OCF "Gaborone-1" – Removal of wrong/obsolete text from Device Identity clause – Security WG CR 3237

Legal Disclaimer

7.1 Device Identity

7.1.1 General Device Identity

A Device shall be identified by a Device UUID value that is established as part of the device onboarding and contained in the "deviceuuid" Property of the "/oic/sec/doxm" Resource. Device UUIDs shall be unique within the scope of the corresponding OCF Security Domain, and are expected to be randomly generated and provisioned by the OBT. The DOTS is expected to verify that the chosen new Device UUID does not conflict with Device UUIDs previously introduced into the OCF Security Domain.

Devices maintain an association of their Device UUIDs and their own cryptographic credential(s) via "/oic/sec/cred" Resource. The identity is cryptographically bound in case of a certificate credential, or is bound via internal mappings in the "/oic/sec/cred" Resource otherwise. The "/oic/sec/cred" Resource maintains a list of a Device's own and other Device's credentials. Multiple credentials may be associated with the same Device UUID.A Device is expected to only present credentials associated with its own Device UUID for peer authentication purposes. Devices regard the "/oic/sec/cred" Resource as authoritative when verifying authentication credentials of a peer Device.

In case of an authenticated connection, the Device UUID is treated as a Client’s identity for purposes of the Access Control check for the target Resource. The Device UUID of a Client is matched against the Subject UUIDs in the pre-provisioned entries of Server's "/oic/sec/acl2" Resource. The Server determines Client's Device UUID based on the credential used for the establishment of the session.

An OCF Platform, which may host multiple Devices, is identified by a Platform ID. The Platform ID is globally unique and inserted in the device in an integrity protected manner (e.g. inside secure storage or signed and verified). An OCF Platform may have a secure execution environment, used to secure unique identifiers and secrets. If a Platform hosts multiple Devices, some mechanism is needed to provide each Device with the appropriate and separate security context.

7.1.2 Device Identity for Devices with UAID [Deprecated]

This clause is intentionally left blank.