Problem Description for Authorization in Constrained Environments

draft-seitz-ace-problem-description-03

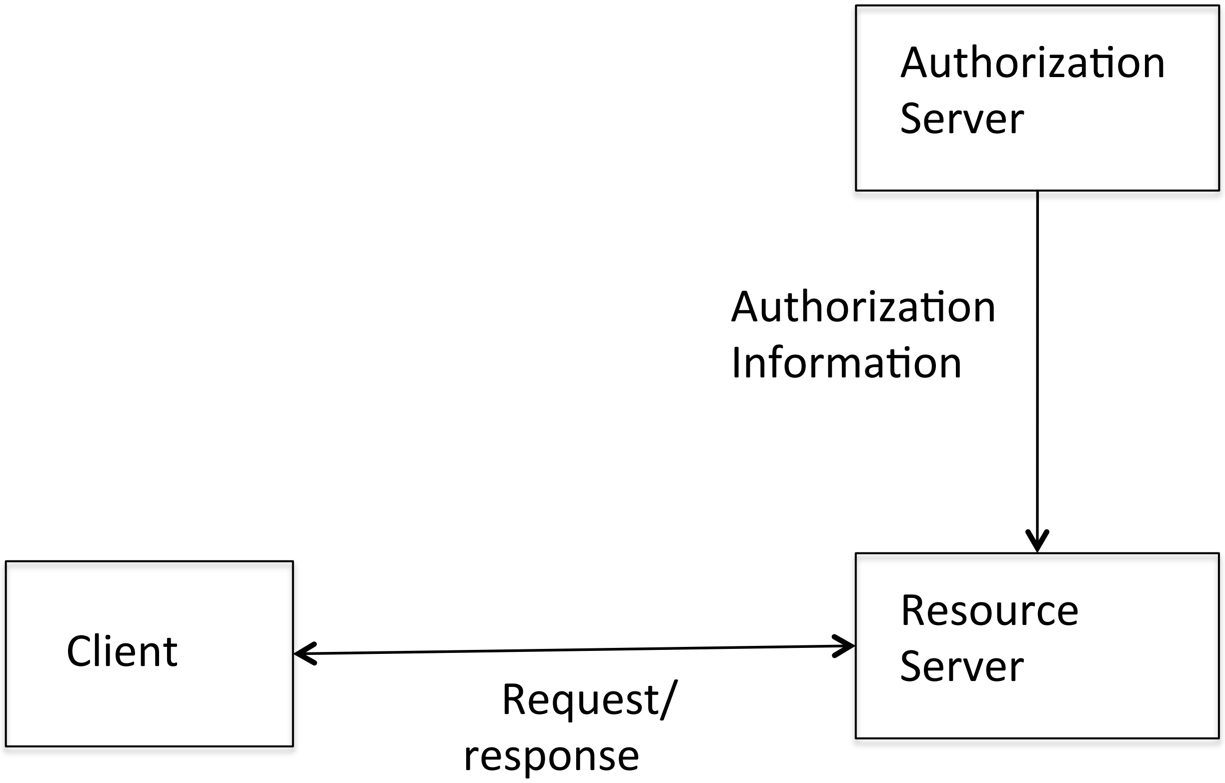
Ludwig Seitz, SICS
Göran Selander, Ericsson

IETF 92 ACE WG, Dallas, March 24, 2015

Terminology and scope

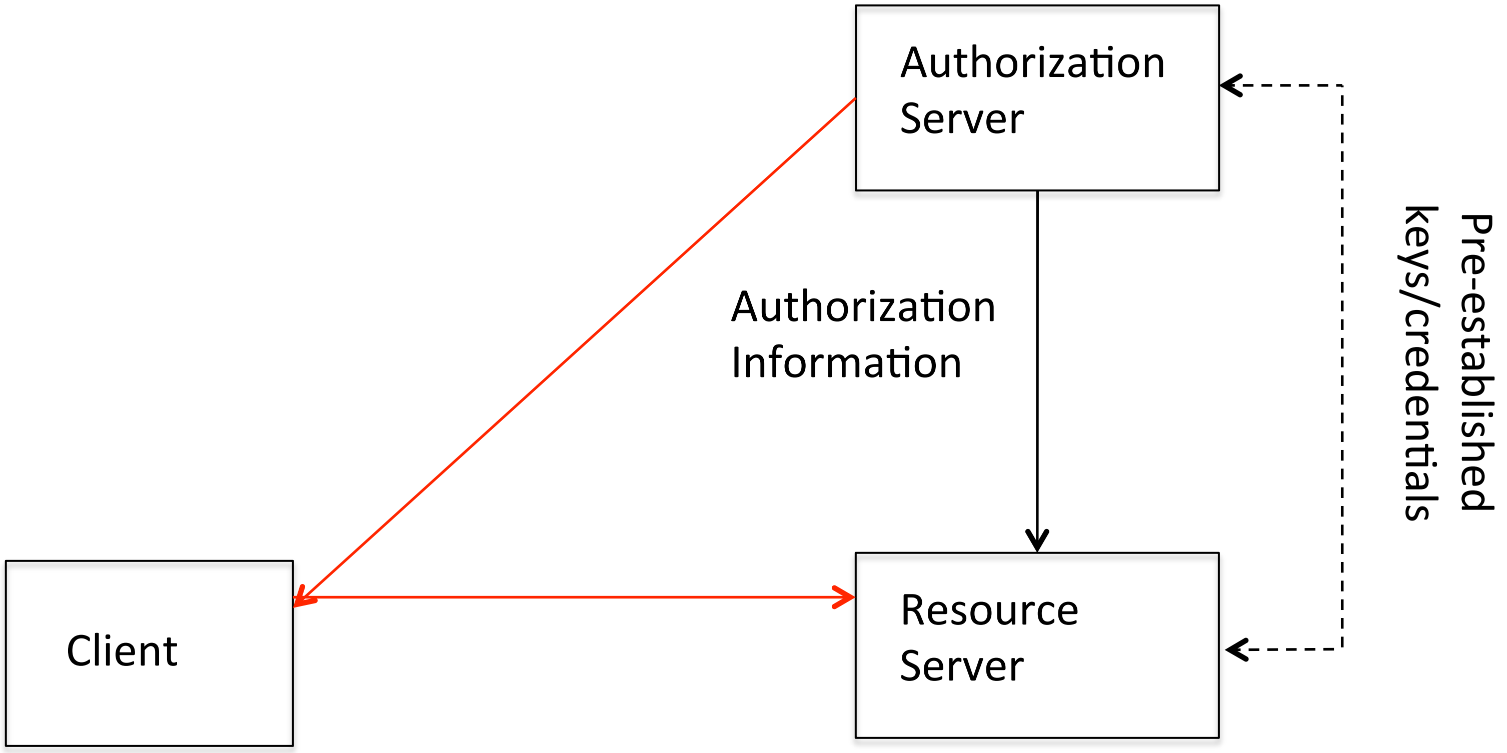
- Oauth/UMA terminology
  - Resources (R), Resource Owner (RO)
  - Client (C), Requesting Party (RqP)
  - Resource Server (RS) hosting R
  - Authorization Server (AS) acting on behalf of RO
- C and/or RS may be constrained, AS is not
- Information flows
  - C requests access to RS, and receives response
  - AS provides authorization information to RS

Problem Statement



These information flows need to be protected end-to-end

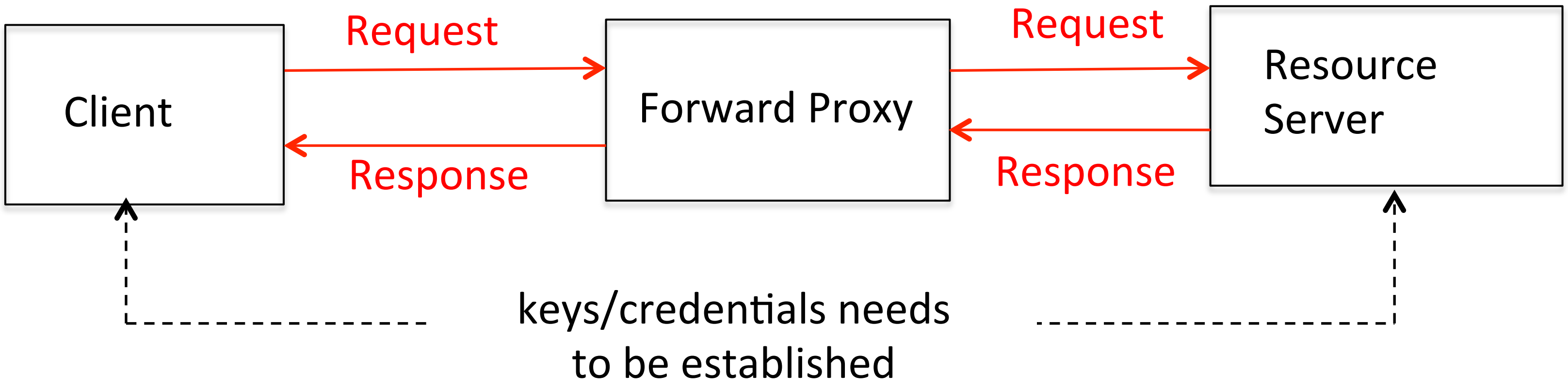
Protection of Authorization Information



- Authorization needs to be protected end-to-end
- Ex. (Pull): AS →C → RS (authorization information)

  Actual message flow (in red) via untrusted node C

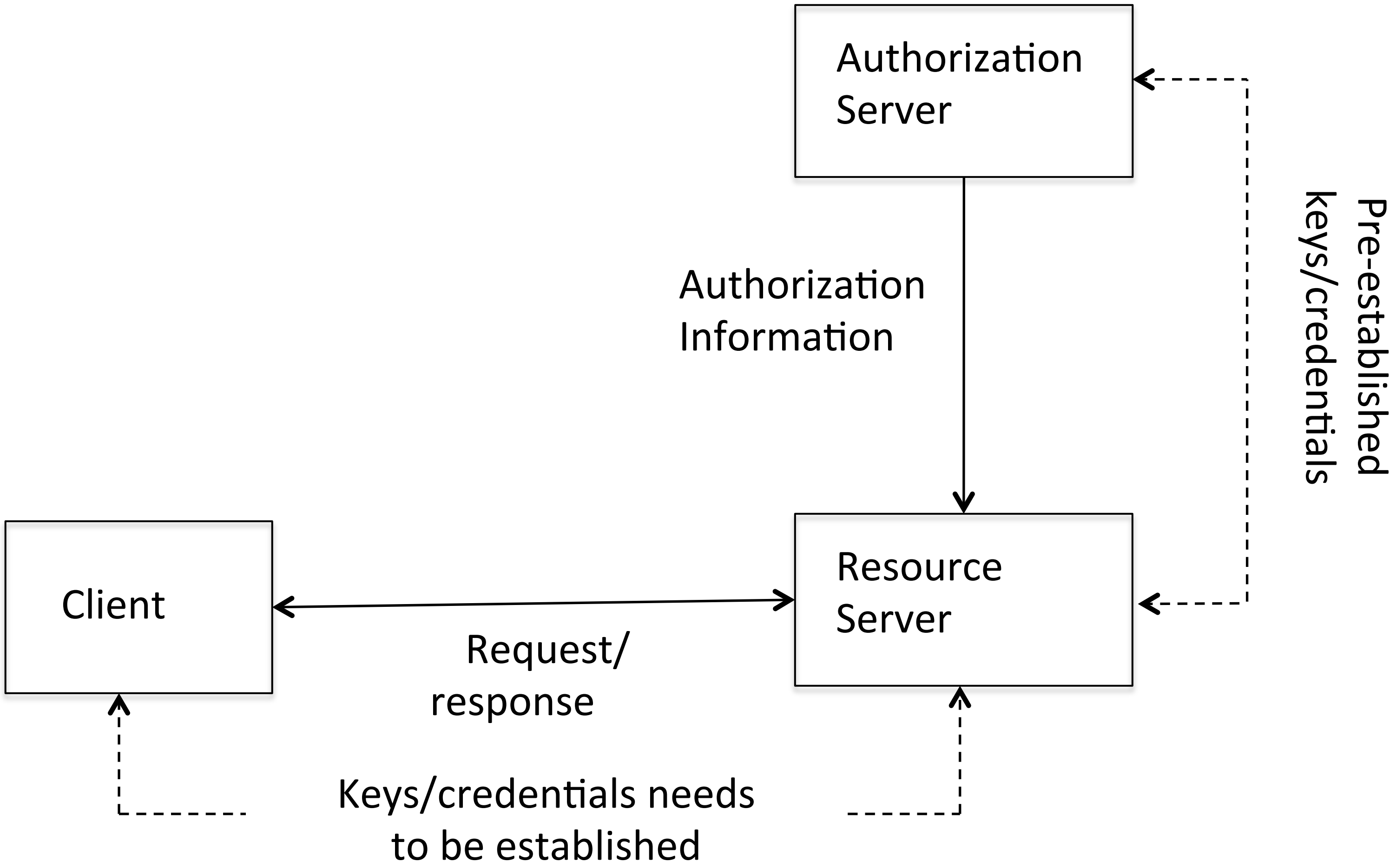
Protection of Request/Response



- Request/response needs to be protected end-to-end
- Ex.: Client <-> Forward Proxy <-> RS (request/response)

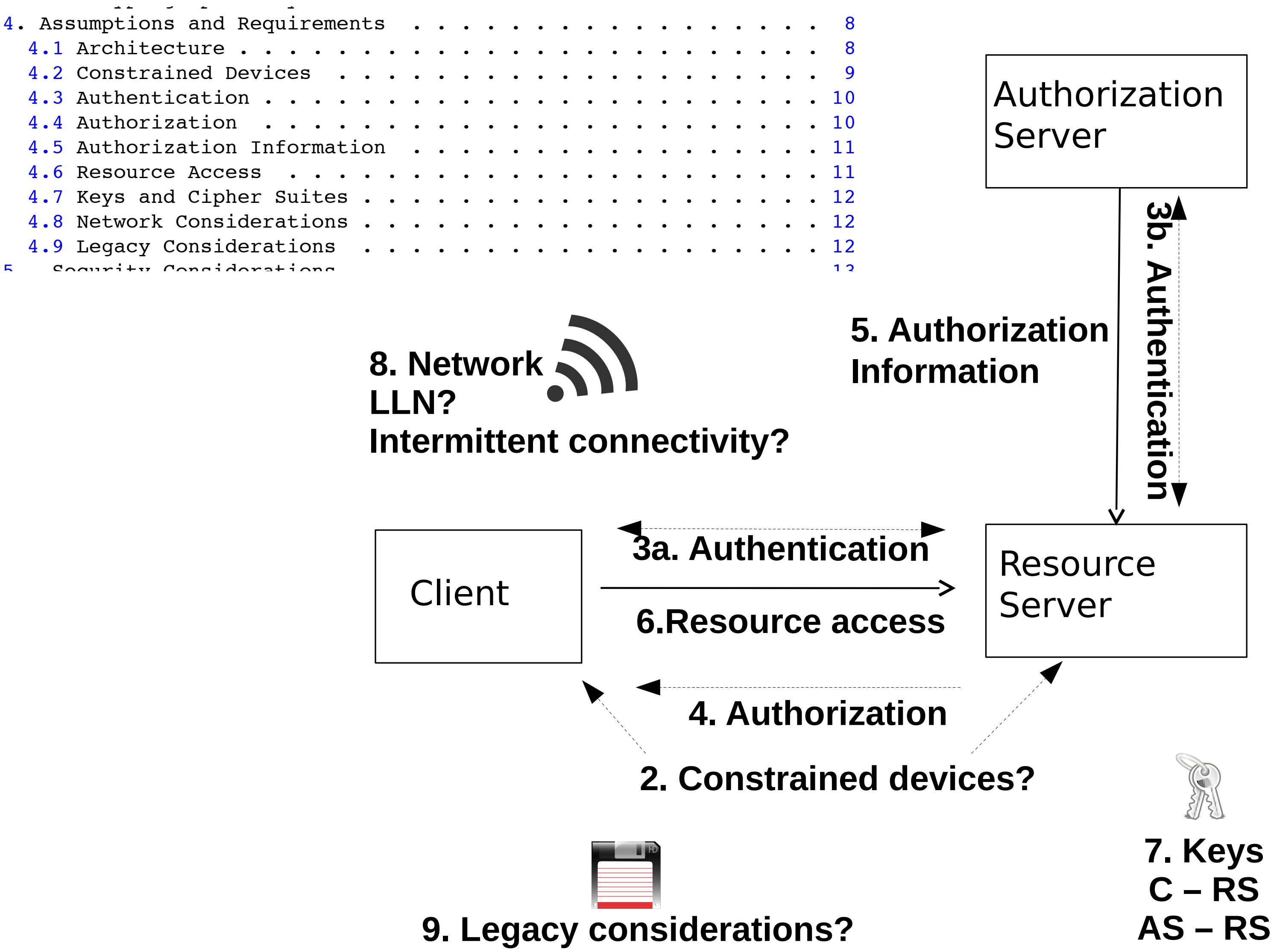
  Actual message flow (in red) via untrusted Forward Proxy

Problem Statement Summary


Authorization Server
Pre-established keys/credentials
Authorization Information
Client
Resource Server
Request/ response
Keys/credentials needs to be established

These information flows need to be protected end-to-end

Assumptions and Requirements



Authorization Server

3b. Authentication

5. Authorization Information

8. Network
LLN?
Intermittent connectivity?

Client

3a. Authentication

6.Resource access

Resource Server

4. Authorization

2. Constrained devices?

7. Keys
C – RS
AS – RS

9. Legacy considerations?