Power of Attorney based device onboarding


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 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 (e.g., 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
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.
  - Scalable and secure
  - Time limited as desired
  - Authorization credentials
  - Low management overhead
Fig 1: Protocol flow of PoA based onboarding
PoA structure

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "RS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "Agent public key": "xx",
  "Principal public key": "xx",
  "Metadata": "Agent name: xx,
    Principal name: xx,
    Agent MAC ID: xx,
    Application type: xx",
  "Resource Owner ID": "xx",
  "Transferable": "x",
  "iat": "Date",
  "exp": "Date"
}
```

SIGNATURE:

```
RSASHA256(
  base64UrlEncode(header) + "+" +
  base64UrlEncode(payload),
  secret
)
```
Implementations

• To enable PoA execution in any system:
  • Open-source library
  • Trustworthy downloadable image (e.g., docker image)
  • PoA integration with OAuth
• Draft: "poa-based-onboarding"
• Review and comments from WG
• Thank you! More questions?
  • Contact: srevat@ltu.se, olov.schelen@ltu.se