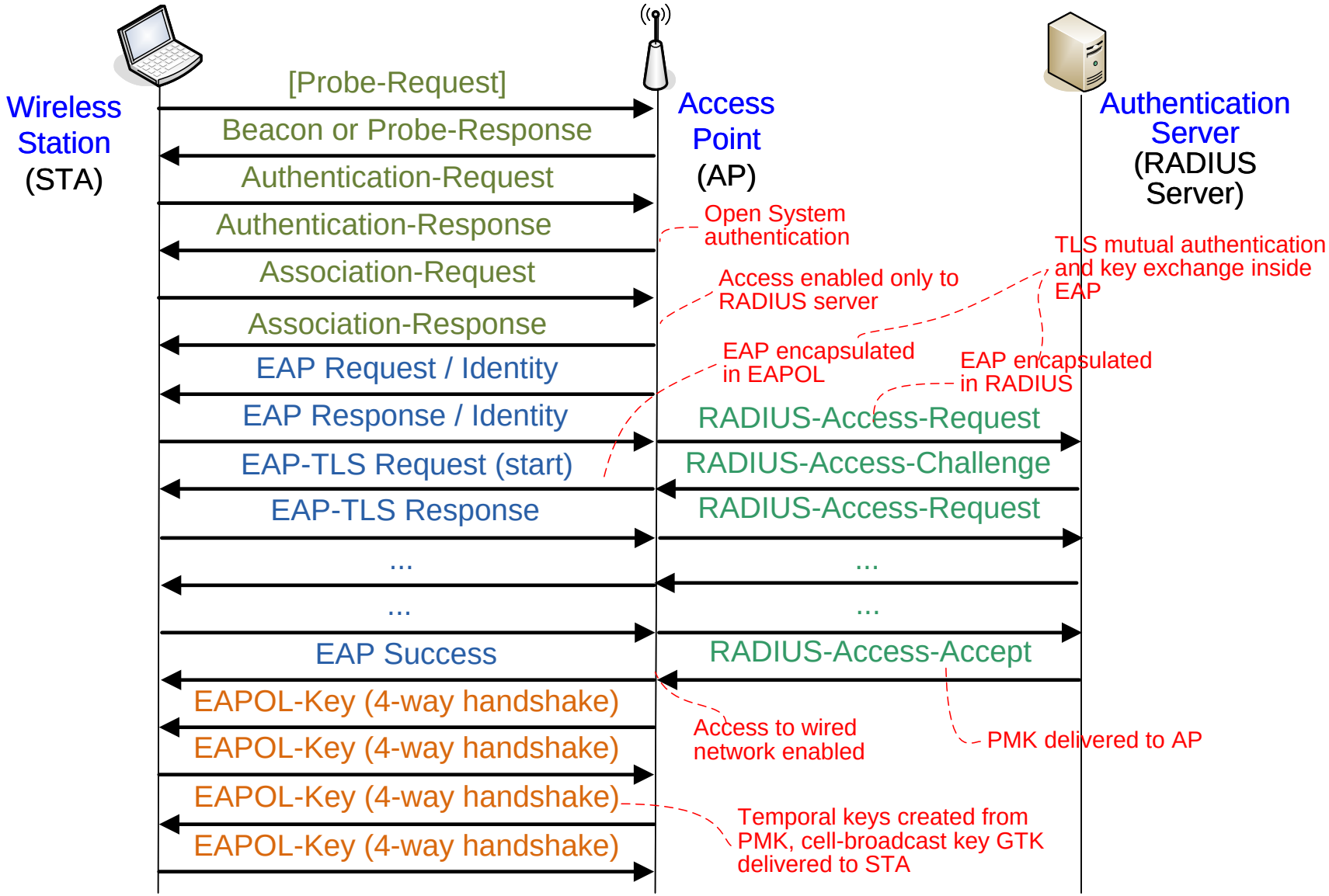
EAP recap


AAA Server
Wireless AP
EAPOL
Trust
Need Internet
Blocked
Give Identity
RADIUS
Auth Port Opened
myid@aalto.fi
myid@aalto.fi
Request
Authentica te
Response
Allow Internet
Internet Port Opened
Success

EAP



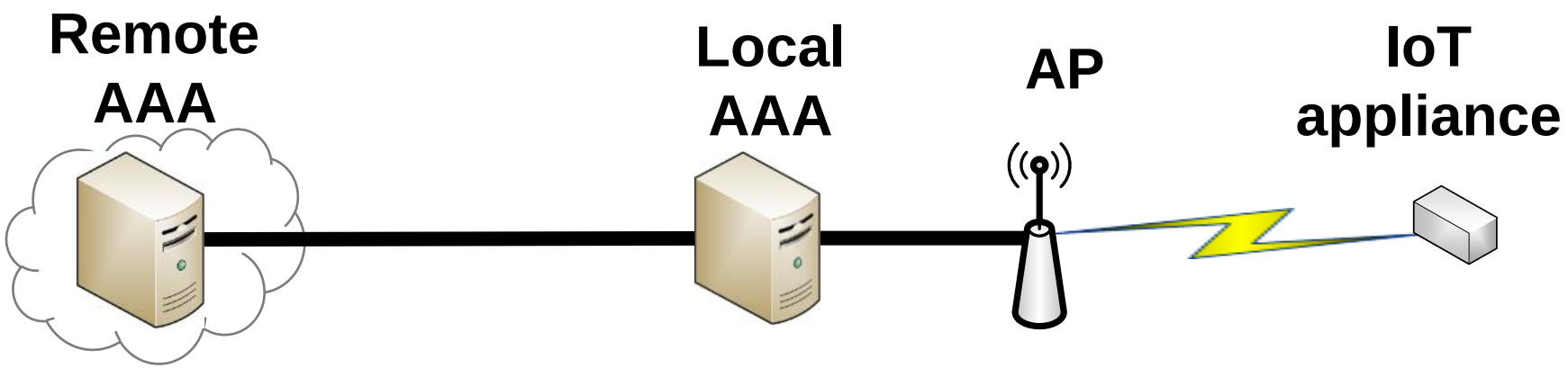
EAP protocol in action



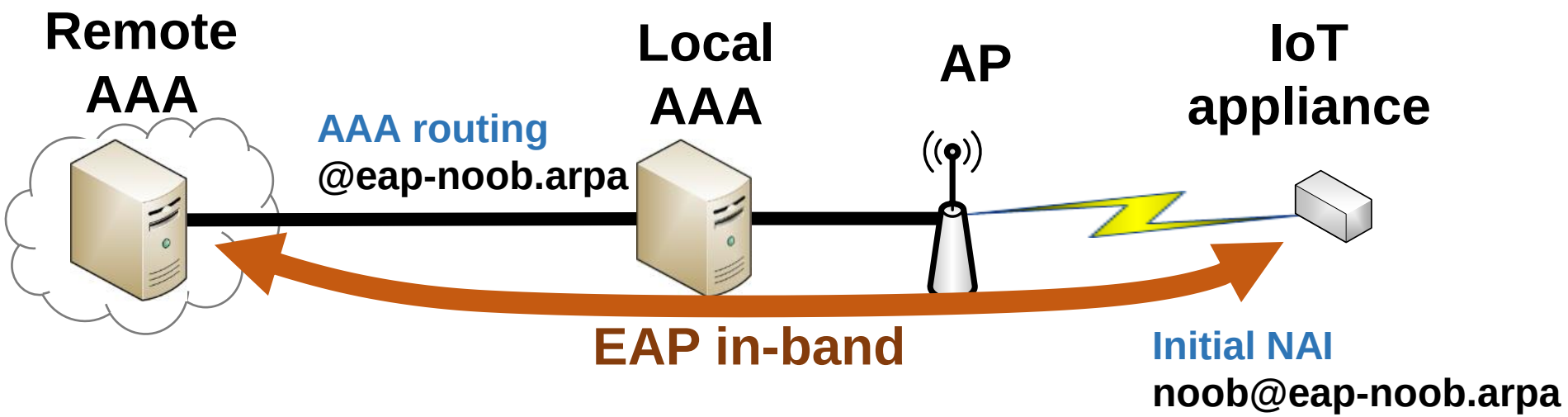
EAP-NOOB

- Cloud-connected IoT appliance
- New IoT appliance has no, no credentials for cloud or Wi-Fi
- Need to:
  - connect the device to access network
  - register the device to AAA/cloud server
  - EAP-NOOB does both
- Security from a single user-assisted out-of-band message between peer device and AAA server

EAP-NOOB - Architecture

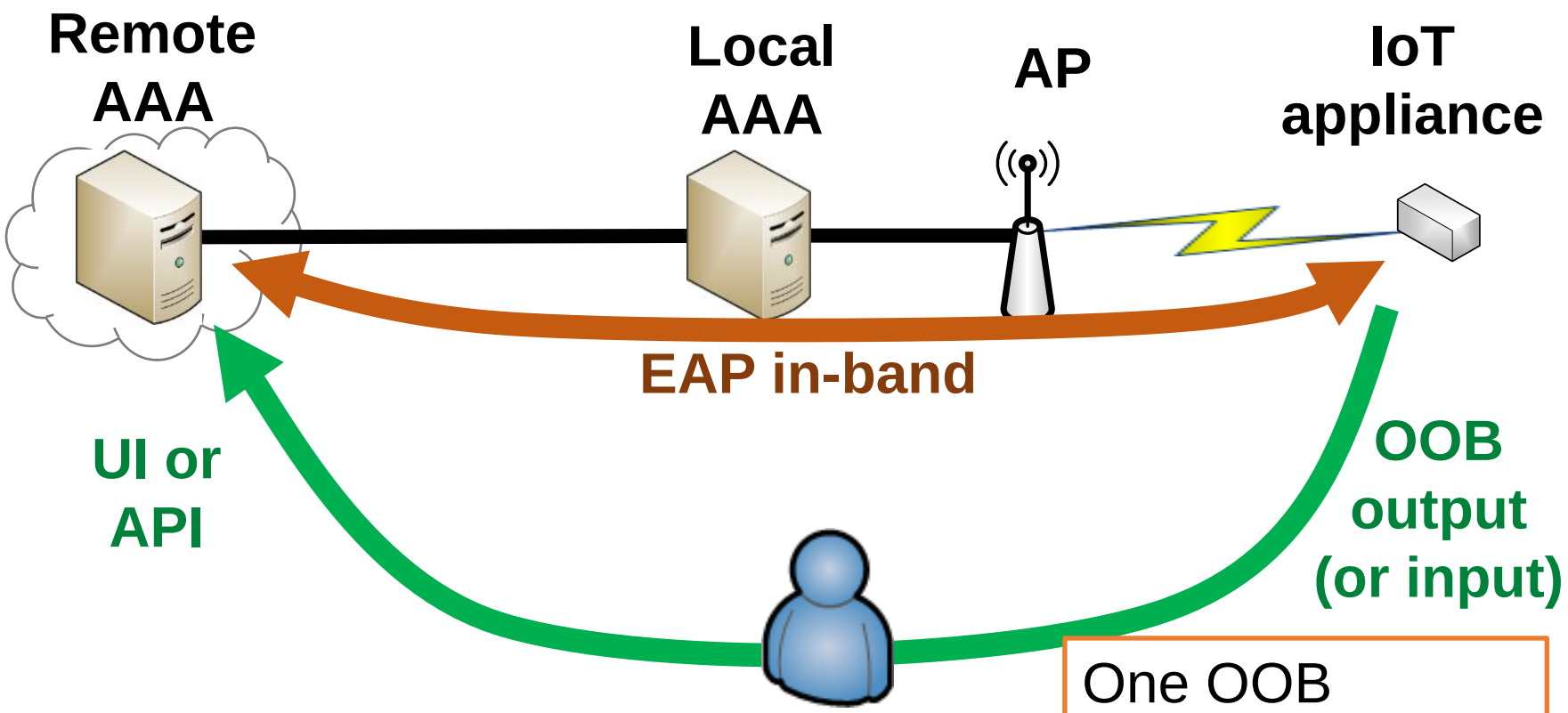


EAP-NOOB - Architecture



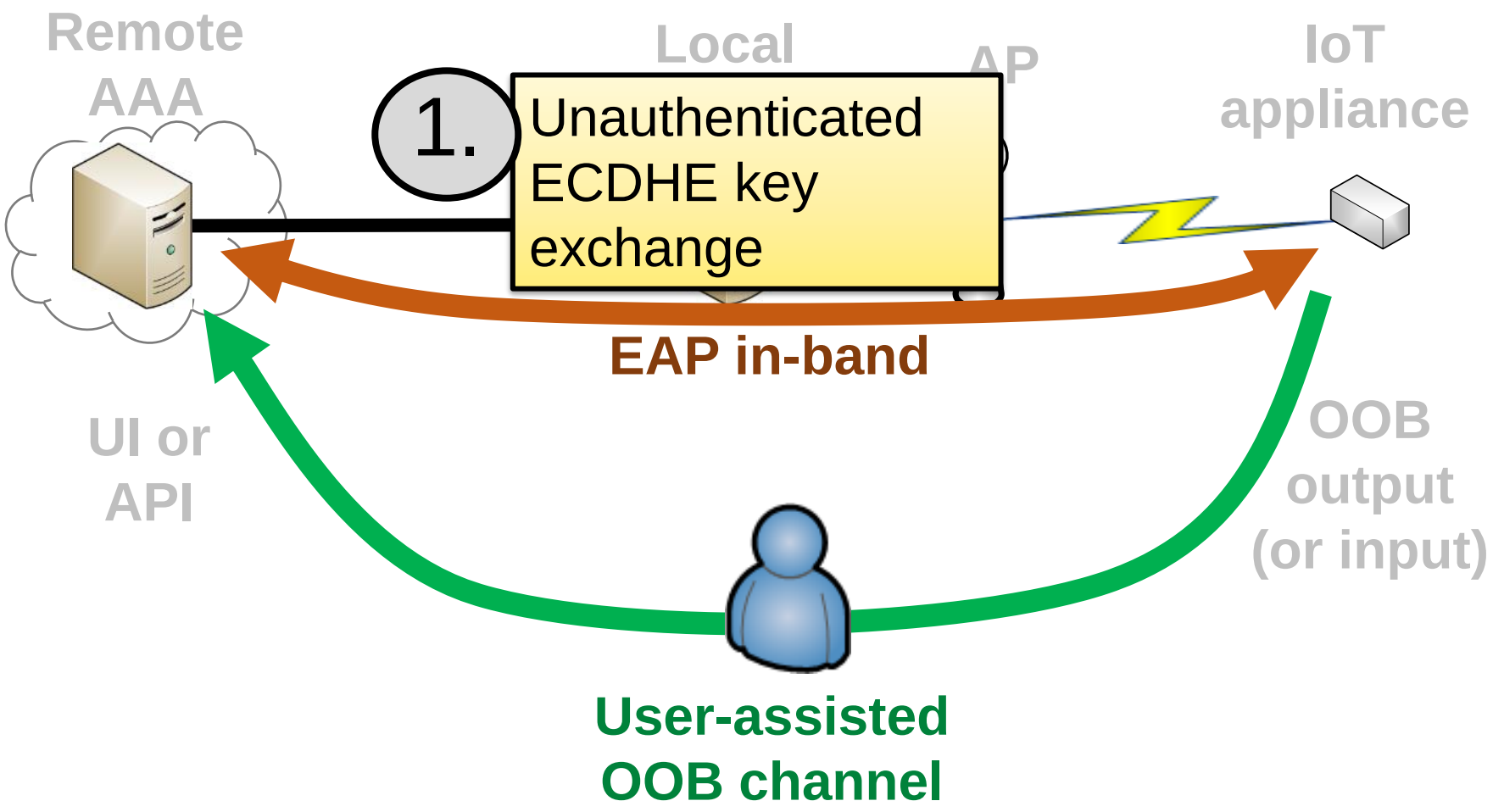
EAP tunnel and AAA routing enable in-band communication with the authentication server *before* the device is registered

EAP-NOOB - Architecture

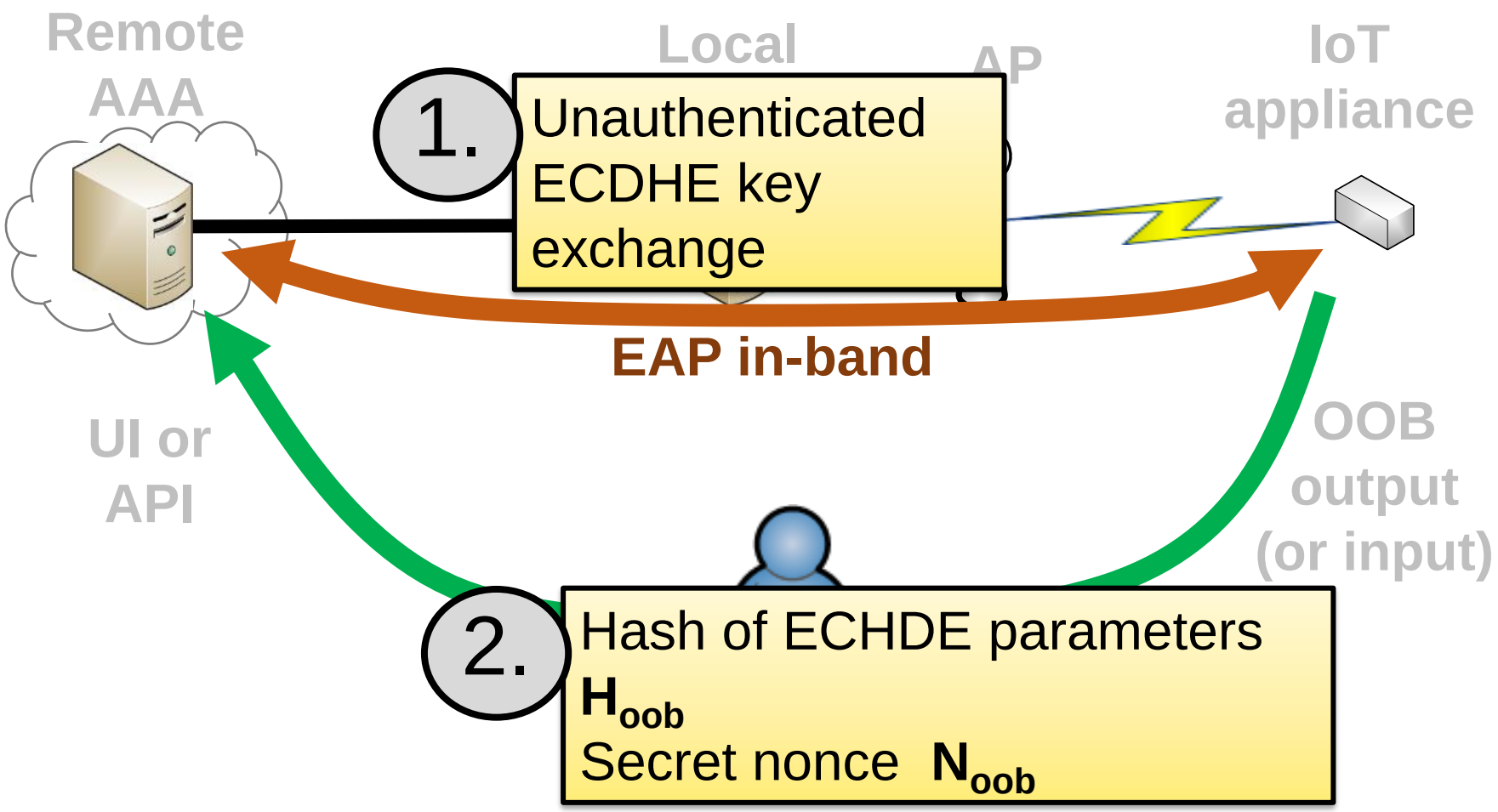


One OOB message in one direction, both directions supported

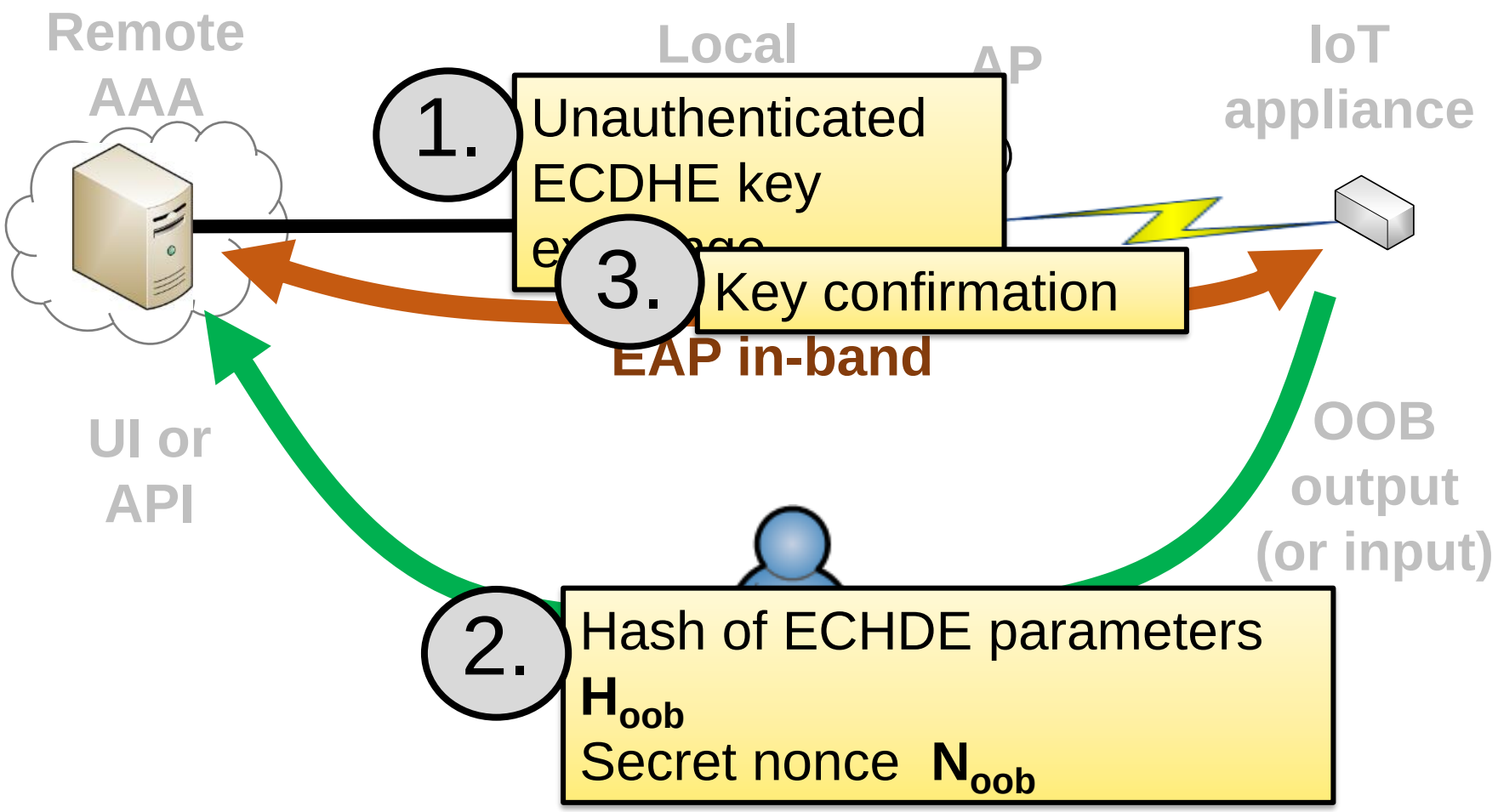
EAP-NOOB - Architecture



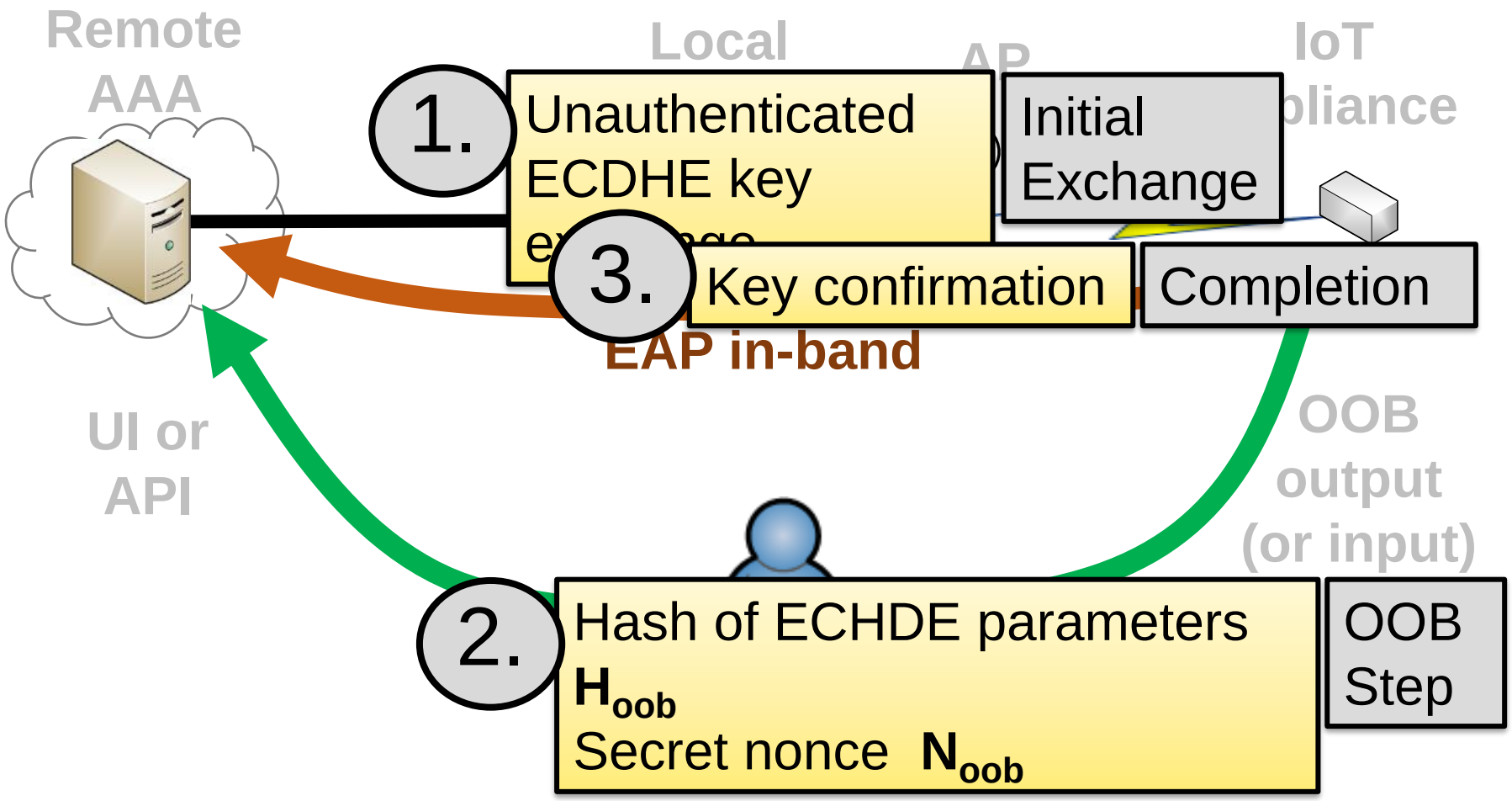
EAP-NOOB - Architecture



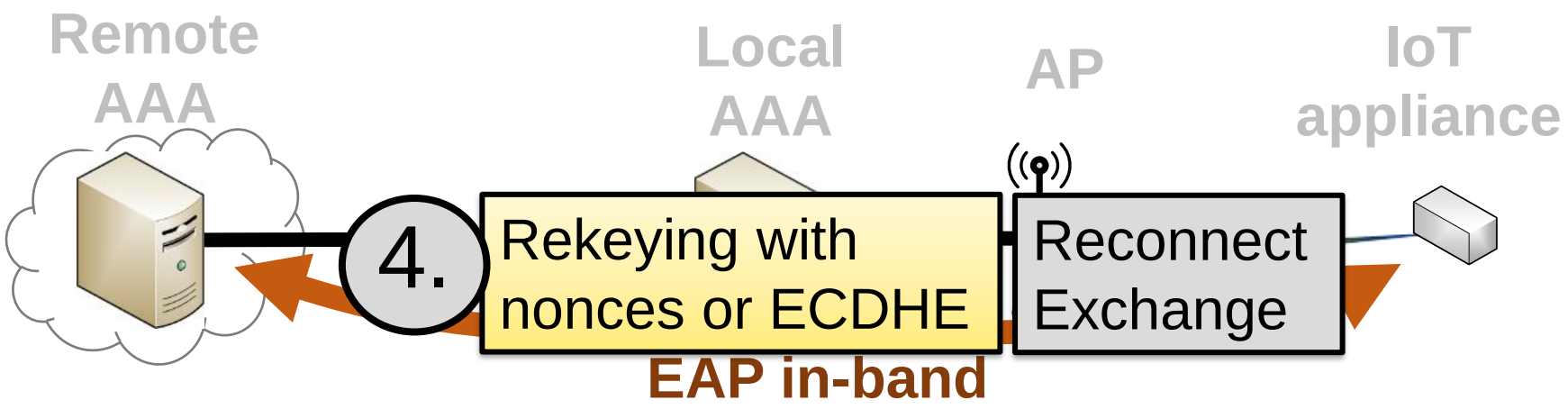
EAP-NOOB - Architecture



EAP-NOOB - Architecture



EAP-NOOB - Architecture



After successful OOB step, persistent association is created. OOB step is *not* repeated

EAP-NOOB – High level protocol overview

- Protocol for new devices:
  1. Initial exchange in-band: ECDH over EAP
  2. Out-of-band step: one user-assisted message, in either direction
  3. Completion exchange in-band: authentication and key confirmation over EAP

- OOB step should not be not repeated. Reconnect exchange for rekeying, algorithm upgrade etc.

EAP-NOOB - Architecture

- No preconfigured credentials or other relation for AAA server or peer device
- Peer with no input UI may probe all wireless networks around it for EAP-NOOB support
- Initial exchange and completion are in different EAP conversations to allow OOB step
- Initial NAI is always “noob@eap-noob.arpa”
  - Must configure trust between access network and AAA/cloud server for “@eap-noob.arpa”

EAP-NOOB - Architecture

- Authentication protocol details (with OOB from peer to server):
  - Initial ECDH without authentication
  - **OOB message** contains **secret N_{oob}** and **fingerprint H_{oob}**
  - **MAC with N_{oob} authenticates ECDH key in both directions**
  - Additionally, **H_{oob} authenticates ECDH key to AAA server**
  - Knowing N_{oob} authorizes the server and user to take control of the peer device

- OOB channel should protect both secrecy and integrity
  - Double protection: failure of one of these does not cause complete loss of security