Device and
Certificate Lifecycle
Issues and Challenges

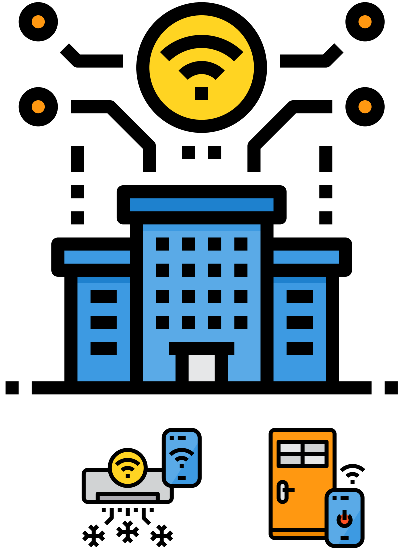
Michael Richardson <mcr+ietf@sandelman.ca>
IETF IOTOPS WG

For discussion: not related to only one draft

RFC8576 – Lifecycle Diagram

```
 _Manufactured           _SW update          _Decommissioned
/                       /                   /
|   _Installed          |   _ Application   |   _Removed &
|  /                    |  / reconfigured   |  /  replaced
|  |   _Commissioned    |  |                |  |
|  |  /                 |  |                |  |   _Reownership &
|  |  |    _Application |  |   _Application |  |  / recommissioned
|  |  |   /   running   |  |  / running     |  |  |
|  |  |   |             |  |  |             |  |  |             \\
+##+##+###+#############+##+##+#############+##+##+##############>>>
    \/  \______________/ \/  \_____________/ \___/         time //
    /           /         \          \           \
Bootstrapping  /      Maintenance &   \     Maintenance &
              /      rebootstrapping   \   rebootstrapping
        Operational                Operational
```

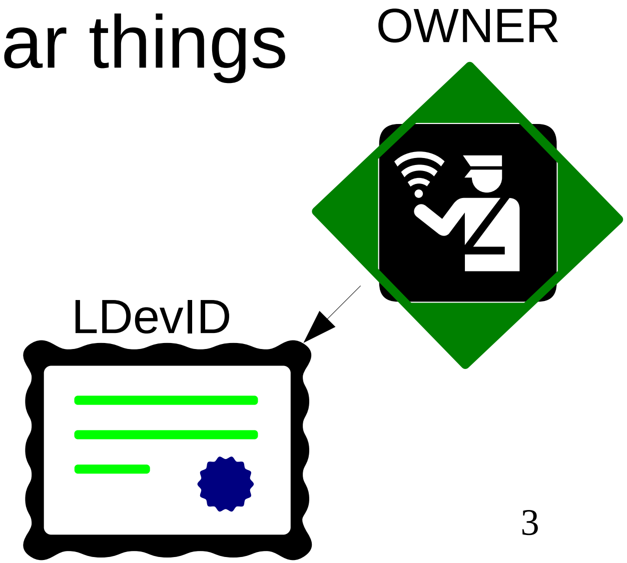
Figure 1: The Lifecycle of a Thing in the Internet of Things



Smart Building
Multi-tenant
Many changes

Owners Sign Certificates

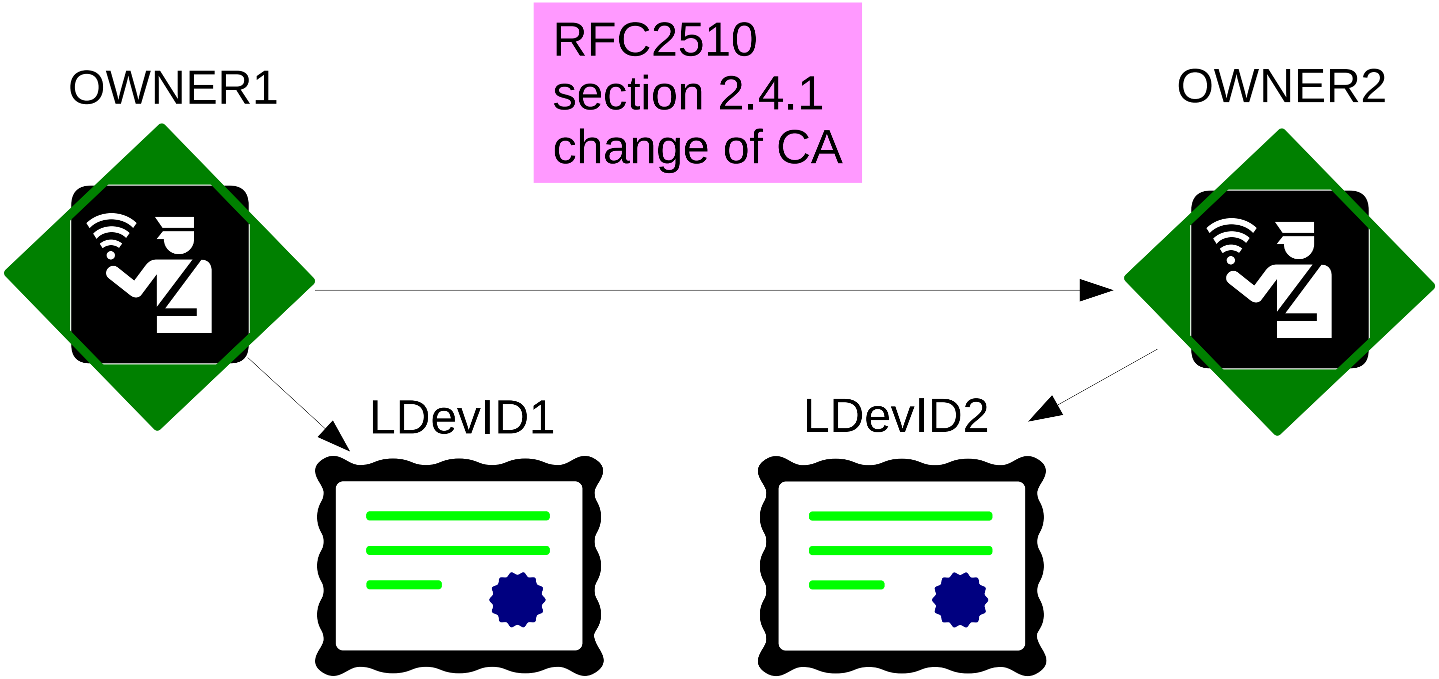
- BRSKI shows onwership by having Registrar sign LDevID for each device!
  - It appears that FIDO IoT$_{\text{(Intel SDO)}}$, CHIP, DeviceAuthority, and others do similar things involving a cryptographic identity



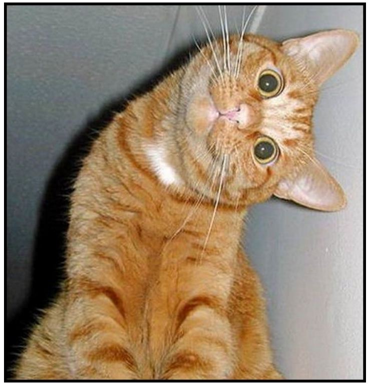
Devices Identified by Certificates

- LDevID can be used for 802.1X (WPA-Enterprise), and this most uniquely identifies the device, regardless of MAC randomization, or even if IP is not involved.
- LDevID certificates are ideal for ownership, but there are privacy challenges
  - This **is** something we need to work on at the IETF.
  - Randomized (MADINAS) MAC address efforts mean that those who were using MAC addresses as unique keys are doomed, and have to find another solution

Orderly Changes of Ownership



Disorderly (flash) changes of ownership



device has to get a new owner, without cooperation of old owner

- reset, redo-onboarding?

- sometimes has to occur without stopping operation
  - some critical piece of equipment

Addressing the gaps

- Long Lived certificates, with “frequent” checking
- Short-lived certificates, (STAR), always renewing
- Enterprise Private CAs for everyone
  - flash re-owning due to CA failure?
- Exorcising previous tenants