Nimble out-out-of-band authentication for EAP

draft-aura-eap-noob-00

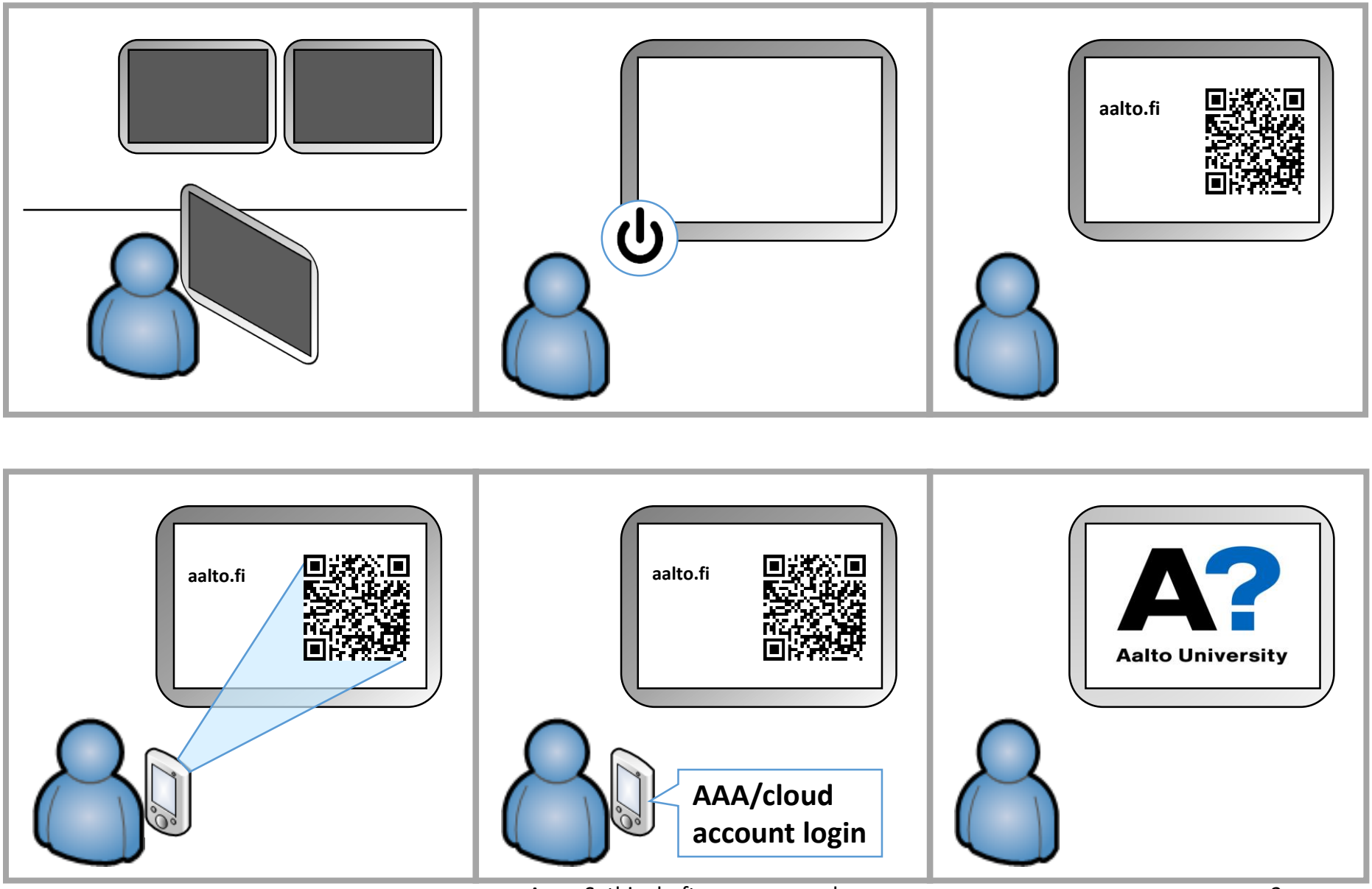
Tuomas Aura, Aalto University, Finland

Mohit Sethi, Ericsson Research, Finland

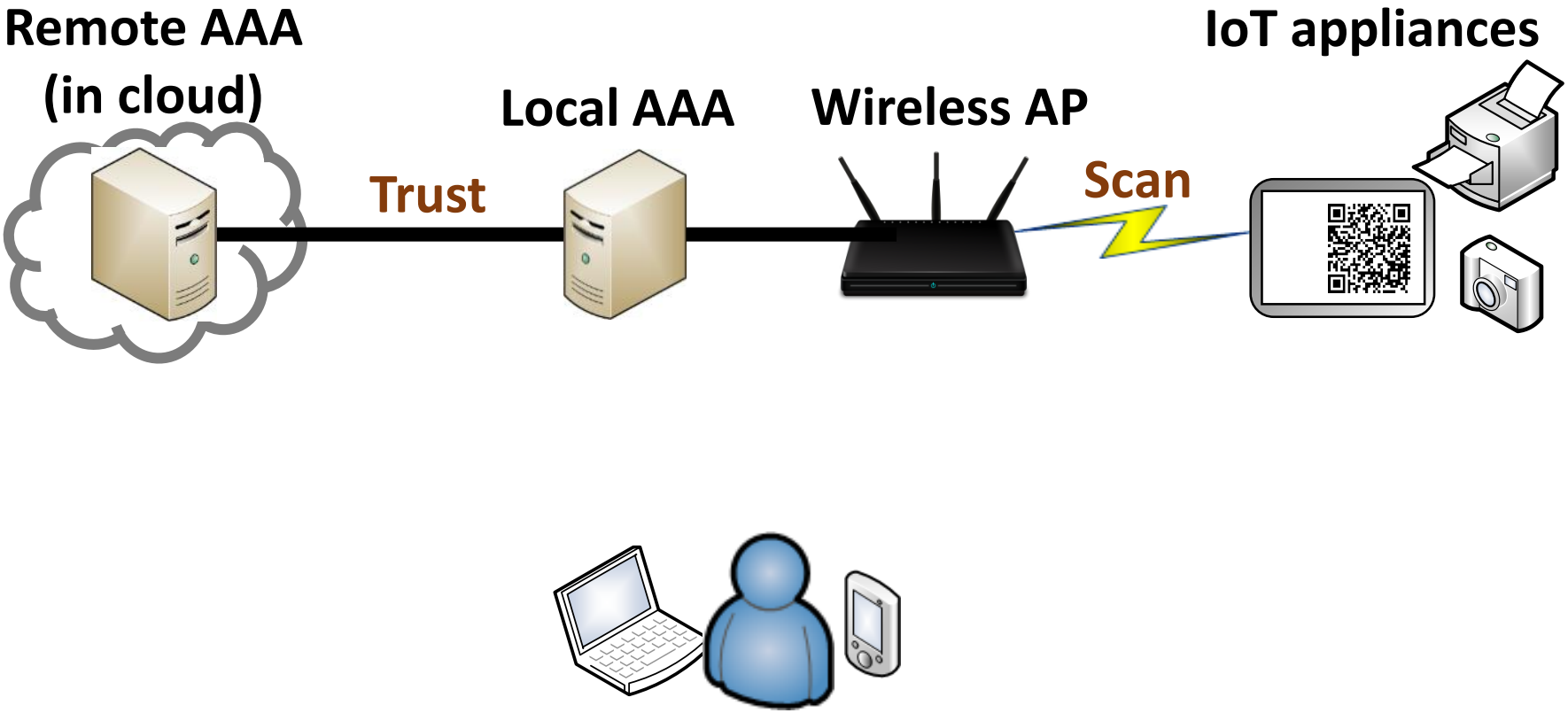
EAP-NOOB rationale

- Cloud-connected IoT appliance
- **New IoT appliance** has no owner or domain, no credentials for cloud or Wi-Fi
- Need to
  - **(1) connect the device to access network**
  - **(2) 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

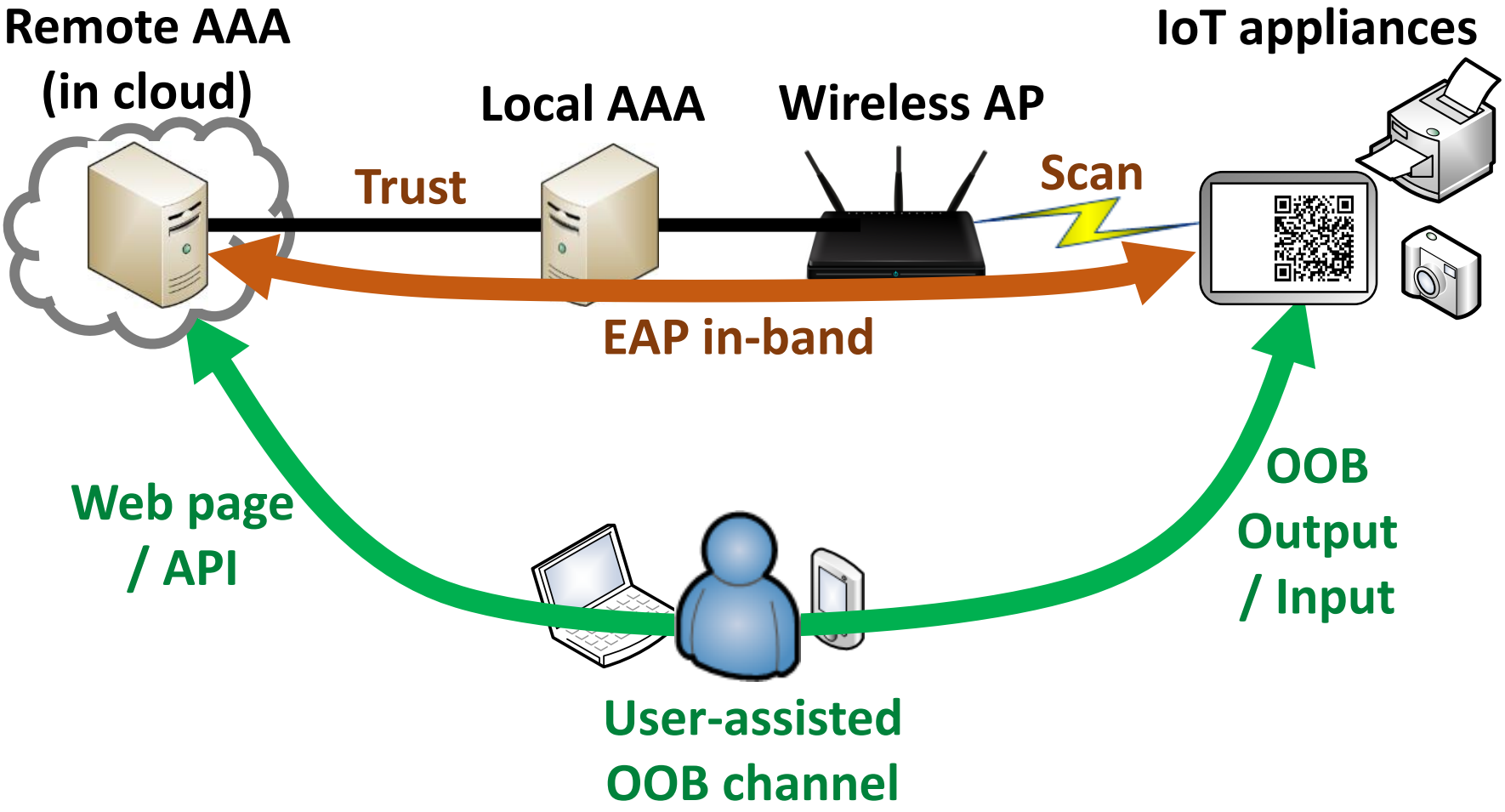
EAP-NOOB user experience example



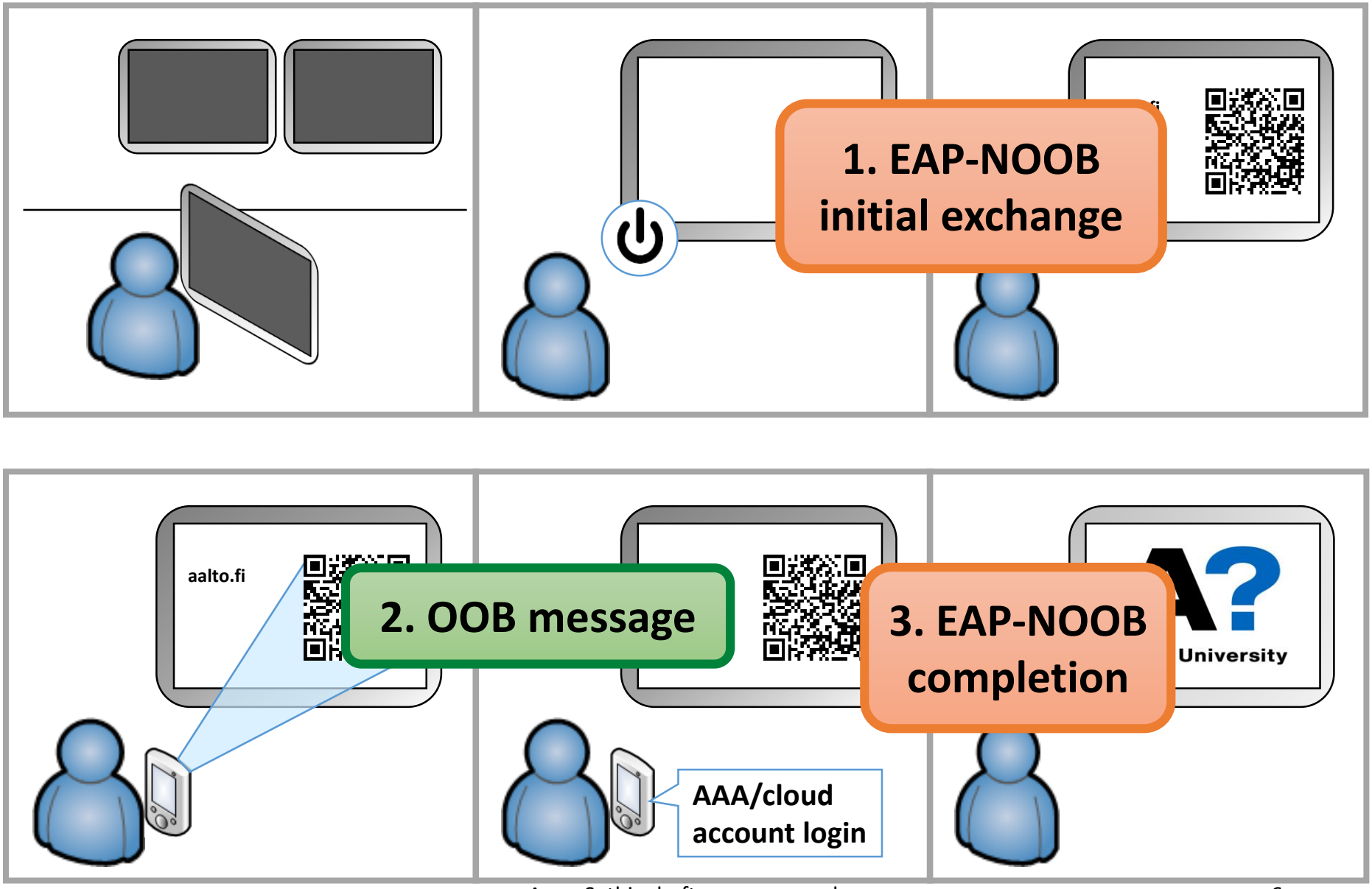
Scenario: cloud-connected IoT appliance



Scenario: cloud-connected IoT appliance



EAP-NOOB in the background



EAP-NOOB protocol – high level view

- 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.

Creative use of EAP

- 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.net”
  - Must configure trust between access network and AAA/cloud server for “@eap-noob.net”

EAP-NOOB security details

- 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

Deploying EAP-NOOB

What is the cost?

- The EAP method implemented only in AAA/cloud server and peer devices
- No changes to the Authenticator (AP)
- No new code in access-network AAA server
- Access network admin chooses a AAA/cloud server and configures realm-to-server mapping for "@eap-noob.net"
- User must have accounts for accessing the organization's AAA/cloud server
- When OOB message is encoded as QR or NFC tag and scanned on smart phone, no phone app needed
- Home users would need WPA2-Enterprise and user accounts

Next steps

- Requested features (thank you for the feedback so far!)
  - **Application scenarios** and requirements document
  - **AAA roaming support**: registering new devices when roaming e.g. on Eduroam
  - Optional **vendor certificates** for authentic peer device model and id, and for detecting virtual vs. physical peer devices
  - Advertising EAP-NOOB support and domain in 802.11 (??)

- TODO list of smaller issues:
  - Configuration of domain-specific NAI after initial registration
  - Specify the URL format for the OOB message
  - Check for message fragmentation (vendor certs will mess this up)
  - **Reliability and usability evaluation**: experiments with timeouts and multiple access networks in the same space
  - **Updating persistent association** after each ECDH rekeying or at least after algorithm update

Thank you for listening!

- Is anyone else interested in EAP-NOOB?
- Standards track
- Individual submission / AD-sponsored / suitable working group?