Power of Attorney based authorization

Draft: https://www.ietf.org/archive/id/draft-vattaparambil-irtf-dinrg-poa-00.txt

Sreelakshmi

Olov Schelén

Ulf Bodin

Power of Attorney traditionally

- PoAs are legal documents that are used to delegate our privileges to someone we trust.
- Here the secondary party legally acquires some ownership and rights as the primary person as specifically regulated by the PoA.
- We examine the PoA from a digital standpoint, so that it can be used in situations where the user needs to use a trusted device or entity to act/work on his/her behalf.

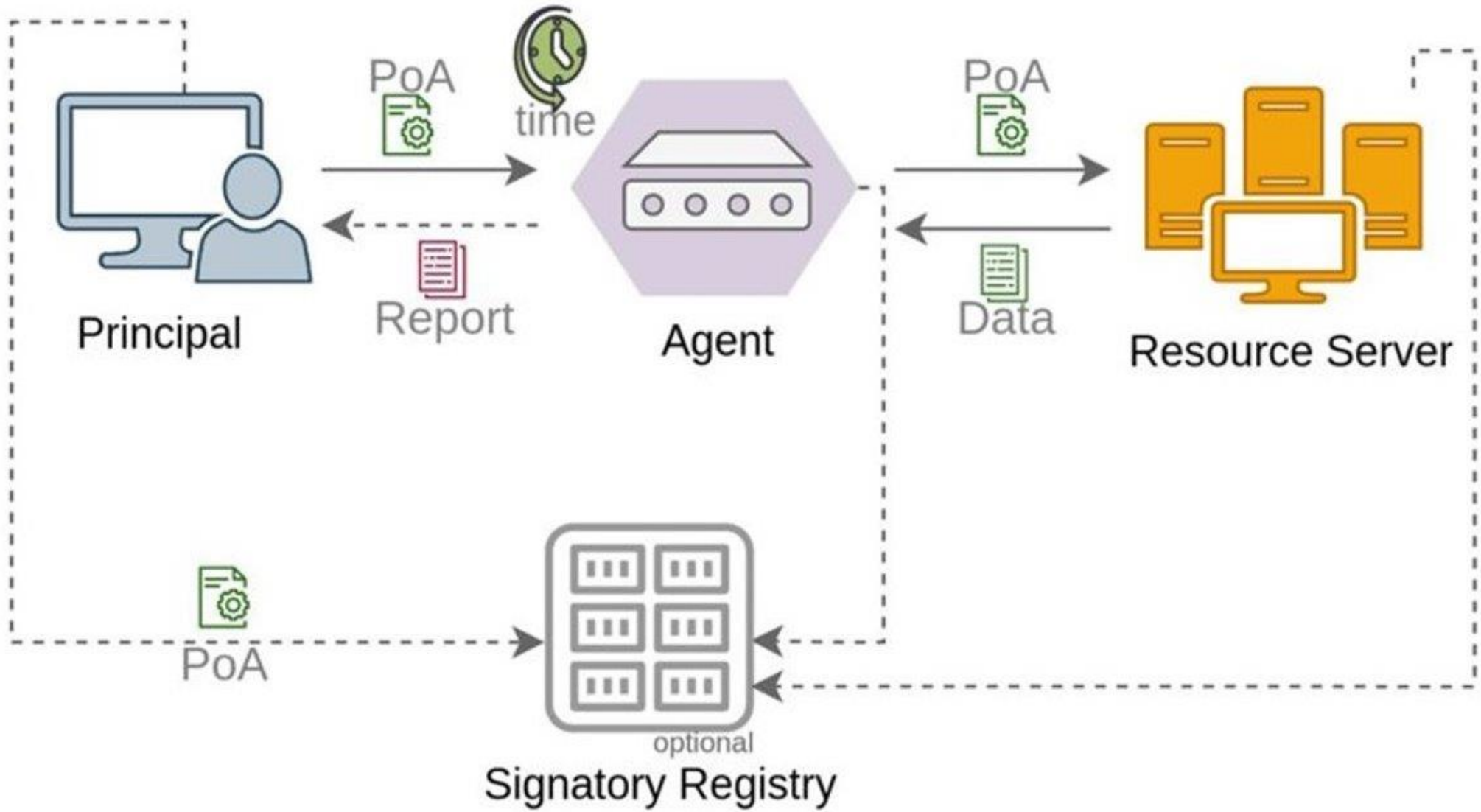
Positioning and Motivation

- We propose Power of Attorney (PoA) based authorization
  - PoA is a digital document that the principal signs and directs to an agent
- To authorize entities (e.g., semi-autonomous devices) with an identity (called agents) to act on behalf of a resource owner (called principal), with some defined credentials
  - Example: CPS onboarding and subgranting

Outline: We first present PoA, then discuss how PoA complements state of the art authorization, and alternatives.

PoA properties

- Self-contained and decentralized (e.g., like PGP)
  - May be supported by optional signatory registry
- Separation in time between signing of a PoA and acting upon it
  - The principal may not be online or available when the PoA is used
- Enabling multi-level subgranting (delegation)
  - e.g., "I give you a quite general master PoA, on which you can generate other, typically more specific PoAs (chain of PoAs)"
- Includes detailed credentials and expiration time
- Can contain additional integrity info such as device/software hashes


PoA
time
PoA
Principal
Report
Agent
Data
Resource Server
PoA
optional
Signatory Registry

Example: PoA approach for onboarding

- Establish trust chains between the target network owner and **subcontractors** for **automatic onboarding** of devices
- Then between **subcontractor** and their devices
- At onboarding, the **ownership** of the device may be kept by the subcontractor
- PoA from the target network owner ensures policies for subcontractors to submit devices for onboarding
- PoA from the subcontractor to devices ensures that only devices that work on behalf of a subcontractor can onboard.

- Together providing efficient and effective onboarding of devices to a target network.
  - Admin scalability and security
  - Time limited as desired
  - Authorization credentials
  - Low management overhead

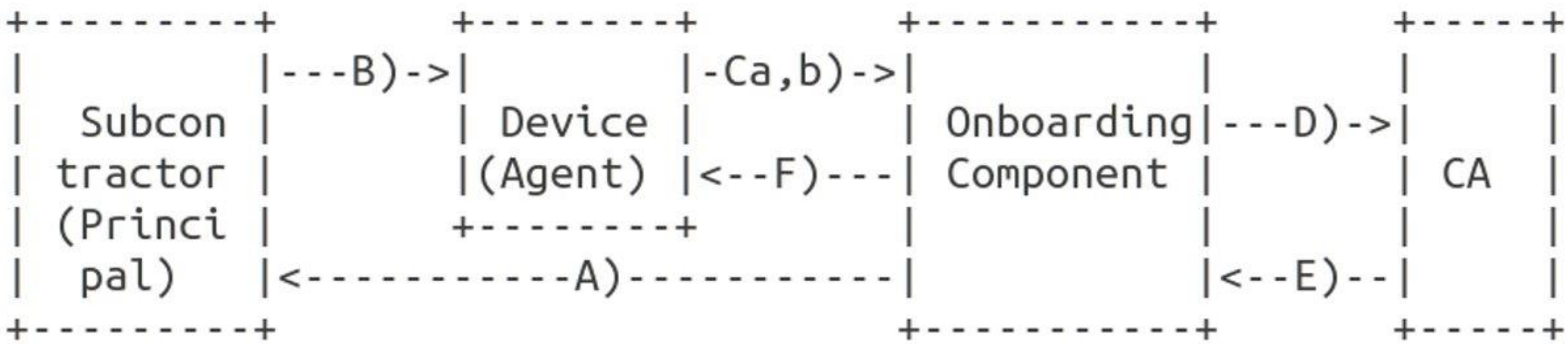
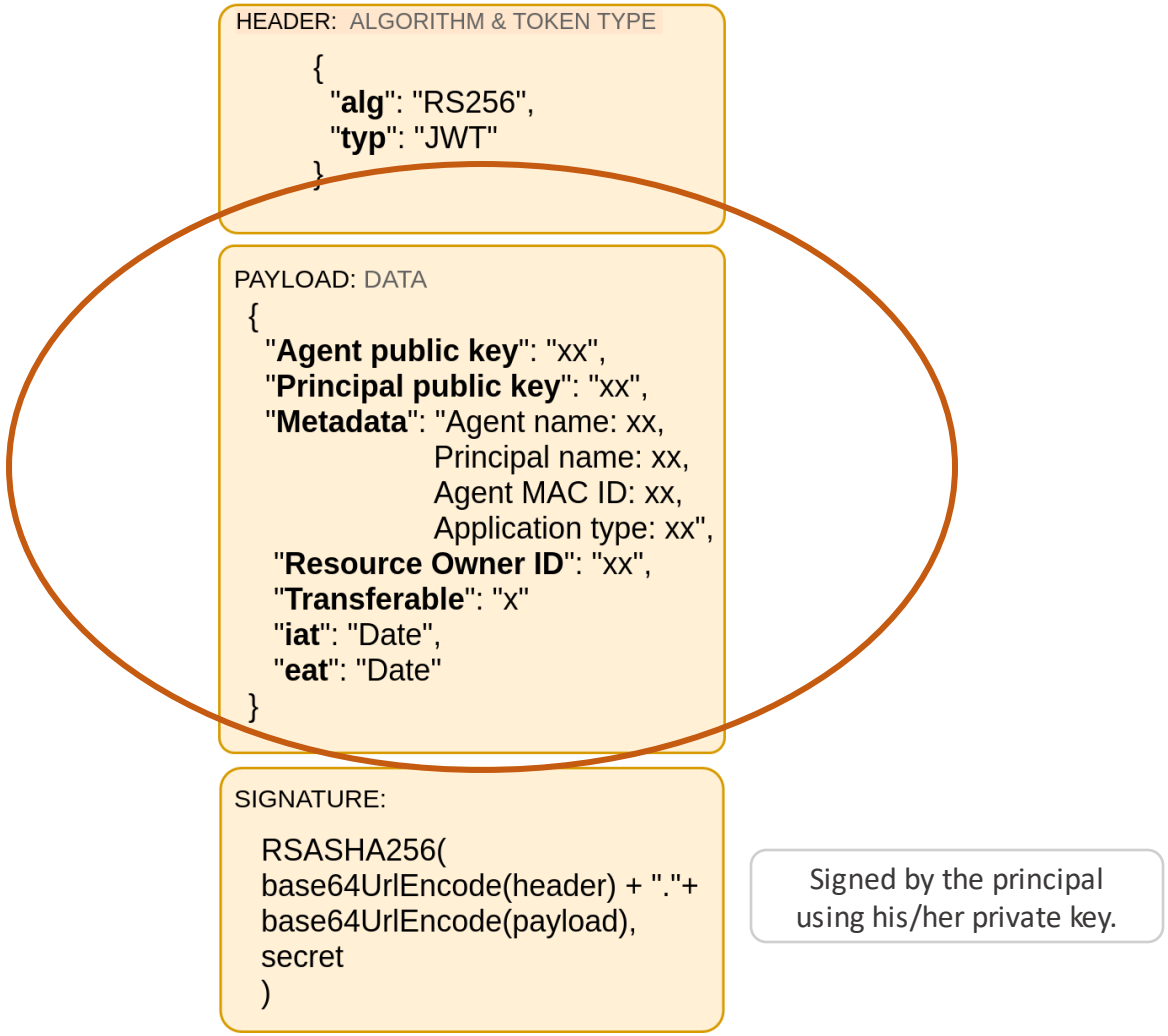


Fig 1: Protocol flow of PoA based onboarding

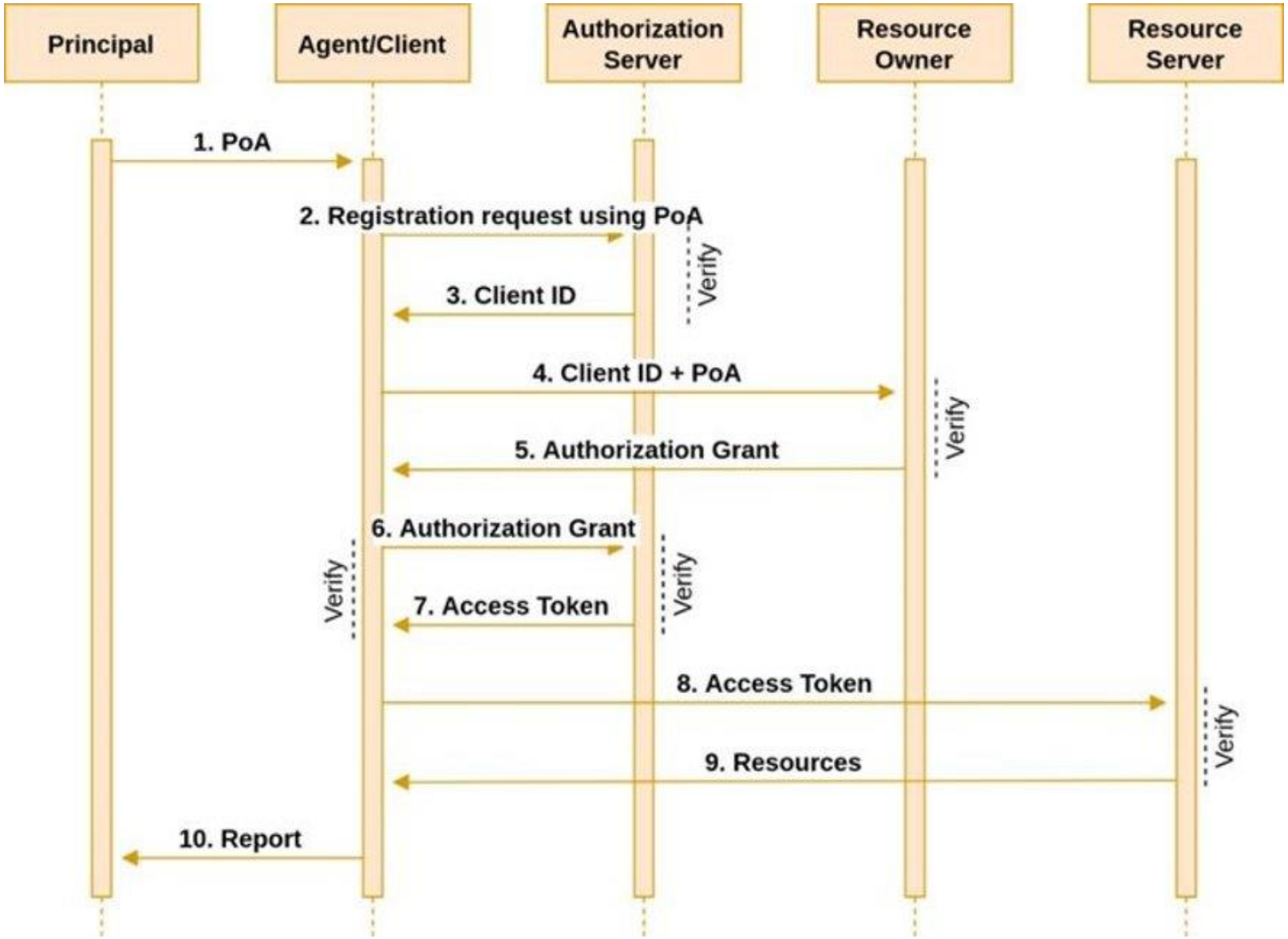
PoA structure



Implementations

- To enable PoA execution in any system:
  - Open-source library
  - Trustworthy downloadable image (e.g., docker image)
  - PoA integration with OAuth

PoA-OAuth integration



Future work

- Implementation of PoA library (Java) and docker image.
- Security analysis

- Draft: "PoA-based authorization technique" https://www.ietf.org/archive/id/draft-vattaparambil-irtf-dinrg-poa-00.txt
- Source code (proof of concept): https://github.com/sreelakshmivs/poaLibraryCode
- Review and comments from WG
- Thank you! More questions?
  - Contact: srevat@ltu.se, olov.schelen@ltu.se

Alternative approaches

- Proxy signature
- OAuth
- UMA
- GNAP