Explanation of UML Diagrams

# Overview

This file describes the various UML sequence diagrams that may be incorporated into OIC specifications. They cover various phases of device lifecycle from initial on-boarding, and provisioning to normal operation. Ongoing credential management sequences show how on-going credential management may occur given a dynamic network.

# Device Commissioning Stage Machine

## Ready for OTM (RFOTM)

A device that is ready for owner transfer will not be owned so that an on-boarding tool will be able to discover these devices and begin the owner transfer method.

## Ready for Provisioning (RFP)

A device that is read for provisioning will have successfully competed the owner transfer method and be able to successfully connect to the production network. However it may not be able to interact with peer devices directly without additional provisioning. It will however be able to interact with provisioning services.

## Ready for Normal Operation (RFNO)

A device that is ready for normal operation is fully provisioned according to the provisioning service(s) and the device provisioning status reflects this as well.

## On-boarding Reset (OR)

The device may be reset at any time causing the device to go through all the previous states before returning to normal operation.

# UML Sequence Diagrams

There are several UML sequence diagrams showing specific security resources and properties that may be affected when performing each of the state transitions. This section briefly describes each diagram in the context of the device commissioning state machine.

## RFOTM-RFP

The RFOTM-RFP.txt sequence diagram shows the steps that an on-boarding tool and a new device may perform as part of the initial on-boarding. Within the context of RFOTM processing the device and on-boarding tool may select a specific method for transferring device ownership. Device specific limitations may dictate which OTMs can be supported.

Several sample owner transfer method sequences are captured as well.

### DOXM-JW

Sequence for the "just works" owner transfer method.

### DOXM-MFGCERT

Sequence for the "manufacturer certificate" owner transfer method.

### DOXM-RDP

Sequence for the "random pin" owner transfer method.

### DOXM-VS

Sequence for a vendor specific owner transfer method where the vendor specific details of have been left blank.

## RFP-RFNO\_ClientLed

This sequence diagram shows how device provisioning may be achieved given the device is ready for provisioning and transitioning to ready for normal operation. Client directed provisioning means the provisioning service or services drive the provisioning steps.

## RFP-RFNO\_ServerLed

This sequence diagram shows how device provisioning may be achieved given the device is ready for provisioning and transitioning to ready for normal operation. Server directed provisioning means the provisioning service responds to device initiated provisioning requests. This sequence diagram presumes a single client is contacted for all provisioning needs. A single client may host multiple provisioning services defined by the resource model.

## RFP-RFNO\_ServerLedS

This sequence diagram shows how device provisioning may be achieved given the device is ready for provisioning and transitioning to ready for normal operation. Server directed provisioning means the provisioning service responds to device initiated provisioning requests. This sequence diagram presumes multiple clients are contacted for all provisioning needs. Each client specializes in terms of the type of service offered.

# Other Sequence Diagrams

## Dynamic Credential Management

When a new or guest device enters the domain the other devices it interacts with may need to have credentials provisioned to enable peer to peer interactions. The following sequence diagrams demonstrate how this may be achieved. These operations may take place when the device is in a RFNO state.

### PairwiseKeysCMS

This sequence shows how a Credential Management Service may be used to manage pair-wise symmetric keys between two devices

### PairwiseKeysDH

Devices that do not share a common CMS may wish to negotiate pairwise keys directly. This sequence shows how, in the absence of a Credential Management Service, peer devices may negotiate shared symmetric keys without a CMS.

## Key Refresh

Credentials may have an expiration date specified creating the need for key refresh. The following sequence diagrams show how credential refresh may be achieved using a CMS and a device-to-device approach. These operations may take place when the device is in a RFNO state.

### CMSMediatedRefresh

When a CMS provisioned credential expires the device may proactively request credential refresh. Normally, this will happen before the credential expires.

### Device-DeviceRefresh

Devices that do not share a common CMS may agree on an expiration date. They may proactively refresh the credential before that date to ensure continuing ability to securely communicate.