# Project Cerberus
# Firmware Update Specification

**Author:**
**Bryan Kelly**, Principal Firmware Engineering Manager, Microsoft

# Revision History

| Date | Description |
|---|---|
| 28/8/2017 | Version 1.0 |

# 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 after a trusted session has been established. 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.

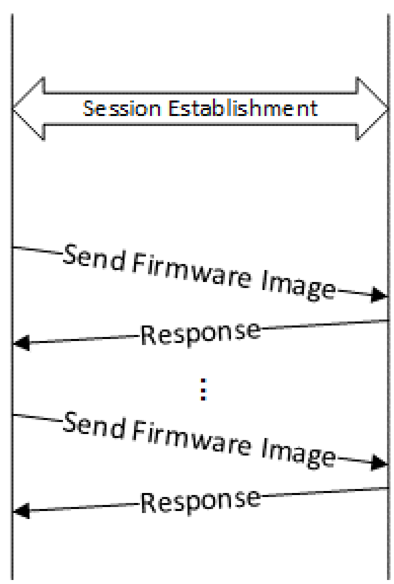


**Figure 1 Send New Firmware Image Command Flow**

## 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.

The response to the 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.

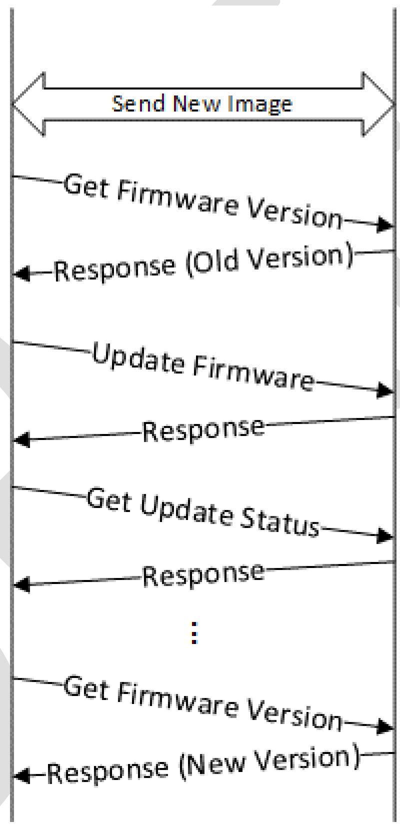


**Figure 2 Image Update Command Flow**

## 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 Process

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

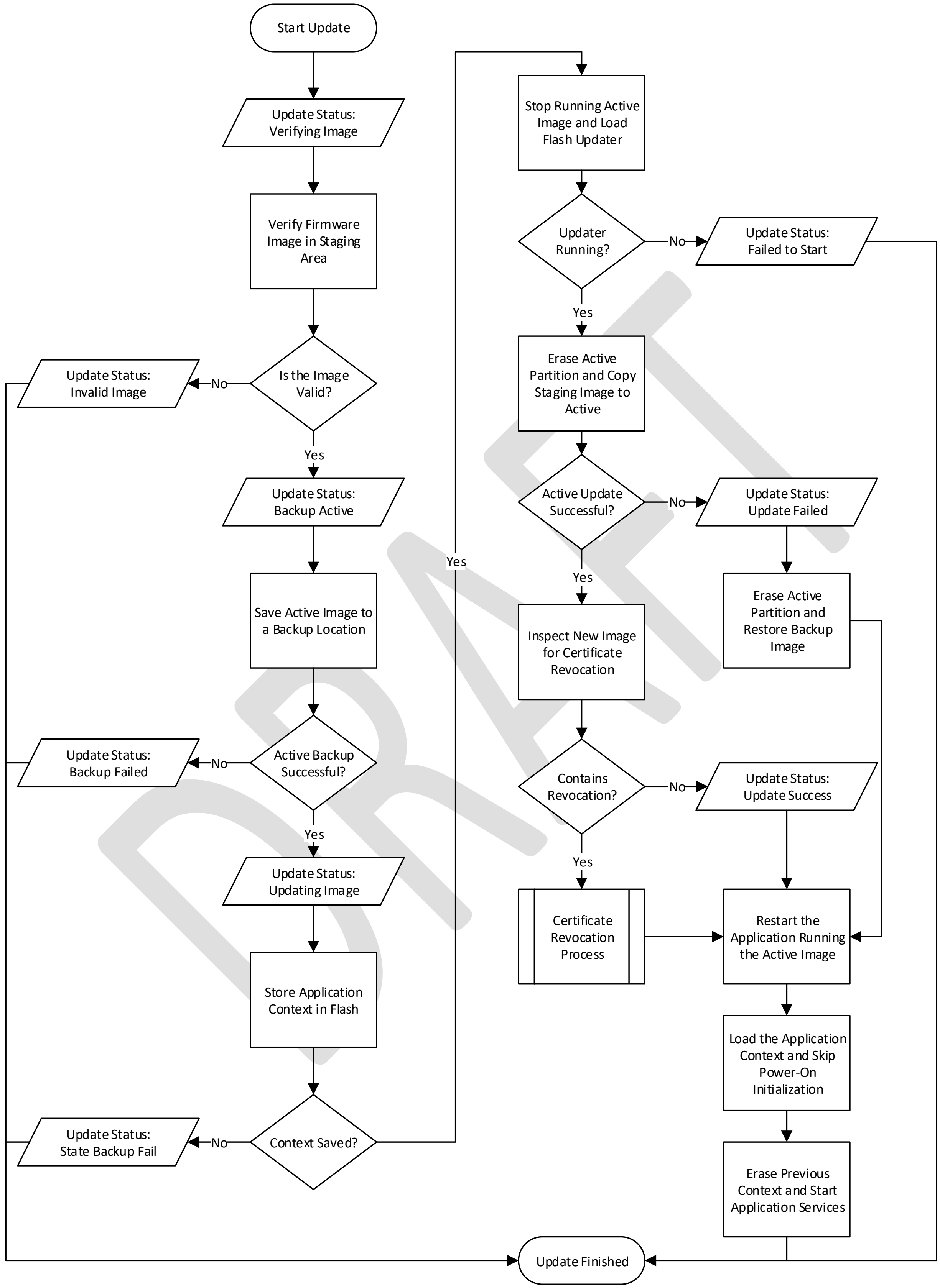


**Figure 3 Firmware Update Process**

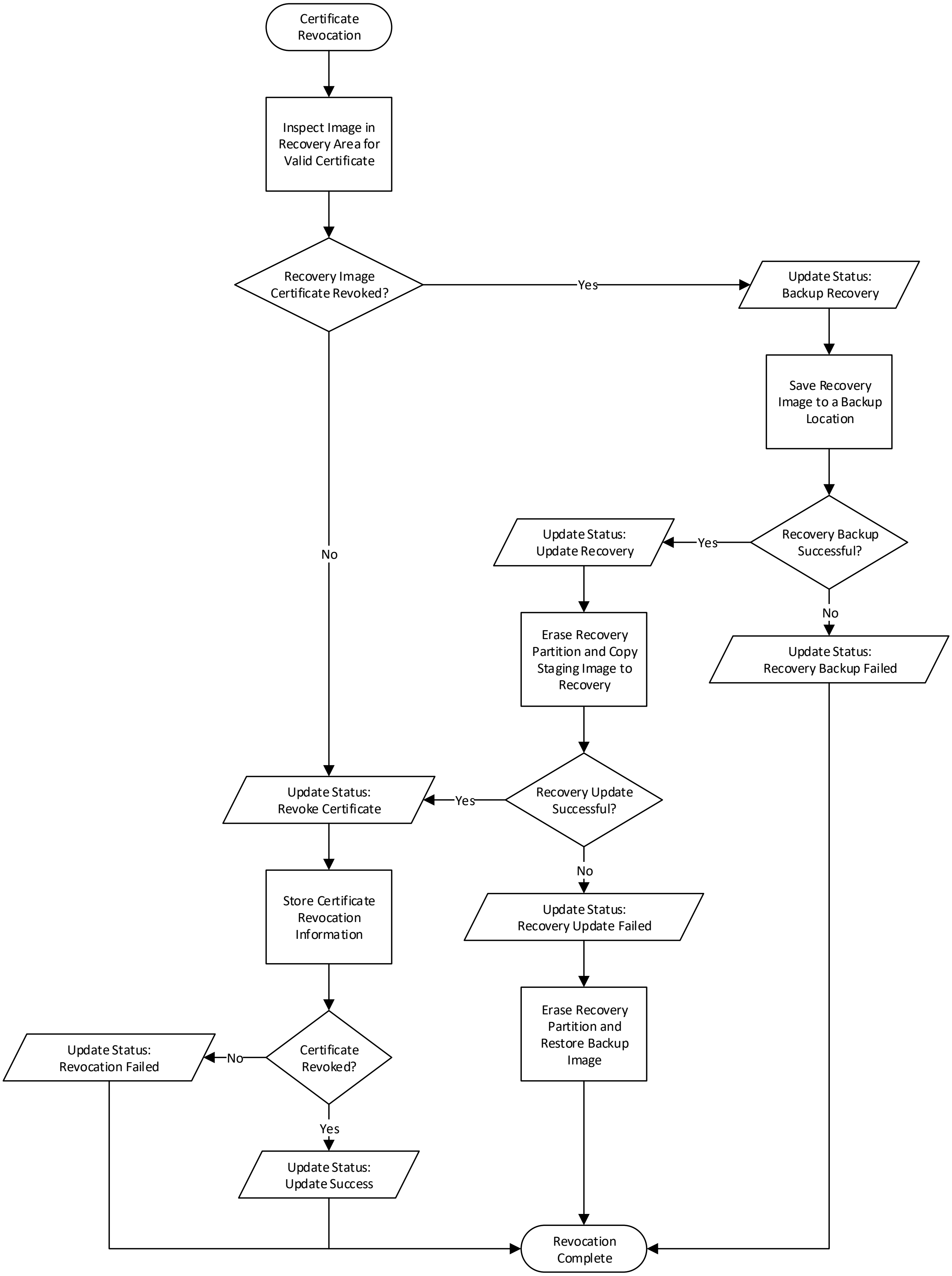


Figure 4 Update with Certificate Revocation

# 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 firmware updater which will get validated using the certificate programmed into the device. The second is the certificate that is used to validate the main application image. This certificate is also validated using the root certificate in the device. The last part in the main application image, and 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.

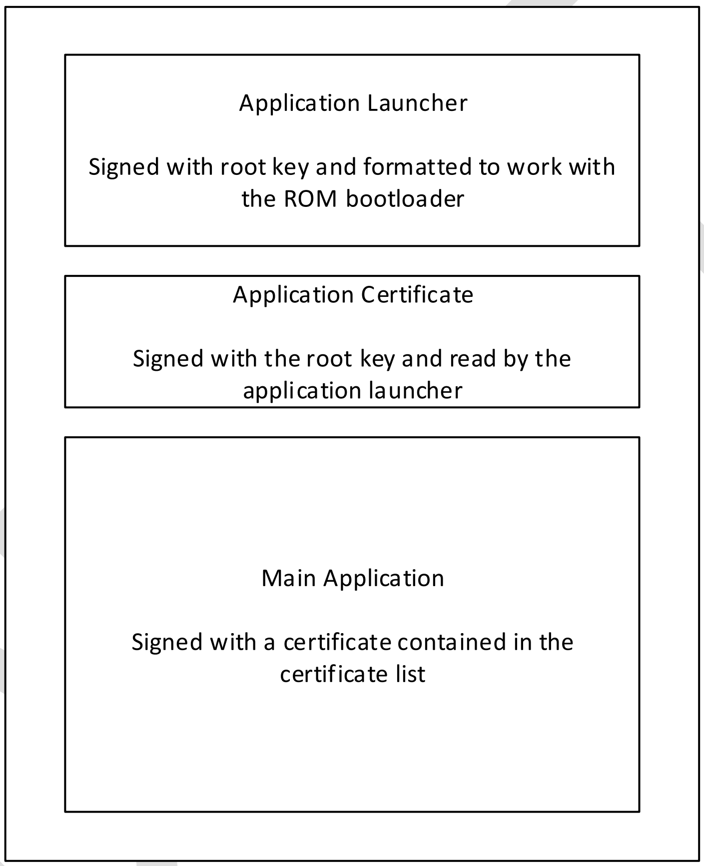


**Figure 5 Firmware Image Format**

## 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.

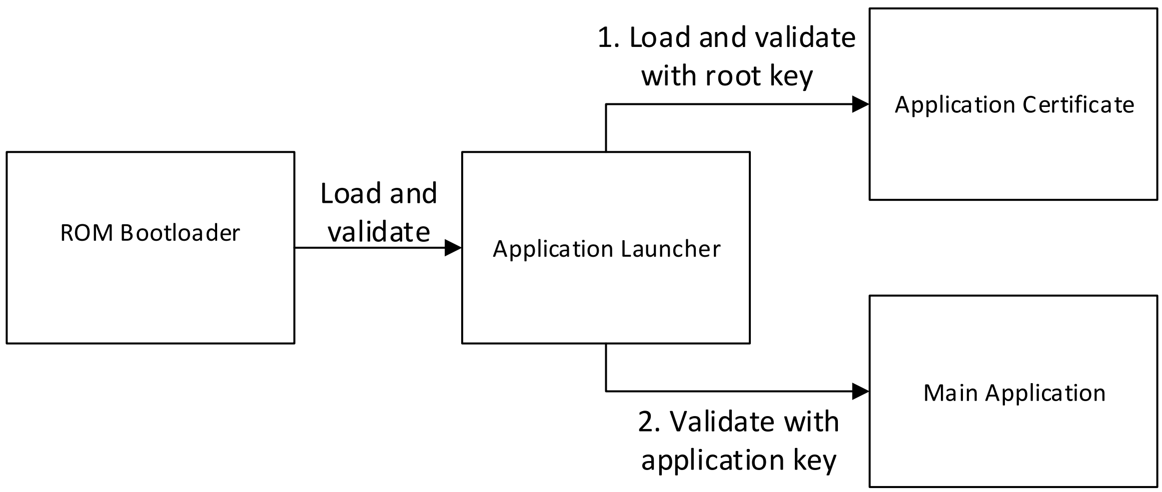


Figure 6 Boot-Time Verification Flow

## 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.

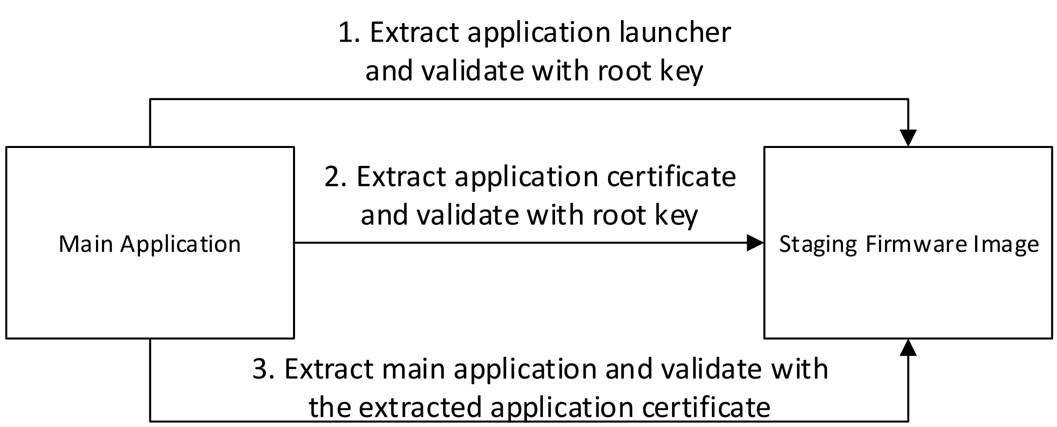


Figure 7 Update Verification Flow

## 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.

| Length (Bytes) | Value |
|---|---|
| 1 | Certificate ID<br>A certificate ID shall have at most one bit set. A certificate ID of 0 can never be revoked and should only be used when the maximum number of revocations has been exhausted. |
| 1 | Revocation Bit Mask<br>Each bit represents a certificate ID that has been revoked and should no longer be considered valid. |
| 256 | RSA-2048 Application Public Key |
| 256 | RSA-2048 PFM Public Key |
| 256 | RSA-2048 Root Public Key |
| 256 | Certificate Signature<br>This is an RSA-2048 encrypted SHA-256 hash of all previous information using the root key. |

Table 1 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<br>This is an RSA-2048 encrypted SHA-256 hash of all previous information using the application key from the certificate. |

Table 2 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.

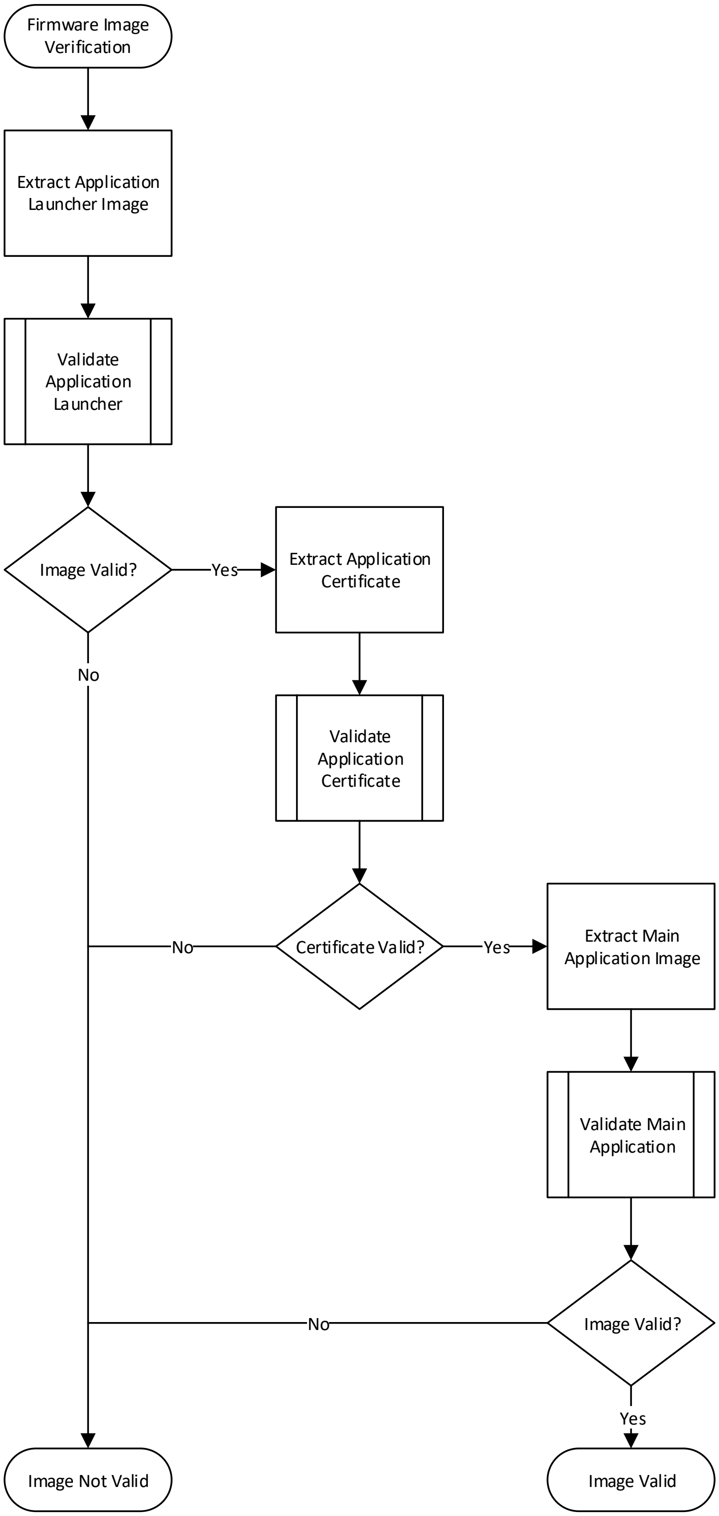


**Figure 8 Firmware Image Verification**

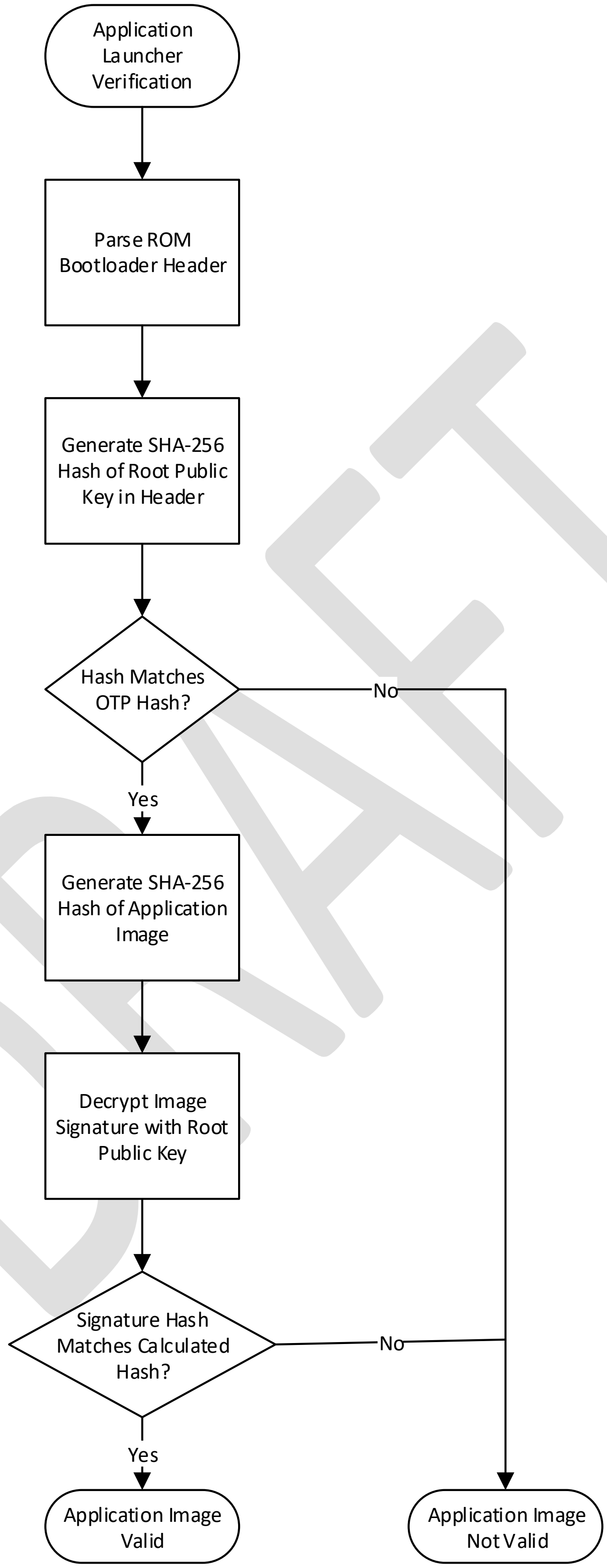


Figure 9 Application Launder Verification

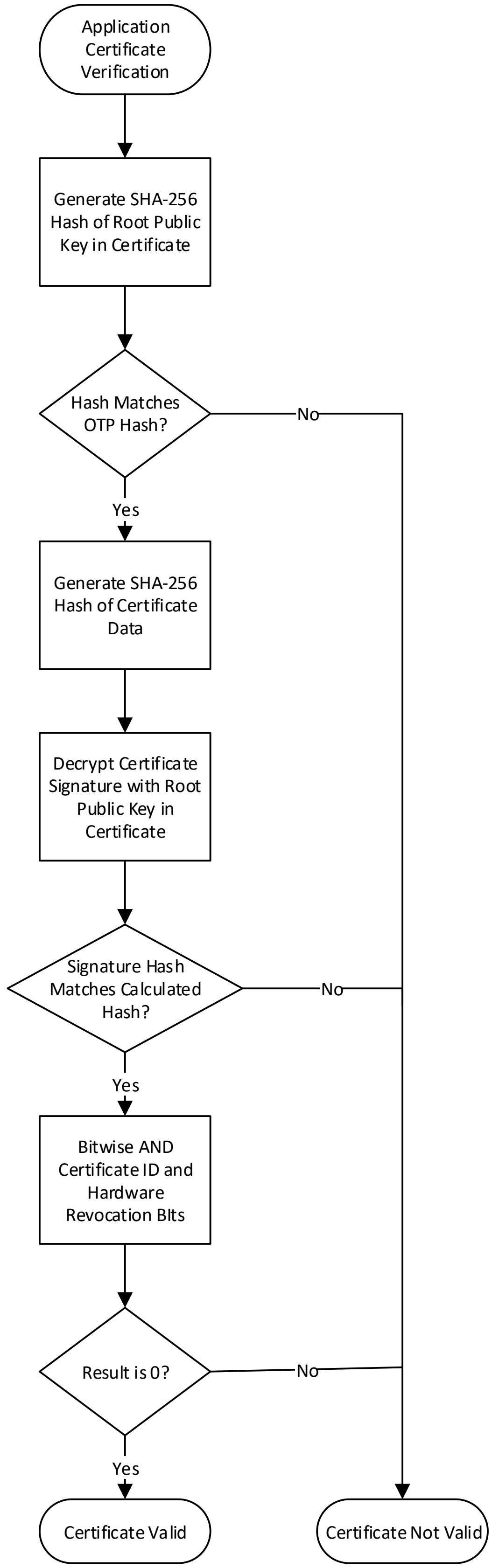


Figure 10 Application Certificate Verification

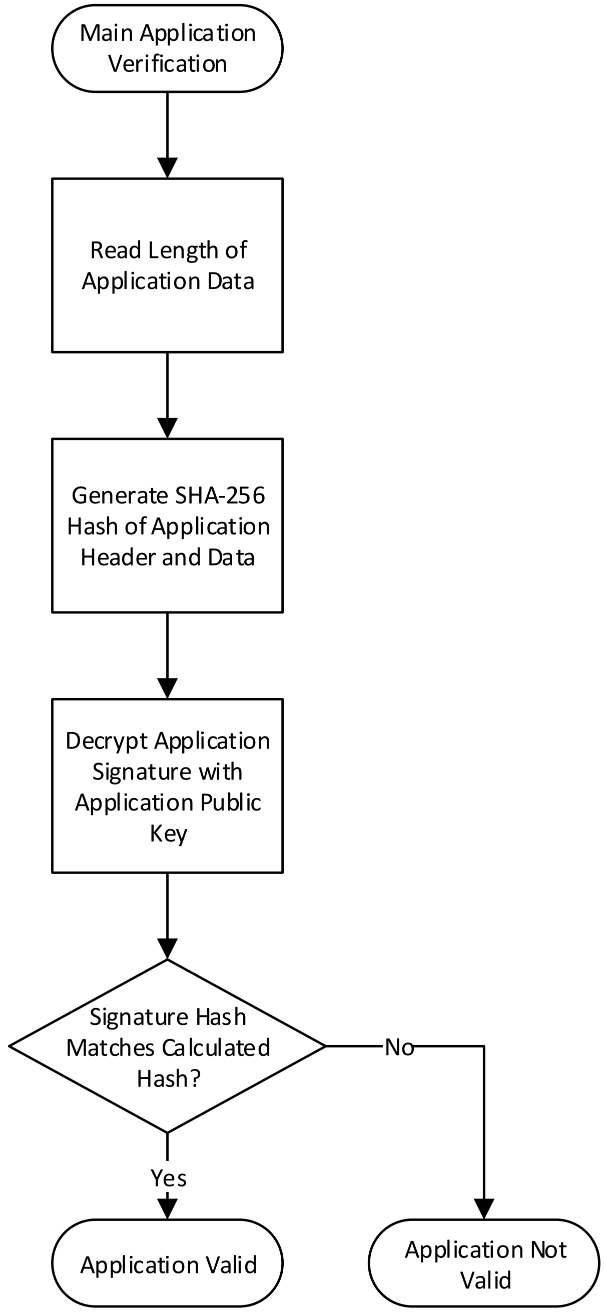


Figure 11 Main Application Verification

# 4 Platform Firmware Manifest (PFM) Updates

The Cerberus RoT firmware contains 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, but it is not desirable to upgrade the entire Cerberus firmware to achieve this update.

## 4.1 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. After a secure session is established over I2C, the updated PFM can be transmitted to the RoT. This updated PFM will be stored in a staging area, much like firmware images, before it gets applied as the active PFM.

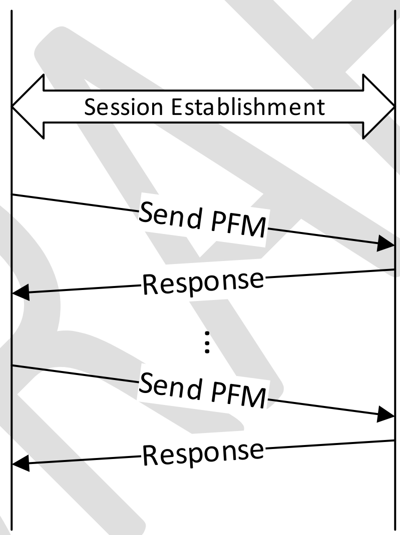


Figure 12 Send New PFM Command Flow

## 4.2 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. The PFM must be signed with the PFM key from the Application Certificate. This signature will be used to validate the PFM prior replacing the active PFM.

Just like firmware updates, the command to update the PFM will return immediately and only report if the command was received correctly. In order to find out the PFM update status, the Cerberus RoT must be queried.

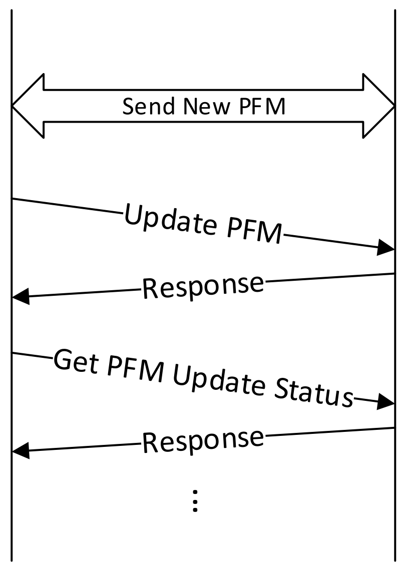


Figure 13 Update PFM Command Flow

## 4.3 PFM Image 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 | PFM Length |
| n | PFM Data |
| 256 | Signature<br>This is an RSA-2048 encrypted SHA-256 hash of all previous information using the PFM key from the certificate. |

## 4.4 PFM Update Process

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

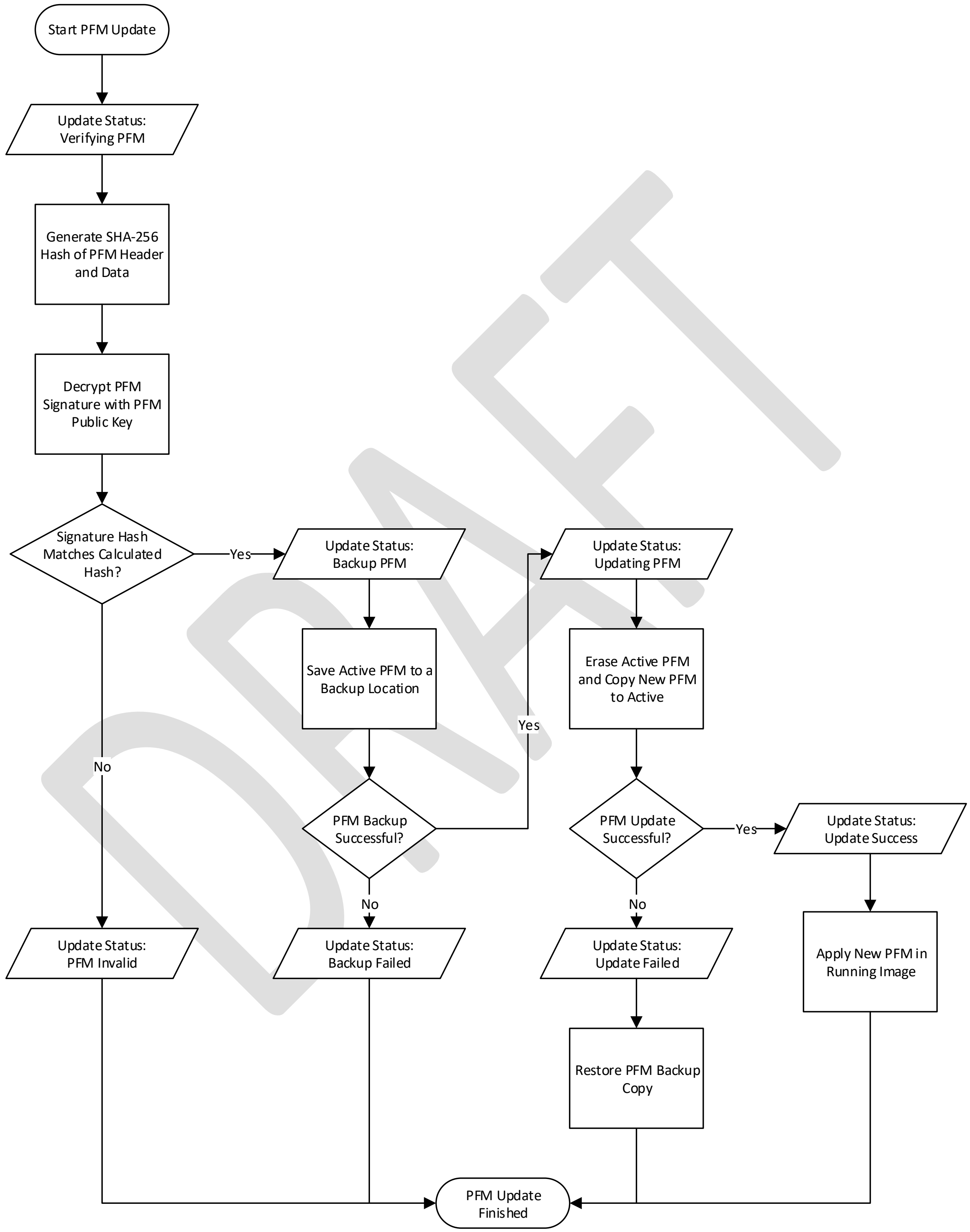




Figure 14 PFM Update Process