Application Note

Boot Flow Options on TDA4 devices

Diwakar Dhyani, Doredla Sudheer Kumar, J Keerthy, Brijesh Jadav

ABSTRACT

TDA4 and DRA8 devices supports multiple boot flow and different combinations. This application note includes all of the boot flow options available on the TDA4 and DRA8 devices, Customers can select the most appropriate boot flow option based on the the use case.

Table of Contents

Trademarks

1 Introduction

This application note provides the details of all the available boot flow option on TDA4 and DRA8 devices. Different combinations are still possible. The intent is to demonstrate some of the commonly used boot flows and the corresponding boot images.

The RTOS, Linux and QNX software development kits (SDKs) for TDA4x and DRA82x processors support multiple boot flows. These boot flows are intended to be customized by customers and partners as part of the path to production software

This document mainly focuses on Linux and RTOS SDK boot flow options.

There are two bootloaders in Processor SDK (RTOS/Linux):

- SBL - Secondary Boot Loader (RTOS Bootloader)
- SPL - Secondary Program Loader (SPL) (Linux Boot Loader)

The following boot flows are for High Secure (HS) devices. For General Purpose (GP) devices, the same boot flow applies with authentication bypassed due to the absence of customer keys.

1.1 ROM Loading Bootloader

In some of the devices like TDA4VE, TDA4AL, TDA4VL, AM68, TDA4VH-Q1, TDA4AH-Q1, TDA4VP-Q1, TDA4AP-Q1 ROM can load the bootloader in two ways

1. Legacy: In this flow, boot binary only has SPL or SBL. Once ROM loads SBL or SPL, the ROM loads system firmware.
2. Combined boot flow: In this flow, a boot binary blob has both Secondary bootloader (SBL) and System Firmware (SYS-FW) embedded in the boot image with a single X509 certificate. This method helps with the following situations:
   a. Allows ROM to load and run both the bootloader and SYS-FW in parallel without any dependency.
   b. Optimizes ROM boot time by minimizing different x509 certificate parsing and authentication

For more details on this, see *J784S4 J742S2 Technical Reference Manual*.

2 Secondary Program Loader

Linux bootloader uses Secondary Program Loader (SPL) and U-Boot to boot various CPUs. There are two ways to boot up to linux using SPL boot flow

- Normal Boot flow
- Falcon Boot flow

2.1 Normal Boot Flow

1. After Power on Secure ROM runs on M3/M4 core.
2. Release reset of R5, Public ROM starts of MCU R5F.
3. Public ROM reads the tiboot3.bin from boot media and sends this to secure ROM for authentication, after authentication secure ROM loads R5 SPL to MCU R5F and TIFS (TI Foundational Security firmware) to M3/M4 core.
4. R5 SPL reads tispl.bin from the boot media, authenticates using TIFS service and then loads ATF (ARM Trusted Firmware),OPTEE (Open Portable Trusted Execution Environment),A72 spl to the respective location.
5. Release A72 reset and load DM firmware.
6. A72 SPL authenticates and loads uboot.img.
7. U-Boot authenticates and loads the remote core fw on Main R5F.
8. U-Boot authenticates and loads the remote core fw on Main C7x.
9. U-Boot load Linux.

Note

There are two ways to load remote core firmware (Main R5F FW,C7x FW) by U-Boot or by Linux. On High Security device U-BOOT needs signed remote core firmware whereas while loading using Linux firmware does not need to be signed.

OPTEE is optional – Customers who do not need runtime secure calls from Linux can bypass OPTEE and save time.

To remove the optee from the boot flow, use the following command while building ATF.

make CROSS_COMPILE="$CROSS_COMPILE_64" ARCH=aarch64 PLAT=k3 TARGET_BOARD=j784s4 K3_USART=0x8

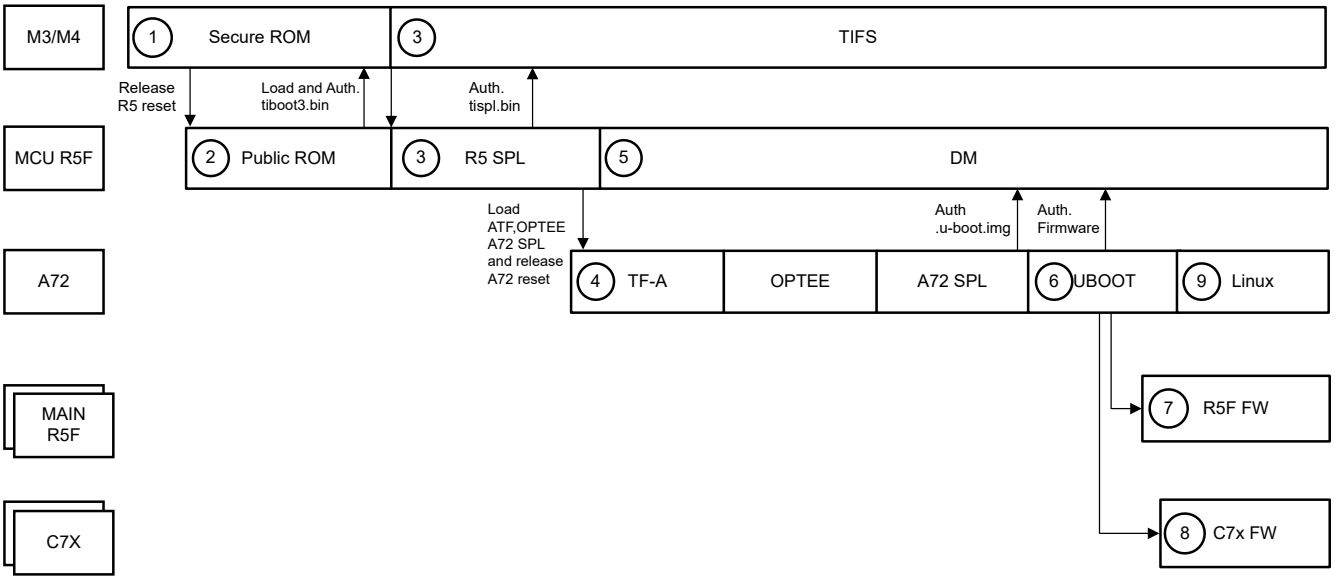

Figure 2-1. Normal Boot Flow

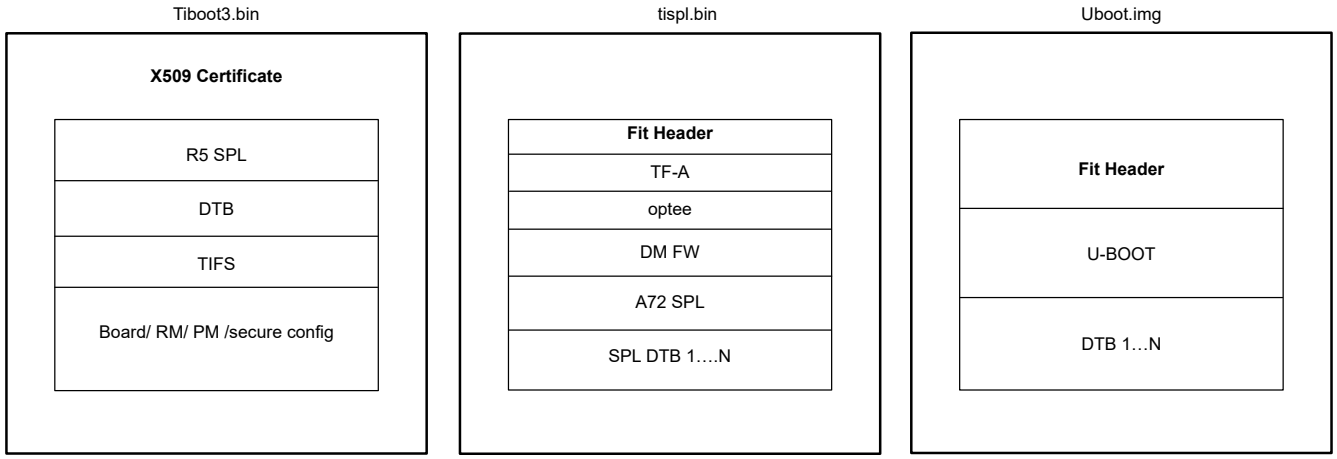

Figure 2-2. Image Format (Normal Boot Flow)

2.2 Falcon Boot Flow

Falcon mode allows direct booting to the Linux kernel, bypassing the U-Boot stage for faster boot time.

1. After Power on secure Rom runs on M3/M4 core
2. Release reset of R5, Public ROM starts of MCU R5F
3. Public Rom reads the tiboot3.bin from boot media and sends this to secure ROM for authentication. After authentication secure ROM loads R5 SPL to MCU R5F and TIFS to M3 and M4 core.
4. R5 SPL reads tispl.bin from boot media, authenticates using TIFS service and then loads ATF, OPTEE, and Linux to the respective location.
5. Release reset on A72 and load DM to itself.
6. Linux loads the remote core fw on Main R5F.
7. Linux loads the remote core fw on Main C7x

Note

Loading remote core firmware require DM (Device Manager) services, that is the reason for loading the firmware from Linux once the DM is up and running on the MCU R5F.

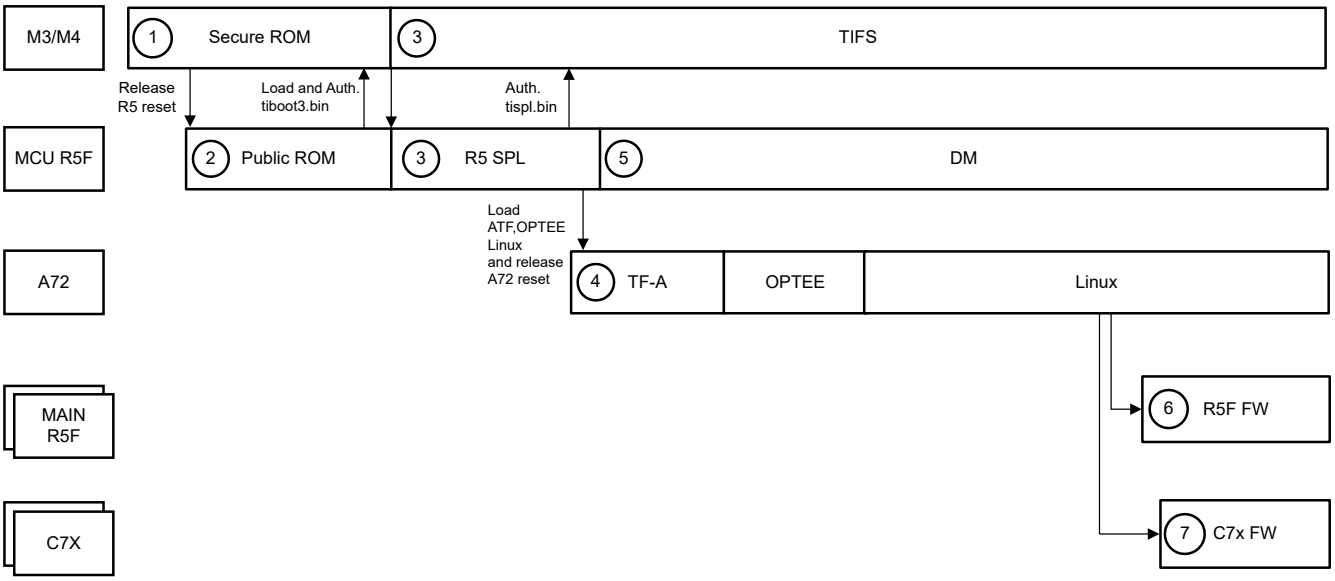

Figure 2-3. Falcon Boot Flow

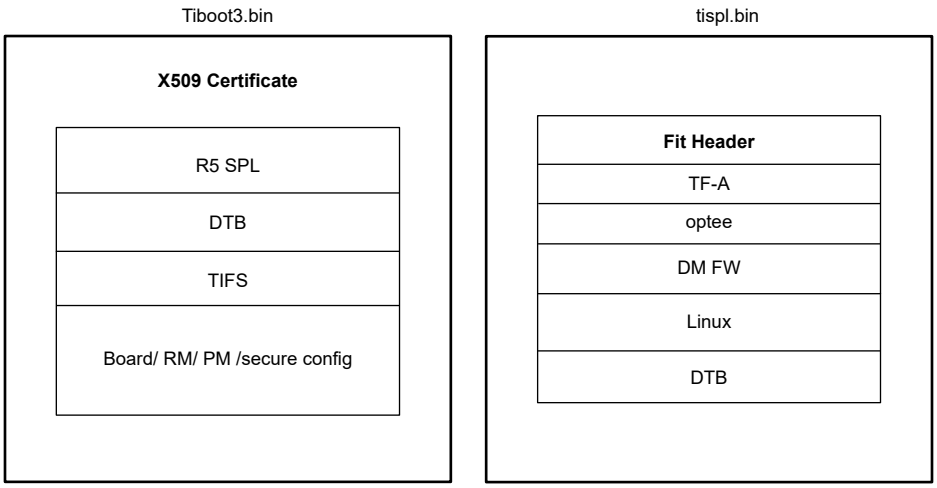

Figure 2-4. Falcon Boot Flow

See *E2E™ design support forum* for more information.

3 Secondary Boot Loader

RTOS Bootloader is referred to as Secondary Boot Loader (SBL). There are multiple ways to boot HLOS using SBL.

- Development Boot Flow
- Optimized Boot Flow
- Boot APP (Tertiary bootloader)

3.1 Development Boot Flow

1. After Power on Secure ROM runs on M3 and M4 core
2. Release reset of R5, Public ROM starts on MCU R5F
3. Public Rom reads the tiboot3.bin from boot media and sends this to secure ROM for authentication and loads R5 SBL to MCU R5F.
4. R5 SBL reads tifs.bin from boot media, authenticates and then loads on M3/M4 core using secure ROM service.
5. SBL authenticates combined app image using TIFS service and loads remote core firmware on Main R5F.
6. SBL loads remote core firmware on C7x.
7. SBL loads ATF, OPTEE and A72 SPL to the respective location.
8. SBL releases the reset of A72 and loads DM firmware on MCU R5F.
9. A72 SPL authenticates and loads U-Boot.img, if U-Boot image is present separately in the boot media.
10. U-Boot authenticates and load Linux.

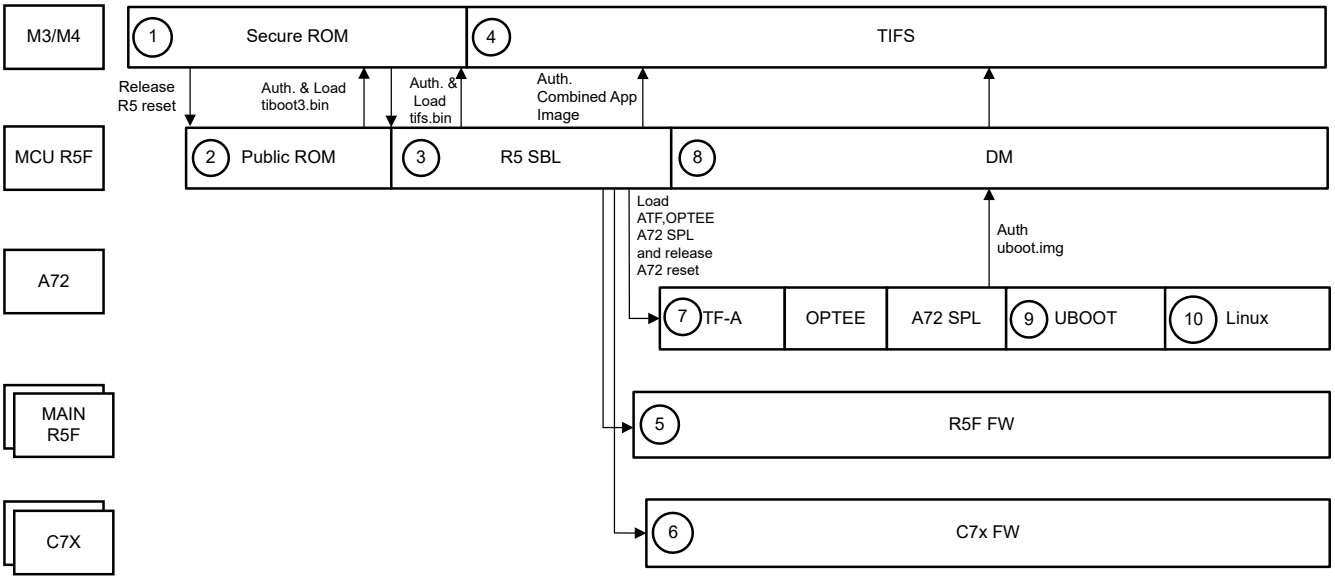

Figure 3-1. Development Boot Flow

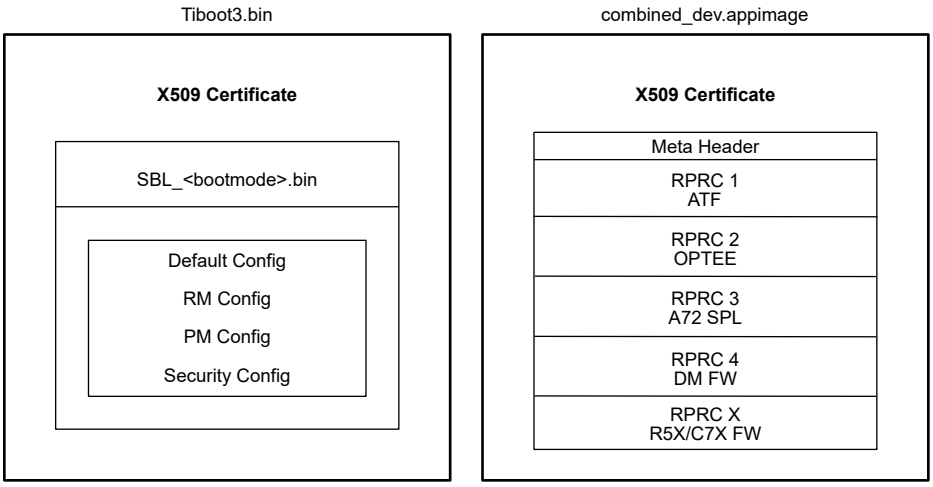

Figure 3-2. Image Format (Development Boot Flow)

3.2 Optimized Boot Flow

1. After Power on Secure ROM runs on M3 and M4 core
2. Release reset of R5, Public ROM starts on MCU R5F
3. Public ROM reads the tiboot3.bin from boot media and sends this to secure ROM for authentication and after authentication, public ROM loads R5 SBL to MCU R5F.
4. R5 SBL reads tifs.bin from boot media, authenticates and then loads on M3 and M4 core using secure ROM service.
5. SBL authenticates combined app image using TIFS service and load remote core firmware on Main R5F.
6. SBL loads remote core firmware on C7x.
7. SBL loads ATF, OPTEE and Linux to the respective location. This flow eliminates the U-Boot stage by loading Linux directly from SBL, reducing boot time.
8. SBL releases the reset of A72 and load DM.

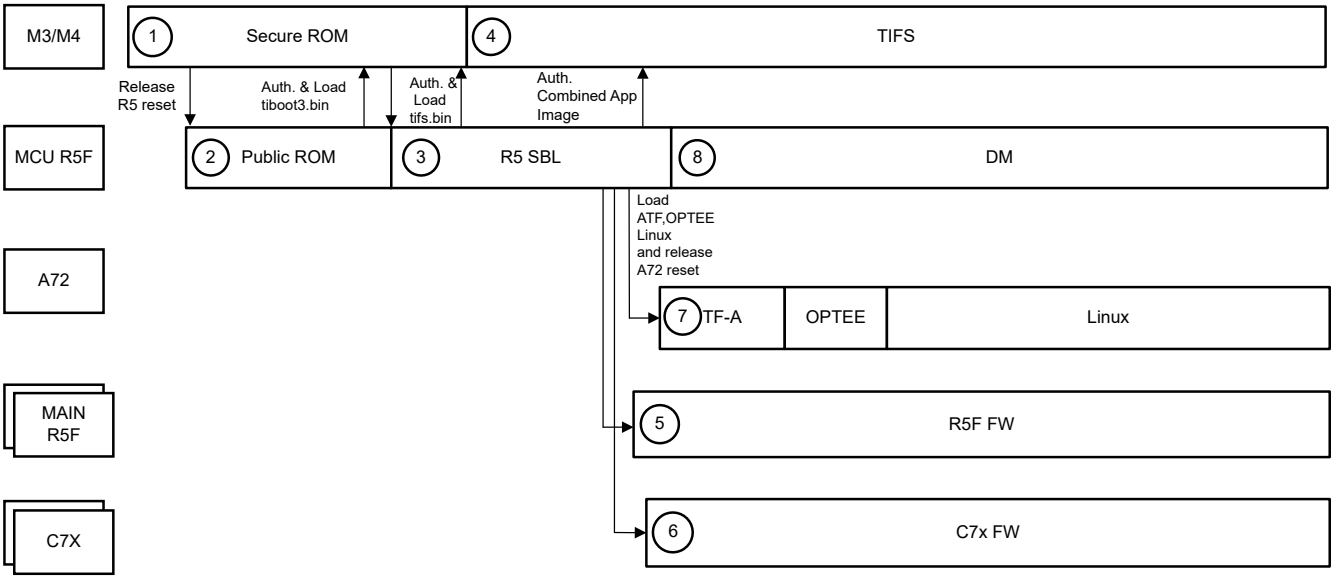

Figure 3-3. Optimized Boot Flow

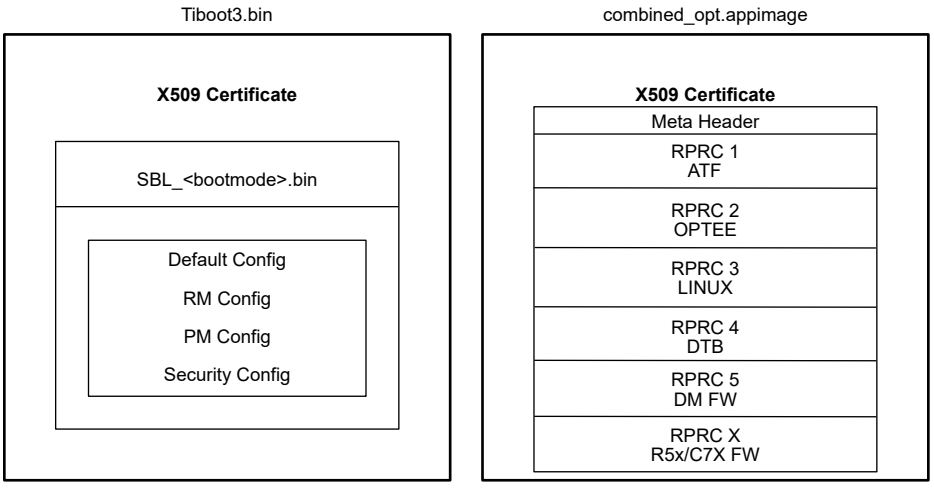

Figure 3-4. Image Format (Optimized Boot Flow)

3.3 Boot APP (Tertiary Bootloader)

Boot APP is a tertiary bootloader that provides additional flexibility for complex boot scenarios requiring staged initialization or runtime boot path decisions. The Boot APP runs on MCU R5F after SBL completes and can manage parallel loading tasks.

1. After Power on Secure ROM runs on M3 and M4 core
2. Release reset of R5, Public ROM starts on MCU R5F
3. Public Rom reads the tiboot3.bin from boot media and sends this to secure ROM for authentication and after authentication loads R5 SBL to MCU R5F.
4. R5 SBL reads tifs.bin from boot media, authenticates and then load on M3 and M4 core using secure ROM service.
5. SBL authenticates Boot app using TIFS service and transfers control to Boot APP on MCU R5.
6. Boot APP executes two parallel tasks - Task 1 loads the Device Manager (DM), while Task 2 loads the application firmware for remote cores. The boot app authenticates late application using TIFS service and loads the remote core firmware on Main R5x.
7. Boot app loads remote core firmware on C7x.
8. Boot app authenticates app images using TIFS service and load ATF, OPTEE and Linux to the respective location and release the reset of A72.

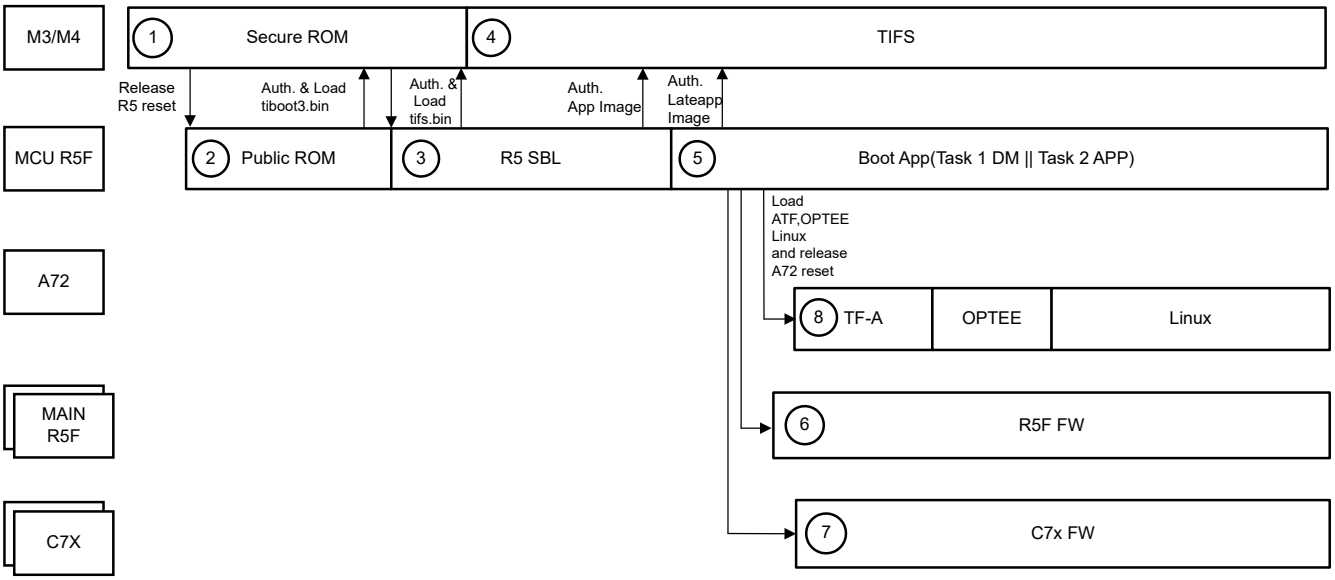

Figure 3-5. Boot APP (Tertiary bootloader) Flow

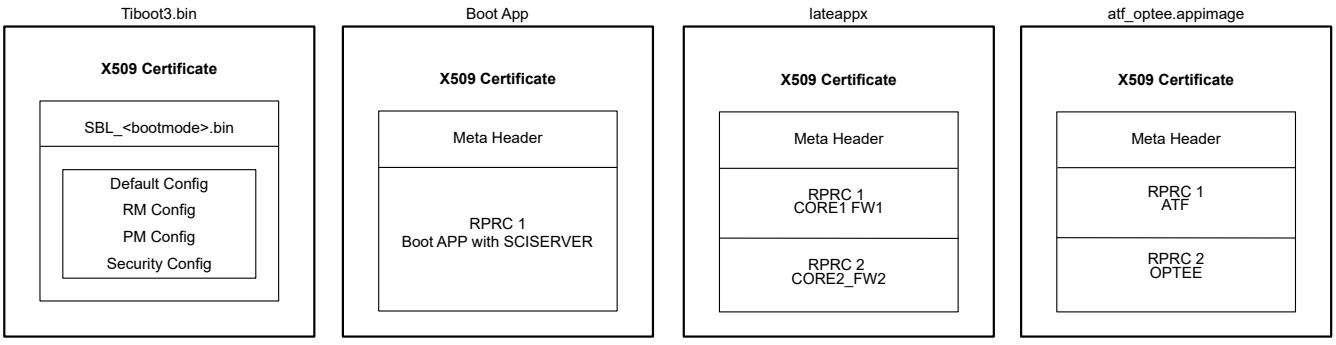

Figure 3-6. Image Format (Boot APP)

4 Summary

This application note describes multiple boot flow options available on TDA4 and DRA8 devices using both SPL (Secondary Program Loader) and SBL (Secondary Boot Loader) bootloaders.

Each boot flow supports both legacy and combined boot modes, with combined mode enabling parallel loading of bootloader and system firmware for optimized ROM boot time. All flows support authentication on High Secure (HS) devices and can load firmware on multiple cores including MCU R5F, Main R5F, C7x, and A72.

These are a few of the boot options validated with the SDK. Customers can design with boot flow based on specific requirements and use cases.

5 References

1. Texas Instruments, *J721S2 Linux Normal Boot Flow*, webpage.
2. Texas Instruments, *SBL Overview*, webpage.
3. Texas Instruments, *RTOS Combined app image flow*, webpage.
4. Texas Instruments, *RTOS BOOT APP*, webpage.
5. Texas Instruments, *System Firmware Authentication and Decryption Requests — TISCI User Guide*, webpage.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you fully indemnify TI and its representatives against any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale, TI’s General Quality Guidelines, or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

TI objects to and rejects any additional or different terms you may propose.

Last updated 10/2025