OCF “Ipanema” – OBT: change psk_identity_hint field for Random PIN OTM – Security WG CR 3276

Legal Disclaimer

Changes to clauses 7.3

7.3 Random PIN / Shared Credential based OTM

Details of this OTM are provided in clause 7.3.5 of ISO/IEC 30118-2:2018. The following points are pertinent to the DOTS:

- This OTM relies on the Device generating a random number that is communicated to the DOTS over an Out of Band Communication Channel.
  - The Platform hosting a DOTS which supports this OTM shall provide a user interface for manual input of the random number.
  - A DOTS may support other vendor-defined Out of Band Communication Channel for receiving the random number from the Device. Security considerations regarding Out of Band Communication channel are provided in clause 7.3.5.3 of ISO/IEC 30118-2:2018.
- A DOTS shall support receiving a ServerKeyExchange message in the DTLS handshake either with "psk_identity_hint" field formatted as specified in clause 7.3.5.2 of ISO/IEC 30118-2:2018, or with "psk_identity_hint" field comprising only a Device UUID (to ensure backwards compatibility with Devices conforming to older releases). When the DOTS receives the ServerKeyExchange, then
  - The DOTS can identify the new Device with which it is establishing the DOC by matching the "deviceuuid" part of the "psk_identity_hint" field with the "deviceuuid" Property of the "/oic/sec/doxm" Resource being sent in responses when the new Device is in RFOTM and when a Device Onboarding Connection is not currently established. The DOTS shall compute the PIN-authenticated pre-shared key (PPSK) using the algorithm specified in clause 7.3.5.2 of ISO/IEC 30118-2:2018.

Furthermore, the following requirements apply to the DTLS handshake messages for this OTM:

- The DOTS shall set the "psk_identity" field of the ClientKeyExchange message to the string "oic.sec.doxm.rdp".

NOTE: The string "oic.sec.doxm.rdp" is the URN defined for the Random PIN-based OTM in Table 18 of ISO/IEC 30118-2:2018, and is included to allow future OTMs to re-use the DTLS ciphersuites without confusion about which OTM should be applied.

All DOTS shall implement the mandatory ciphersuites and should implement the optional ciphersuites for Devices specified for this OTM in clause 11.3.2.2 of ISO/IEC 30118-2:2018.

Further security considerations for this OTM are provided in clause 7.3.5.3 of ISO/IEC 30118-2:2018.

End of changes