OPEN CONNECTIVITY FOUNDATION®

OCF 2.0.1 Security Primer for Device Vendors

Q1 2019

Nathan Heldt-Sheller

The Primary Roles of the OCF Security Layer

From a "normal" (non-security-expert) developer's perspective, the OCF Security Layer has two primary functions:

1. **Device Onboarding** – "pairing" a New Device (e.g. Out of Box) to the owner's domain. An example would be connecting a newly-installed lightbulb (a Server Device) to the home's OCF lighting control (a Client Device application).

2. **Access Control** – filtering incoming requests to a Device, and making a "Granted" or "Denied" decision for each request before it is passed to the Resource endpoint.
   Note: for the security-minded, this includes authentication in addition to authorization.

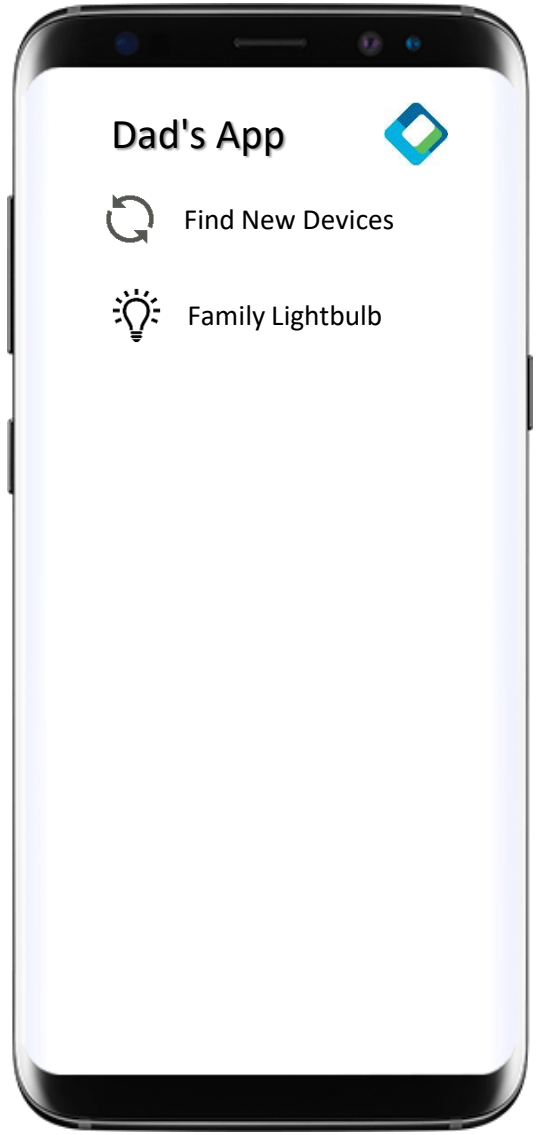
Both of these functions are achieved via a set of "Security Virtual Resources" (SVRs), which provide the interface through which Device Onboarding is accomplished, and Access Control is configured.

Onboarding a New Device (Lightbulb) Using an App (OBT) on Mom's Phone

1. Mom screws in the new lightbulb
2. Mom opens the OCF App on her Phone
3. Mom clicks the "refresh" icon and finds the lightbulb
4. Mom clicks the "+" button and onboards the lightbulb to the Smith Home network
    1. Behind the scenes, the OBT performs the Certificate-based OTM
    2. When finished, Mom's App is now able to control the lightbulb
5. Mom is prompted "Should 'Family' group members to be able to control this lightbulb?"
6. Mom clicks "yes"
    1. Other Clients that are part of the Family group can now control the lightbulb as well

Dad's Phone is added to the Smith Home domain

1. Dad installs and opens OCF App, but is not yet joined to the Smith Home domain
2. Mom opens the OCF App on her Phone
3. Mom clicks the "refresh" icon and finds Dad's phone. Mom's phone prompts her to onboard Dad's phone
    1. Mom clicks "yes" and Dad's phone is onboarded, but still doesn't have access to the lightbulb
4. Mom's phone prompts her to add Dad to the Family Group
    1. Mom clicks "yes" and Dad can now control the Lightbulb



How This All Works in OCF: Introducing the Security Virtual Resources (SVRs)

Although there are quite a few SVRs defined in the OCF Security Specification, there are just **four that are essential to understanding basic security function**:

1. **/oic/sec/doxm (or "/doxm") – The Device Owner Transfer (Xfer) Method Resource**
   The /doxm Resource provides the interface for taking ownership of a Device. Usually, taking ownership is the first step in onboarding a new Device into the owner's domain.

2. **/oic/sec/pstat (or "/pstat") – The Provisioning Status Resource**
   The /pstat Resource is used to manage further provisioning of a Device, after ownership is established. Specifically, the /pstat Resource is used to put the Device in "Ready for Normal Operation" (RFNOP) state, which signals that the Device is fully configured and ready to start its normal steady-state functioning (e.g. a lightbulb in "RFNOP" is ready to handle "on/off/dim" requests from the Lighting Controller App).

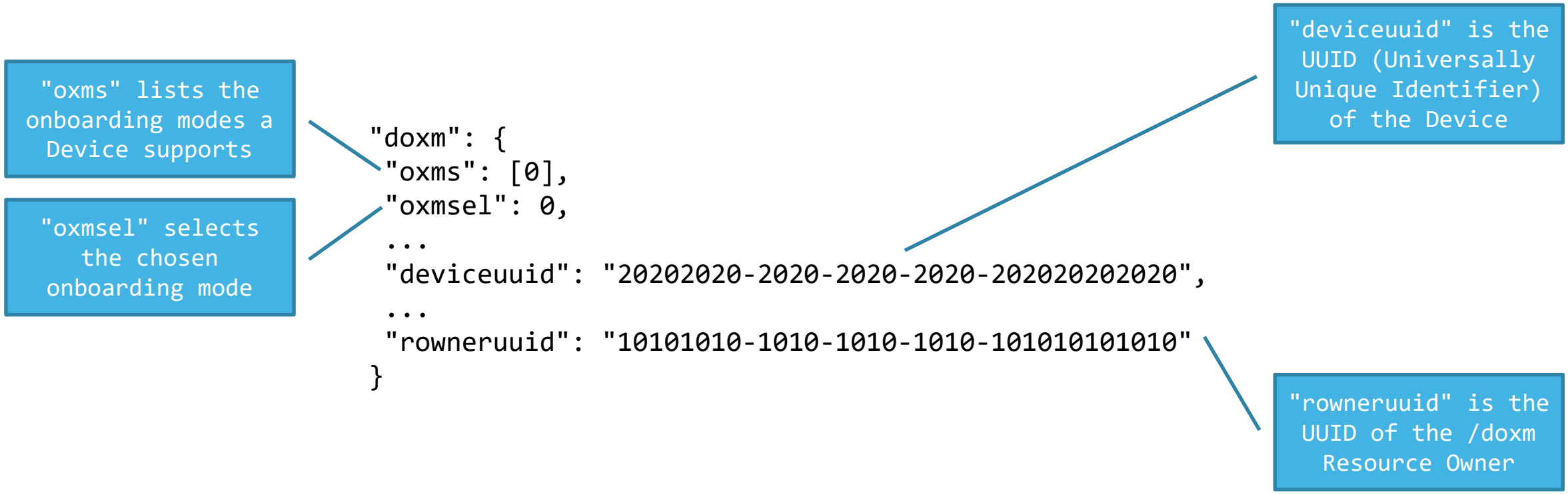
3. **/oic/sec/acl2 (or "/acl2") – the Access Control List Resource**
   The /acl2 Resource is used to configure the access control policy on the Device (i.e. which Clients are allowed to access which Resources, and what the access-modes – Retrieve vs. Update, etc – are allowed).

4. **/oic/sec/cred (or "/cred") – The Credentials Resource**
   The /cred Resource stores the credentials – cryptographic keys, certificates, etc. – that are required to establish secure connections, and verify Client identity, among other things.

Understanding /doxm

/oic/sec/doxm (or "/doxm") – The Device Owner Transfer (Xfer) Method Resource

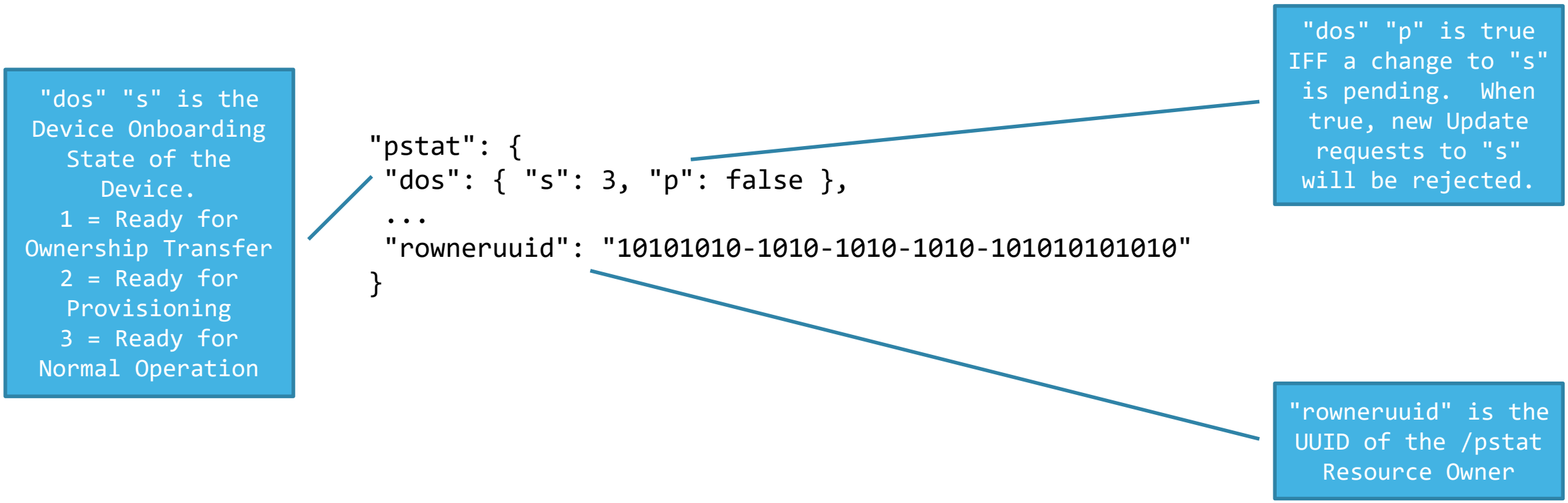
The /doxm Resource provides the interface for taking ownership of a Device. Usually, taking ownership is the first step in onboarding a new Device into the owner's domain.



Understanding /pstat

/oic/sec/pstat (or "/pstat") – The Provisioning Status Resource

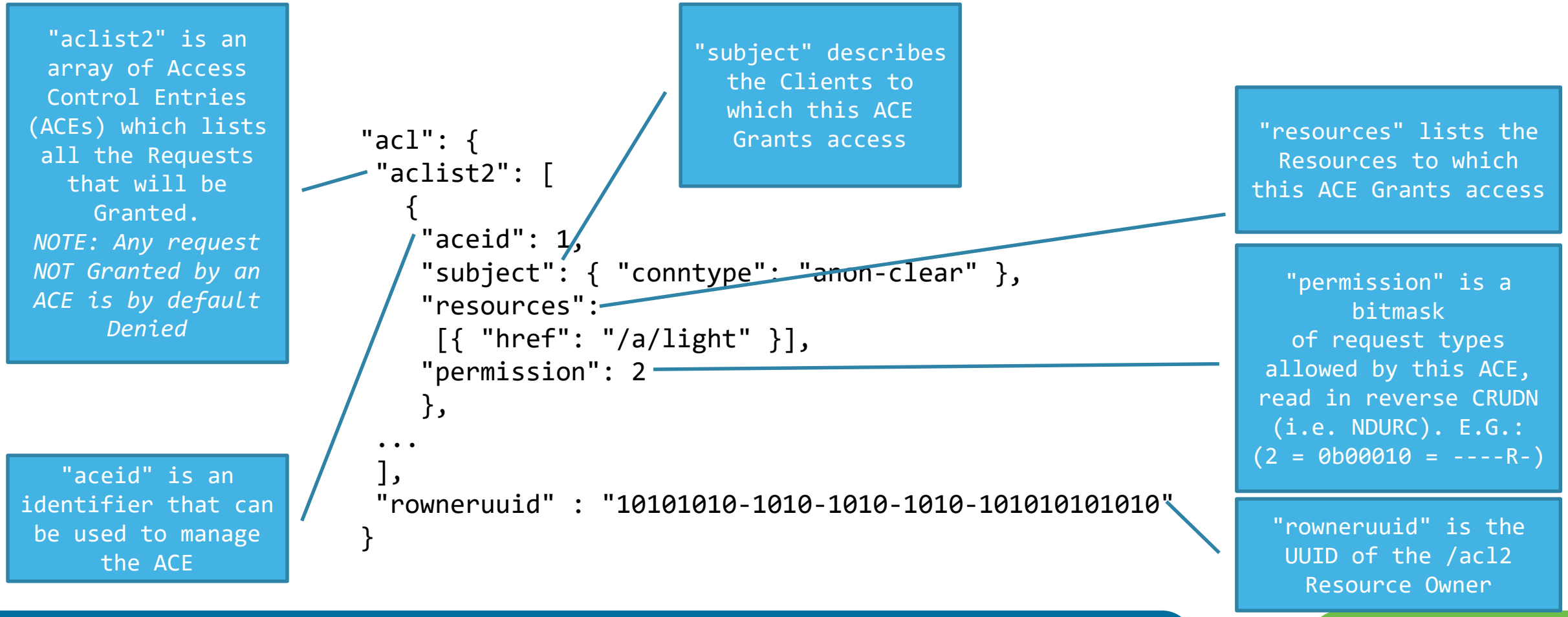
The /pstat Resource is used to manage further provisioning of a Device, after ownership is established.



Understanding /acl2

/oic/sec/acl2 (or "/acl2") – the Access Control List Resource

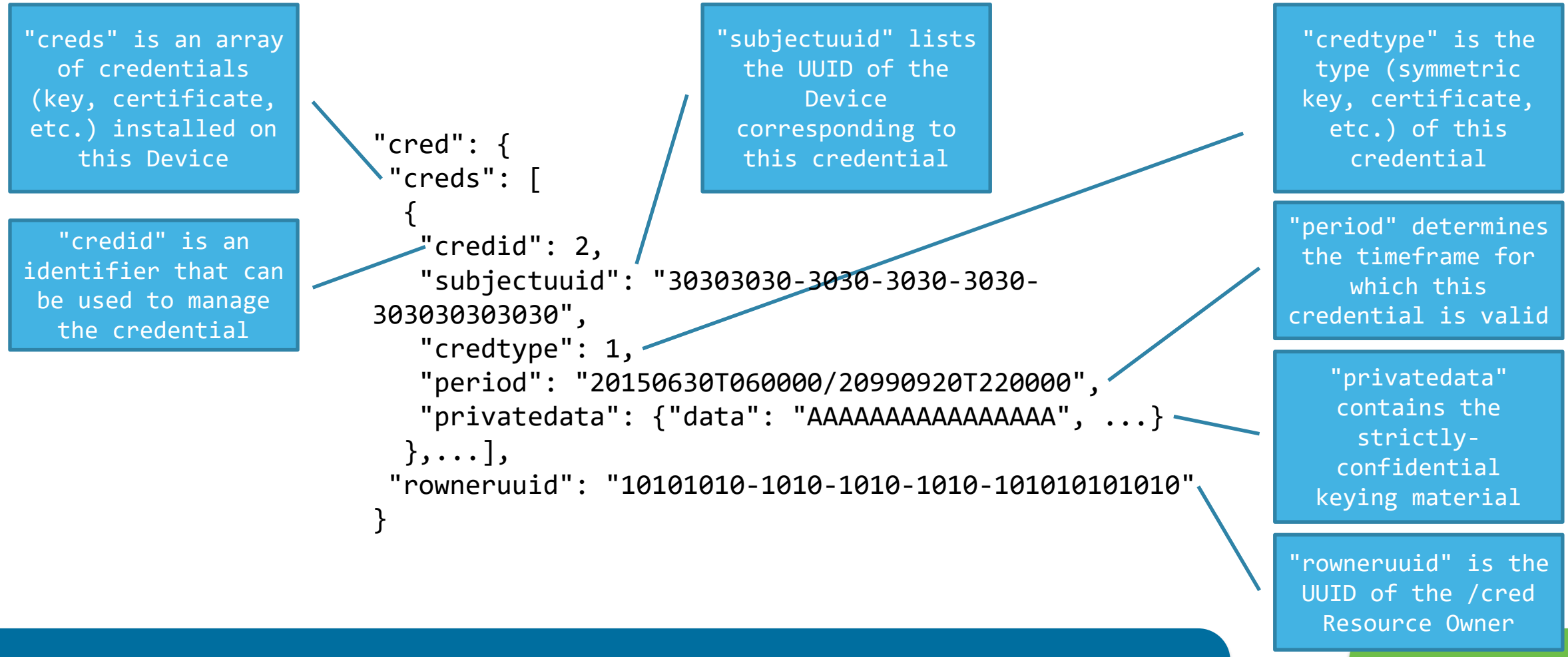
The /acl2 Resource is used to configure the access control policy on the Device (i.e. which Clients are allowed to access which Resources, and what the allowed access-modes – Retreive vs. Update, etc – are allowed.



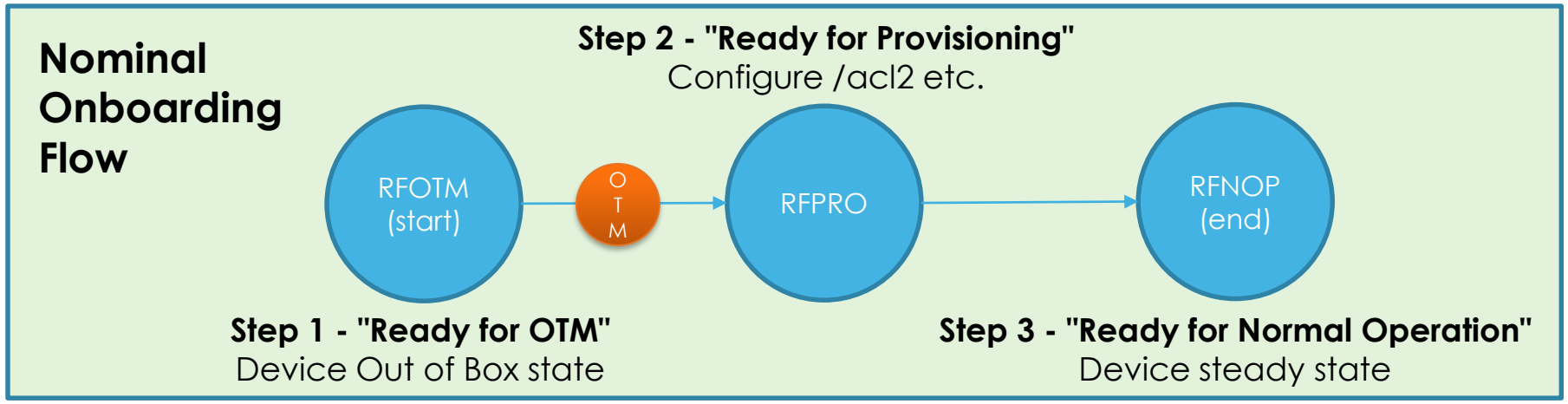
Understanding /cred

/oic/sec/cred (or "/cred") – The Credentials Resource

The /cred Resource stores the credentials – cryptographic keys, certificates, etc. – that are required to establish secure connections, and verify Client identity, among other things.



Onboarding Methods (OTMs) at a Glance

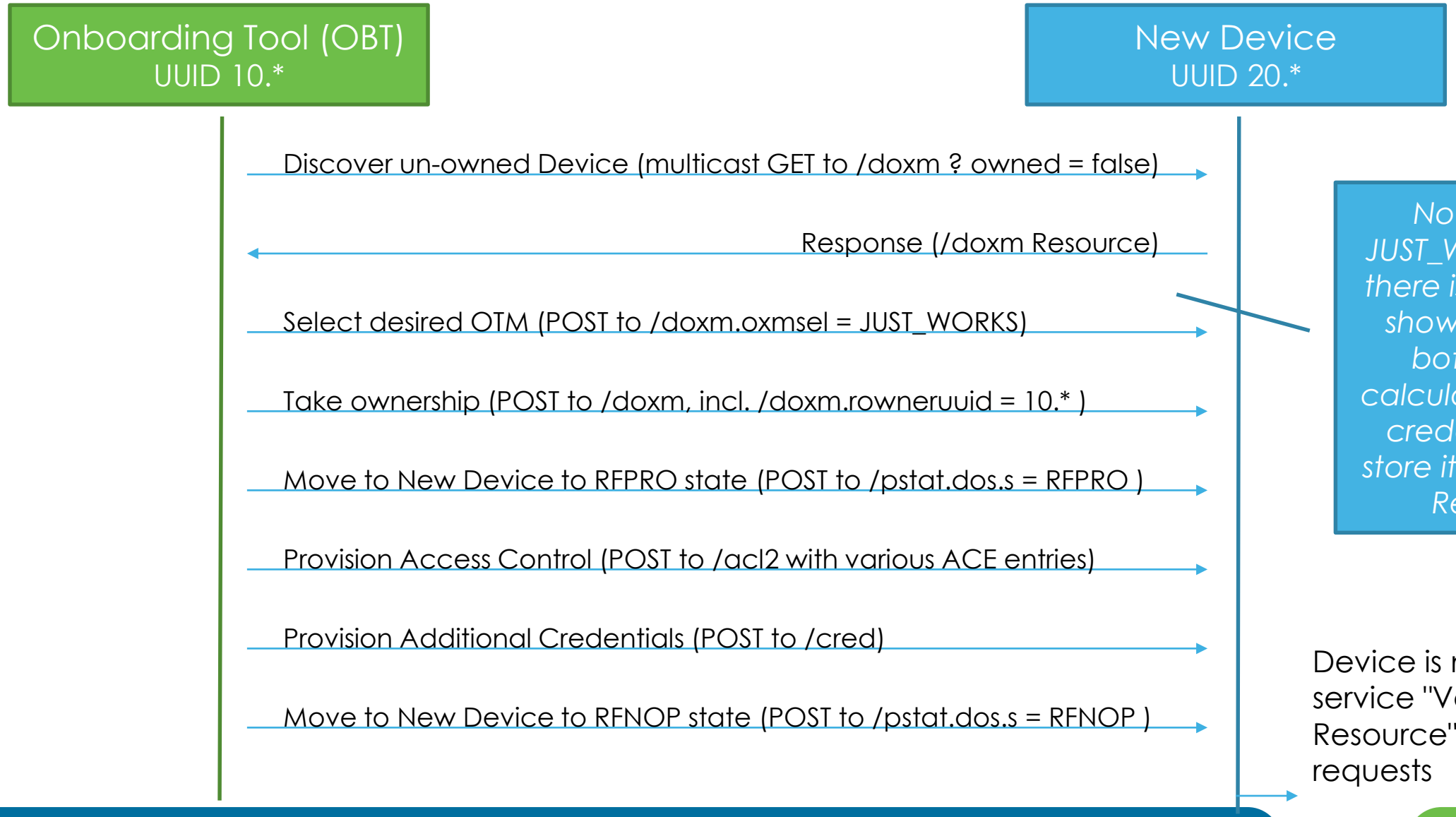


JustWorks OTM – the most basic onboarding method for getting Device into RFNOP
+ simple and functional
- vulnerable to MitM attacks on the onboarding network

Random PIN OTM – require the User to enter a PIN to complete onboarding
+ resists MitM
- requires User Input (higher touch)
- requires PIN display and Input method to communicate PIN from Server->User->OBT

Certificate OTM – New Device supplies a Certificate to Onboarding Tool
+ best assurance and most informed onboarding decision via Cert meta-data
- requires Certificate capabilities (incl. Root Cert in OBT)

Onboarding a Device – an Incomplete Illustration

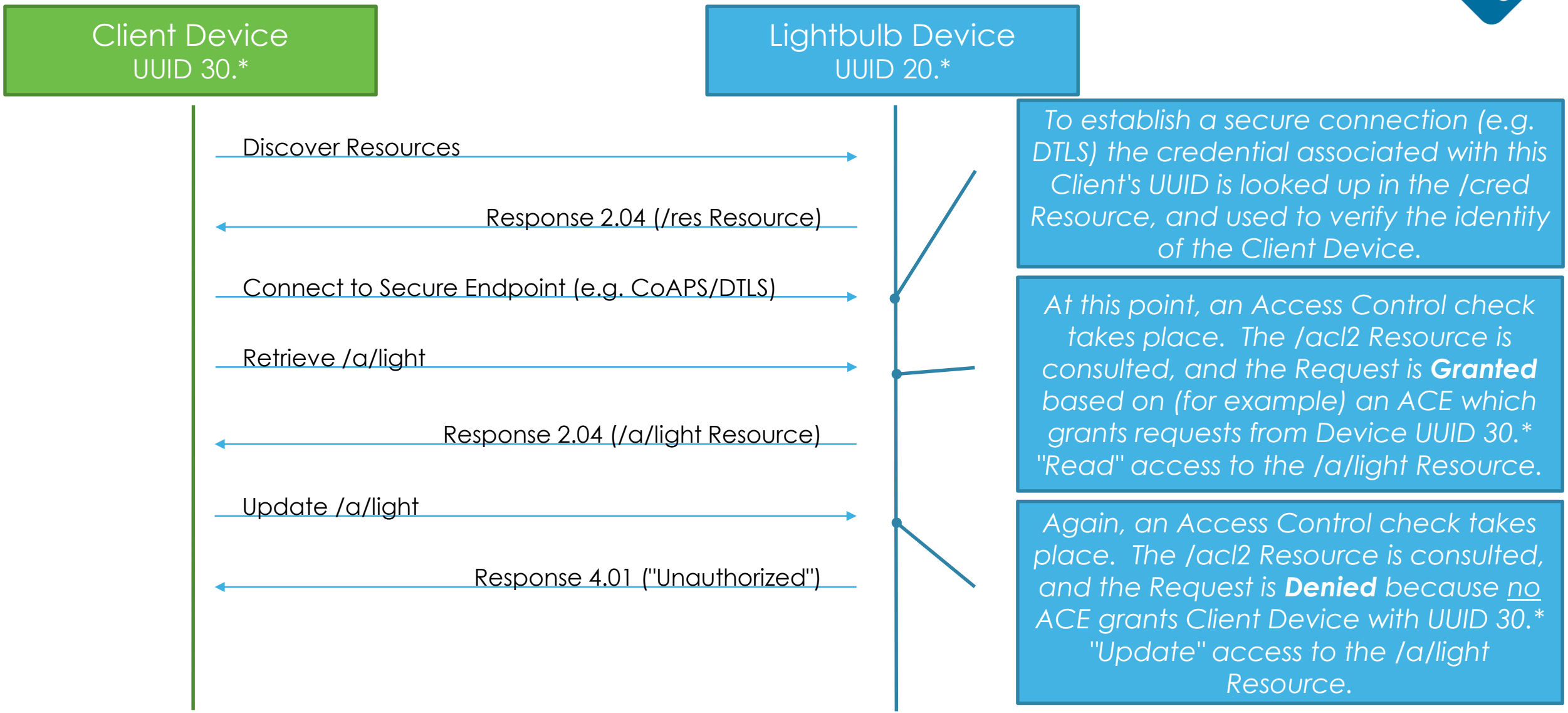


Access Control using Groups and Wildcards

"Access Control" – filtering incoming requests to a Device, and making a "Granted" or "Denied" decision for each request before it is passed to the Resource endpoint.

- OCF defines the /acl2 Resource, which contains "Access Control Entry" objects (ACE2), to configure Access Control for a Device.
- Within an ACE2, there is a "subject" Property, which determines the Client(s) which may be Granted access by the ACE2, and this is where Group Access comes in
- Separate but related in the "resources" Property, which determines the Resource(s) to which the ACE2 applies

Processing a Request with Access Control applied



"subject" Groups

- **Two pre-defined groups, via the "conntype" Parameter of the ACE2 "subject" property:**
  - **"anon-clear"** – all Subjects which are connected via anonymous, clear-text channel
  - **"auth-crypt"** – all Subjects which are connected via authenticated, encrypted channel

```
{
    "aceid": 1,
    "subject": { "conntype": "anon-clear" },
    ...
}
```

- **Vendor-defined groups, via "roletype" Parameter of the ACE2 "subject" property:**
  - Symmetric keys: (1) "role" per Client, keyed on UUID
  - Certificates: n "roles" per Client, keyed on public key

```
{
    "aceid": 1,
    "subject": { "roletype": "<made_up_string_that_matches_string_in_cred>" },
    ...
}
```

"resources" Wildcards

- Beginning in OCF 2.0, we have reduced the scope of these wildcards
  - **"*"** – all Non-Configuration Resources
    - NCRs exclude discovery and configuration Resources; see Security Specification Terms and Definitions
  - **"+"** – all NCRs exposing a Secure Endpoint
  - **"-"** – all NCRs exposing an Unsecure Endpoint

  - ***With these new definitions, a basic /acl2 configuration where "auth-crypt" has access to "+" and "anon-clear" has access to "-" may be a suitable baseline access control configuration for many Devices. It essentially means that any Client which has been onboarded can access all the Non-Configuration Resources on that Server.***

Symmetric Keys vs. Certs – Credential management and Access Control management implications

- There are security and performance related considerations for both, which should be understood by a Device Vendor choosing its credential model. **OCF's access control model has additional implications that should be taken into account.**

- **Implication to Credential (/cred Resource) Management: using Symmetric Keys requires higher-touch key management.**
  - In short, each time a New Client is added to the domain, the symmetric credential model requires each Server Device in the domain to be provisioned with a new symmetric credential, before the Dad's App can establish an authenticated connection with that Server.
  - By contrast, the certificate model allows the Server Device to mutually authenticate with Dad's App using the Root Cert (or CA Cert) already installed on the Server; the Server isn't touched when Dad's App is added.

- **Implications to Access Control (/acl2 Resource) Management: using Certs enables more granular group-level access.**
  - With a symmetric credential installed on the Server, the New Client will match all "conntype":"auth-crypt" ACEs, and thus gain that level of access permission
    - Furthermore, a Client-specific ACE – naming the New Client by its UUID – can be installed to give the Client additional access permission
  - In a certificate model, the New Client will also match all "auth-crypt" ACEs, but can also be granted access to any "role" ACEs, on a per-role basis
    - The OBT just needs to the New Client a "role certificate" which is then supplied to the Server during connection establishment, and authorizes the New Client to effectively join the security group named in the "role"

Security Profiles (/sp) at a Glance

1. "Baseline" sets the minimum requirement for every OCF Device
2. On top of "Baseline", each Security Profile defines an optional set of additional security features and requirements
3. If a Device Vendor chooses to meet these requirements, and the Device can be certified by OCF as such, the /sp Resource can tell an Onboarding Tool/Client which Profiles the Device supports. This can aid the Client in determining how trustworthy a given Device is.

The OCF 2.0.1 Profiles

- **Baseline Profile**
  - The minimum security requirements for every OCF Device
- **Black Profile**
  - Requires use of the OCF PKI
  - Additional improved robustness requirements above Baseline Profile
- **Blue Profile**
  - Requires auditing of the Manufacturer CA
  - Additional improved robustness requirements above Baseline Profile
- **Purple Profile**
  - Requires a handful of specific security features
  - Requires auditing of the Manufacturer CA
  - Additional improved robustness requirements above Baseline Profile

OPEN CONNECTIVITY FOUNDATION®