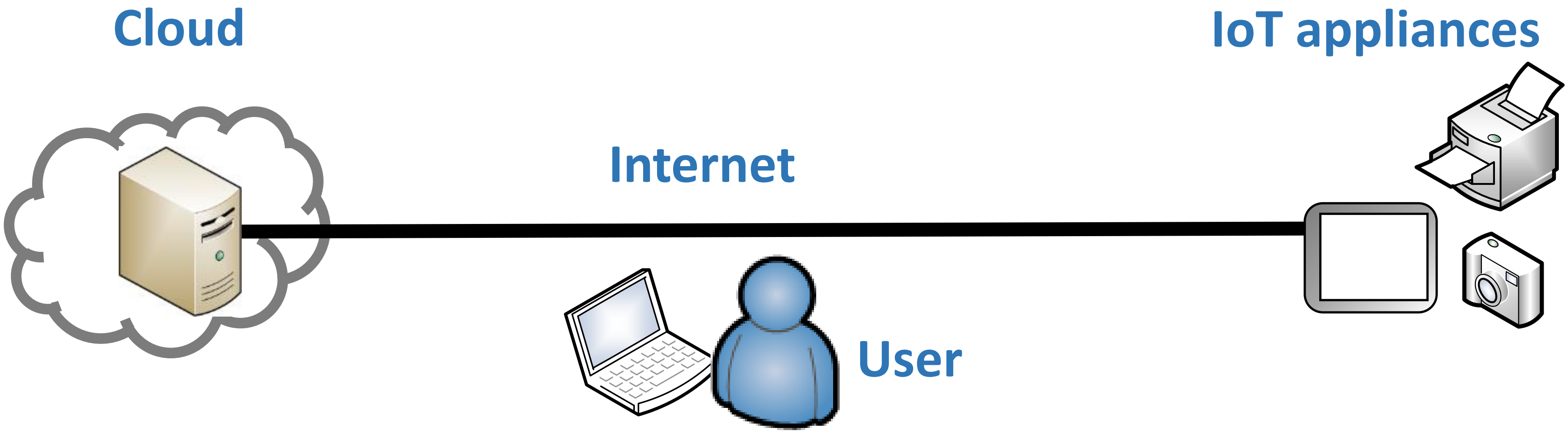
Connecting IoT appliances securely to the cloud (eap-noob)

Tuomas Aura, Aalto University, Finland

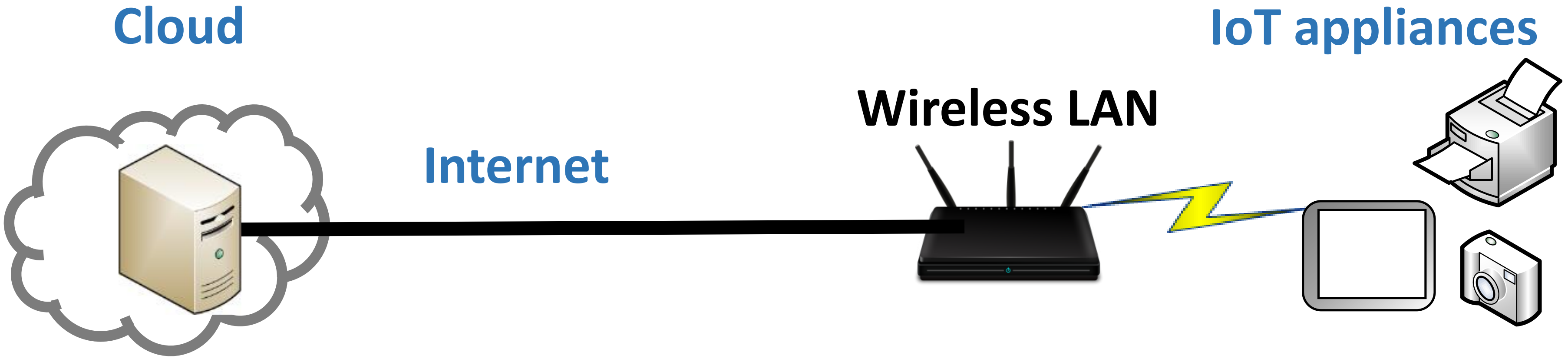
joint work with Mohit Sethi, Ericsson, and others

Connecting devices to cloud



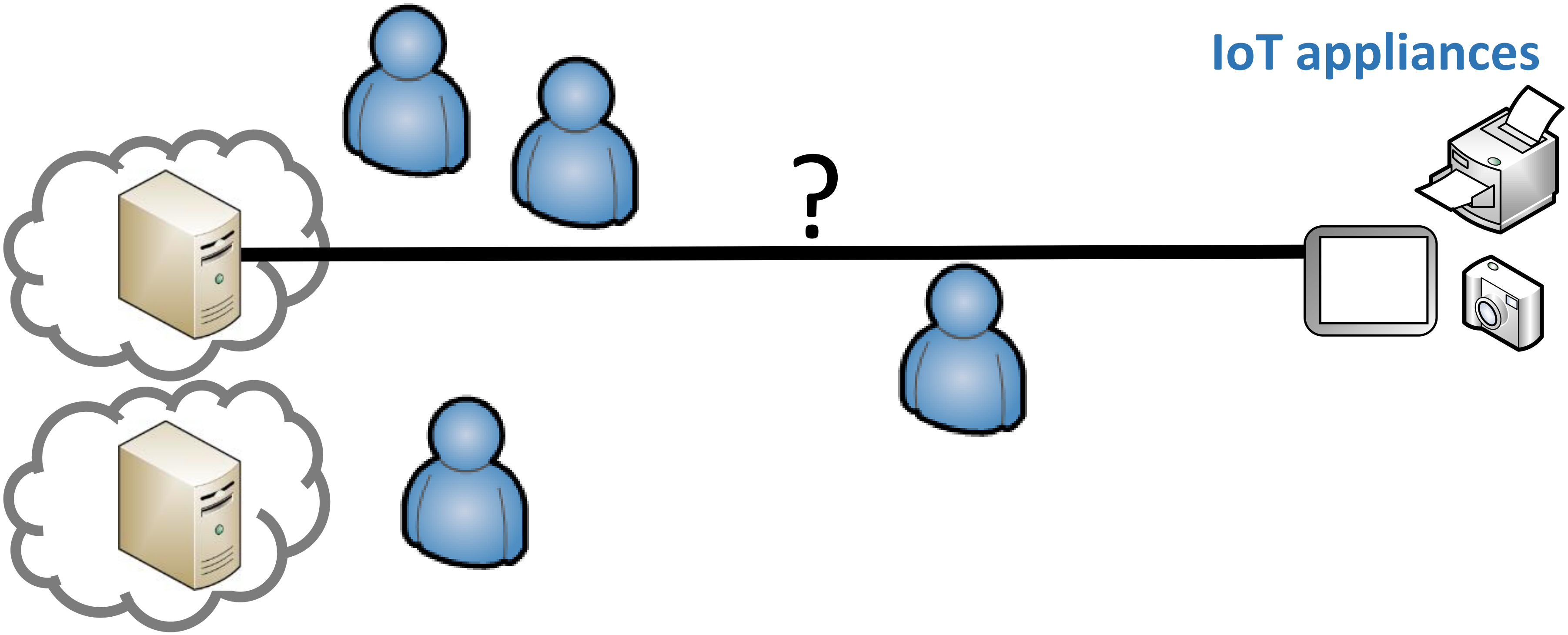
- Authenticated key exchange?
  - Goals: learn peer identity, create a secure connection
- Device pairing?
  - Physical access to device – but only at one end
  - No pre-established credentials
  - Possibly no pre-established identities or trusted parties

Wireless network access



- Wireless access credentials?
  - Before the device can connect to the cloud, it needs Internet access

Device ownership



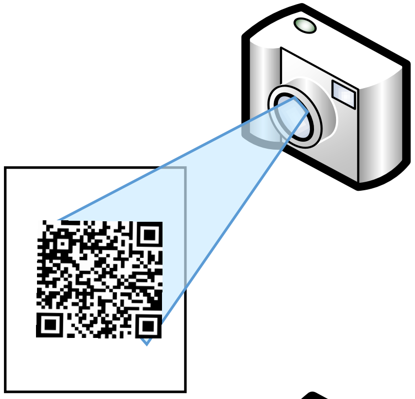
- Which cloud service owns the device?
- Which cloud-service user owns the device?
- For example, consider a device that a university secretary just bought at the gadget superstore

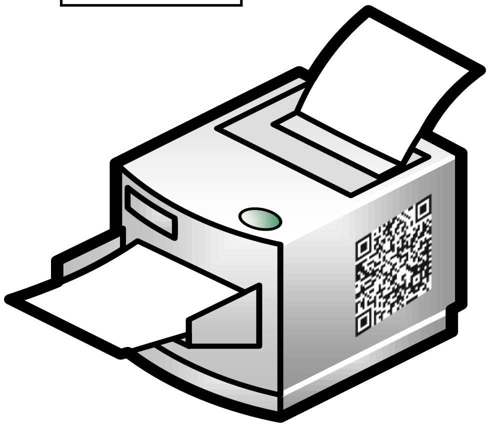
Scalability

- Up to thousands of smart appliances
- Installers are untrained staff and consumers
- Some devices redeployed regularly

Existing configuration methods

- Consumer methods:
  - User enters network and cloud credentials
  - Automatic entry: bar code, blinking LED, sound
  - WPS + static QR code printed on the device (?)
- Scalable industry methods:
  - Device certificates + register of purchased devices + (D)TLS
  - Outsourced management



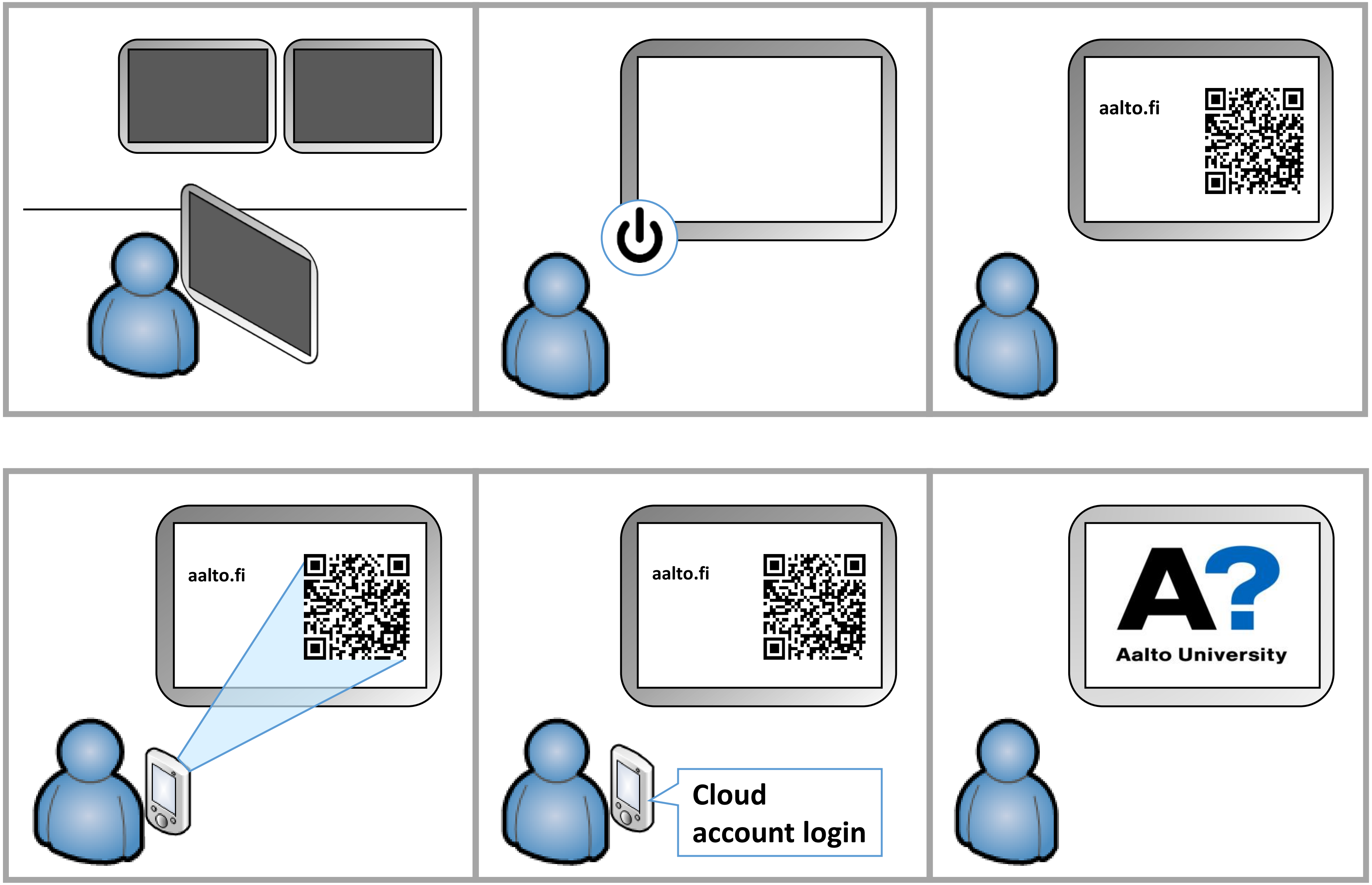


EAP-NOOB

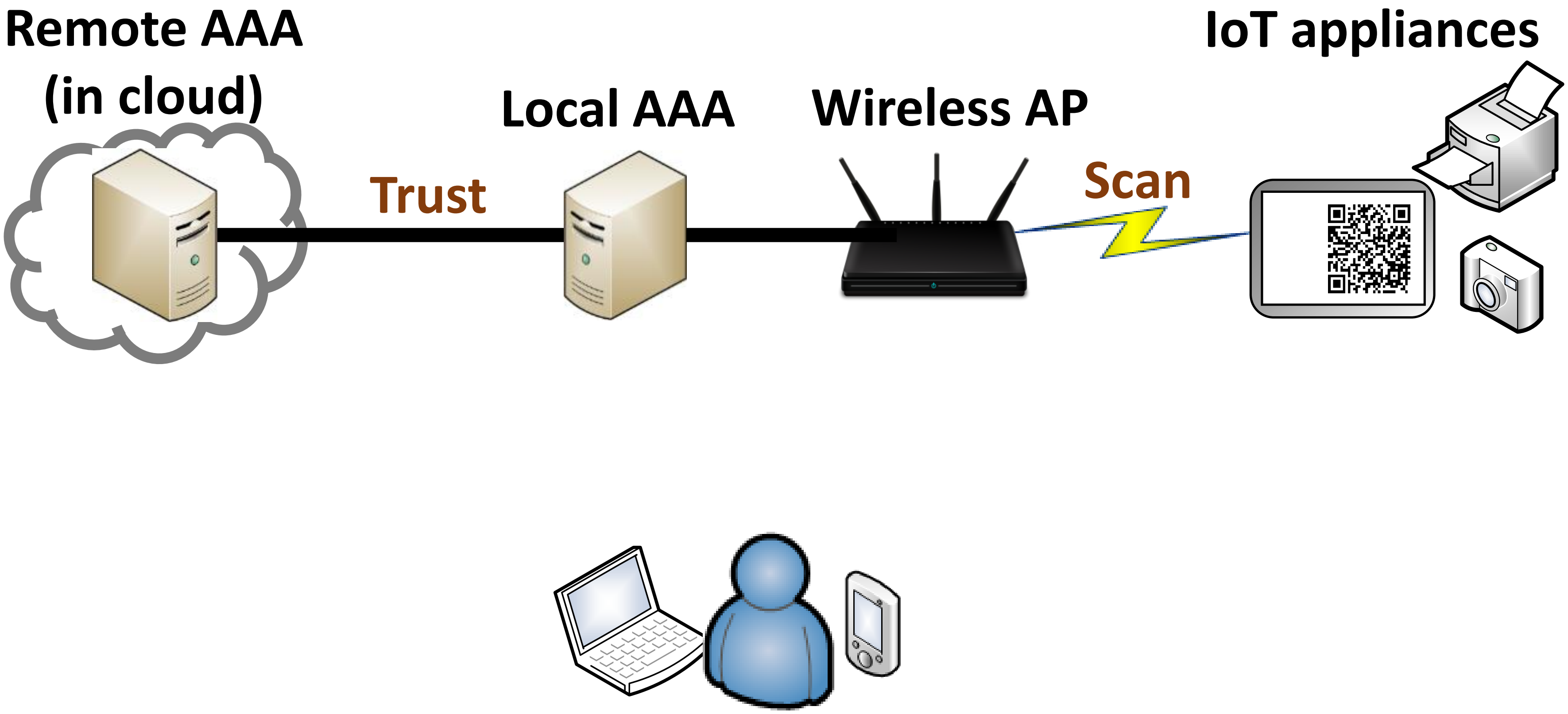
- EAP method for nimble out-of-band (OOB) authentication of cloud-connected IoT appliances
- **New IoT appliance** has no owner or domain, no credentials for cloud or Wi-Fi
- What EAP-NOOB does:
  1. **connect the device to access network**
  2. **register the device to AAA/cloud server**
- Security from a **single user-assisted out-of-band message** between peer device and AAA server

(Generalization of EAP method from Ubicomp 2014)

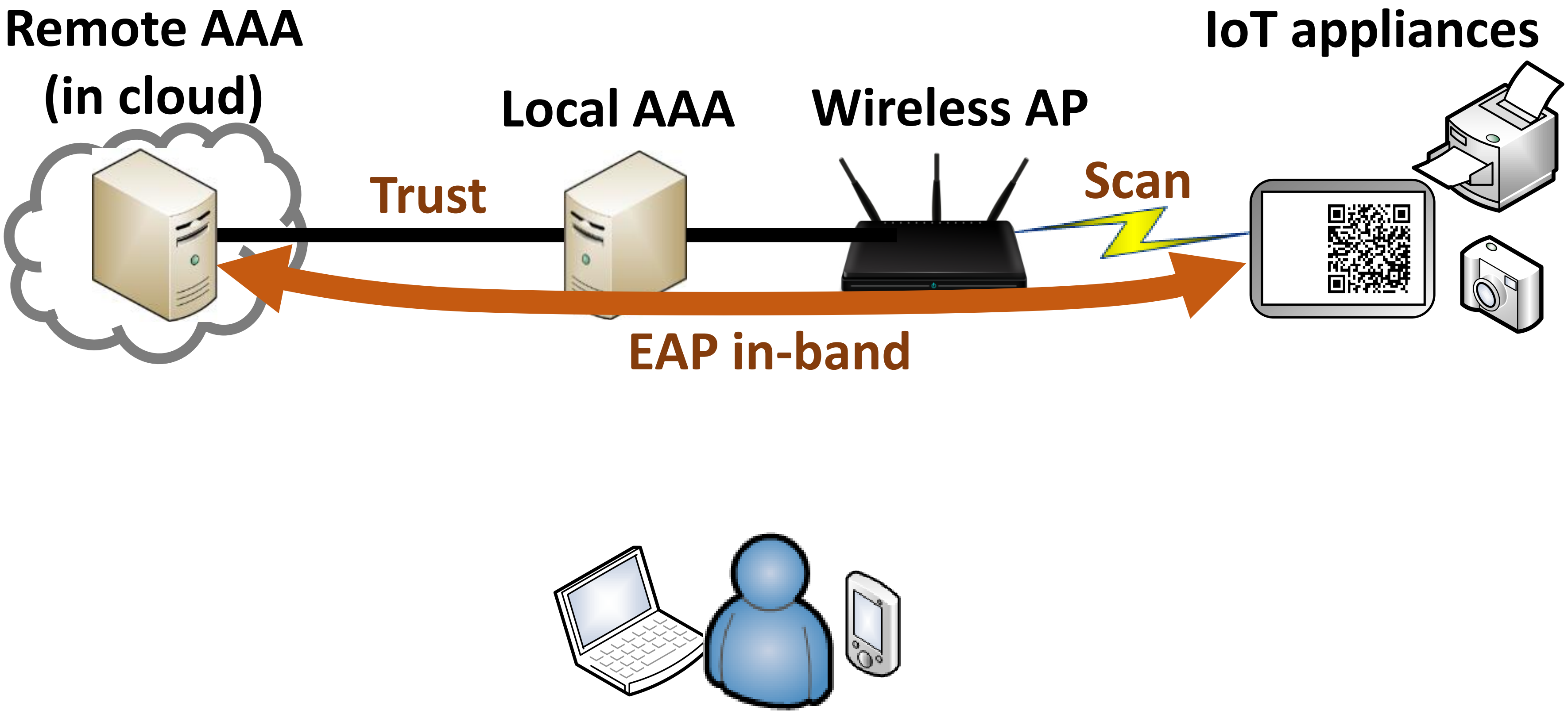
EAP-NOOB: user experience



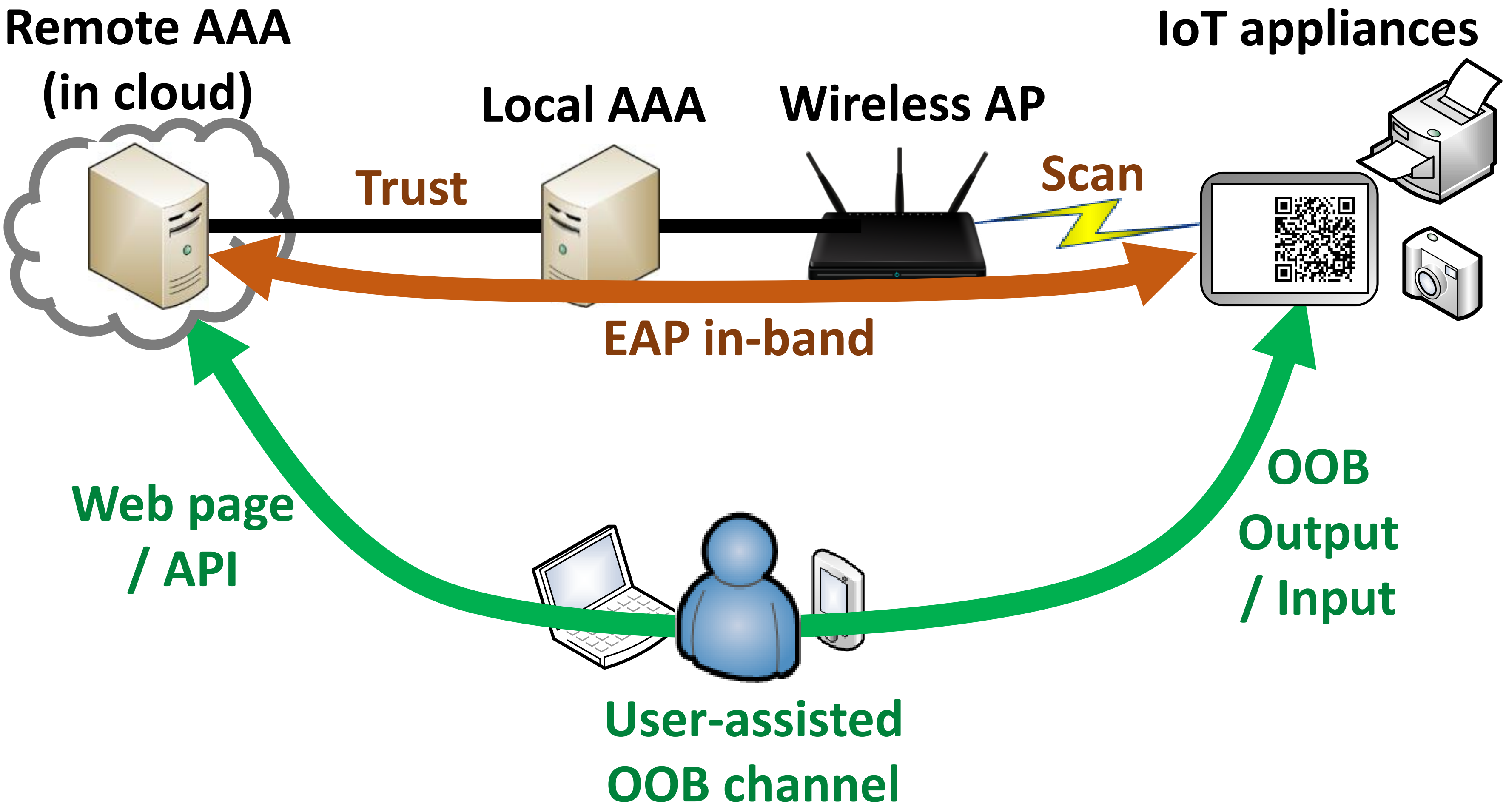
EAP-NOOB


Remote AAA
(in cloud)
Local AAA
Wireless AP
IoT appliances
Trust
Scan

EAP-NOOB


Remote AAA
(in cloud)
Local AAA
Wireless AP
IoT appliances
Trust
Scan
EAP in-band

EAP-NOOB



Remote AAA
(in cloud)
Local AAA
Wireless AP
IoT appliances
Trust
Scan
EAP in-band
Web page
/ API
OOB
Output
/ Input
User-assisted
OOB channel

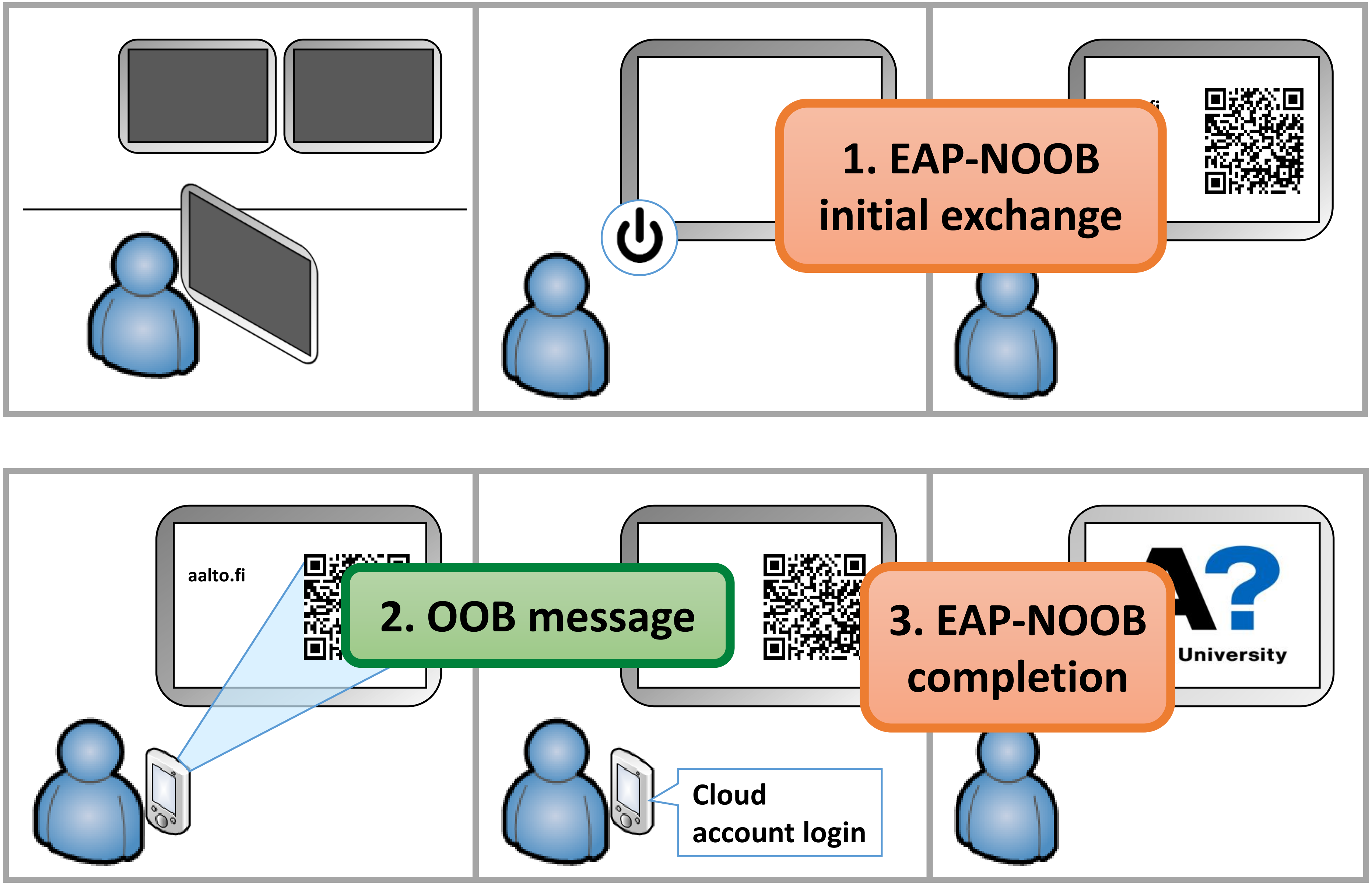
EAP-NOOB protocol – high level view

- 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.

EAP-NOOB in the background



1. EAP-NOOB initial exchange

2. OOB message

3. EAP-NOOB completion

Cloud account login

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

- The EAP method must be implemented in AAA/cloud server and peer devices
  - Our implementation: **Linux wpa_supplicant (device) and hostapd (server)**
- No changes to the Authenticator (AP)
- No new code in access-network AAA server
  - Realm-to-server mapping for “@eap-noob.net”
- User accounts at the AAA/cloud server
- No phone app needed for QR codes
- Requires WPA2-Enterprise to be used at home

Ongoing work

- IETF Internet-Draft: **draft-aura-eap-noob**
- The Eduroam case:
  - How to use your device while roaming?
  - How to configure new device while roaming?
- Server-to-device OOB and device discovery
  - Which devices does the cloud offer to the user?
- OOB channel message formats
- Protocol verification
  - Complexity mainly from two OOB directions
  - Simple Promela model exists, more to do