SCIM device use cases

Janelle Allen, Eliot Lear

How are these identities the same and how are they different?

The systems in which their credentials reside both need to be primed (provisioned)

Why SCIM?

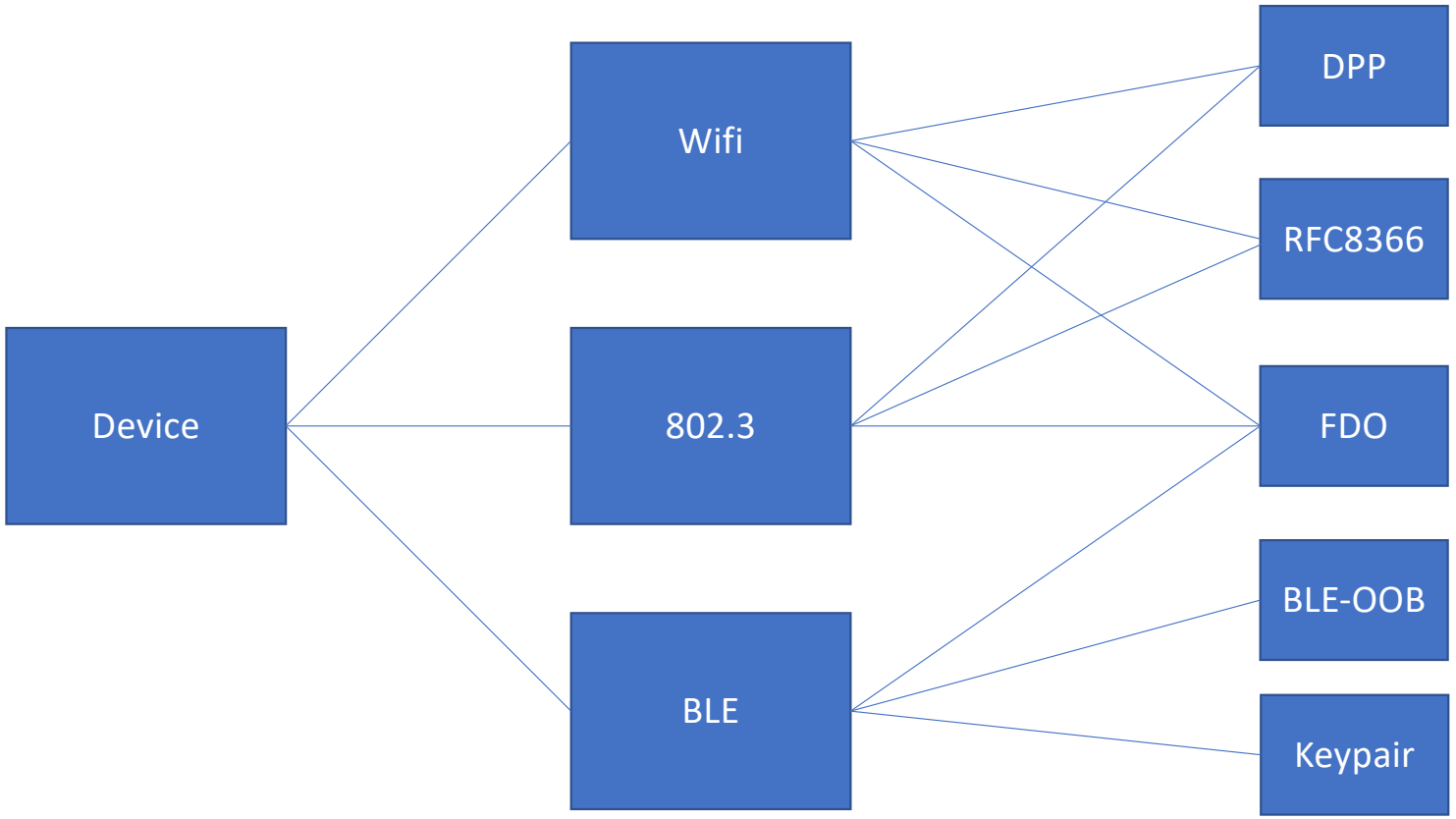
- This is a provisioning function
  - Create a new device
  - Delete an old device
  - (maybe) update an existing devices
  - Group devices
- This is a bulk device identity authentication/authorization function
- Why not SCIM? ;-)

Key Goals

- Automate flow of onboarding of devices that an enterprise acquires
- Allow for standardized approach
- Allow for Multiple L2 Technologies
  - Wifi
  - LoRa
  - 802.3 (Wired)
  - BLE
- Allow for multiple bootstrapping / authentication technologies
  - DPP (Wifi Alliance)
  - Vouchers (RFC 8366)
  - Naked certs?
  - BLE OOB
  - Fido FDO Vouchers

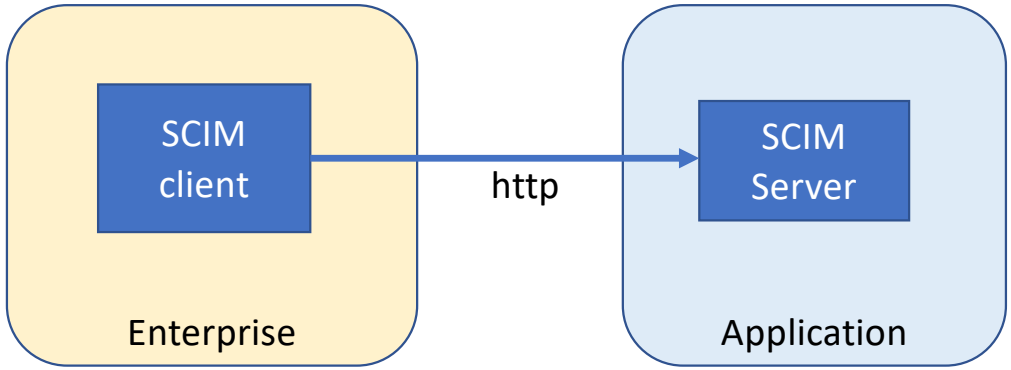
Deliver via a **normalized** schema (we have been developing in JSON schema)

What's this "fully normalized" business?

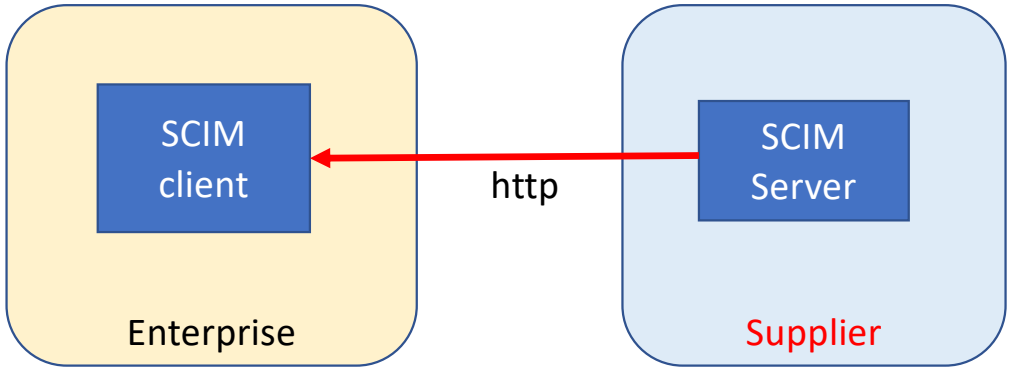


No Technology Religion

Another difference - directionality



"Add this user to your service"



"Add this device to your inventory"

Summary of variances from normal SCIM

- Bootstrapping credential movement is **required**
- A **supplier** may be the SCIM client
  - SCIM model ponders the the enterprise being the SCIM client
  - The **supplier** is providing a device, it must provide its credentials.
- Device identities are scoped based on the supplier
- Device attributes will vary based on L2/L3 capabilities
- Desire to carry other stuff
  - SBOM information
  - Device type

Questions/ Issues

- What is the relationship between users and devices?
  - Also… RBAC… maybe a group owns a device?
    - “Facilities owns lightbulbs”
  - Given backward nature of the communication, this is a question.
  - Lifecycle questions here…what is the supplier role?
- Should that be exposed here?
- Which schema language, please?
- Need real $refs in schema.
- Discuss here, please.

Next Steps

- A draft?