OCF "Fargo" – OBT / DOTS shall generate random Device UUID – Security WG CR 2935

Legal Disclaimer

START OF CHANGE

5.3 DOTS

5.3.1 Assuming ownership of a Device

The DOTS shall support all OTMs in clause 7.

An overview is provided in Clauses 5.3.3 and 7.2 of ISO/IEC 30118-2:2018.

The following steps shall be performed to take ownership of a Device. The Device is presumed to be in RFOTM.

1) The DOTS performs a multicast retrieve on the "/oic/sec/doxm" Resource using "owned=false" query parameter as described in ISO/IEC 30118-2:2018.
2) Before proceeding, the DOTS shall obtain acknowledgement from the OBT End-User that the OBT End-User approves the DOTS assuming ownership of the discovered Device(s). See security considerations in clause 5.3.3.
3) The DOTS selects a mutually supported OTM from the the "oxms" Property of the "/oic/sec/doxm" Resource. See security considerations in clause 5.3.3.
4) The DOTS shall UPDATE the "oxmsel" property of "/oic/sec/doxm" the value corresponding to the OTM being used, before performing other OTM steps.
5) The DOTS shall initiate a DTLS Session as specified for the OTM configured to the oxmsel Property of the "/oic/sec/doxm" Resource. Details are provided in clause 7.
6) The DOTS shall send an UPDATE request message to /oic/sec/pstat to set the value of "om" to 0b 0000 0100 to select Client-directed provisioning.
7) The DOTS shall update the "devowneruuid" Property of the "/oic/sec/doxm" Resource with the UUID of the DOTS.
8) The DOTS may RETRIEVE the updated "deviceuuid" Property of the "/oic/sec/doxm" Resource after the DOTS has updated the "devowneruuid" Property value of the "/oic/sec/doxm" Resource to a non-nil-UUID value.
9) The DOTS shall UPDATE the "deviceuuid" of the "/oic/sec/doxm" Resource. The updated value shall be a random value that the DOTS has generated. The DOTS should use a FIPS 800-90A-compliant RNG to guarantee the sufficient entropy.

END OF CHANGE