OCF 2.3 – Clarifying Owned State Behavior – Sec WG CR 2692

Legal Disclaimer

Background

This document reflects the changes to the OCF Security Specification resulting from development by the Core Technology Working Group, Bridging TG and Remote and Bridging Security TG.

Background information regarding these requirements.

The original draft requirements put together for this issue were something like:

1. VODs can only be onboarded, if Bridge is onboarded.
2. When Bridge is onboarded, "List of onboarded VODs" shall be updated to reflect current network state.
3. When VOD is off-boarded, it shall be removed from "List of onboarded VODs".
4. Bridge can be off-boarded, and that doesn't impact VODs.

When drafting this CR, it became clear that there is no clear definition of "onboarded" - the closest definition being for "Onboarding Tool" which is defined as "*A logical entity within a specific IoT network that establishes ownership for a specific device and helps bring the device into operational state within that network.*" The original intent of the above four requirements was related to ownership of VODs and Bridges, and was not related to provisioning of VODs and Bridges (" [bringing] the device into operational state within that network"). For this reason, it makes more sense for the requirements to talk about Devices being "owned" or "unowned" or transitioning from one to the other. A separate CR (BZ 2665) will address definitions for adjectives "Owned" and "Unowned" as applied to Devices.

*** Section Z.1.1 (Append this new text to existing text) ***

A Bridge and the VODs created by that Bridge shall operate as independent Devices, with the following exceptions:

- If a Bridge creates a VOD while the Bridge is in an Unowned State, then the VOD shall be created in an Unowned State.
- An Unowned VOD shall not accept DTLS connection attempts nor TLS connection attempts nor any other requests, including discovery requests, while the Bridge (that created that VOD) is Unowned.
- At any time when a Bridge is transitioning from Owned to Unowned State, all Unowned VODs (created by that Bridge prior to the transition) shall drop any existing TLS and/or DTLS connections.
- At any time when a Bridge is transitioning from Unowned to Owned State, the Bridge shall trigger all Unowned VODs (created by that Bridge prior to the transition) to become accessible in RFOTM state, with internal state as if the VOD has just transitioned from RESET to RFOTM.
- If a Bridge creates a VOD while the Bridge is in an Owned State, then the VOD shall become accessible in RFOTM state, with internal state as if the VOD has just transitioned from RESET to RFOTM.

Table X intends to clarify this behaviour.

Bridge state	Additional dependencies on VOD behaviour	
	VOD is Unowned (either just created, or created previously)	VOD is Owned
From unboxing Bridge until just prior to the end of transition of Bridge from Unowned to Owned	No accepting DTLS connection attempts nor TLS connection attempts nor any other requests, including discovery requests	Not applicable
At end of transition from Unowned to Owned	VOD becomes accessible in RFOTM following Bridge's transition. Internal state as if just transitioned from RESET.	As per normal Device
Owned	As per normal Device	As per normal Device
At Start of transition from Owned to Unowned	Drop any established TLS/DTLS connections, even if already partway through Device ownership	As per normal Device
Start of transition from Owned to Unowned, until just prior to the end of transition from Unowned to Owned.	No accepting DTLS connection attempts nor TLS connection attempts nor any other requests, including discovery requests	As per normal Device

Table X - Dependencies of VOD Behaviour on Bridge state, as clarification of accompanying text.

The "vods" Property of the oic.r.vodlist Resource on a Bridge reflects the details of all currently Owned VODs which have been created by that Bridge since the most recent hardware reset (if any) of the Bridge Platform (which removes all the created VODs), regardless of whether the VODs have the same owner as the Bridge or not. The entries in the "vods" Property are added and removed according to the following criteria:

- Whenever a VOD created by a Bridge transitions from being Unowned to being Owned, then an entry for that VOD shall be added to the "vods" Property of the oic.r.vodlist Resource of that Bridge.
- Whenever a VOD created by a Bridge transitions from being Owned to being Unowned, then entry for that VOD shall be removed from the "vods" Property of the oic.r.vodlist Resource of that Bridge. If that Bridge is currently in Unowned state, then the "oic.r.vodlist" Resource is not accessible, and the entry for that VOD shall be removed from the "vods" Property before or during the transition of that Bridge to the Owned state.
- All other modifications of the list are not allowed.

A Bridge shall only expose a secure OCF Endpoint for the oic.r.vodlist Resource.

**** End of new text ****