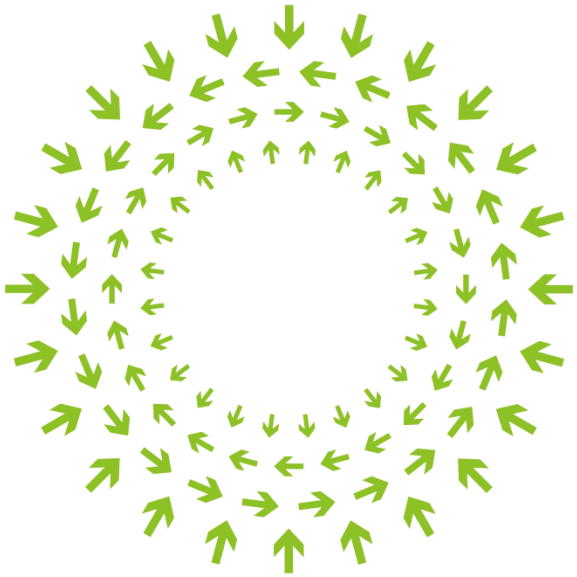

OPEN

Compute Project

Project Cerberus
Firmware Update Specification

Author:
Christopher Weimer, Senior Firmware Engineer, Microsoft
Bryan Kelly, Principal Firmware Engineering Manager, Microsoft

Revision History

Date	Description
28/8/2017	Version 1.0
18/4/2018	Updates to the PFM section
4/3/2019	Align with the update flows described in the challenge protocol. Add information about CFM, PCD, recovery image, and host firmware updates. Provide detailed update status codes.
6/26/2019	Add configuration reset status codes.
5/21/2020	Updated status codes.

Contents

Table of Figures

Table of Tables

Summary

Throughout this document, the term “Processor” refers to all Central Processing Unit (CPU), System On Chip (SOC), Micro Control Unit (MCU), and Microprocessor architectures. The document details the procedure for updating the Cerberus firmware image. It also covers the formatting and signing requirements for Cerberus firmware images.

1 Firmware Image Storage

The flash containing the Cerberus RoT firmware will be partitioned into three sections: Active, Recovery, and Staging. The active partition contains the current firmware image being used by the processor. The recovery partition maintains a known-good firmware image that can be used to restore the active image should something go wrong. The staging partition is the storage location for new firmware that has not been applied yet.

2 Firmware Update

2.1 New Firmware Image

Before any update process can be started, the new firmware image must be sent to the device. The image will be sent over the I2C bus. Since the firmware components are signed and must be verified prior to them being used, no trust with the sender is required. The received image will be saved in the Staging area of the RoT flash memory, and any image information previously stored in this area of flash will be lost.

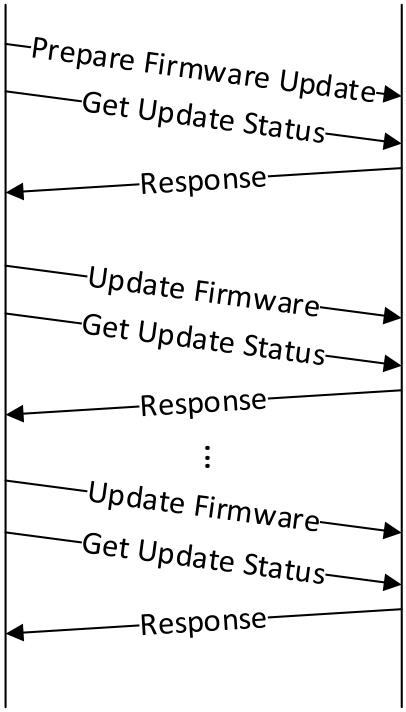

Figure 1 Send New Firmware Image Command Flow

2.2 Update Active Image

Once a new firmware image has been completely stored in the Staging area of flash, the device can be directed to use that image as the new running image. The update will only occur if the new image is verified to be a good. Verification of the new image is done using the same procedure as is used while booting the device. Once the image has been verified, it will be copied into the Active partition.

Any response to the activate firmware update command will be immediate and will only indicate if the request to start the update process has been processed correctly. To find out if the update is successful, the device must be polled for update status. The update status command will always report the state of the last update attempt until the device is reset or a new update request is received.

Once the update is complete, the RoT will start running the new image. Loading the new image will not be the same as a complete reset of the device. The current context of the system will be retained, so any active sessions will remain active. Also, boot-time initialization will not be re-run.

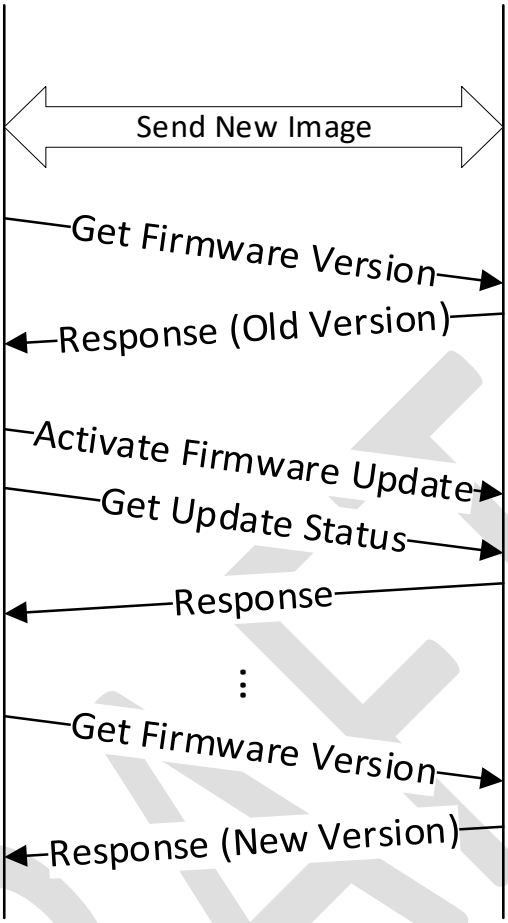

Figure 2 Image Update Command Flow

2.3 Invalidating Signing Certificates

When it is necessary to revoke a signing certificate, a firmware image must be created and signed with the new certificate. As part of the image metadata, it will indicate that the old certificate is no longer valid, and it will be revoked as part of the update process. A side-effect of revoking a certificate is that the recovery image will no longer be valid if it was signed with the revoked certificate. To ensure there is always an image that can be used for firmware recovery operations, the image in the Recovery partition will also be updated when the recovery image has been invalidated due to certificate revocation.

2.4 Firmware Update Options

A firmware image may need to convey additional information about an update that is taking place. These options will be carried as a header on the main firmware image, and they can be parsed by the firmware update routine to ensure proper verification and installation of the new firmware image. These options can include:

- Mechanisms to force updating of the recovery image.
- Anti-rollback capabilities without requiring revocation of the signing certificate.
- Information about the contents of the firmware image.

2.5 Firmware Update Process

The following diagrams describe the process executed by the RoT to update the firmware.

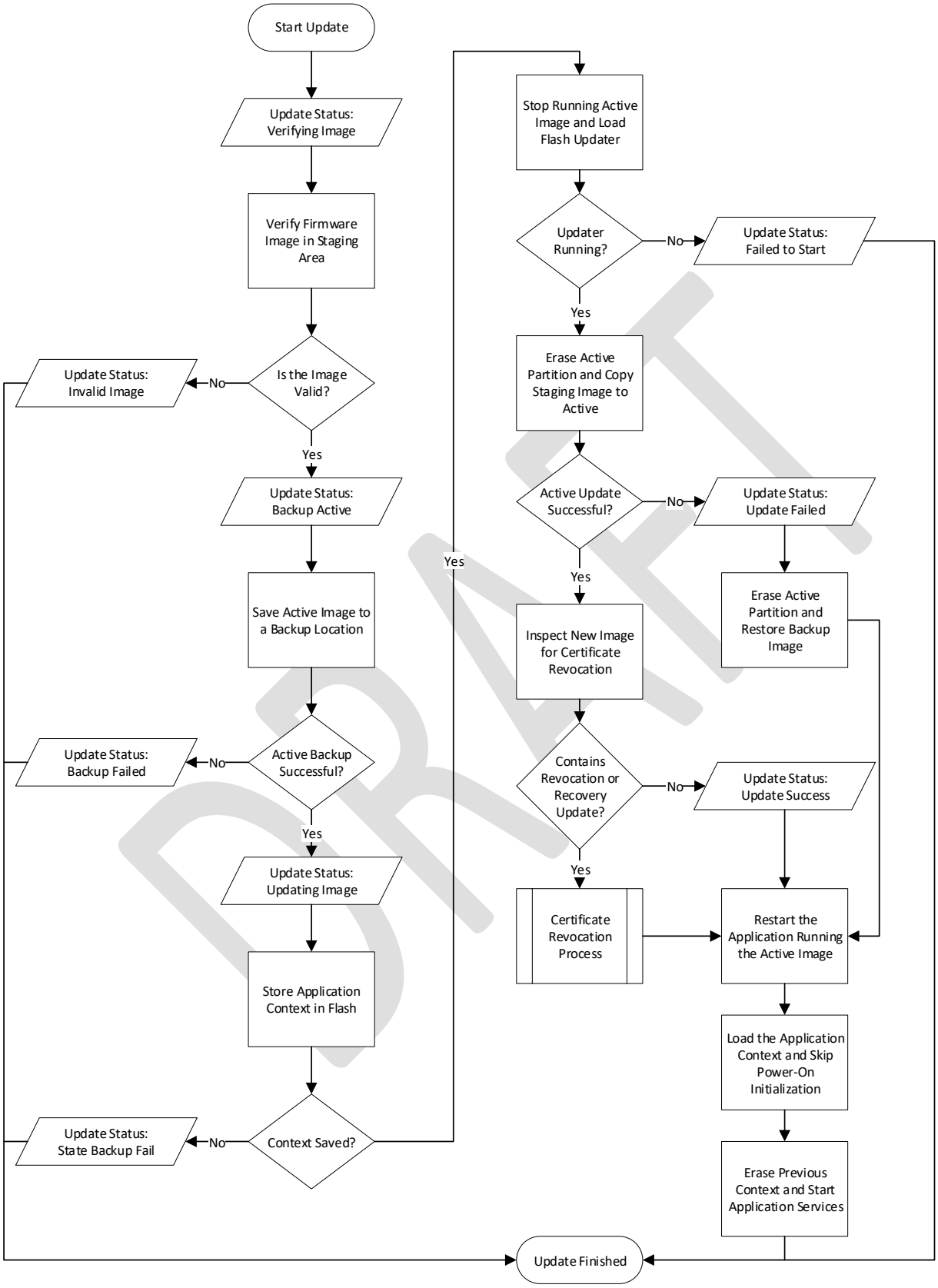

Figure 3 Firmware Update Process

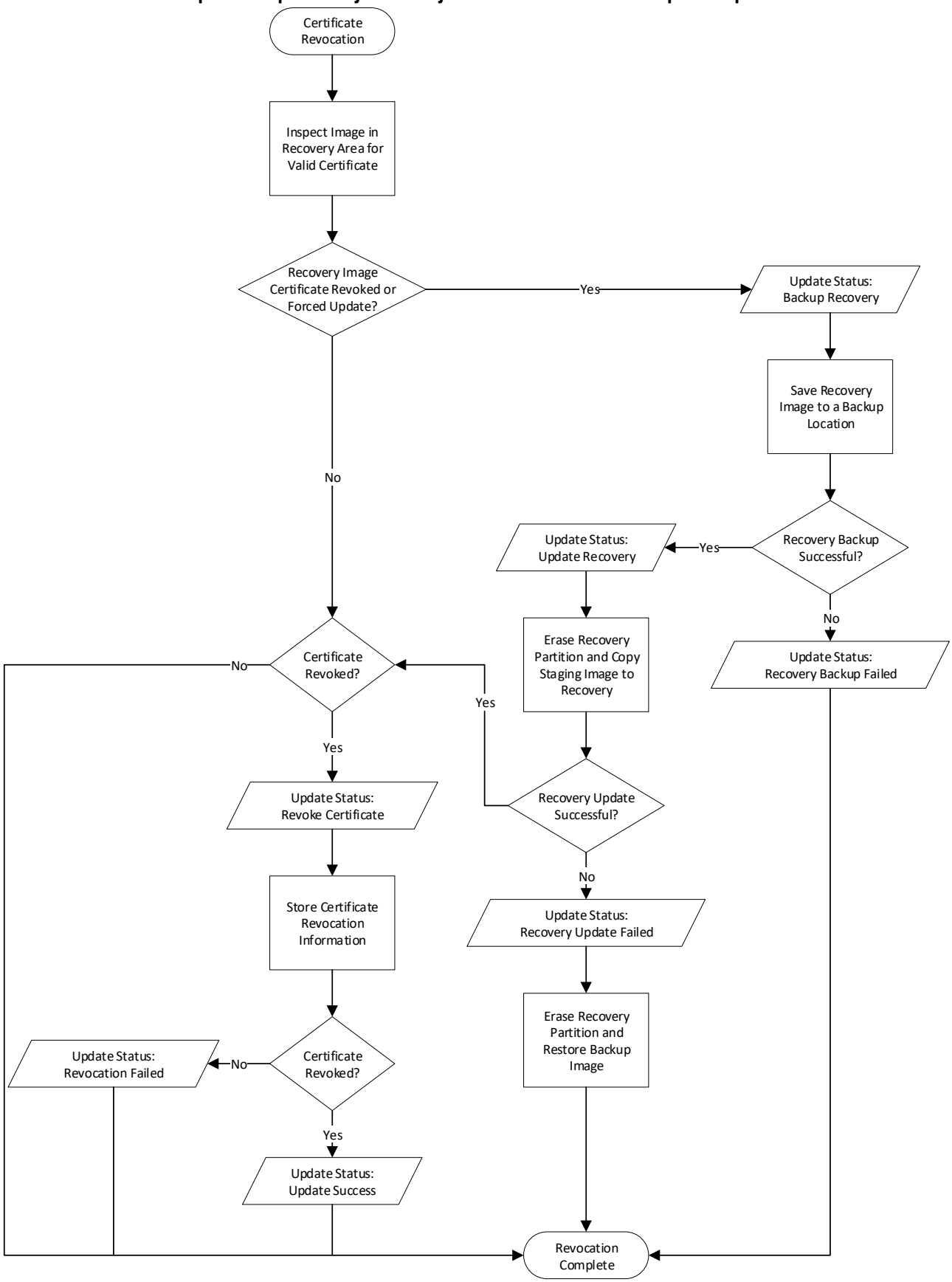

Figure 4 Update with Certificate Revocation

2.6 Firmware Update Status

The Update Status request with an ID of 00 will be used to query for firmware update status. The response payload will be the following:

Payload	Description
1	Overall Status 00 = Operation successful 01 = Operation starting 02 = Failed to start update process 03 = Verifying the received image 04 = Failed to receive entire update image 05 = Failure while verifying received image 06 = Received image not valid 07 = Backing up active image 08 = Failed to back up active image 09 = Saving current application state 0A = Application state was not saved 0B = Updating the active image with the staging image 0C = Failed to update the active image 0D = Checking for certificate revocation 0E = Failed certification revocation checking 0F = Checking recovery image for required updates 10 = Failed checked the recovery image 11 = Backing up recovery image 12 = Failed to back up recovery image 13 = Updating the recovery image with the staging image 14 = Failed to update the recovery image 15 = Revoking previous certificate 16 = Certificate revocation failed 17 = No update operation run since last reboot 18 = Failed to prepare staging area for update 19 = Preparing staging area for update data 1A = Failed to write received data to staging region 1B = Writing update data to staging region 1C = Request made before previous operation has completed 1D = Update service is not running 1E = Update status cannot be determined 1F = System state currently does not allow for update operations
2:4	Device specific error code

Table 1 Firmware Update Status Response

3 Image Format and Verification

Both at boot and prior to running a firmware update, the validity of an image must be verified. In both cases, the same firmware components will get validated. The firmware image contains three different sections of data to facilitate this verification process. The first is the application launcher and RIoT Core which will get validated by the ROM bootloader. The second is the certificate that is used to validate the main application image. This certificate is validated using the

root certificate in the device. The last part is the main application image, which is signed with the application certificate. This certificate will be checked to see if it has been revoked, and if not, will be used to validate the main application.

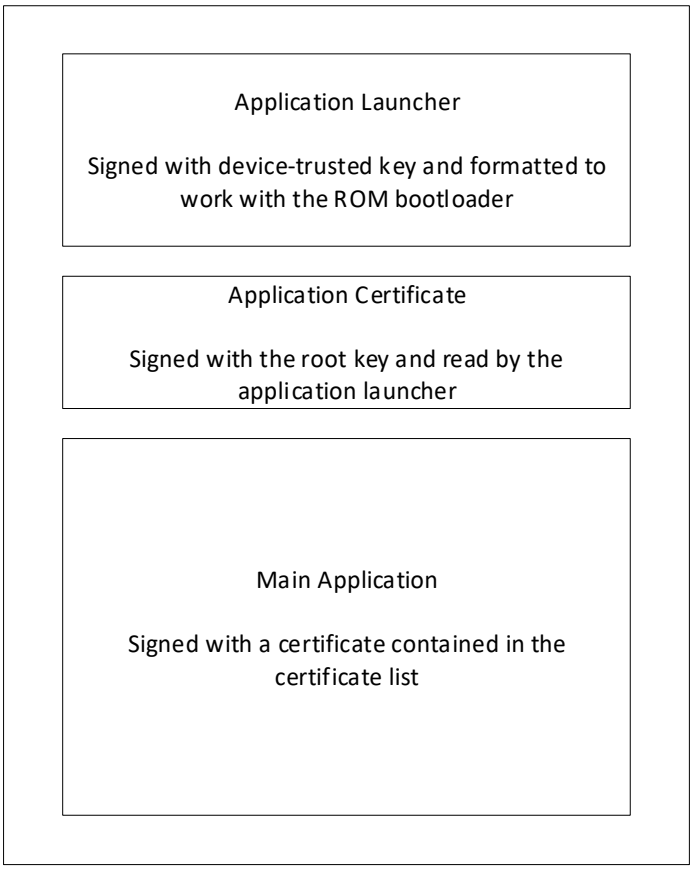

Figure 5 Firmware Image Format

3.1 Boot-Time Verification

While booting, the verification chain starts with the ROM bootloader verifying and running the application launcher. The application loader verifies the application certificate, then uses this certificate to verify the main application. If the main application is determined to be valid, it is executed.

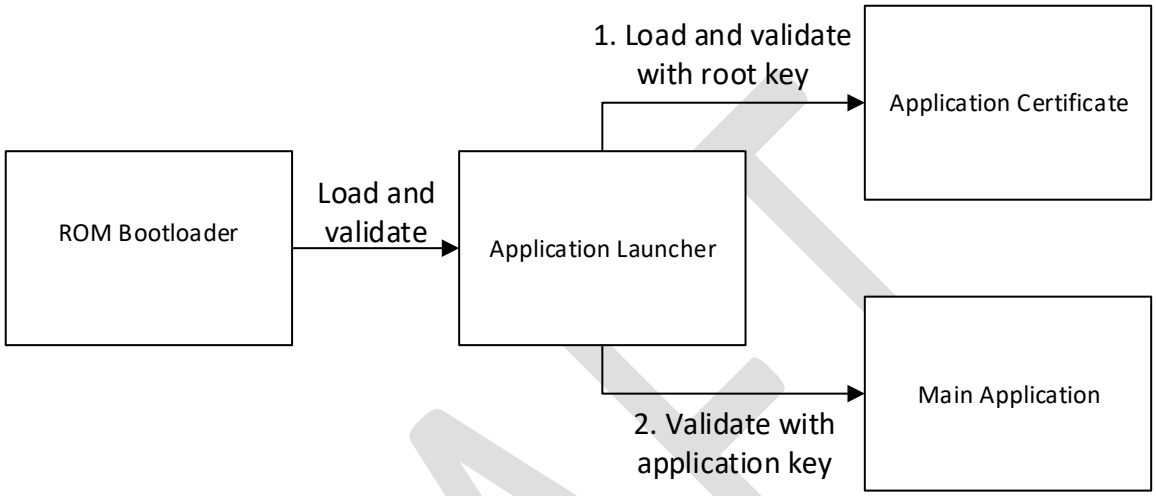

Figure 6 Boot-Time Verification Flow

3.2 Image Update Verification

When verifying an image for a firmware update, the main application must be able to verify all pieces of the new image. The main application will parse each component of the firmware image to ensure that it is valid prior to starting the update.

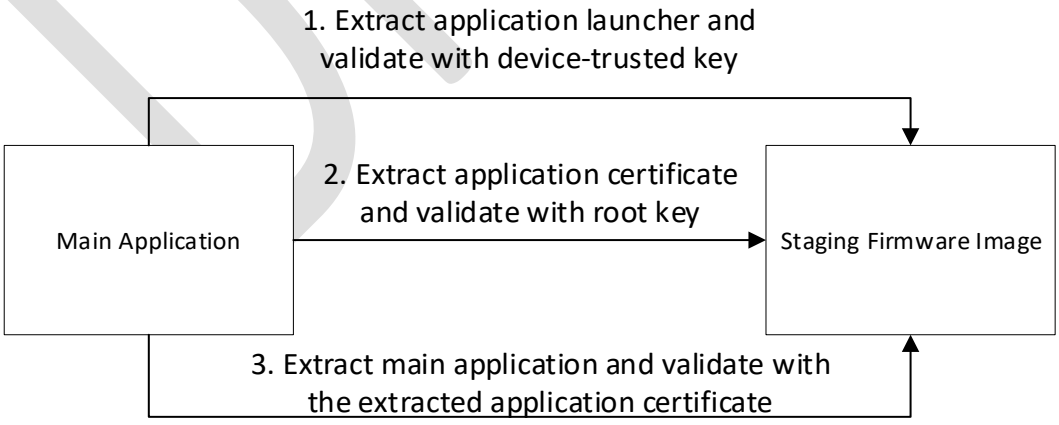

Figure 7 Update Verification Flow

3.3 Application Launcher Format

The image format of the application launcher is determined by the ROM bootloader of the RoT.

3.4 Application Certificate Format

The application certificate will immediately follow the application launcher in the firmware image and contains the public keys for the certificates used for component validation. It also indicates which application certificates have been revoked.

Value
Certificate ID The Certificate ID is used to enforce revocation. Refer to the Processor Cryptography spec for details.
Application Public Key
PFM Root Public Key
Root Public Key
Certificate Signature This is the SHA-256 RSA or ECDSA signature of all previous information using the root key.

Table 2 Application Certificate Format

3.5 Main Application Format

The main application will immediately follow the application certificate in the firmware image. The image contains a header that provides the signature of the application.

Length (Bytes)	Value
4	Application Length
n	Application Data
256	Signature This is an RSA-2048 encrypted SHA-256 hash of all previous information using the application key from the certificate.

Table 3 Main Application Format

3.6 Update Verification

The following diagrams describe the process executed by the RoT to validate a firmware image prior to update.

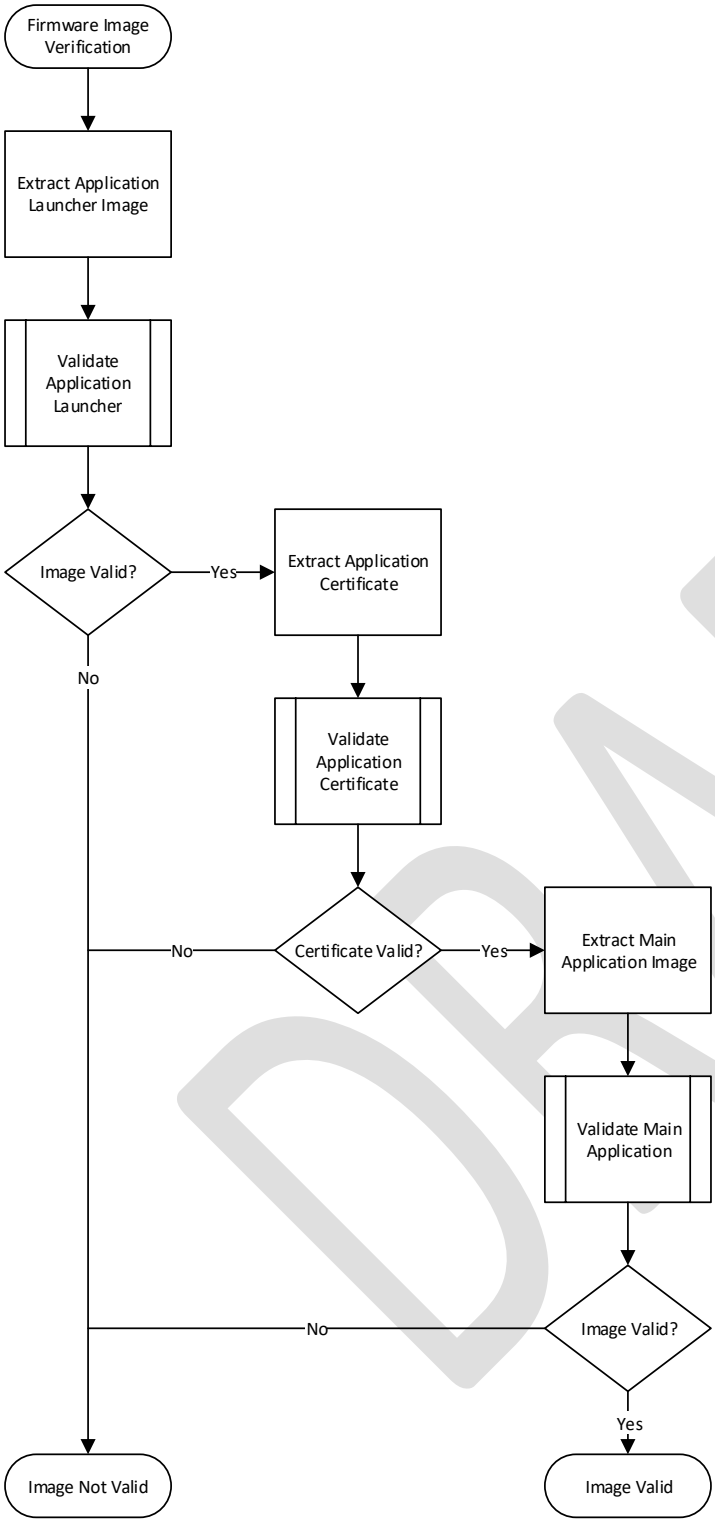

Figure 8 Firmware Image Verification

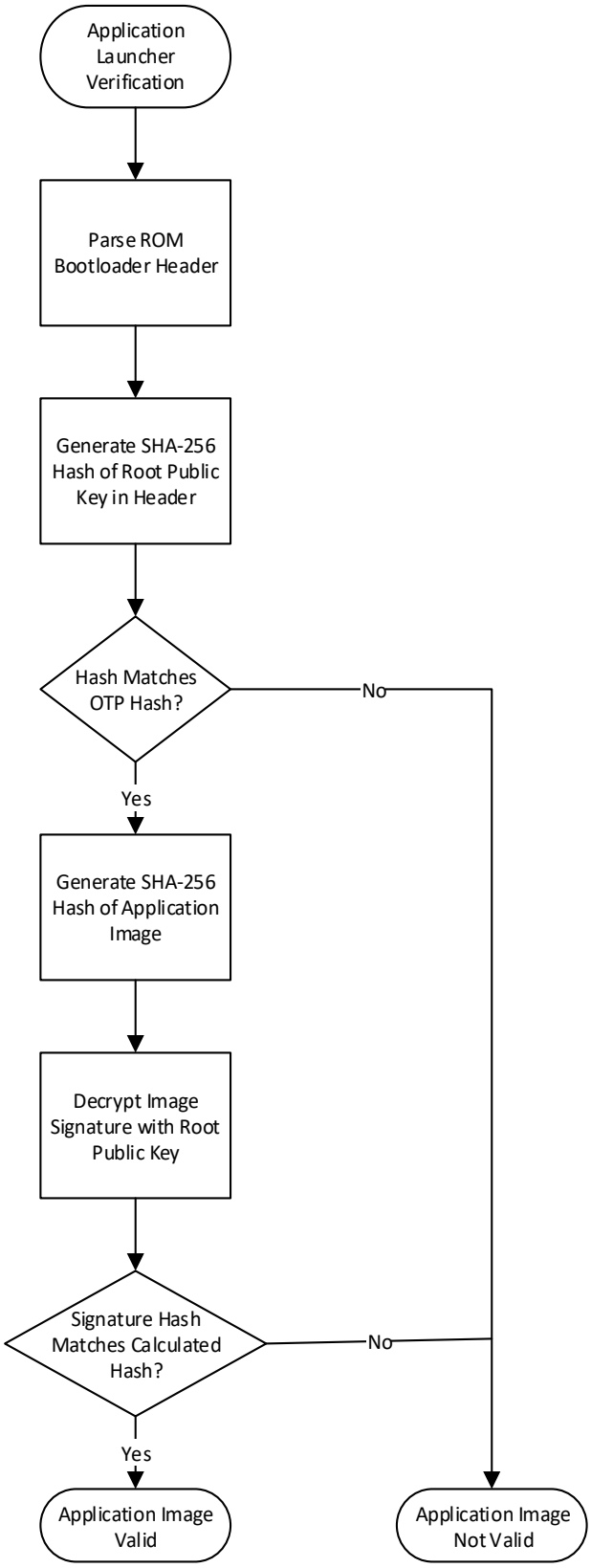

Figure 9 Application Launder Verification

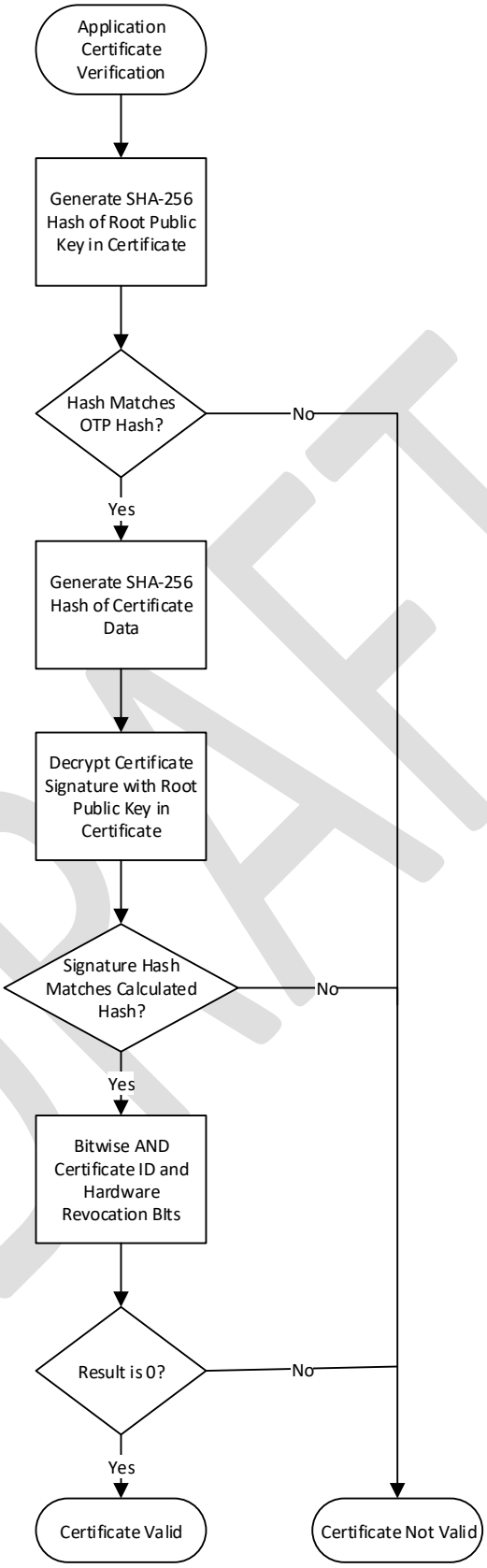

Figure 10 Application Certificate Verification

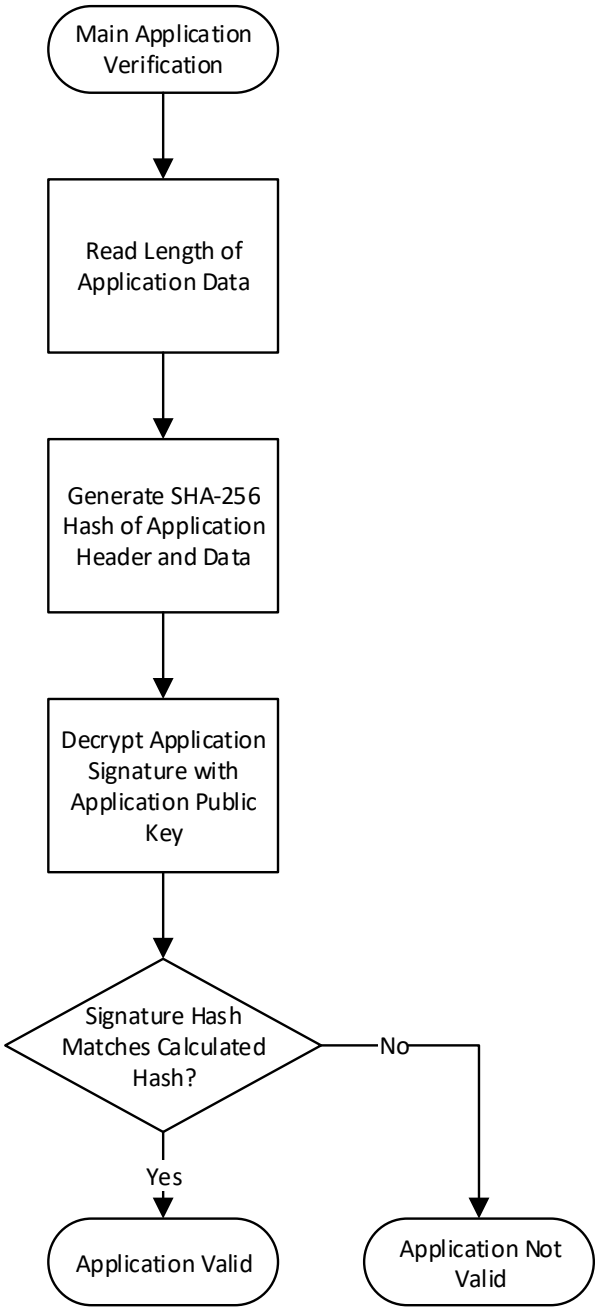

Figure 11 Main Application Verification

4 Platform Firmware Manifest (PFM) Updates

The Cerberus RoT firmware accesses a manifest detailing the firmware allowed for the other devices in the platform. As new firmware becomes available for these components, the Platform Firmware Manifest (PFM) needs to be updated for that component, but it is not desirable to upgrade the entire Cerberus firmware to achieve this update. It is therefore possible to run an update process that is only intended to update PFMs.

4.1 PFM Management

Each component that is being protected by Cerberus has a PFM containing information necessary to verify the authenticity of the firmware for that component. For each PFM, Cerberus manages up to two PFM instances: the active PFM and pending PFM. The active PFM contains the information that is currently being used by Cerberus to validate component firmware. The pending PFM contains updated information that should be used by Cerberus but has not yet been made active.

Prior to initial provisioning, Cerberus will have no PFMs. Once a PFM has been provided to Cerberus and activated, the PFM cannot be removed to return to the unprovisioned state.

4.1.1 PFM Activation

Cerberus will not allow a new PFM to be activated until it has successfully validated flash contents. By doing so, it proves the contents of flash contain an image that is supported by the new PFM and that on the next reboot, Cerberus would allow the component to load the firmware. If this requirement were not in place, it would be easy to get into a situation where an updated PFM removes support for the active image, which would result in an authentication failure on the next reboot. If this failed component were imperative to being able to update PFMs, such as the BMC, the system would be in an unrecoverable state.

The same flow is true for initial provisioning as for PFM updating. The first PFM that is provided to Cerberus for a component will not be activated until it has successfully validated the flash for that component. The flash must be fully validated, in the same way that a component firmware update must be validated, before the first PFM can be activated.

4.1.2 Validation Sequence

With two possible PFMs and two sets of flash, there are four combinations of PFM and flash that may need validation when errors are encountered. Of these combinations, activating a new PFM takes priority over activating a new flash image. This is to ensure that the latest information about which firmware is allowed to run is being used.

The following is the order of validation attempts. The sequence ends at the first successful validation, and any validation combination that is not valid for the current state will be skipped.

1) Pending PFM validates a firmware update.
2) Pending PFM validates active firmware.
3) Active PFM validates a firmware update.
4) Active PFM validates active firmware.

4.2 Send PFM Update

The process for sending a new PFM to the Cerberus RoT is similar to the process of sending a new firmware image. The area that will hold the updated PFM must first be erased. This is followed by a sequence of commands that send the PFM data. This process will discard any pending PFM that may have already been present in the device.

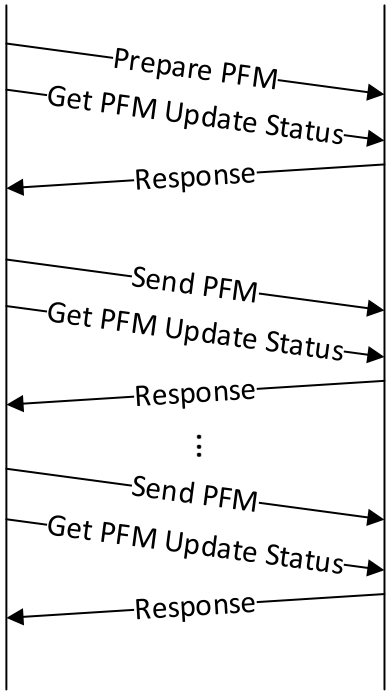

Figure 12 Send New PFM Command Flow

4.3 Update Active PFM

After the new PFM has been transmitted to the RoT, Cerberus can be directed to apply that PFM as the active PFM to use for component validation. Cerberus will first validate that the received PFM is valid. Once the PFM is determined to be valid, it will be marked as the pending PFM. Upon next reboot of the component or of Cerberus, the RoT will attempt to activate the PFM. The update status can be queried to determine if Cerberus accepted or rejected the new PFM.

A valid PFM requires two things:

1) A valid signature using the PFM key from the Application Certificate.
2) An identifier greater than the identifier for the current active PFM.

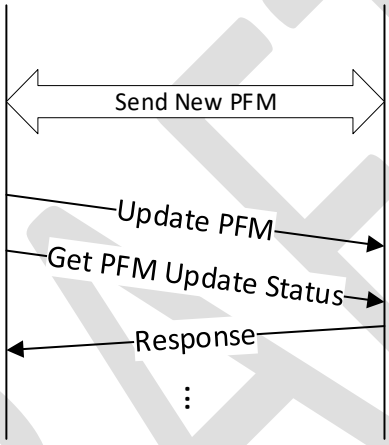

Figure 13 Update PFM Command Flow

4.4 PFM Update Process

The follow diagram describes the process taken by the Cerberus RoT to update the PFM.

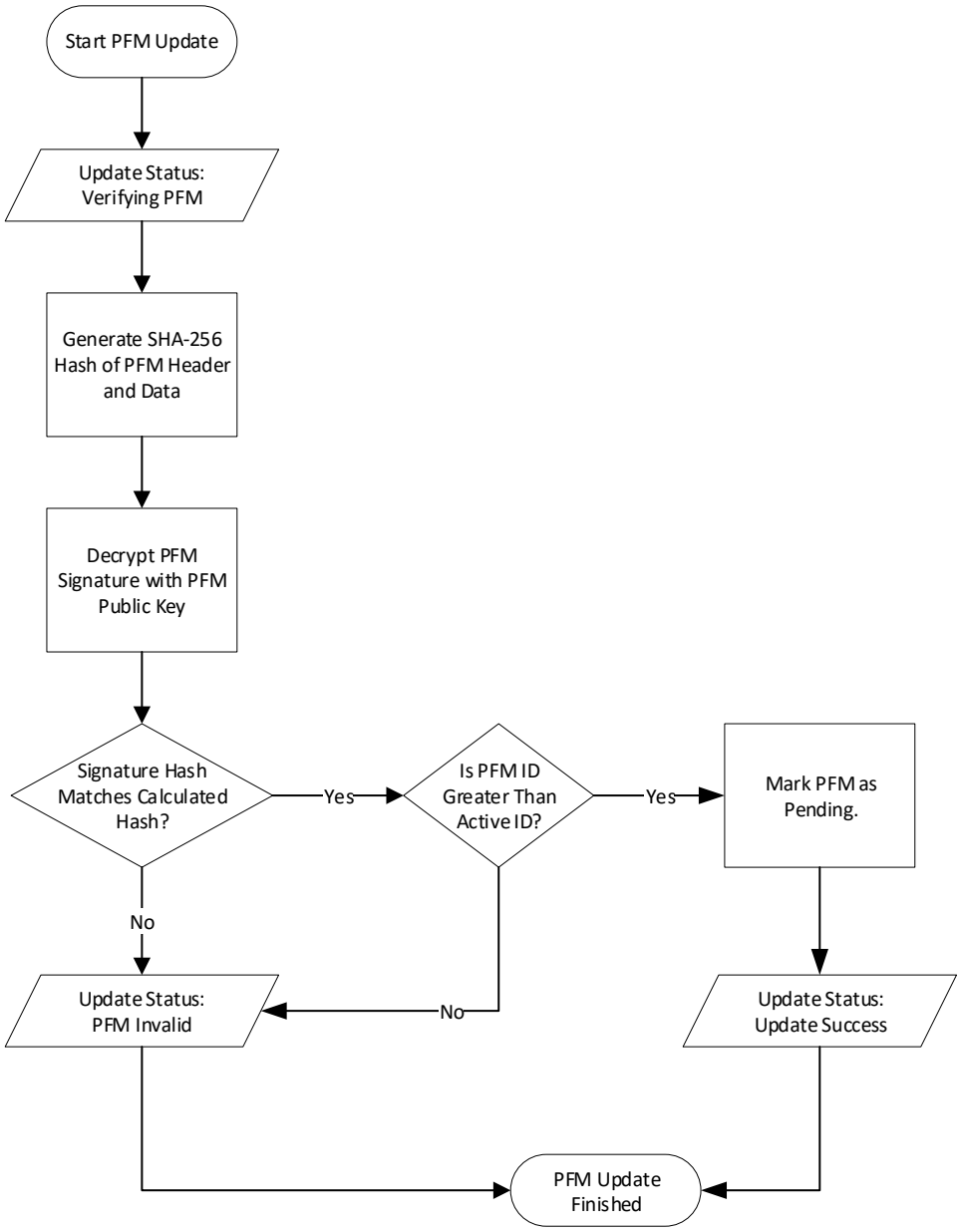

Figure 14 PFM Update Process

4.5 PFM Update Status

The Update Status request with an ID of 01 will be used to query for PFM update status. The response payload will be the following:

Payload	Description
1	Overall Status 00 = Operation successful 01 = Operation starting 02 = Request made before previous operation has completed 03 = Preparing pending region for PFM data 04 = Failed to prepare pending region 05 = Writing PFM data to pending region 06 = Failed to write received data to pending region 07 = Validating received PFM 08 = Failed to validate the new PFM 09 = Unspecified error occurred during operation processing 0A = No PFM operation run since last reboot 0B = PFM update service is not running 0C = Update status cannot be determined 0D = Attempting activation of pending PFM 0E = Failed to activate pending PFM 0F = PFM validation successful, but host reboot required for activation 10 = Error during activation that prevents host access to flash, retrying to correct error
2:4	Device specific error code

Table 4 PFM Update Status Response

5 Component Firmware Manifest (CFM) Updates

To manage attestation for slave devices, a PA-RoT needs information about these devices. The Component Firmware Manifest (CFM) is the configuration file that provides this information. Management of CFMs happens in a very similar fashion to PFMs.

5.1 Send CFM Update

The flow is the same as for PFMs, but it uses the CFM prepare, data, and update status commands. Refer to Section 4.2 for details.

5.2 Update Active CFM

The flow is the same as for PFMs, but it uses the CFM activate and status commands. Refer to Section 4.3 for details.

5.3 CFM Update Status

The Update Status request with an ID of 02 will be used to query for CFM update status. The status returned is the same as for PFM updates. Refer to Section 4.5 for details.

6 Platform Configuration Data (PCD) Updates

The Platform Configuration Data (PCD) provides static information that is specific to a platform that Cerberus RoT firmware needs to operate correctly. Management of this configuration data is very similar to PFM management.

6.1 Send PCD Update

The flow is the same as for PFMs, but it uses the PCD prepare, data, and update status commands. Refer to Section 4.2 for details.

6.2 Update Active PCD

The flow is the same as for PFMs, but it uses the PCD activate and status commands. Refer to Section 4.3 for details.

6.3 PCD Update Status

The Update Status request with an ID of 03 will be used to query for PCD update status. The status returned is the same as for PFM updates. Refer to Section 4.5 for details.

7 Host Firmware Updates

Outside of sending new PFMs and CFMs, the host firmware update is not handled by Cerberus. However, Cerberus has knowledge that an update has occurred and must validate it. Sending a new PFM, update the host firmware, or both will trigger Cerberus validation flows.

The Update Status request with an ID of 04 will be used to query for validation status of host firmware. The response payload will be the following:

Payload	Description
1	Overall Status 00 = No host firmware validation pending 01 = Pending PFM to be verified on host reboot 02 = Host firmware update to be verified on host reboot 03 = Pending PFM and firmware update to be verified on host reboot 04 = A validated host firmware update will activate on host reboot 05 = A validated pending PFM and firmware update will activate on host reboot 06 = Pending PFM to be verified against flash for the first time
2:4	Device specific error code

Table 5 Host Firmware Update Status Response

8 Host Recovery Image Updates

The recovery image for host firmware is treated just like any other configuration data in Cerberus firmware.

8.1 Send Recovery Image Update

The flow is the same as for PFMs, but it uses the recovery image prepare, data, and update status commands. Refer to Section 4.2 for details.

8.2 Update Recovery Image

The flow is the same as for PFMs, but it uses the recovery image activate and status commands. Refer to Section 4.3 for details.

8.3 Recovery Image Update Status

The Update Status request with an ID of 05 will be used to query for recovery image update status. The response payload will be the following:

Payload	Description
1	Overall Status 00 = Operation successful 01 = Operation starting 02 = Request made before previous operation has completed 03 = Preparing staging region for recovery image data 04 = Failed to prepare staging region 05 = Writing recovery image data to staging region 06 = Failed to write received data to staging region 07 = Validating received recovery image 08 = Failed to validate the new recovery image 09 = Unspecified error occurred during operation processing 0A = No recovery image operation run since last reboot 0B = Recovery image update service is not running 0C = Update status cannot be determined
2:4	Device specific error code

Table 6 Recovery Image Update Status Response

9 Configuration Reset

Removing configuration from the device is a lengthy process and cannot be completed within the normal timeouts allowed for request processing. The Update Status request with an ID of 06 will be used to query for the progress of configuration reset requests.

Payload	Description
1	Overall Status 00 = Operation successful 01 = Operation starting 02 = Request made before previous operation has completed 03 = Erasing PFMs and CFMs to return to the unprotected state 04 = Failed to restore the unprotected state 05 = Erasing all configuration information to return to the default state 06 = Failed to restore the default state 07 = No recovery image operation run since last reboot 08 = Configuration reset service is not running 09 = Unspecified error occurred during operation processing 0A = Status cannot be determined
2:4	Device specific error code

Table 7 Configuration Reset Status Response