参考資料

Application Note

TDA4 デバイスのブート フロー オプション

TEXAS INSTRUMENTS

概要

TDA4 デバイスと DRA8 デバイスは、複数のブート フローとさまざまな組み合わせに対応しています。このアプリケーション ノートには、TDA4 デバイスと DRA8 デバイスで利用可能なすべてのブート フロー オプションが記載されています。お客様は使用事例に基づいて、最適なブート フロー オプションを選択できます。

目次

商標

1 概要

このアプリケーション ノートには、TDA4 デバイスと DRA8 デバイスで利用できるすべてのブート フロー オプションの詳細が記載されています。ほかにもさまざまな組み合わせが可能です。この目的は、一般的に使用されるブート フローとそれに対応するブート イメージのいくつかを示すことです。

TDA4x プロセッサと DRA82x プロセッサ向けの RTOS/Linux/QNX ソフトウェア開発キット (SDK) は、複数のブート フローをサポートしています。これらのブート フローは、お客様やパートナーが量産ソフトウェアの開発過程の一部としてカスタマイズされることを意図しています。

本書では主に、Linux と RTOS の SDK のブート フロー オプションを取り上げています。

プロセッサ SDK (RTOS/Linux) には、次の 2 つのブート ローダがあります:

- SBL - セカンダリ ブート ローダ (RTOS ブートローダー)
- SPL - セカンダリ プログラム ローダ (SPL) (Linux ブート ローダ)

以下のブート フローは、高セキュア (HS) デバイス向けです。汎用 (GP) デバイスの場合、カスタマー キーがないため、認証をバイパスした場合も同じブート フローが適用されます。

1.1 ROM ロード ブートローダー

TDA4VE、TDA4AL、TDA4VL、AM68、TDA4VH-Q1、TDA4AH-Q1、TDA4VP-Q1、TDA4AP-Q1 などのデバイスの中には、ROM によって 2 つの方法でブートローダーをロードできます。

1. レガシー:このフローでは、ブート バイナリには SPL または SBL のみが存在します。ROM により SBL または SPL がロードされると、ROM によりシステム ファームウェアがロードされます。
2. 複合ブート フロー:このフローでは、ブート バイナリ blob に、1 つの X509 証明書があるブート イメージに埋め込まれたセカンダリ ブートローダー (SBL) とシステム ファームウェア (SYS-FW) の両方が存在します。この方法は次の状況の場合に便利です。
   a. ROM により、依存することなく、ブートローダーと SYS-FW の両方が同時にロードされて実行されるようにすることができます。
   b. 異なる x509 証明書の解析と認証を最小化することで、ROM ブート時間を最適化します。

詳細については、『J784S4 J742S2 テクニカル リファレンス マニュアル』を参照してください。

2 セカンダリ プログラム ローダ

Linux ブートローダーは、セカンダリ プログラム ローダ (SPL) と U-Boot を使用して各種 CPU をブートします。SPL ブート フローを使用して Linux にブートする方法は 2 つあります。

- 通常ブート フロー
- Falcon ブート フロー

2.1 通常ブート フロー

1. 電源オンの後、セキュア ROM が M3/M4 コアで実行されます。
2. R5 のリセットを解除します。マイコン R5F のパブリック ROM が開始されます。
3. パブリック ROM により、ブート メディアから tiboot3.bin が読み取られ、認証用のセキュア ROM に送信されます。認証後、セキュア ROM により R5 SPL がマイコン R5F にロードされ、TIFS (TI Foundational Security ファームウェア) が M3/M4 コアにロードされます。
4. R5 SPL により、ブート メディアから tispl.bin が読み取られ、TIFS サービスを使用して認証が行われ、ATF (ARM Trusted Firmware)、OPTEE (Open Portable Trusted Execution Environment)、A72 spl がそれぞれの場所にロードされます。
5. A72 リセットを解除し、DM ファームウェアをロードします。
6. A72 SPL により uboot.img が認証されてロードされます。
7. U-Boot により、メイン R5F 上のリモート コア fw が認証されてロードされます。
8. U-Boot により、メイン C7x 上のリモート コア fw が認証されてロードされます。
9. U-Boot により Linux がロードされます。

注

U-Boot または Linux によるリモート コア ファームウェア (メイン R5F FW、C7x FW) のロード方法は 2 つあります。高セキュリティ デバイスでは、U-BOOT には署名付きのリモート コア ファームウェアが必要ですが、Linux を使用してロードする場合はファームウェアの署名は不要です。

OPTEE はオプションです。Linux からのランタイム セキュア コールを必要としないお客様は、OPTEE をバイパスして時間を節約できます。

ブート フローから optee を削除するには、ATF の構築中に次のコマンドを使用します。

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

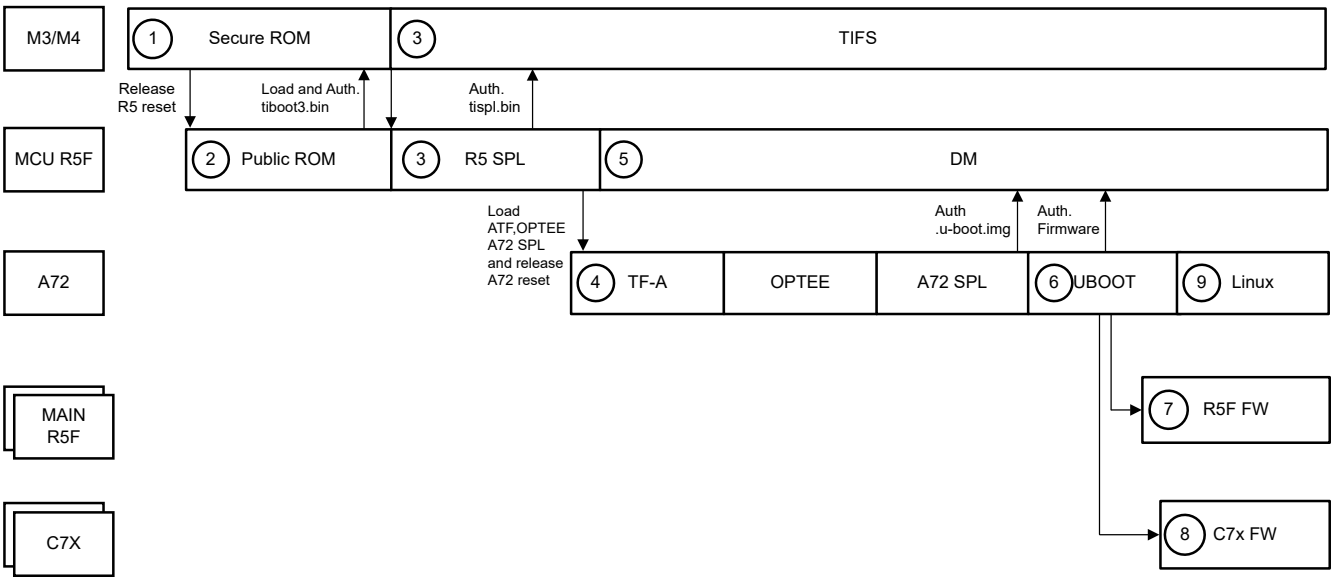

図 2-1. 通常ブート フロー

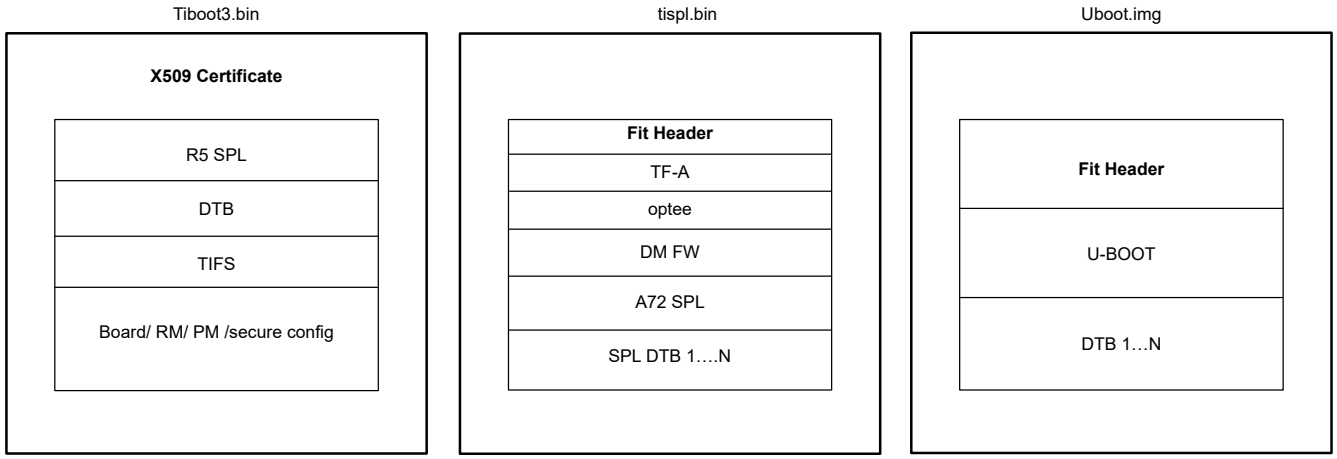

図 2-2. イメージ フォーマット (通常ブート フロー)

2.2 Falcon ブート フロー

Falcon モードでは、U-Boot ステージをバイパスして Linux カーネルに直接ブートすることで、起動時間を短縮できます。

1. 電源オンの後、セキュア ROM が M3/M4 コアで実行されます。
2. R5 のリセットを解除します。マイコン R5F のパブリック ROM が開始されます。
3. パブリック ROM により、ブート メディアから tiboot3.bin が読み取られ、認証用のセキュア ROM に送信されます。認証後、セキュア ROM により R5 SPL がマイコン R5F に、TIFS が M3 と M4 コアにロードされます。
4. R5 SPL により、ブート メディアから tispl.bin が読み取られ、TIFS サービスを使用して認証が行われ、ATF、OPTEE、Linux がそれぞれの場所にロードされます。
5. A72 でリセットを解除し、DM をそれ自体にロードします。
6. Linux により、メイン R5F 上のリモート コア fw がロードされます。
7. Linux により、メイン C7x 上のリモート コア fw がロードされます。

注

リモート コア ファームウェアをロードするには、DM (デバイス マネージャ) サービスが必要です。DM が RSF 上で起動して実行される Linux からファームウェアをロードするのは、デバイス マネージャー サービスがマイコン RSF ファームウェアのロードを必要とするためです。

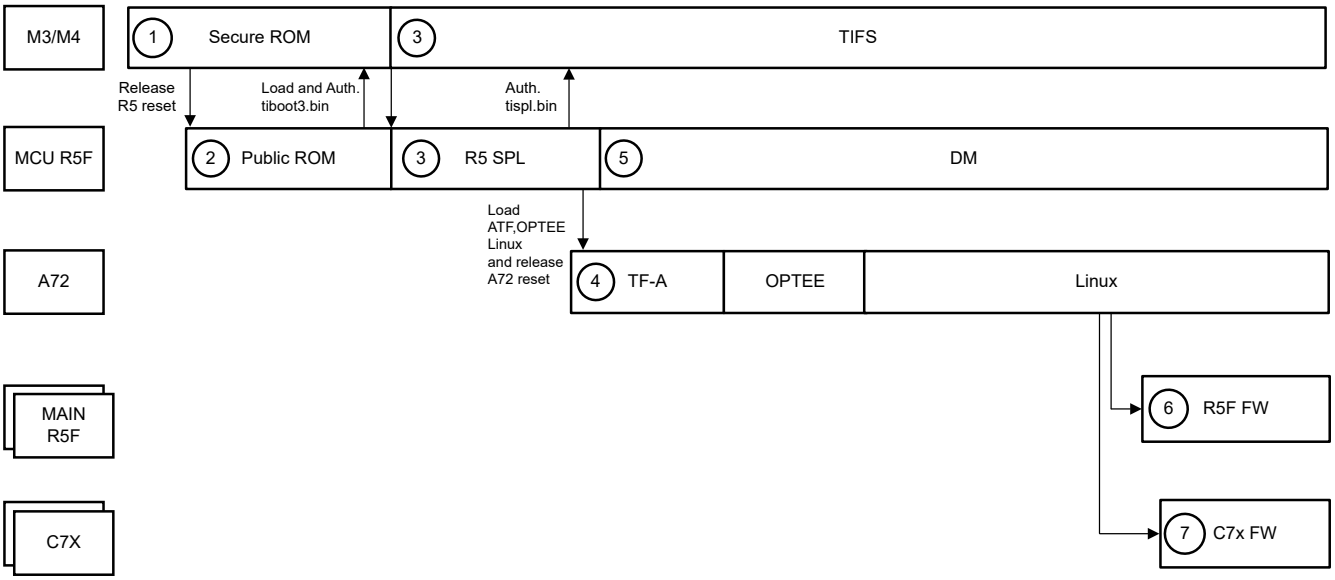

図 2-3. Falcon ブート フロー

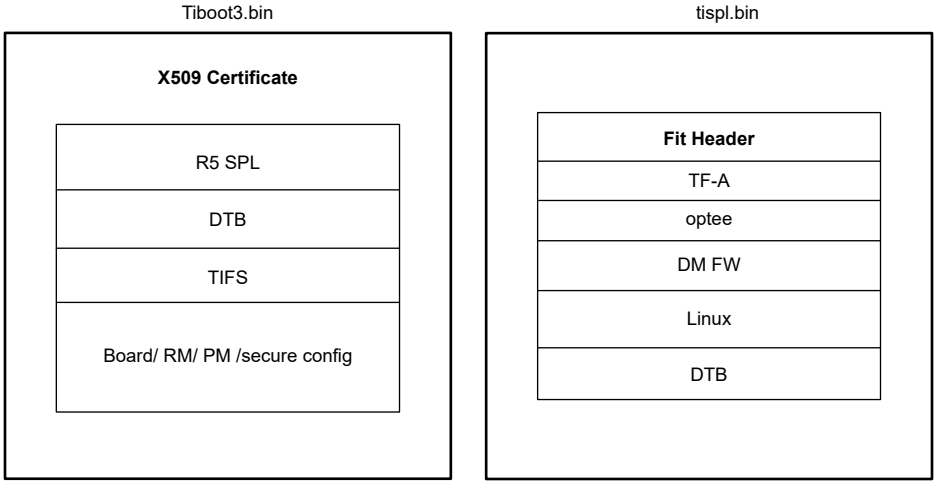

図 2-4. Falcon ブート フロー

詳細については、E2E™ 設計サポート フォーラムをご覧ください。

3 セカンダリ ブート ローダ

RTOS ブートローダーは、セカンダリ ブート ローダ (SBL) と呼ばれます。SBL を使用して HLOS をブートする方法は複数あります。

- 開発ブート フロー
- 最適化ブート フロー
- ブート アプリケーション (第 3 ブートローダー)

3.1 開発ブート フロー

1. パワーオン後、セキュア ROM が M3 と M4 コアで実行されます。
2. R5 のリセットを解除します。マイコン R5F でパブリック ROM が開始されます。
3. パブリック ROM により、ブート メディアから tiboot3.bin が読み取られ、認証用のセキュア ROM に送信され、R5 SBL がマイコン R5F にロードされます。
4. R5 SBL により、ブート メディアから tifs.bin が読み取られ、認証された後、セキュア ROM サービスを使用して M3/M4 コアにロードされます。
5. SBL により、TIFS サービスを使用して複合アプリ イメージが認証され、メイン R5F にリモート コア ファームウェアがロードされます。
6. SBL により C7x にリモート コア ファームウェアがロードされます。
7. SBL により、ATF、OPTEE、A72 SPL がそれぞれの場所にロードされます。
8. SBL により A72 のリセットが解除され、マイコン R5F 上で DM ファームウェアがロードされます。
9. U-Boot イメージがブート メディア内に個別に存在する場合は、A72 SPL によって U-Boot.img が認証されてロードされます。
10. U-Boot により Linux が認証されてロードされます。

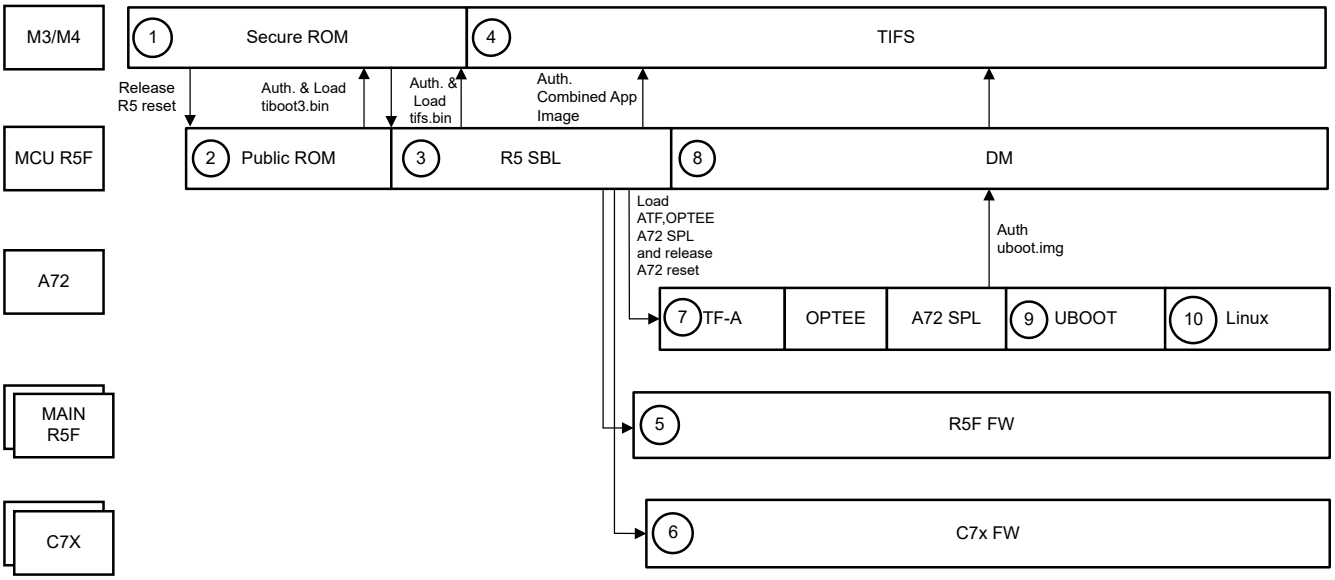

図 3-1. 開発ブート フロー

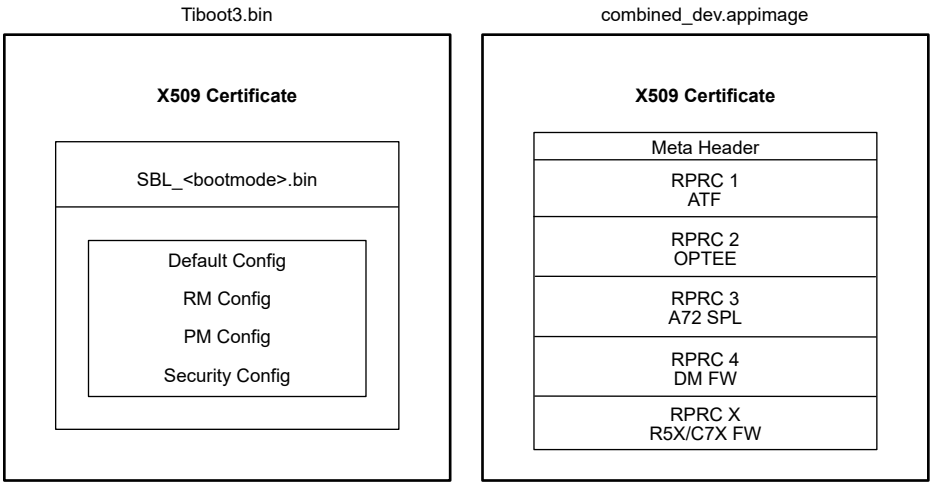

図 3-2. イメージ フォーマット (開発ブート フロー)

3.2 最適化ブート フロー

1. パワーオン後、セキュア ROM が M3 と M4 コアで実行されます。
2. R5 のリセットを解除します。マイコン R5F でパブリック ROM が開始されます。
3. パブリック ROM により、ブート メディアから tiboot3.bin が読み取られ、認証用のセキュア ROM に送信され、認証後、パブリック ROM により R5 SBL がマイコン R5F にロードされます。
4. R5 SBL により、ブート メディアから tifs.bin が読み取られ、認証された後、セキュア ROM サービスを使用して M3 と M4 コアにロードされます。
5. SBL により、TIFS サービスを使用して複合アプリ イメージが認証され、メイン R5F にリモート コア ファームウェアがロードされます。
6. SBL により C7x にリモート コア ファームウェアがロードされます。
7. SBL により、ATF、OPTEE、Linux がそれぞれの場所にロードされます。このフローでは、Linux を SBL から直接ロードすることで U-Boot ステージが不要になり、ブート時間が短縮されます。
8. SBL により A72 のリセットが解除されるので、DM をロードします。

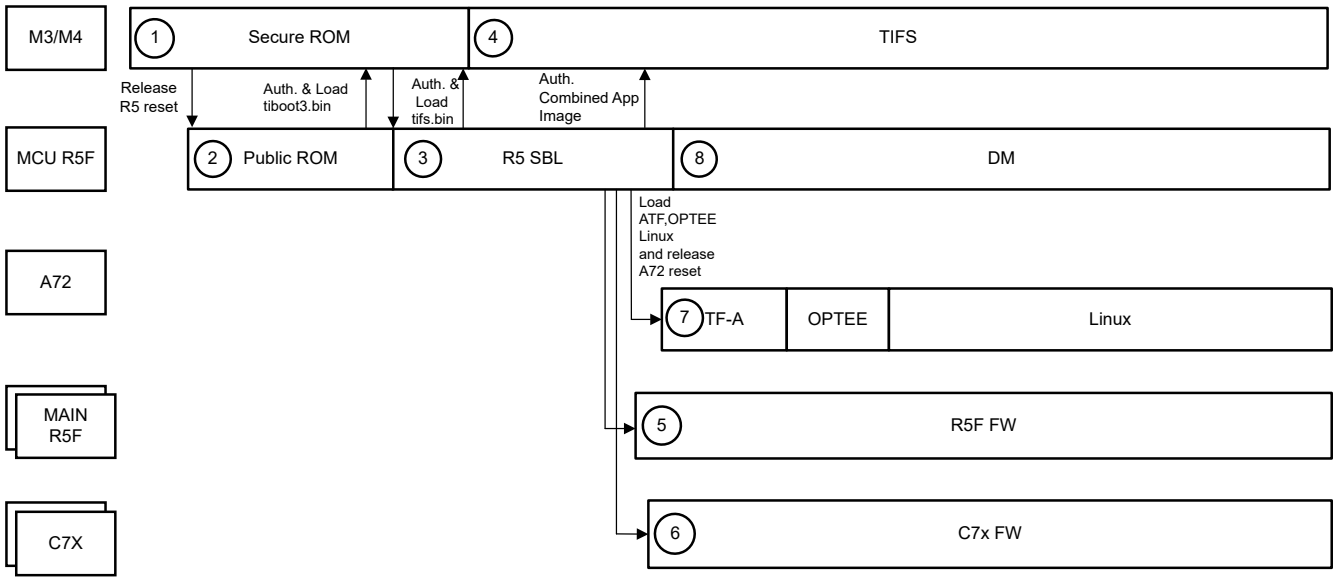

図 3-3. 最適化ブート フロー

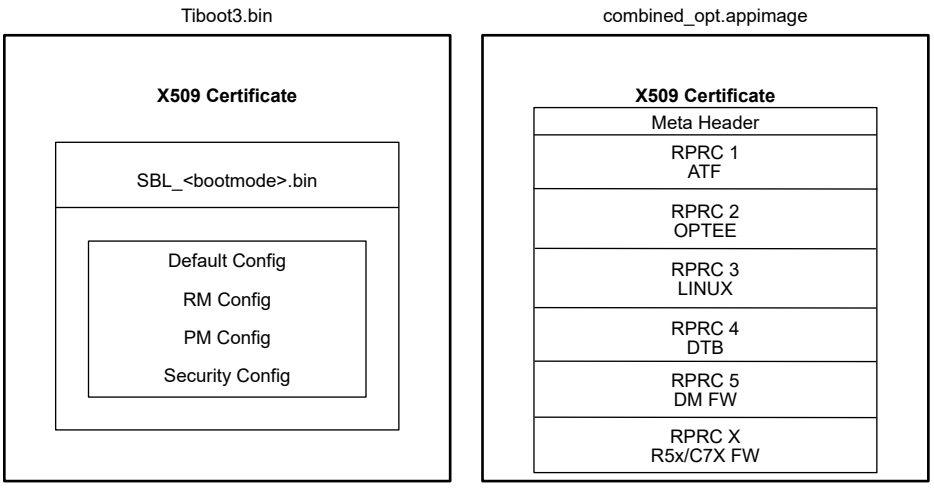

図 3-4. イメージ フォーマット (最適化ブート フロー)

3.3 ブート アプリケーション (第 3 ブートローダー)

ブート アプリケーションは、段階的な初期化またはランタイム ブート パス決定が必要な複雑なブート シナリオに対応する柔軟性を提供する 3 番目のブートローダーです。このブート アプリケーションは、SBL の完了後に マイコン R5F 上で動作し、並列ロード タスクを管理できます。

1. パワーオン後、セキュア ROM が M3 と M4 コアで実行されます。
2. R5 のリセットを解除します。マイコン R5F でパブリック ROM が開始されます。
3. パブリック ROM により、ブート メディアから tiboot3.bin が読み取られ、認証用のセキュア ROM に送信され、認証後に R5 SBL がマイコン R5F にロードされます。
4. R5 SBL により、ブート メディアから tifs.bin が読み取られ、認証された後、セキュア ROM サービスを使用して M3 と M4 コアにロードされます。
5. SBL により、TIFS サービスを使用してブート アプリケーションが認証され、マイコン R5 上のブート アプリケーションにコントロールが転送されます。
6. ブート アプリケーションによりは 2 つの並列タスクが実行されます。タスク 1 はデバイス マネージャ (DM) のロード、タスク 2 はリモート コア用のアプリケーション ファームウェアのロードです。ブート アプリケーションにより、TIFS サービスを使用し最新アプリケーションが認証され、メイン R5x にリモート コア ファームウェアがロードされます。
7. ブート アプリケーションにより C7x にリモート コア ファームウェアがロードされます。
8. ブート アプリにより、TIFS サービスを使用してアプリ イメージが認証され、ATF、OPTEE、Linux がそれぞれの場所にロードされたら、A72 のリセットを解除します。

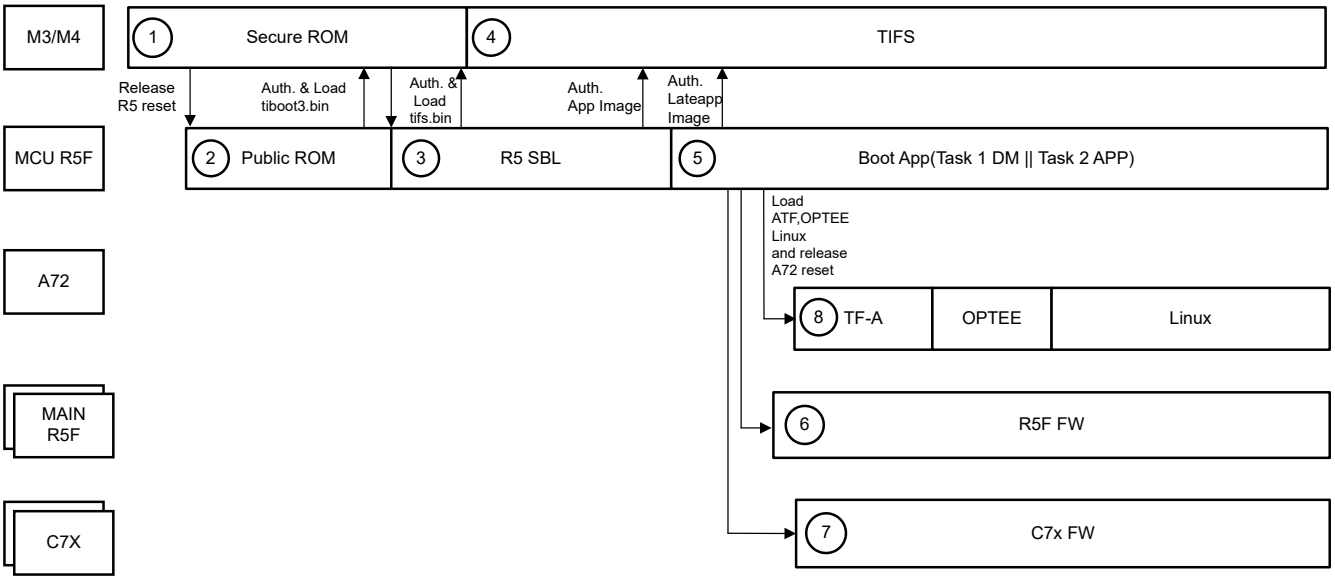

図 3-5. ブート アプリケーション (第 3 ブートローダー) のフロー

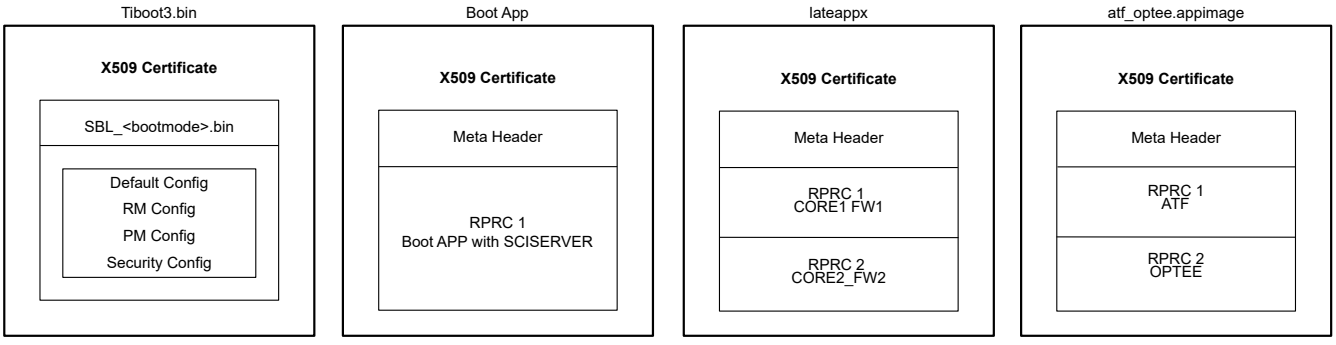

図 3-6. イメージ フォーマット (ブート アプリケーション)

4 まとめ

このアプリケーション ノートでは、SPL (セカンダリ プログラム ローダ) および SBL (セカンダリ ブート ローダ) ブートローダーの両方を使用する TDA4 デバイスと DRA8 デバイスで使用できる複数のブート フロー オプションについて説明します。

各ブート フローは、レガシー モードと複合ブート モードの両方に対応しており、複合モードにより、ブートローダーとシステム ファームウェアの同時ロードが可能になり、ROM ブート時間を最適化できます。すべてのフローはハイ セキュア (HS) デバイスでの認証に対応しており、マイコン R5F、メイン R5F、C7x、A72 を含む複数のコアにファームウェアをロードできます。

これらは、SDK を使用して検証されたブート オプションの一部です。お客様は、特定の要件と使用事例に基づき、ブート フローを使用して設計を行うことができます。

5 参考資料

1. テキサス インスツルメンツ、「J721S2 Linux 通常ブート フロー」、Web ページ。
2. テキサス インスツルメンツ、「SBL の概要」、Web ページ。
3. テキサス インスツルメンツ、「RTOS 複合アプリケーション イメージ フロー」、Web ページ。
4. テキサス インスツルメンツ、「RTOS ブートアプリ」、Web ページ。
5. テキサス インスツルメンツ、「システム ファームウェアの認証・復号化リクエスト — TISCI ユーザー ガイド」、Web ページ。

重要なお知らせと免責事項

テキサス・インスツルメンツは、技術データと信頼性データ (データシートを含みます)、設計リソース (リファレンス デザインを含みます)、アプリケーションや設計に関する各種アドバイス、Web ツール、安全性情報、その他のリソースを、欠陥が存在する可能性のある「現状のまま」提供しており、商品性および特定目的に対する適合性の黙示保証、第三者の知的財産権の非侵害保証を含むいかなる保証も、明示的または黙示的にかかわらず拒否します。

これらのリソースは、テキサス・インスツルメンツ製品を使用する設計の経験を積んだ開発者への提供を意図したものです。(1) お客様のアプリケーションに適した テキサス・インスツルメンツ製品の選定、(2) お客様のアプリケーションの設計、検証、試験、(3) お客様のアプリケーションに該当する各種規格や、その他のあらゆる安全性、セキュリティ、規制、または他の要件への確実な適合に関する責任を、お客様のみが単独で負うものとします。

上記の各種リソースは、予告なく変更される可能性があります。これらのリソースは、リソースで説明されている テキサス・インスツルメンツ製品を使用するアプリケーションの開発の目的でのみ、テキサス・インスツルメンツはその使用をお客様に許諾します。これらのリソースに関して、他の目的で複製することや掲載することは禁止されています。テキサス・インスツルメンツや第三者の知的財産権のライセンスが付与されている訳ではありません。お客様は、これらのリソースを自身で使用した結果発生するあらゆる申し立て、損害、費用、損失、責任について、テキサス・インスツルメンツおよびその代理人を完全に補償するものとし、テキサス・インスツルメンツは一切の責任を拒否します。

テキサス・インスツルメンツの製品は、テキサス・インスツルメンツの販売条件、または ti.com やかかる テキサス・インスツルメンツ製品の関連資料などのいずれかを通じて提供する適用可能な条項の下で提供されています。テキサス・インスツルメンツがこれらのリソースを提供することは、適用されるテキサス・インスツルメンツの保証または他の保証の放棄の拡大や変更を意味するものではありません。

お客様がいかなる追加条項または代替条項を提案した場合でも、テキサス・インスツルメンツはそれらに異議を唱え、拒否します。

郵送先住所:Texas Instruments, Post Office Box 655303, Dallas, Texas 75265

重要なお知らせと免責事項

TI は、技術データと信頼性データ (データシートを含みます)、設計リソース (リファレンス デザインを含みます)、アプリケーションや設計に関する各種アドバイス、Web ツール、安全性情報、その他のリソースを、欠陥が存在する可能性のある「現状のまま」提供しており、商品性および特定目的に対する適合性の黙示保証、第三者の知的財産権の非侵害保証を含むいかなる保証も、明示的または黙示的にかかわらず拒否します。

これらのリソースは、TI 製品を使用する設計の経験を積んだ開発者への提供を意図したものです。(1) お客様のアプリケーションに適した TI 製品の選定、(2) お客様のアプリケーションの設計、検証、試験、(3) お客様のアプリケーションに該当する各種規格や、その他のあらゆる安全性、セキュリティ、規制、または他の要件への確実な適合に関する責任を、お客様のみが単独で負うものとします。

上記の各種リソースは、予告なく変更される可能性があります。これらのリソースは、リソースで説明されている TI 製品を使用するアプリケーションの開発の目的でのみ、TI はその使用をお客様に許諾します。これらのリソースに関して、他の目的で複製することや掲載することは禁止されています。TI や第三者の知的財産権のライセンスが付与されている訳ではありません。お客様は、これらのリソースを自身で使用した結果発生するあらゆる申し立て、損害、費用、損失、責任について、TI およびその代理人を完全に補償するものとし、TI は一切の責任を拒否します。

TI の製品は、 TI の販売条件 、 TI の総合的な品質ガイドライン 、 ti.com または TI 製品などに関連して提供される他の適用条件に従い提供されます。TI がこれらのリソースを提供することは、適用される TI の保証または他の保証の放棄の拡大や変更を意味するものではありません。 TI がカスタム、またはカスタマー仕様として明示的に指定していない限り、TI の製品は標準的なカタログに掲載される汎用機器です。

お客様がいかなる追加条項または代替条項を提案する場合も、TI はそれらに異議を唱え、拒否します。

最終更新日：2025 年 10 月