OCF 1.0 Security CR – Bug 1485

Legal Disclaimer

(From Section 13.2 – Credential Resource)

Multiple credential types are anticipated by the OCF framework, including pair-wise pre-shared keys, asymmetric keys, certificates and others. The credential resource uses a Subject UUID to distinguish the OCF Clients and support services it recognizes by verifying an authentication challenge.

In order to provide an interface which allows management of the "creds" Array Property, the RETRIEVE, UPDATE and DELETE operations on the oic.r.cred Resource SHALL behave as follows:

1. **A RETRIEVE SHALL return the full Resource representation, except that any write-only Properties SHALL be omitted (e.g. private key data).**
2. **An UPDATE SHALL replace or add to the Properties included in the representation sent with the UPDATE request, as follows:**
    a. **If an UPDATE representation includes the "creds" array Property, then:**
        i. **Supplied creds with a "credid" that matches an existing "credid" SHALL replace completely the corresponding cred in the existing "creds" array.**
        ii. **Supplied creds without a "credid" SHALL be appended to the existing "creds" array, and a unique (to the cred Resource) "credid" SHALL be created and assigned to the new cred by the Server. The "credid" of a deleted cred should not be reused, to improve the determinism of the interface and reduce opportunity for race conditions.**
3. **Supplied creds with a "credid" that does not match an existing "credid" SHALL be appended to the existing "creds" array, using the supplied "credid".A DELETE without query parameters SHALL remove the entire "creds" array, but SHALL NOT remove the oic.r.cred Resource.**
4. **A DELETE with one or more "credid" query parameters SHALL remove the cred(s) with the corresponding credid(s) from the "creds" array.**

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	Interfaces	Description	Related Functional Interaction
/oic/sec/cred	Credentials	urn:oic.r.cred	baseline	Resource containing credentials for device authentication, verification and data protection	Security

…

(From Section 13.5.2 - ACL Resource)

When the ACE subject is specified as the wildcard string "*" any requestor is matched. The OCF server may authenticate the OCF client, but is not required to.

In order to provide an interface which allows management of the "aclist" Array Property, the RETRIEVE, UPDATE and DELETE operations on the oic.r.ace2 Resource SHALL behave as follows:

1. **A RETRIEVE SHALL return the full Resource representation.**
2. **An UPDATE SHALL replace or add to the Properties included in the representation sent with the UPDATE request, as follows:**
    a. **If an UPDATE representation includes the "aclist" array Property, then:**
        i. **Supplied ACEs with an "aceid" that matches an existing "aceid" SHALL replace completely the corresponding ACE in the existing "creds" array.**
        ii. **Supplied ACEs without an "aceid" SHALL be appended to the existing "aces" array, and a unique (to the acl2 Resource) "aceid" SHALL be created and assigned to the new ACE by the Server. The "aceid" of a deleted ACE should not be reused, to improve the determinism of the interface and reduce opportunity for race conditions.**
        iii. **Supplied ACEs with an "aceid" that does not match an existing "aceid" SHALL be appended to the existing "aces" array, using the supplied "aceid".**
3. **A DELETE without query parameters SHALL remove the entire "aclist" array, but SHALL NOT remove the oic.r.ace2 Resource.**
4. **A DELETE with one or more "aceid" query parameters SHALL remove the ACE(s) with the corresponding aceid(s) from the "aclist" array.**

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	Interfaces	Description	Related Functional Interaction
/oic/sec/acl2	ACL2	urn:oic.r.acl2	baseline	Resource for managing access	Security