OCF “Gaborone-1” – Proposed editorial changes to the OCF Onboarding Tool Specification 2.1.0 – Security WG CR 3242

1 Scope

2 Normative References

3 Terms, definitions, and abbreviated terms

4 Document Conventions and Organization

5 Services and Availability in the OBT

5.1 Purpose of the OBT

The following OBT functions are specified:

- A Device Ownership Transfer Service (DOTS) establishes ownership of Devices being added to the OCF Security Domain. This function is described in clause 5.3.
- A Credential Management Service (CMS) manages the credentials and Roles of Devices in the OCF Security Domain. This function is described in clause 5.4.
- An Access Management Service (AMS) manages the access of Devices in the OCF Security Domain. This function is described in clause 5.5.
- Optional: A Mediator facilitates further configuration of Devices in the OCF Security Domain for various purposes including Wi-Fi configuration (see ISO/IEC 30118-7:2018) and OCF Cloud access (see ISO/IEC 30118-X:2018).

The OBT demands a higher level of security hardening than regular OCF Devices in order to preserve integrity and confidentiality of sensitive credentials being stored.

As mentioned, to accommodate a scalable and modular design, these functions are considered as services that could be deployed on separate Devices. Currently, the deployment assumes that these services are all deployed as part of an OBT. Regardless of physical deployment scenario, the same security-hardening requirement applies to any physical server that hosts the services discussed here.

The Device Onboarding States are defined in clause 8 of ISO/IEC 30118-2:2018. Table 1 provides an overview of the access granted to the OBT components according to the Device Onboarding States.

Table 1 –Overview of OBT access in Device Onboarding States

Device Onboarding State	Description		Applicable Resources & Access	Entity Authorized to READ/WRITE	Purpose	"/oic/sec/doxm:owned"
RESET	Full reset of OCF Device to manufacturer default.		No Access	No Access	Remove info in SVRs.	FALSE
RFOTM	Ready for Ownership Transfer Mechanism.	Prior to successful OTM	"/oic/sec/doxm" (R: all, W: oxmsel)	Any	R: Determine supported OTMs W: Select an OTM	FALSE
		After successful OTM	"/oic/sec/doxm" (RW) "/oic/sec/cred"(RW)	DOTS	Claim ownership. Establish credentials for authenticating DOTS, AMS, CMS & optionally other Devices	
			(At discretion of End User of DOTS) "/oic/sec/sp" (RW)	DOTS	R: Determine supported Security Profiles. W: Set current security profile.	
			(At discretion of End User of DOTS) "/oic/sec/acl2" (RW)	DOTS	Configure further ACEs	
			"/oic/sec/pstat" (RW)	DOTS	Transition to RFPRO or RESET	
RFPRO	Ready for Provisioning.		"/oic/sec/cred" (RW)	CMS or matching ACE	Establish credentials for authenticating Devices in normal operation, including Roles	TRUE
			"/oic/sec/acl2" (RW)	AMS or matching ACE	Establish ACEs for normal operation	
			"/oic/sec/sp" (RW)	DOTS or matching ACE	R: Determine supported Security Profiles. W: Set current security profile	
			"/oic/sec/pstat" (RW)	DOTS, CMS, AMS or matching ACE	Transition to RFNOP	
RFNOP	Ready for Normal Operation.		"/oic/sec/pstat"	DOTS, CMS, AMS or matching ACE	Transition to RFPRO, SRESET or RESET	TRUE
			Vertical Resources	Matching ACE	Normal Operation	
SRESET	Soft RESET.		"/oic/sec/cred" (RW)	CMS	Corrections as needed	TRUE
			"/oic/sec/acl2" (RW)	AMS	Corrections as needed	
			"/oic/sec/doxm" (RW)	DOTS	Corrections as needed	
			"/oic/sec/pstat" (RW)	DOTS, CMS or AMS	Transition to RFPRO or RESET	

5.2 General OBT requirements

No changes

5.3 DOTS

5.3.1 Assuming ownership of a Device

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 "oxms" Property of the "/oic/sec/doxm" Resource. See security considerations in clause 5.3.3.

5.4 CMS

No changes

5.5 AMS

Clause 6.2 of ISO/IEC 30118-X:2018 provides normative requirements on the AMS when configuring ACE entries of a Device which supports OCF Cloud.

The AMS determines an appropriate ACL configuration for each Server based on the rules for ACL evaluation and enforcement at Servers specified in clause 12 of ISO/IEC 30118-2:2018. The formatting of the ACL Resource specified in clause 13.5 of ISO/IEC 30118-2:2018.

6 Certificate management requirements

6.1 Issuing identity certificates and role certificates

A CMS shall perform the following steps to issue an identity certificate or role certificate to a Device.

1) If the Device has the "/oic/sec/csr" Resource, then
   a) The CMS shall send a RETRIEVE request to the "/oic/sec/csr" Resource on the Device, to obtain a certificate signing request for which the CMS will create a certificate.
   b) The CMS shall issue (or otherwise obtain) a certificate chain using the certificate signing request returned by the new Device and complying with clause 9.4.2 of ISO/IEC 30118-2:2018.
2) If the Device does not have the "/oic/sec/csr" Resource, then the CMS shall issue (or otherwise obtain) a certificate chain using the using a public key pair generated by the CMS, and complying with clause 9.4.2 of ISO/IEC 30118-2:2018.
3) The CMS shall send a request to the Device to add an entry to the "creds" Property of the "/oic/sec/cred" Resource of the Device meeting the following criteria:
   – The "subjectuuid" Property shall have the value of "deviceuuid" Property of the "/oic/sec/doxm" Resource.
   – The "credtype" Property shall have the value "8" corresponding to Asymmetric Signing Key with Certificate.

– The "credusage" Property shall have the value of "oic.sec.cred.cert" or "oic.sec.cred.rolecert" corresponding to an identity certificate or role certificate as respectively.
– The "publicdata" Property shall contain the newly-created certificate chain.

See clause 13.3.1 of ISO/IEC 30118-2:2018 for details of a request adding an entry to the "creds" Property of the "/oic/sec/cred" Resource.

7 Ownership Transfer Methods

7.1 Preamble

OTM Implementation requirements are discussed in clause 7.3.1 of ISO/IEC 30118-2:2018.

7.2 Just Works Owner Transfer Method

This OTM is specified in clause 7.3.4.1 of ISO/IEC 30118-2:2018.

7.3 Random PIN / Shared Credential based Owner Transfer Method

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

7.4 Manufacturer Certificate Based Owner Transfer Method

Details of this OTM are provided in clause 7.3.6 of ISO/IEC 30118-2:2018. The following points are pertinent to the DOTS:

- The DOTS shall validate the certificate presented by the Device in the DTLS handshake against the Trust Anchors contained in its entries of the "/oic/sec/cred" Resource that have a "credusage" Property populated with "oic.sec.cred.mfgtrustca".
- The certificate profiles are specified in clause 9.4.2 of ISO/IEC 30118-2:2018.

All DOTS are expected to implement the mandatory and optional ciphersuites for Devices specified for this OTM in clause 11.3.2.3 of ISO/IEC 30118-2:2018.

7.5 Vendor-Specific Owner Transfer Methods

Clauses 7.3.1 and 7.3.7 of ISO/IEC 30118-2:2018 provide requirements for Vendor-specific OTMs.