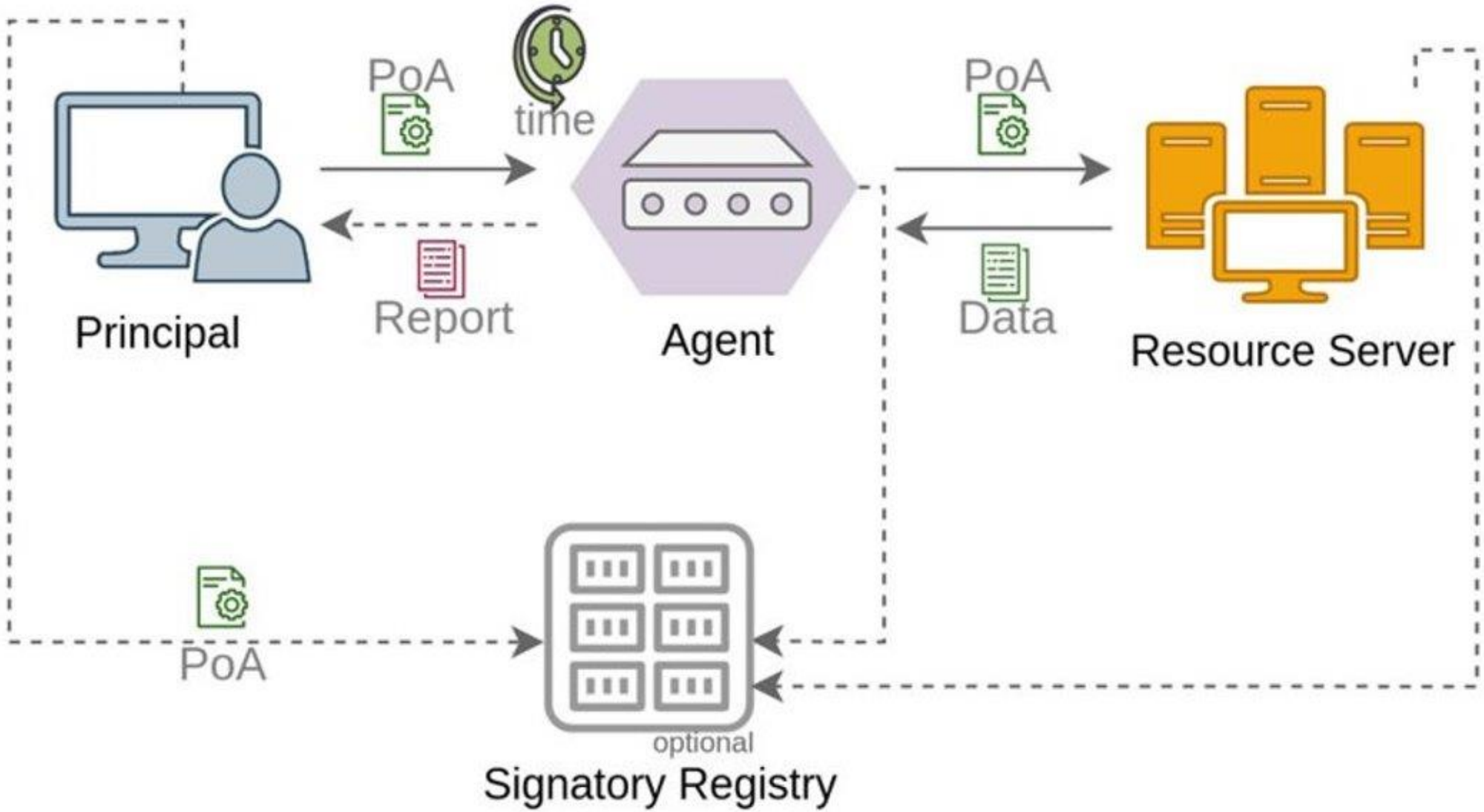
Power of Attorney based device onboarding and IETF

Sreelakshmi
Olov Schelen
Ulf Bodin

PoA overview

- 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)
  - Includes detailed credentials and expiration time


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

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)"
- Can contain additional integrity info such as device/software hashes

PoA-onboarding motivation

- Onboarding must be administratively scalable (eg: industrial site)
- Site owner must have a secure method to delegate onboarding credentials to subcontractors and integrators
  - so they can onboard their devices permanently or temporarily to a target network
- Onboarding should not require all parties in the trust chain to be online
- Onboarding should not necessarily involve transfer of ownership

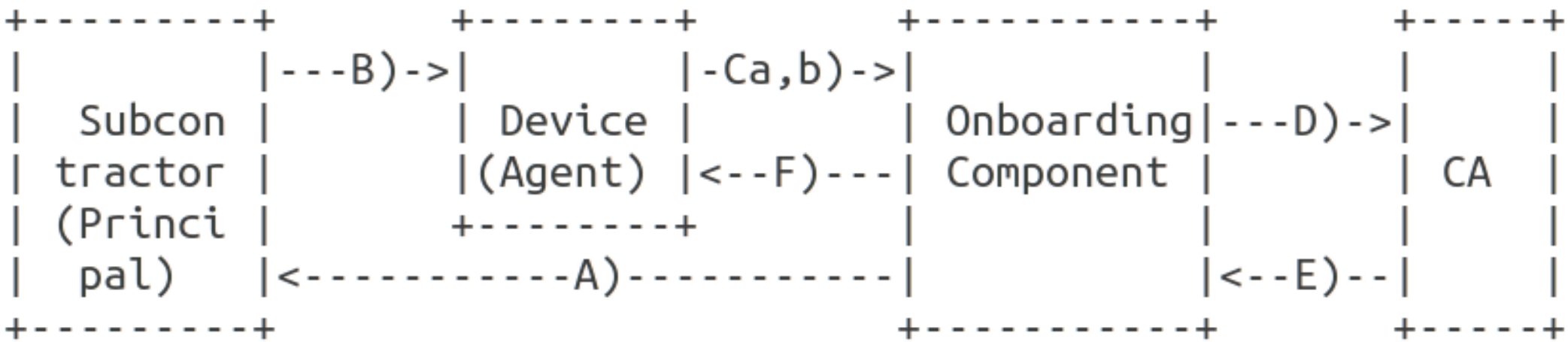


Fig 1: Protocol flow of PoA based onboarding

PoA Library

- Python library: https://test.pypi.org/project/poalib-srevat/
- Application Source code: https://github.com/sreelakshmivs/PoAapplicationPart

PoA ongoing works

- Internet Draft, WG: IoTops.
- Draft name: "poa-based-onboarding"
  - Link: https://datatracker.ietf.org/doc/draft-vattaparambil-iotops-poa-based-onboarding/
- IETF presentation: In the iotops (IoT operations wg). The questioning and discussion were detailed .
  - 36 m 30 s into this recording: https://www.youtube.com/watch?v=12Sagg32HT8

Ongoing works

- OAuth extension using PoA
- Developing a java library for the PoA based authorization.
- Positioning of PoA with respect to other internet standards.

Thank you