OCF "Essen" – Access Token Marshalling – Security WG CR 2906

Legal Disclaimer

Device Provisioning by Mediator

The Mediator and the Device shall use the secure session to provision the Device to connect with the OCF Cloud.

The Mediator obtains an Access Token from the OCF Cloud as described in OCF Cloud Specification. This Access Token is then used by the Device for registering with the OCF Cloud as described in clause 7. The OCF Cloud maintains a map where Access Token and Mediator provided Device ID are stored. At the time of Device Registration OCF Cloud validates the Access Token and associates the TLS session with corresponding Device ID.

The Mediator provisions the Device, as described in OCF Cloud Specification. The Mediator provisions OCF Cloud URI to the "cis" Property of "oic.r.coapcloudconf" Resource, OCF Cloud UUID to the "sid" Property of "oic.r.coapcloudconf" Resource and per-device Access Token to the "at" Property of "oic.r.coapcloudconf" Resource on Device. Provisioned "at" is to be treated by Device as an Access Token with "Bearer" token type as defined in IETF RFC 6750. The provisioned "at" value follows a proprietary data format, and may include multiple values marshalled/concatenated together into a single string (e.g. "{\"token\":\"abc\", \"client_id\":\"1234\", \"idp\":\"identityProvider1\"}" is a valid "at" Property value).

For the purposes of access control, the Device shall identify the OCF Cloud using the OCF Cloud UUID in the Common Name field of the End-Entity certificate used to authenticate the OCF Cloud.

AMS should configure the ACE2 entries on a Device so that the Mediator(s) is the only Device(s) with UPDATE permission for the "oic.r.coapcloudconf" Resource.

The AMS should configure the ACE2 entries on the Device to allow request from the OCF Cloud. By request from the Mediator, the AMS removes old ACL2 entries with previous OCF Cloud UUID. This request happens before "oic.r.coapcloudconf" is configured by the Mediator for the new OCF Cloud. The Mediator also requests AMS to set the OCF Cloud UUID as the "subject" Property for the new ACL2 entries. AMS may use "sid" Property of "oic.r.coapcloudconf" Resource as the current OCF Cloud UUID. AMS could either provision a wildcard entry for the OCF Cloud or provision an entry listing each Resource published on the Device.

If OCF Cloud provides "redirecturi" Value as response during Device Registration, the redirected-to OCF Cloud is assumed to have the same OCF Cloud UUID and to use the same trust anchor. Otherwise, presented OCF Cloud UUID wouldn't match the provisioned ACL2 entries.

The Mediator should provision the "oic.r.coapcloudconf" Resource with the Properties in Table 1. These details once provisioned are used by the Device to perform Device Registration to the OCF Cloud. OCF Device is not expected to have any internal logic based on the values of "at" and "apn" Properties. The values of these Properties are forwarded as-is to the OCF Cloud. After the initial registration, the Device should use updated values received from the OCF Cloud instead. If OCF Cloud User wants the Device to re-register with the OCF Cloud, they can use the Mediator to re-provision the "oic.r.coapcloudconf" Resource with the new values.

Table 1 – Mapping of Properties of the "oic.r.account" and "oic.r.coapcloudconf" Resources

Property Title	oic.r.coapcloudconf	oic.r.account	Description
Authorization Provider Name	apn	authprovider	The name of Authorization Provider through which Access Token was obtained.
OCF Cloud URL	cis	-	This is the URL connection is established between Device and OCF Cloud.
Access Token	at	accesstoken	Access-Token used for communication with OCF Cloud
OCF Cloud UUID	sid	-	This is the identity of the OCF Cloud that the Device is configured to use.