EAP-NOOB : Nimble Out-of-Band Authentication for EAP

EMU WG, IETF 106
Singapore, November 2019

Tuomas Aura, Aalto University
Mohit Sethi, Ericsson
various other contributors

What problems EAP-NOOB solves?

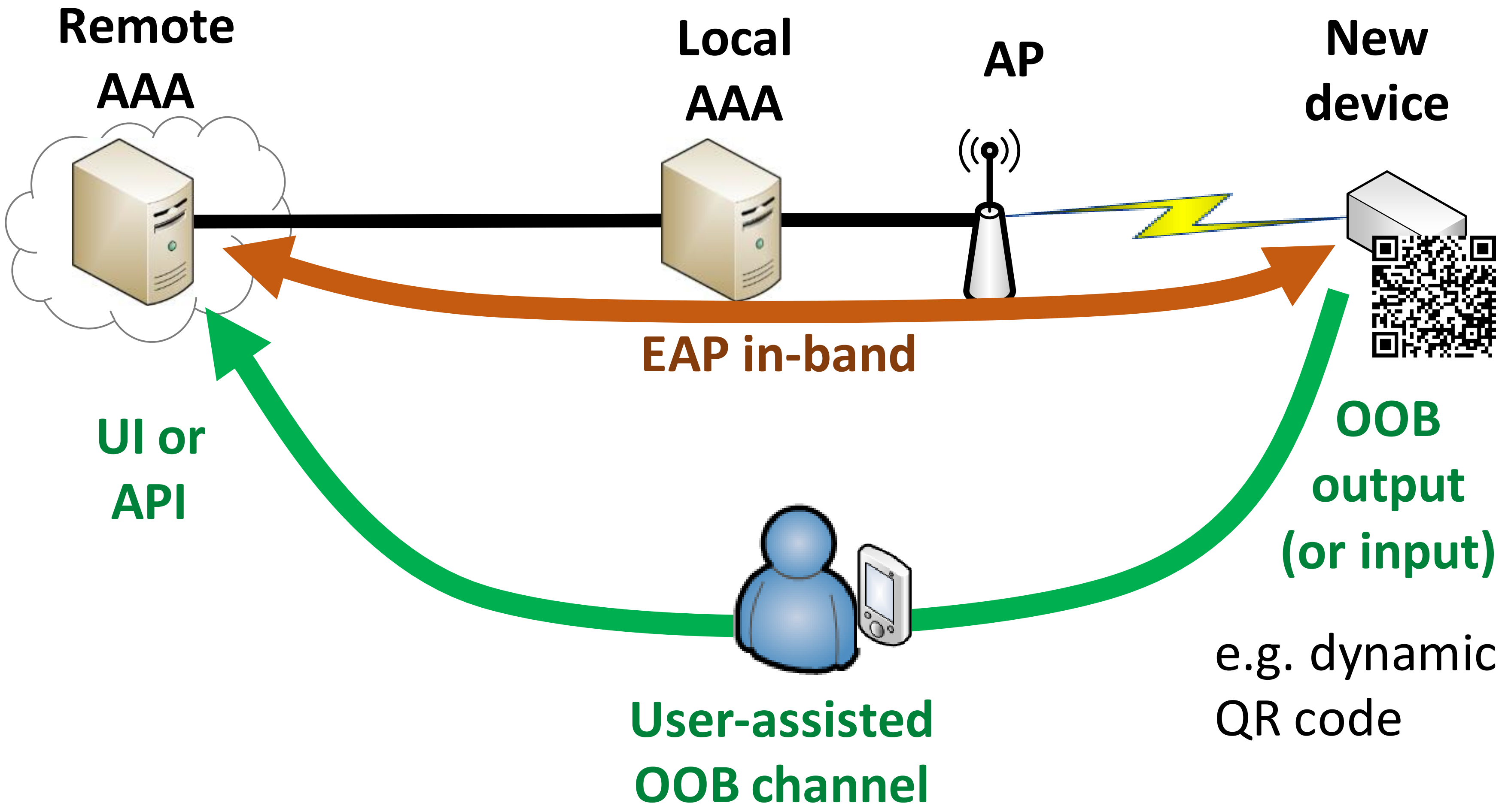
- EAP is a generic authentication framework with many methods, but currently no OOB authentication method
- EMU WG chartering being updated to create one
- EAP-NOOB is a solution for this, suitable for a broad range of EAP applications, stable spec, formal models and verification, open-source implementations

EAP-NOOB overview

- EAP method for bootstrapping smart devices out-of-the-box without professional administration
- User-assisted out-of-band (OOB) authentication
  - E.g. scanning a dynamic QR code, dynamic NDEF tag
- Registration of authenticated devices to AAA
  - Create persistent association between AAA and device and authorize network connectivity at the same time
- Fast reauthentication of previously registered devices without further user interaction

EAP-NOOB architecture

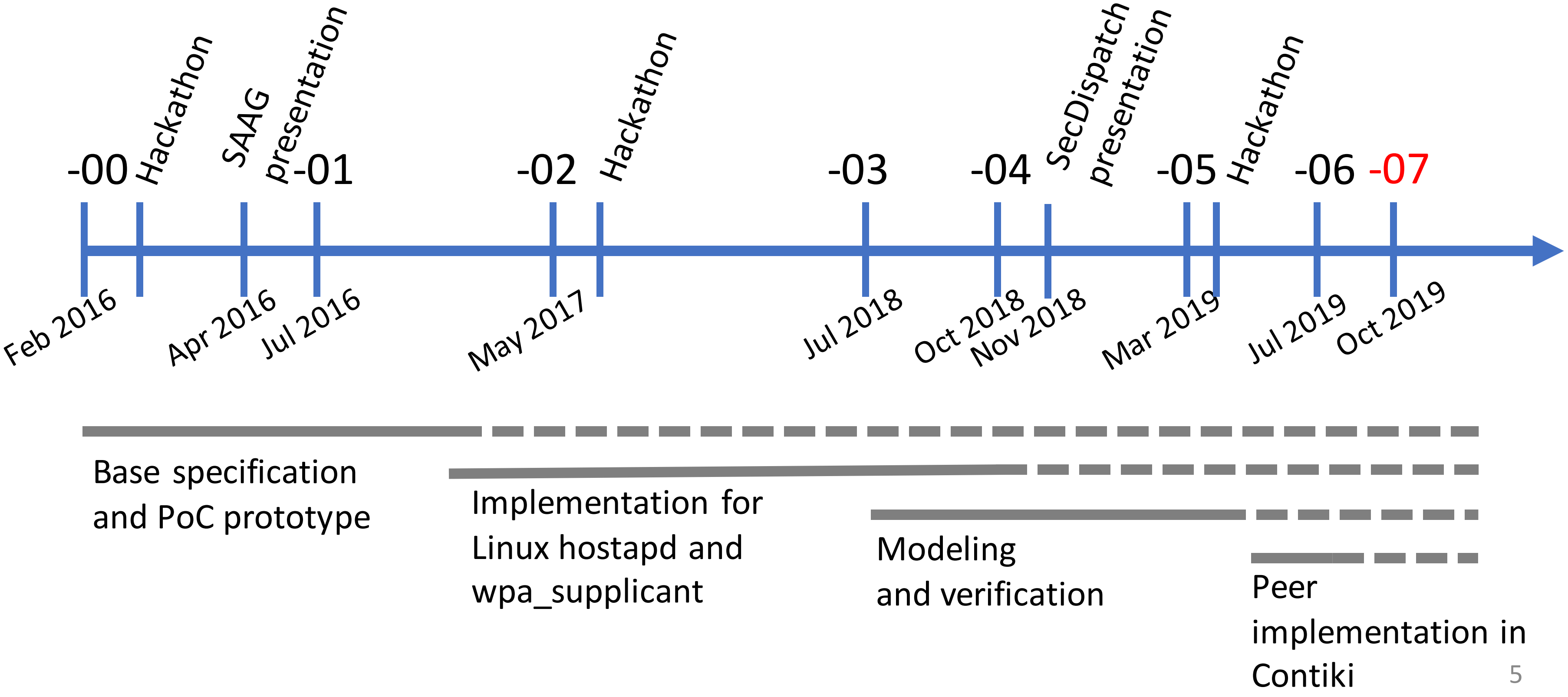
Trick: in-band communication over EAP between peer and server before device is registered



e.g. dynamic QR code

EAP-NOOB: Nimble Out-of-Band Authentication for EAP

draft-aura-eap-noob



New in draft version -07

Minor revisions only:

- Updated example messages
- Update implementation status

EAP-NOOB status summary

- Draft draft-aura-eap-noob-07 is pretty mature
- Implementations:
  - wpa_supplicant and hostapd https://github.com/tuomaura/eap-noob
  - Contiki https://github.com/eduingles/coap-eap-noob
- Formal models in mCRL2 (protocol and DoS-resistance) and ProVerif (authentication)

Requesting EMU WG adoption – to be confirmed on mailing list after rechartering complete

Specific issues:
NAI and roaming

EAP-NOOB and NAI

- Peer initially has no NAI because it is not registered in AAA
- For the initial exchange, peer uses the generic realm eap-noob.net*. Needed for routing EAP-NOOB from new, unregistered peers to the correct AAA server in the network
  - OOB authentication can be delegated to a specialized server that handles the OOB interaction with the user
- EAP-NOOB server registers the peer and assigns it a NAI: PeerId@Realm**

*) Generic realm to be replaced with a .arpa domain

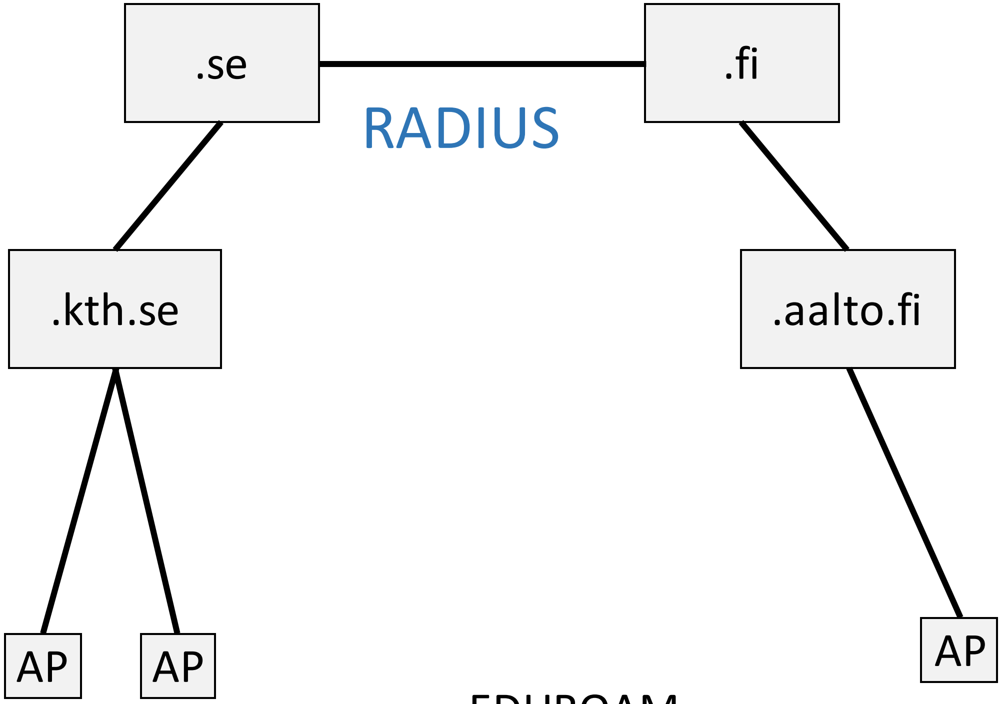
**) If no roaming, can continue to use the generic realm

EAP-NOOB and roaming

Two roaming scenarios:

1. Register device at home, then roam
   - Server assigns a Realm to the peer in Initial Exchange
   - Roaming just works
   - EAP-NOOB supports this scenario out of the box
2. Register device while roaming
   - Requires user interaction with foreign AAA to route the Initial Exchange (one EAP conversation) to home AAA
   - Server assigns a Realm to the peer in Initial Exchange
   - From then on, the roaming just works
   - EAP-NOOB is designed to not prevent this scenario

Roaming scenario 1: register at home



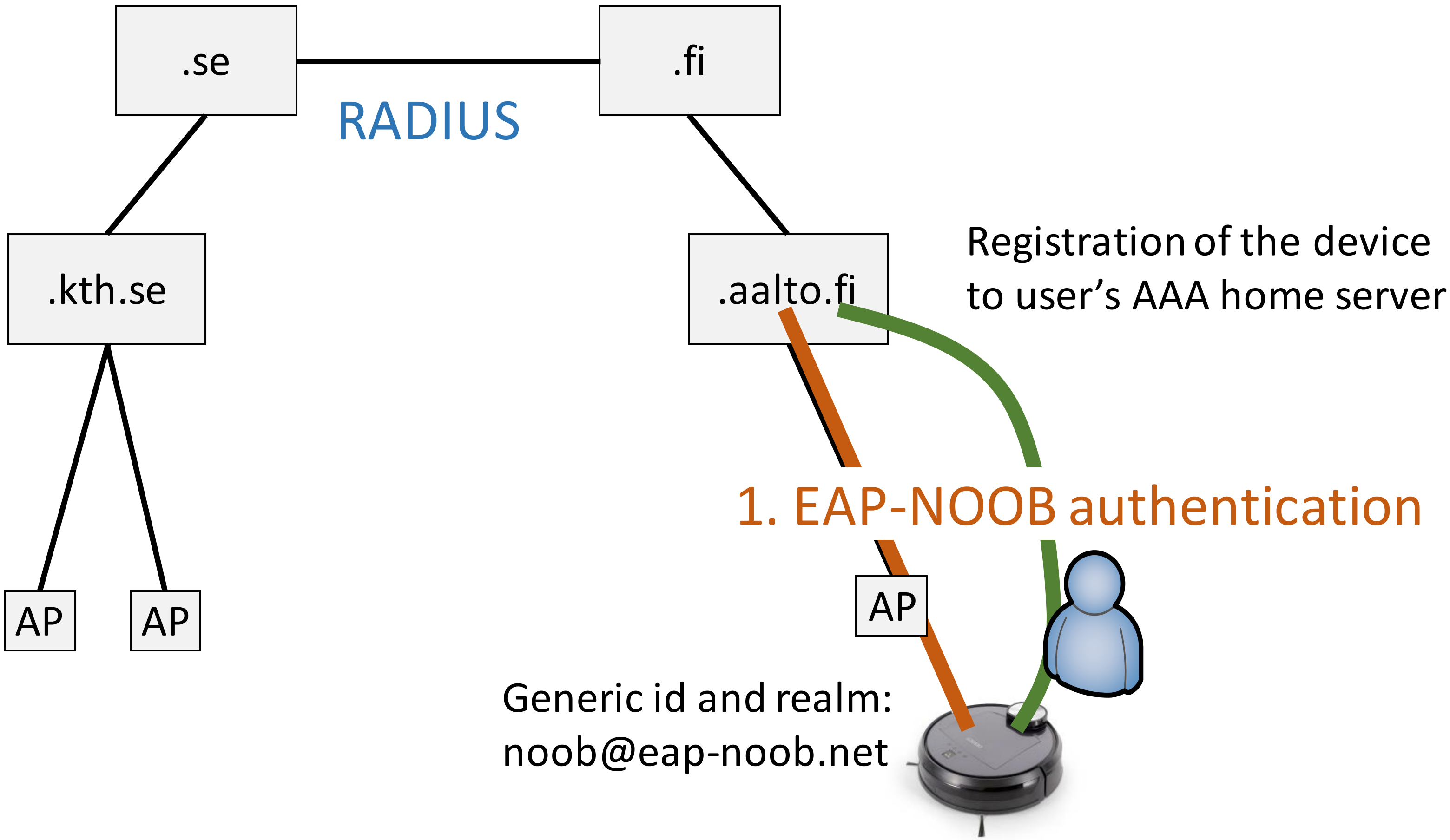
National REN
RADIUS server

Institutional
RADIUS server

Institutional
WLAN

EDUROAM
roaming
example

Roaming scenario 1: register at home

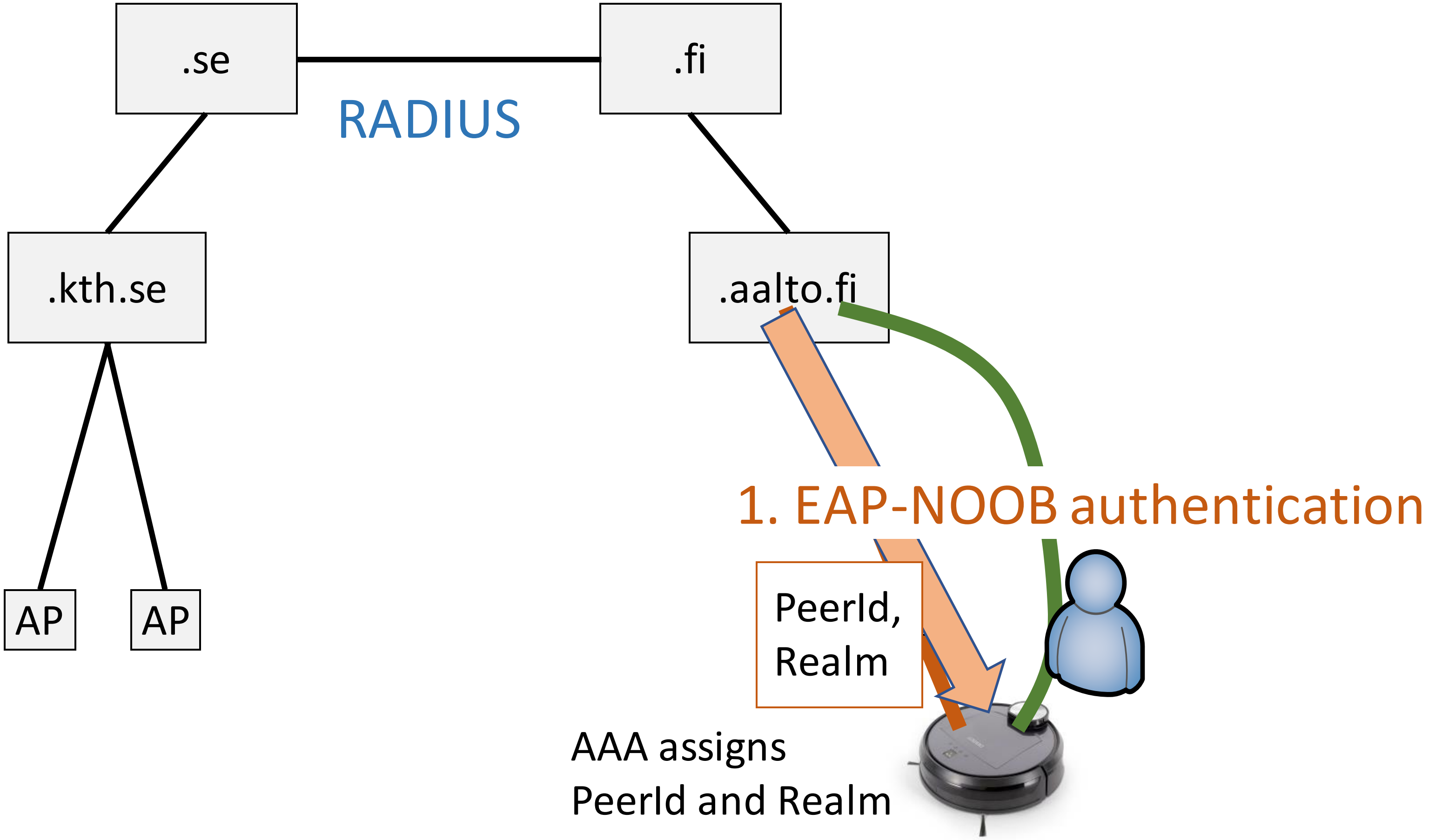


Registration of the device to user's AAA home server

1. EAP-NOOB authentication

Generic id and realm:
noob@eap-noob.net

Roaming scenario 1: register at home



.se

.fi

RADIUS

.kth.se

.aalto.fi

AP

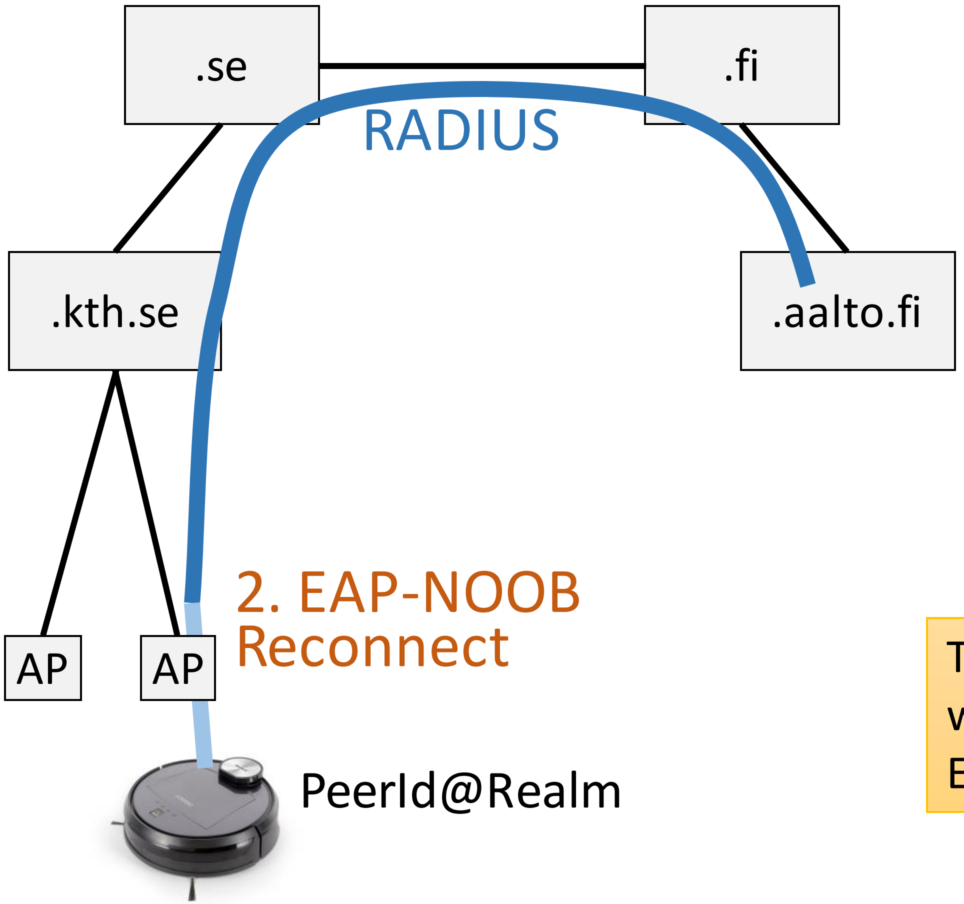
AP

1. EAP-NOOB authentication

PeerId,
Realm

AAA assigns
PeerId and Realm

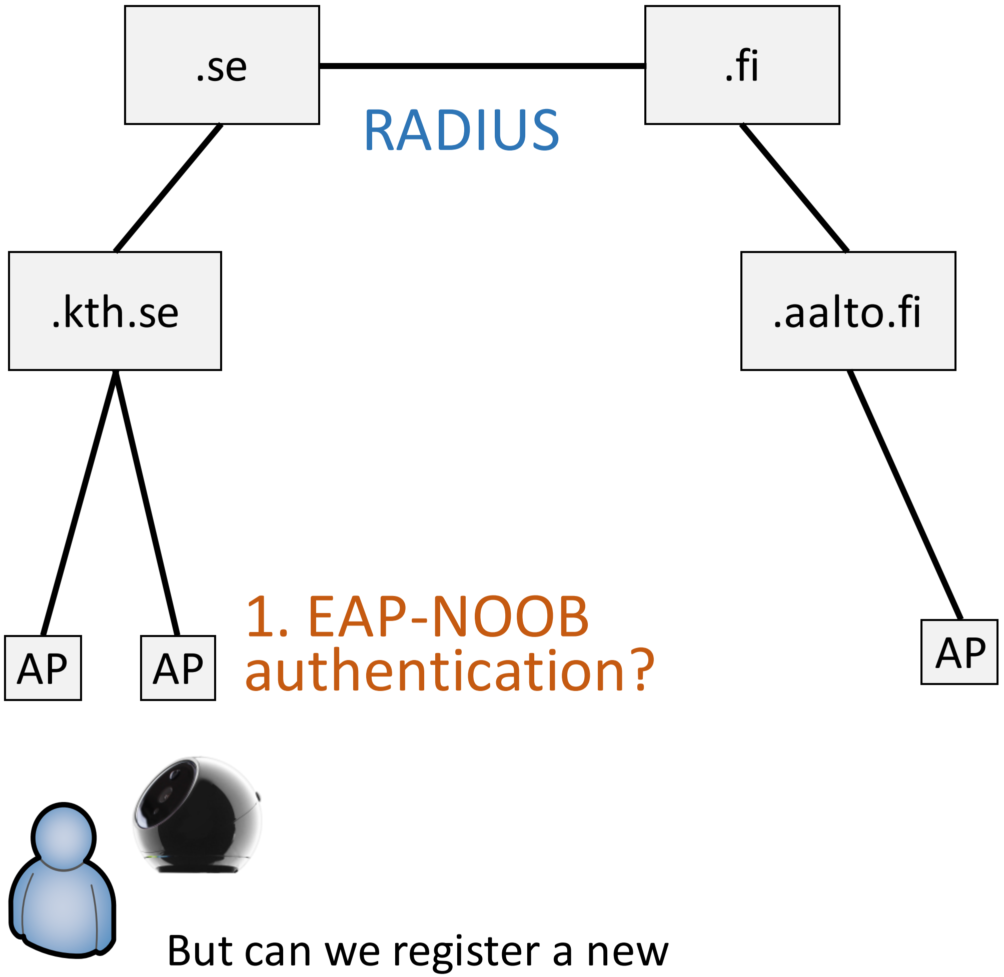
Roaming scenario 1: register at home



Later, the device can roam.

This works well with the current EAP-NOOB spec

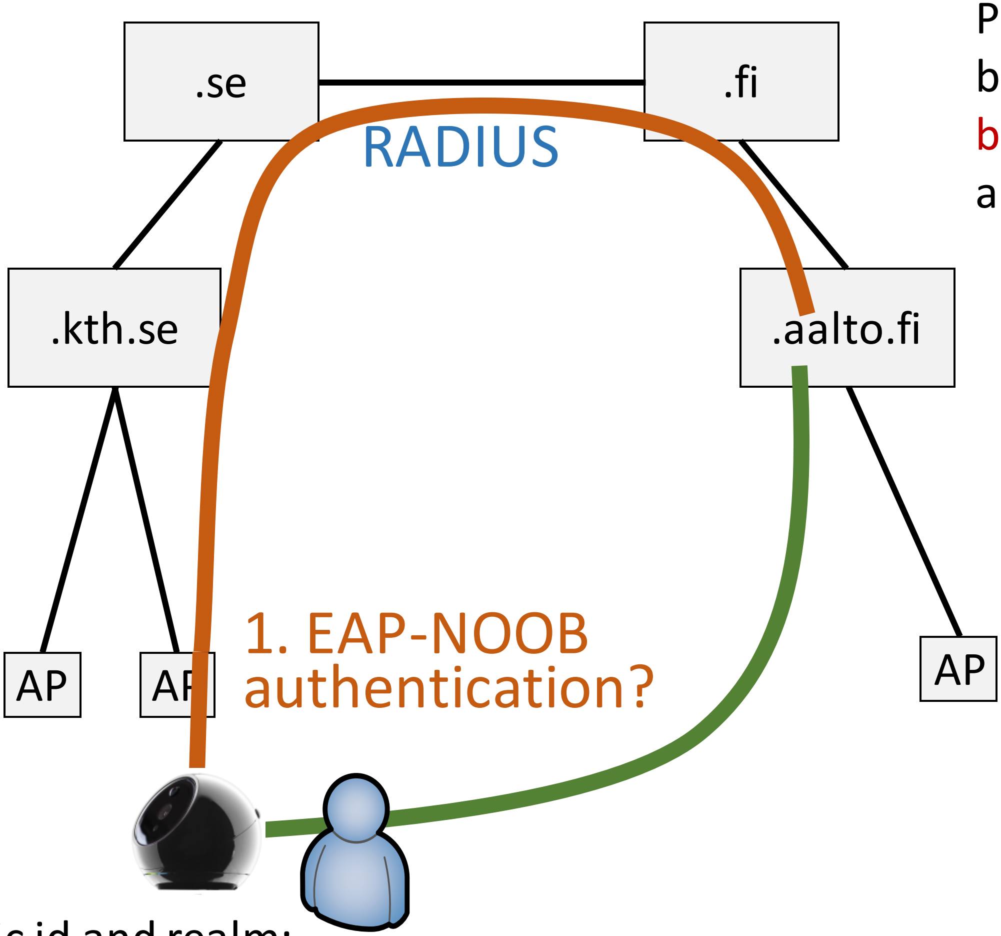
Roaming scenario 2: register while roaming



1. EAP-NOOB authentication?

But can we register a new device while roaming?

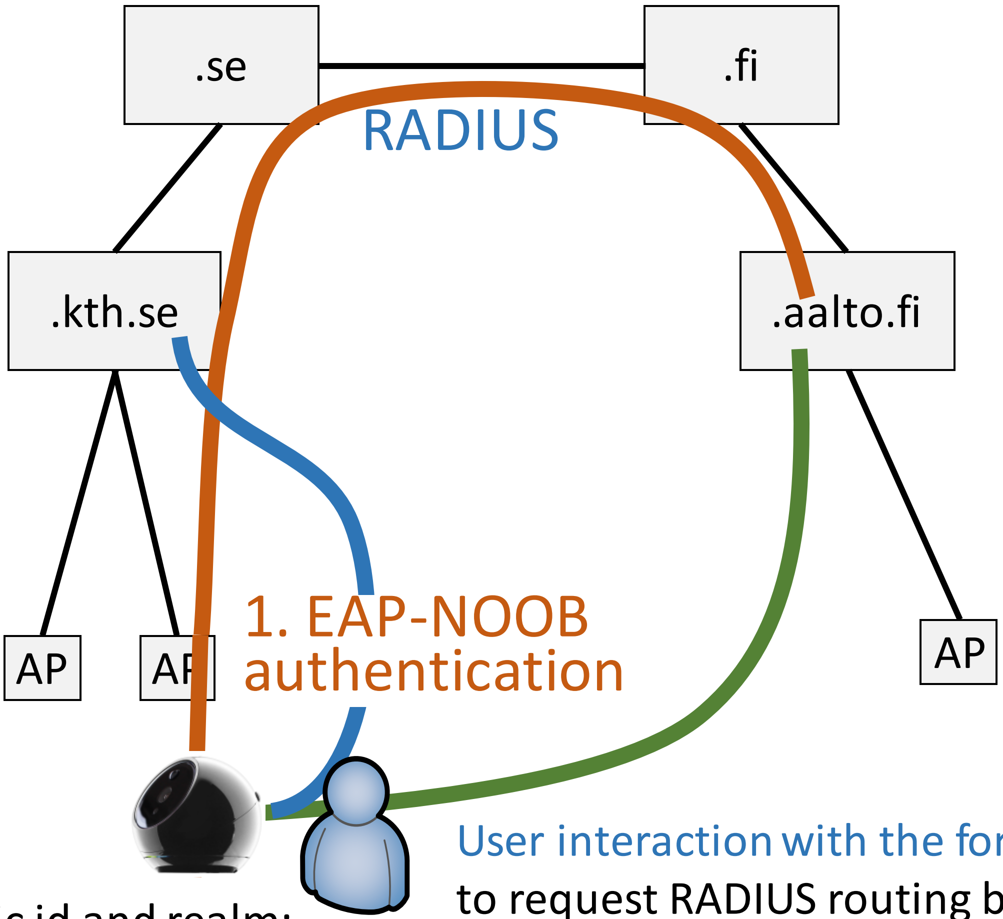
Roaming scenario 2: register while roaming



Generic id and realm:
noob@eap-noob.net

Problem: How to route EAP back to AAA home server before the device has been assigned a Realm?

Roaming scenario 2: register while roaming



Generic id and realm:
noob@eap-noob.net

User interaction with the foreign AAA is needed to request RADIUS routing back home, but only for the initial exchange. EAP-NOOB does not specify this, but also does not prevent it

Backup slides

TODO list

- IANA considerations:
  - Register an EAP method number
  - Register an .arpa domain to replace eap-noob.net
- Evaluation:
  - Timeouts in the protocol need modeling and user testing
  - Recovery from lost last messages: formally verified but should be written up into a report
- Possibly leave hooks for future extensions:
  - Device registration while roaming, identifier randomization, application configuration, e.g. service URL (currently only creating shared key for application layer), manufacturer certificates and other credentials

Formal models and verification

- mCRL2 model
  - Modeling Protocol messages and state machines
  - Deadlock-freeness
  - DoS resistance for intentionally dropped messages
- ProVerif model
  - Cryptographic key-exchange properties
  - Authentication and confidentiality
  - Misbinding: correspondence between user intention and protocol completion