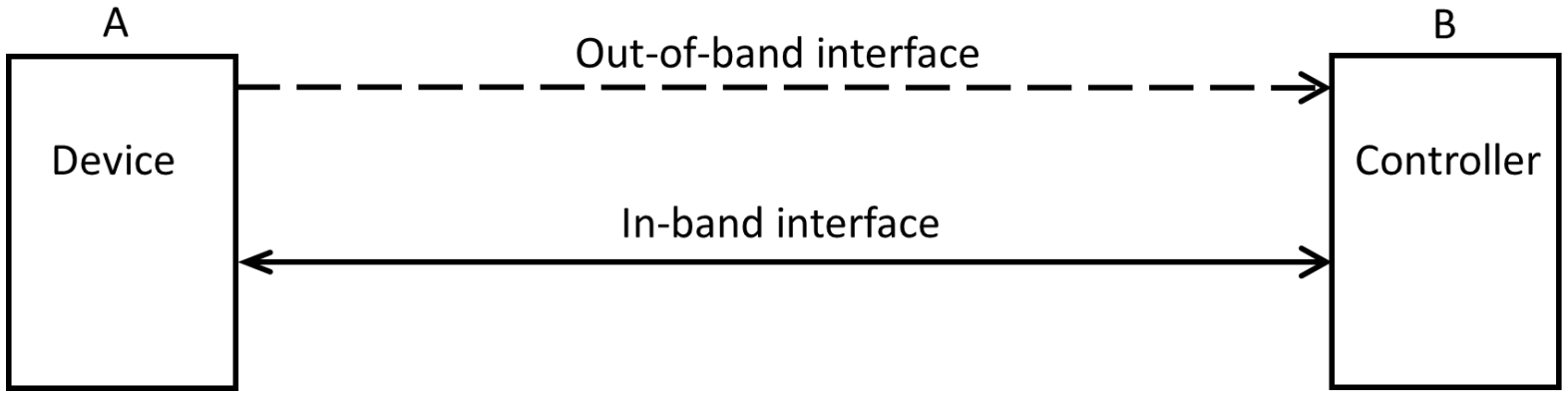
EAP Extension to Allow Peer Configuration

Sandeep Tamrakar, Philip Ginzboorg, Pekka Laitinen

Huawei

Motivation



- We are working on IoT bootstrapping security for consumer IoT devices
- Bootstrap resource constrained devices such as temperature sensor to a resourceful device such as mobile phone (controller)
  - Use OOB channel to transfer information that is used to secure bootstrap process
- In the context of IoT, bootstrapping involves:
  - **Pairing** a resource-constrained IoT device with a controller device such as a smartphone
  - **Taking ownership** by exchanging identities and credentials for mutual authentication and securing communication
  - **Configuring** the device to be **operational**
- Bootstrapping with EAP
  - How to use EAP to bootstrap devices including long term credential provisioning

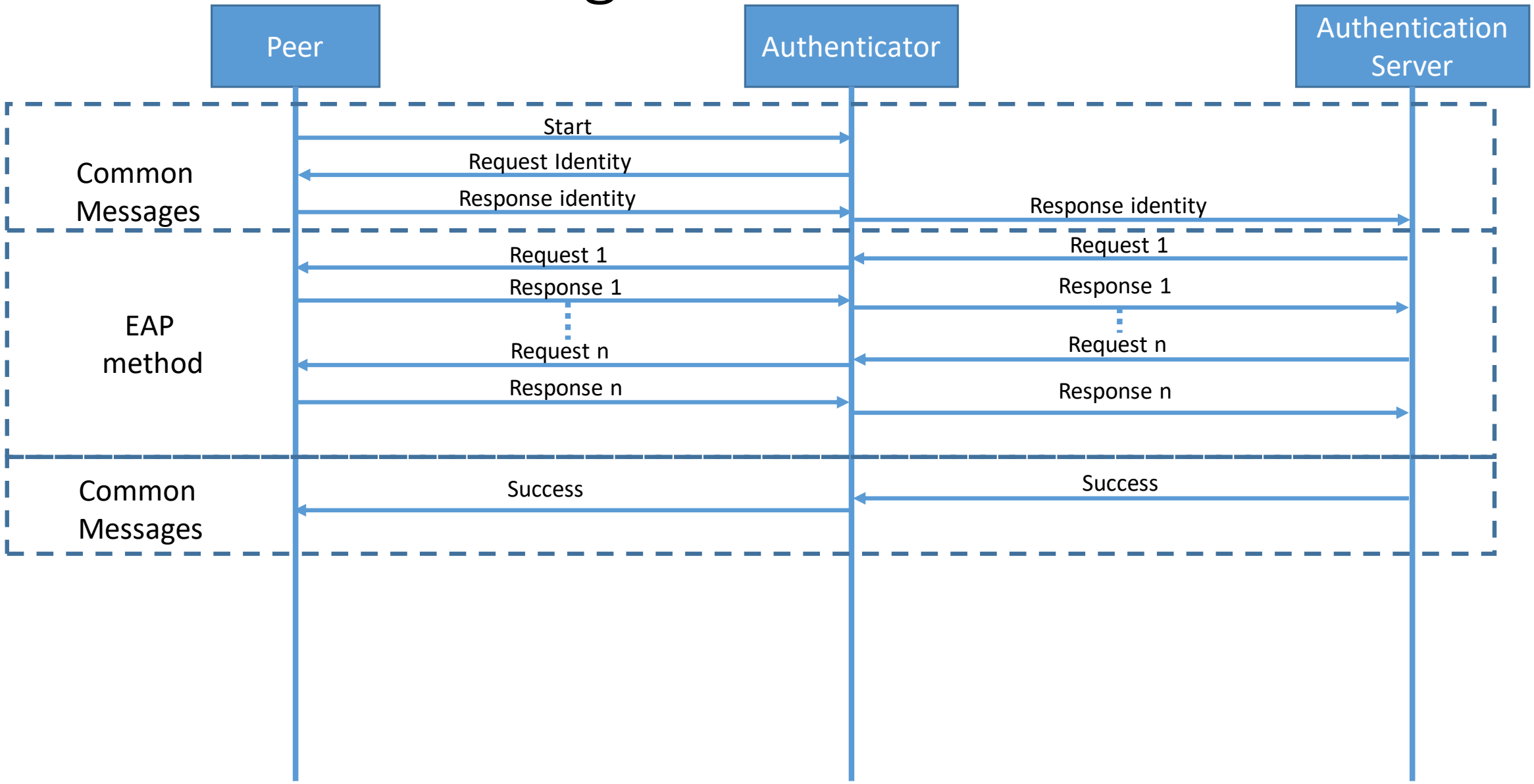
Related Work

- Credentials Provisioning and Management via EAP (EAP-CREDS)
  - A framework that has board goals
  - https://tools.ietf.org/html/draft-pala-eap-creds-05.
- EAP-TEAP
  - Allows peer device to provision client certificates
  - RFC 7170 https://tools.ietf.org/html/rfc7170

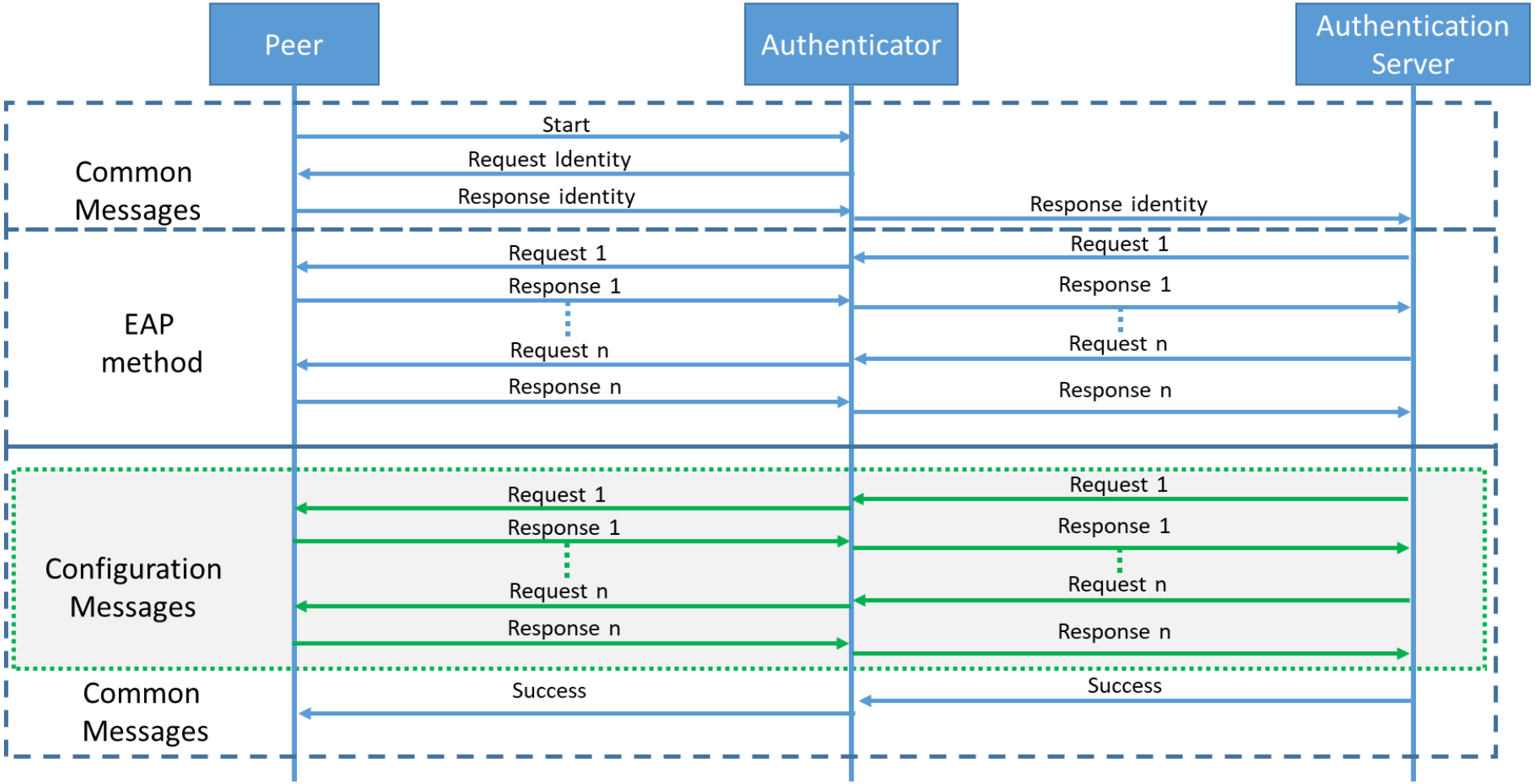
Goal

- Use EAP as a mechanism to enable Peer configuration from an EAP Authentication Server
- The configuration could be used for
  - Provision long-term credentials,
  - Set access control policies
- A simplest possible solution from implementation and specification point of view

Generic EAP Message Flow

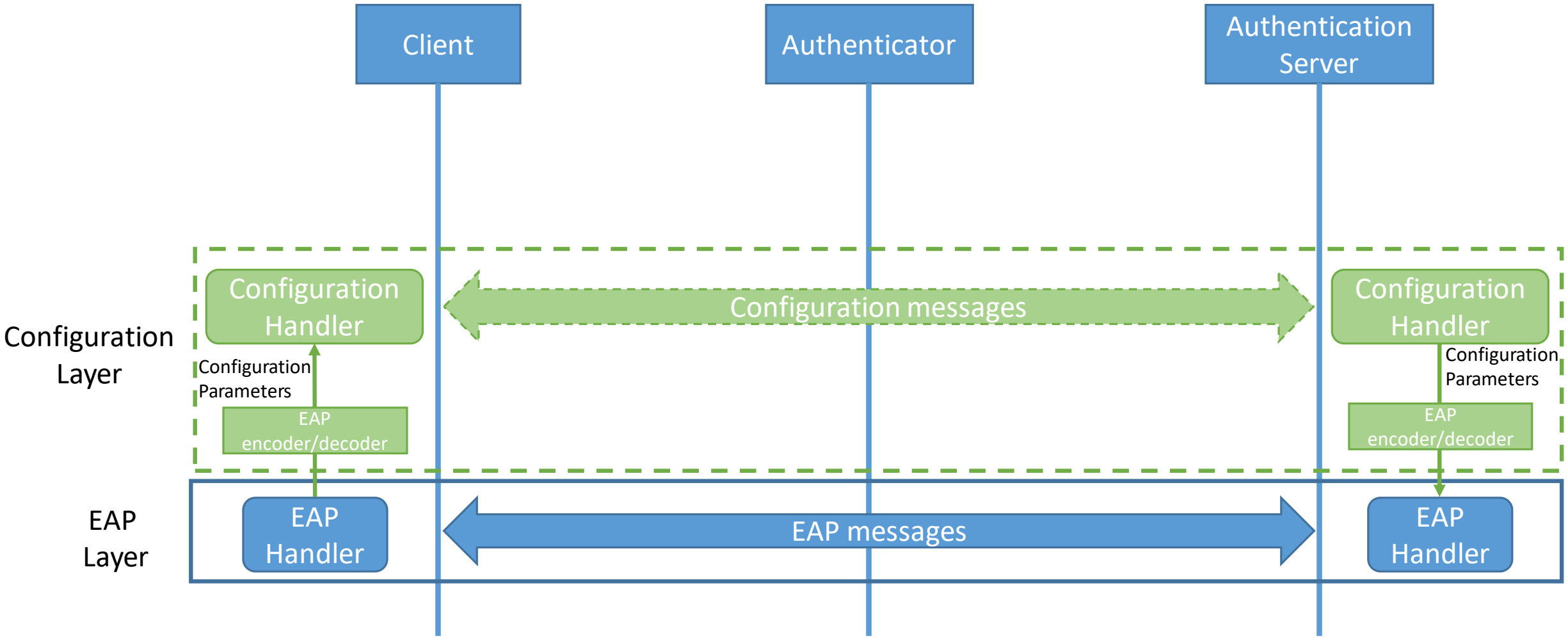


Possible approach for Peer configuration with EAP



- Configuration messages only to be sent after underlying EAP method has completed peer authentication
- Success message may or may not depend on the successful configuration however it must depend on EAP peer authentication

Architecture



Issues to consider

- Message fragmentation
  - A simple way is to fit each payloads **within a single EAP message**
- Push vs pull model
  - Push: Support for **server to push configuration** messages
  - Pull: Let the **peer device request configuration** parameters
- Discovering mechanism
  - A simple and efficient way to find out **if the other end-point supports configuration**
- Security for the configuration
  - Based on EAP session key
  - Using MSK+EMSK for securing the configuration messages
- Avoiding unnecessary roundtrips
  - Probing for configuration needs to be very efficient
- Limits on the number of EAP messages caused by the AP and EAP server

Possible approaches

1. Define new EAP message type for configuration messages
   - EAP request and response type
   - EAP request can be sent in either direction
   - Reuse an existing Notification request and response
2. Define a new EAP method that uses existing EAP tunneling method for authentication
   - Similar to EAP-CREDS
3. Define a mechanism that allows an end-point to indicate that another configuration protocol shall continue after the EAP session has ended
   - Mechanism allowing the configuration protocol to bind with the EAP session
     - E.g. a shared secret from the EAP session

Guidance from EAP group

Thank you.