# OCF 1.0 Security CR - CR24

Legal Disclaimer

## 15.4 Software Update

### 15.4.1 Overview:

The Device lifecycle does not end at the point when a Device is shipped from the manufacturer; the distribution, retailing, purchase, installation/onboarding, regular operation, maintenance and end-of-life stages for the Device remain outstanding. It is possible for the Device to require update during any of these stages, although the most likely times are during onboarding, regular operation and maintenance. The aspects of the software include, but is not limited to, firmware, operating system, networking stack, application code, drivers, etc.

### 15.4.2 Recognition of Current Differences

Different manufacturers approach software update utilizing a collection of tools and strategies: over-the-air or wired USB connections, full or partial replacement of existing software, signed and verified code, attestation of the delivery package, verification of the source of the code, package structures for the software, etc.

It is recommended that manufacturers review their processes and technologies for compliance with industry best-practices, that a thorough security review of these takes place, and that periodic reviews continue after the initial architecture has been established. This specification applies to software updates as recommended to be implemented by OCF Devices; it does not have any bearing on the above-mentioned alternative proprietary software update mechanisms.

### 15.4.3 Software Version Validation

Setting the Initiate Software Version Validation bit in the /oic/sec/pstat.tm Property (see Table 40 of Section 13.6) indicates a request to initiate the software version validation process, the process whereby the Device validates the software (including firmware, operating system, device drivers, networking stack, etc.) against a trusted source to see if, at the conclusion of the check, the software update process will need to be triggered (see below). When the Initiate Software Version Validation bit of /oic/sec/pstat.tm is set to 1 (TRUE) by a sufficiently privileged OCF Client, the Device sets the /oic/sec/pstat.cm Initiate Software Version Validation bit to 0 and initiates a software version check. Once the Device has determined if an update is available, it sets the Initiate Software Version Validation bit in the /oic/sec/pstat.cm property to 1 (TRUE) if an update is available or 0 (FALSE) if no update is available. To signal completion of the Software Version Validation process, the Device sets the Initiate Software Version Validation bit in the /oic/sec/pstat.tm Property back to 0 (FALSE). If the Initiate Software Version Validation bit of /oic/sec/pstat.tm is set to 0 (FALSE) by a Client, it has no effect on the validation process.

### 15.4.4 Software Update

Setting the Initiate Secure Software Update bit in the /oic/sec/pstat.tm property (see Table 40 of Section 13.6) indicates a request to to initiate the software update process. When the Initiate Secure Software Update bit of /oic/sec/pstat.tm is set to 1 (TRUE) by a sufficiently privileged OCF Client, the Device sets the /oic/sec/pstat.cm Initiate Software Version Validation bit to 0 and initiates a software update process. Once the Device has completed the software update process, it sets the Initiate Secure Software Update bit in the /oic/sec/pstat.cm property to 1 (TRUE) if/when the software was successfully updated or 0 (FALSE) if no update was performed. To signal completion of the Secure Software Update process, the Device sets the Initiate Secure Software Update bit in the /oic/sec/pstat.tm Property back to 0 (FALSE). If the Initiate Secure Software Update bit of /oic/sec/pstat.tm is set to 0 (FALSE) by a Client, it has no effect on the update process.

### 15.4.5 Recommended Usage

The Initiate Secure Software Update bit of /oic/sec/pstat.tm should only be set by an OCF Client after the Initiate Software Version Validation check is complete.

The process of updating Device software may involve state changes that affect the Device Operational State (/oic/sec/pstat.dos). Devices with an interest in the Device(s) being updated should monitor /oic/sec/pstat.dos and be prepared for pending software update(s) to affect Device state(s) prior to completion of the update.

Note that the Device itself may indicate that it is autonomously initiating a software version check/update or that a check/update is complete by setting the pstat.tm and pstat.cm Initiate Software Version Validation and Secure Software Update bits when starting or completing the version check or update process. As is the case with a Client-initiated update, Clients can be notified that an autonomous version check or software update is pending and/or complete by observing pstat resource changes.

### 13.6 Provisioning Status Resource:

The *provisioning mode* type is a 16-bit mask enumerating the various device provisioning modes. “{ProvisioningMode}” should be used in this document to refer to an instance of a provisioning mode without selecting any particular value.

| Type Name | Type URN | Description |
|---|---|---|
| Device Provisioning Mode | urn:oic.sec.dpmtype | Device provisioning mode is a 16-bit bitmask describing various provisioning modes |

**Table 39 – Definition of the oic.sec.dpmtype Property**

| Value | Device Mode | Description |
|---|---|---|
| bx0000,0001 (1) | Reset | Device reset mode enabling manufacturer reset operations |
| bx0000,0010 (2) | Take Owner | Device pairing mode enabling owner transfer operations |
| bx0000,0100 (4) | Bootstrap Service | Bootstrap service provisioning mode enabling instantiation of a bootstrap service. This allows authorized entities to install a bootstrap service. |
| bx0000,1000 (8) | Security Management Services | Service provisioning mode enabling instantiation of device security services and related credentials |
| bx0001,0000 (16) | Provision Credentials | Credential provisioning mode enabling instantiation of pairwise device credentials using a management service of type urn:oic.sec.cms |
| bx0010,0000 (32) | Provision ACLs | ACL provisioning mode enabling instantiation of device ACLs using a management service of type urn:oic.sec. ams |
| bx0100,0000 (64) | Initiate Software Version Validation | Software version validation requested/pending (1)<br>Software version validation complete (0) |
| bx1000,0000 (128) | Initiate Secure Software Update | Secure software update requested/pending (1)<br>Secure software update complete (0) |

**Table 40 – Value Definition of the oic.sec.dpmtype Property (Low-Byte)**