Authorizing network access for IoT devices

Mohit Sethi

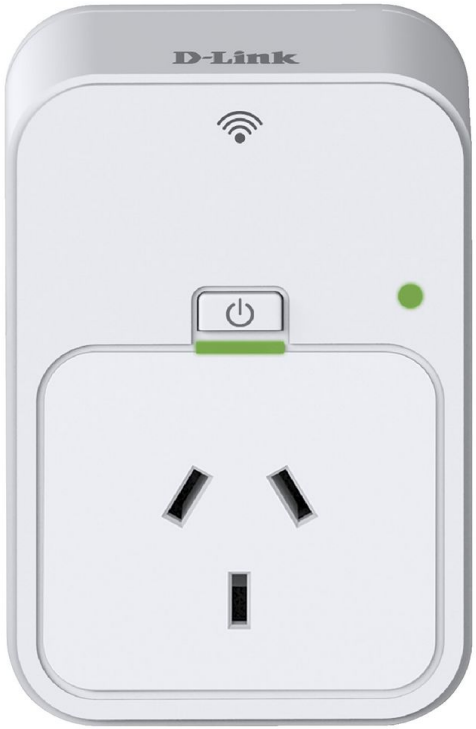
Tuomas Aura

Outline

- Authorizing local network and Internet access for IoT devices
- Cloud-managed network-access authorization
- Bootstrapping security between device and cloud
- EAP-NOOB

Authorizing network access for IoT devices

- New off-the-shelf devices need Internet access
  - for vendor and third-party services in the cloud
  - for software update



Authorizing network access for IoT devices

Two problems:

- Discovery and configuration: which network?
  - For example, need to find the right SSID and cloud server
- Security bootstrapping: identifiers and credentials?
  - For connecting to the network
  - For connecting to the cloud

Authorizing network access for IoT devices

Challenges:

- Limited user interface
- Scalability
- At home, small office, enterprise or industrial environment
  - Clueless users vs. professional admins and support
  - On the other hand, same devices everywhere
- Wi-Fi (WPA-Personal and WPA Enterprise), Zigbee, BTLE

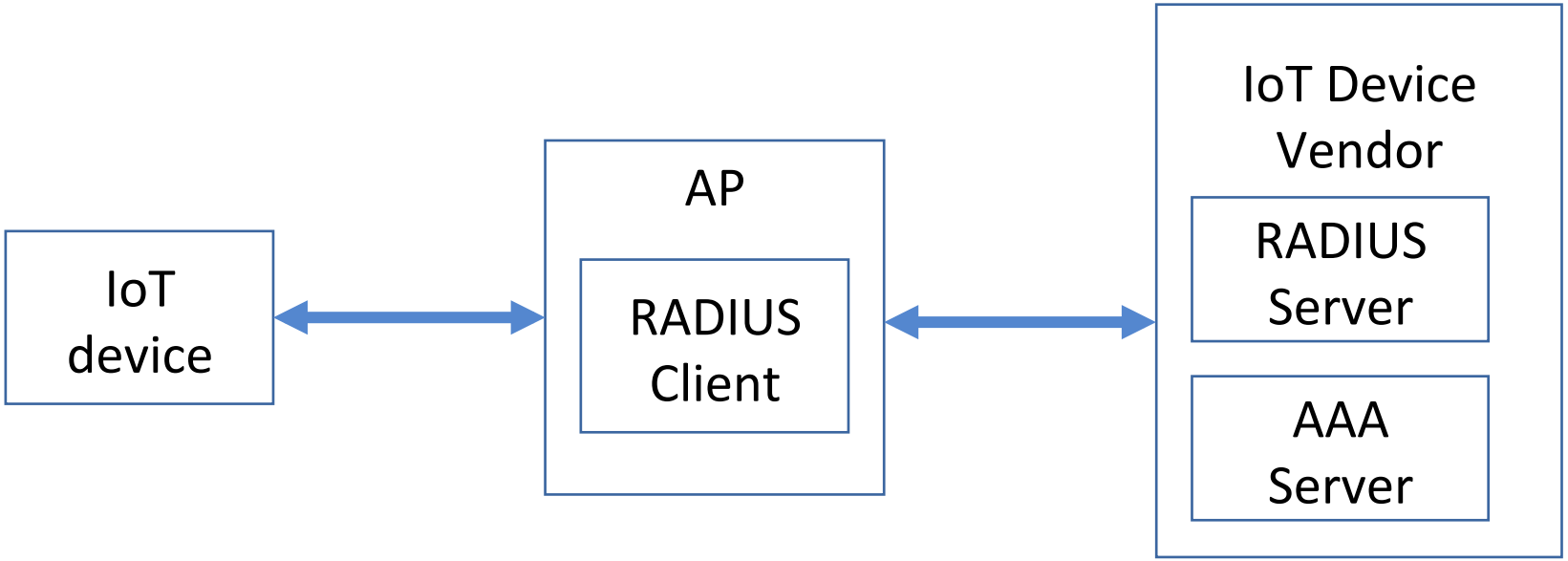
Authorizing network access for IoT devices

Current Solutions for network access authorization:

- Manual configuration and key distribution
  - Pairing with smart phone over Bluetooth
  - Wifi (Un)Protected Setup (WPS)
- Managed solutions
  - RADIUS / DIAMETER / 802.1x
  - Vendor and enterprise certificates

Cloud-managed network access authorization

- Delegating network access authorization and isolation decisions to a remote cloud-based service
  - Device vendors or third parties



Cloud-managed solutions

Some open questions:

- RADIUS implementations are quite limited
  - Can't expect users to understand and configure RADIUS
- Limiting the power of delegates in my LAN?
- Interoperation of multiple delegates in my LAN?
- Isolating devices within my LAN
- Monitoring the behavior of my devices
- Multi-homed, mobile and multi-owner devices

EAP-NOOB

draft-aura-eap-noob

https://github.com/tuomaura/eap-noob

Tuomas Aura

Mohit Sethi

EAP-NOOB

- Nimble out-out-of-band authentication for EAP

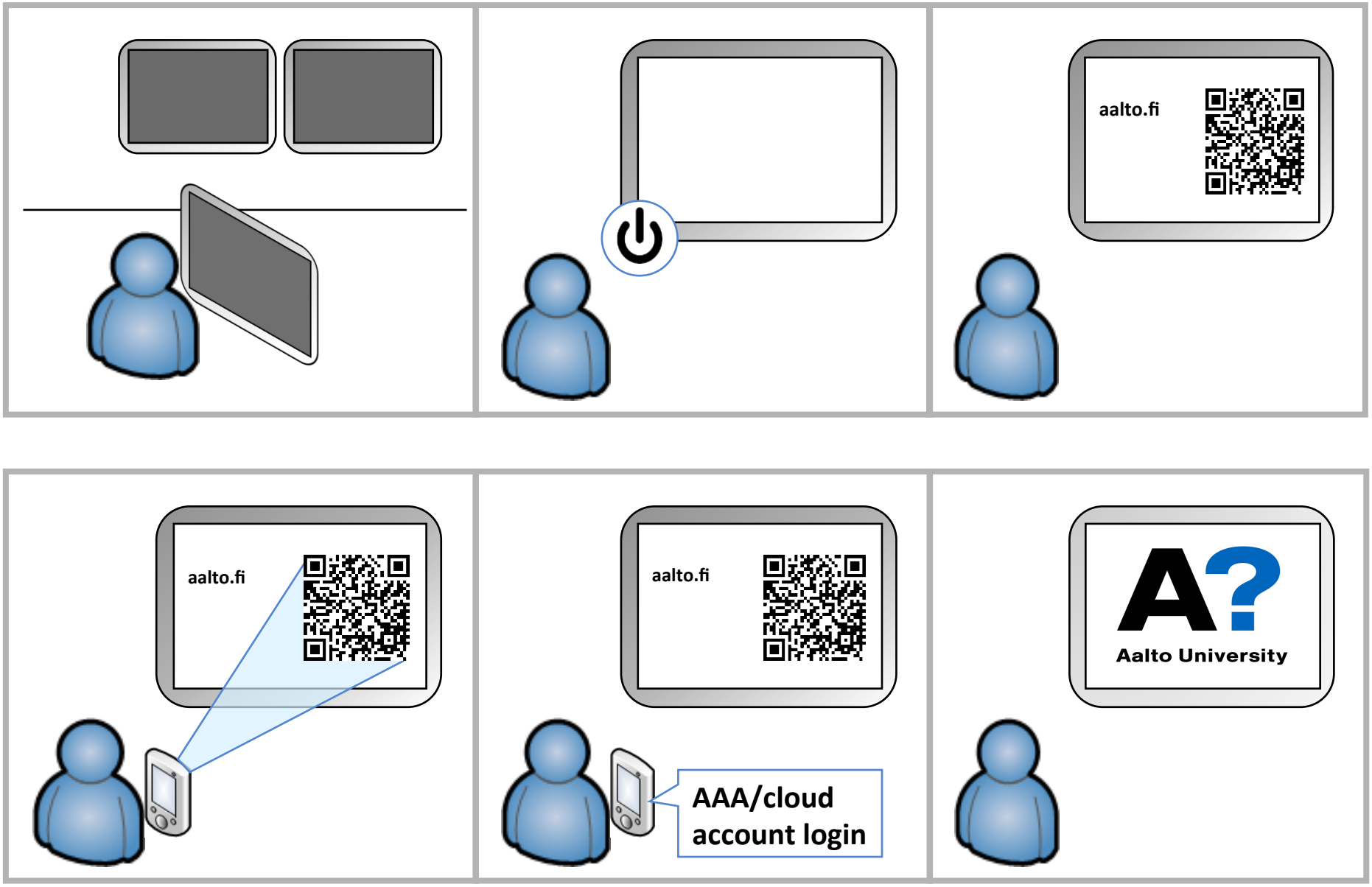
What is special?

- No pre-existing credentials or association needed
- User-assisted OOB authentication associates peer device to authentication server

What is it good for?

- Secure bootstrapping of cloud-connected smart appliances
- Newly unboxed devices have no credentials or owner

EAP-NOOB user experience example

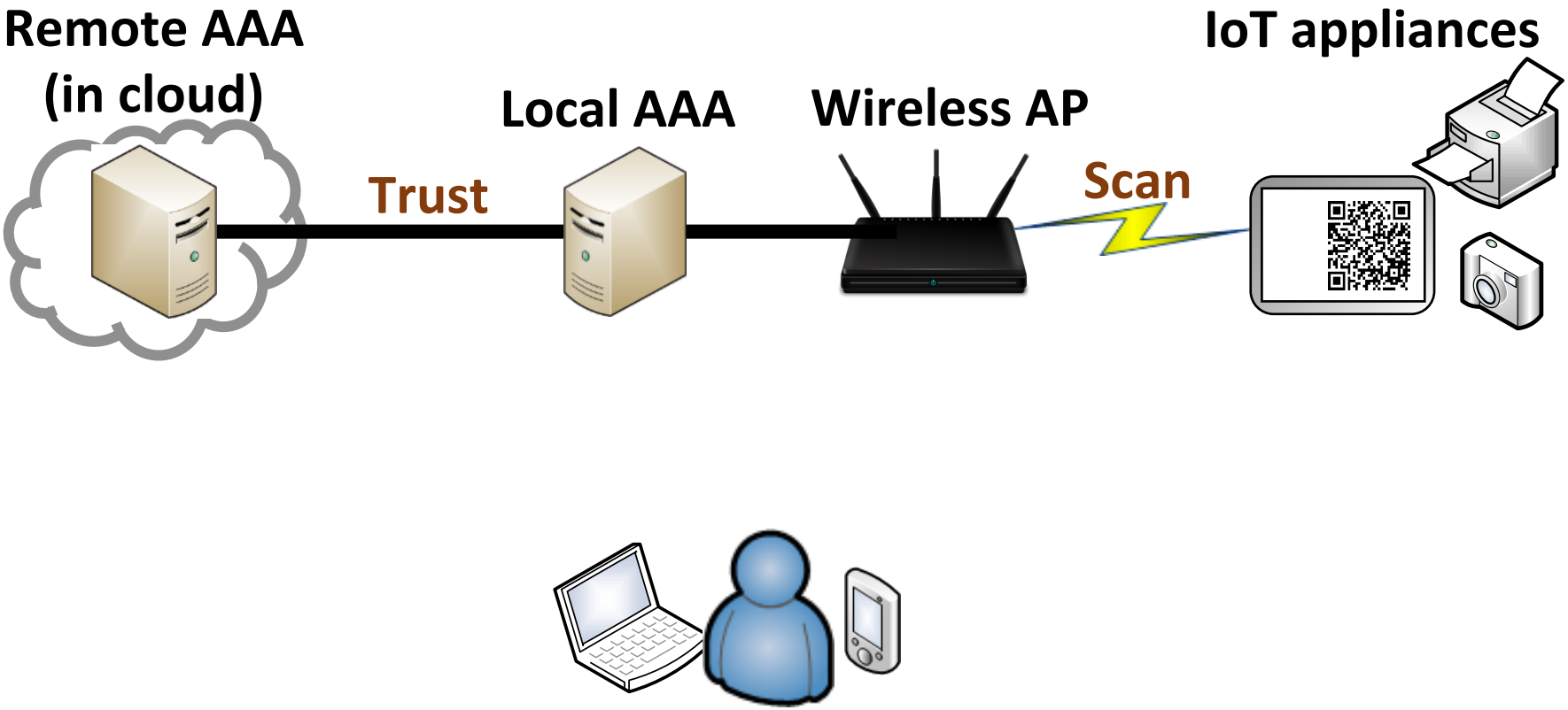


EAP-NOOB

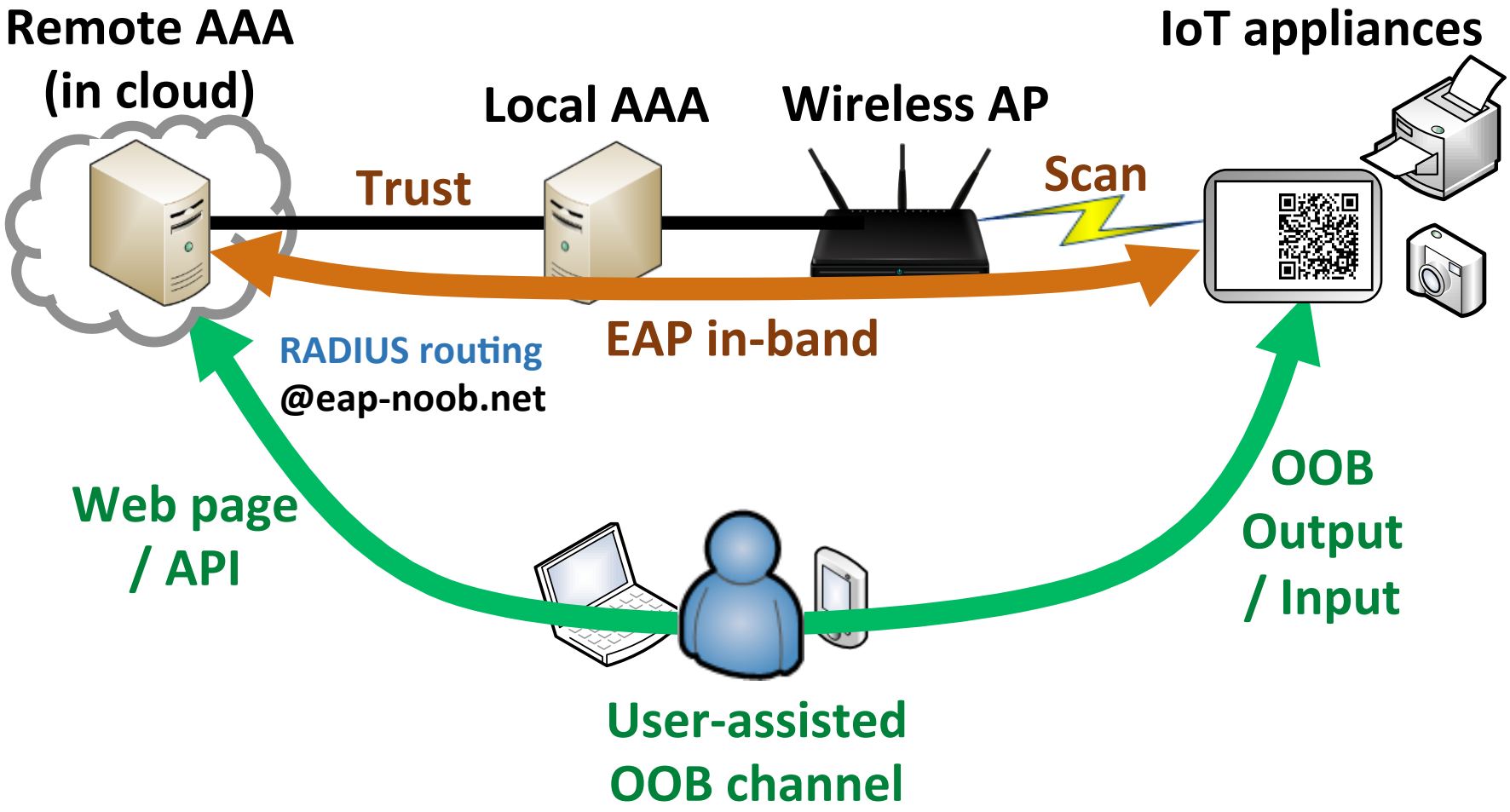
- Device registration to cloud and user account + network access authorized – in one step
- Single user-assisted out-of-band message between peer device and AAA server

How is this possible?

Scenario: cloud-connected IoT appliance



Scenario: cloud-connected IoT appliance



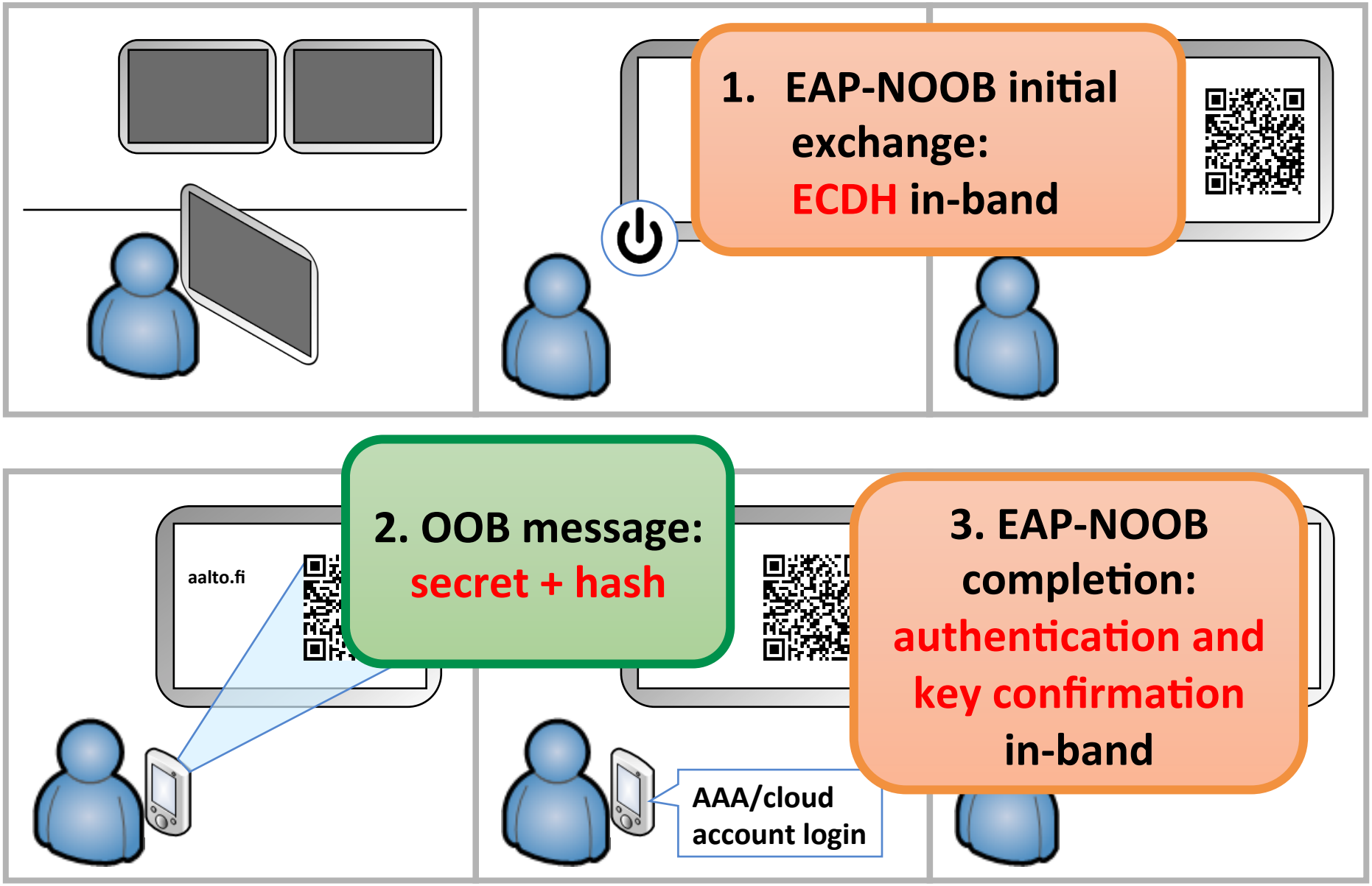
EAP-NOOB

- Device registration to cloud and user account + network access authorized – in one step
- Single user-assisted out-of-band message between peer device and AAA server

How is this possible?

- In-band communication through EAP tunnel before network access is authorized
- User has an account in the cloud-based AAA server and has secure access, e.g. HTTPS
- Access network trusts the AAA server

EAP-NOOB in the background



EAP-NOOB security

- ECDH key exchange in-band + authentication out-of-band
- OOB message in only one direction: peer to server *or* server to peer
- OOB channels must protect confidentiality *or* integrity (both not needed)
- Additionally, user checks that registration was successful or, if it was not, resets the peer device

EAP-NOOB details

- OOB channels: dynamic QR code, dynamic NFC NDEF message, audio cable
- Association becomes persistent until reset by user. Rekeying happens without user interaction
- Potential providers of cloud-based service: device vendor, ISP, content provider, third-party
- Mainly for device-cloud association. Ok for device-device pairing, but not necessarily optimal
- Roaming (e.g. in eduroam) possible after first association at home network

EAP-NOOB lessons

- Security bootstrapping = device registration, taking ownership
- Device names and identifiers often not available and cannot be trusted. Physical access identifies the device
  - Vendor certificates can prove device model and capabilities
- Avoid rerun of user-assisted step at all cost
  - After a few times, average user just won't bother
  - Sending engineer on-site is expensive and does not scale
  - Protocol must recover from accidental and malicious failures
- Timeout, retry and back-off intervals difficult to decide when human user is part of the protocol
- Algorithm agility is harder with no permanently secure master keys
- EAP is useful also in home networks

Next challenges

So, a third-party AAA server authorizes off-the-shelf devices to use my access network!

- Monitoring device behavior in access network
- Situational awareness for access network owner
- Isolation of devices from the access network (e.g. guest VLAN) and from each other
- Authorized access to services and other devices in the access network
- Limiting the power of the cloud-based third-party AAA server
- Multiple co-existing third-party AAA servers