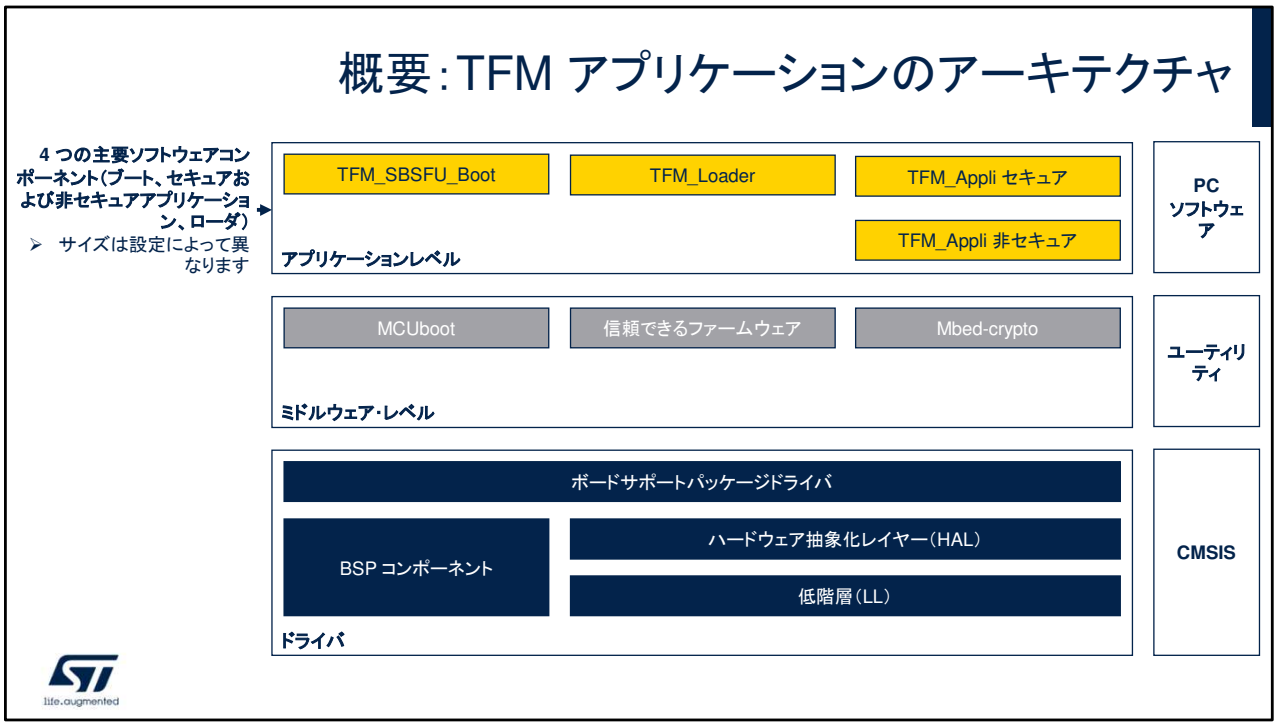
こちらのプレゼンテーションへようこそ。ここでは、TFM Flash メモリのフットプリントに影響するパラメータについて詳しく説明します。



この図は、TFM が依存するソフトウェアレイヤ、ミドルウェア用のユーティリティ、ドライバ用の CMSIS をまとめたものです。
STM32CubeU5 に用意されている TFM ベースのアプリケーションサンプルは、4 つの主要なソフトウェアコンポーネントで構成されており、これはユーザのニーズに応じて設定できます。

- TFM_SBSFU_Boot：セキュア・ブートおよびセキュアファームウェア更新アプリケーション
- TFM_Loader ：USART 上の Ymodem プロトコルに基づくアプリケーションローダ
- TFM_Appli_Secure：非セキュアなユーザアプリケーションにセキュアサービスを提供するセキュアアプリケーション（ランタイム）
- TFM_Appli_NonSecure：非セキュアなユーザアプリケーションです。

以降のスライドに、これらの各コンポーネントの最小構成および完全な構成でのフットプリントの見積もりを示します。

TFM Flash のフットプリント/寸法パラメータ

メモリ・フットプリントはいくつかのシステムパラメータによって決まります

- ハードウェア構成：内部 Flash のみまたは外部 Flash あり、STM32U5 ハードウェアアクセラレーション暗号化機能
- 開発モードまたは量産モード（ログ…）
- ファームウェアイメージ数：1 つのファームウェアイメージ（非セキュアアプリケーションとセキュアアプリケーションの組み合わせ）または 2 つのファームウェアイメージ
- ファームウェアスロット数：プライマリおよびセカンダリスロット（OTA FW 更新 UC を有効化）またはプライマリスロットのみ（アクティブイメージの上書き）
- SBSFU 暗号化方式の設定：RSA または ECC に基づいた非対称暗号化方式、ファームウェア暗号化のサポート
- スタンドアロン・ローカル・ローダの機能
- 非セキュアアプリケーションで必要となるセキュアサービスのタイプと数：
  - 初期証明サービス
  - セキュア・ストレージ・サービス
  - 内部信頼ストレージサービス
  - 暗号サービス
- IDE：STM32CubeIDE、Keil、IAR

life.augmented

3

このスライドは、TFM Flash のフットプリントに影響するパラメータを示しています。
フットプリントは、内部または外部 Flash のハードウェア設定（特にページサイズ）と、Flash 領域で可能な暗号化によって決まります。
イメージの更新に使用されるファームウェアイメージの数とファームウェアスロットの数は、フットプリントに影響します。
サイズには、SBSFU 暗号化方式の設定（RSA または ECC に基づく非対称）も影響します。
イメージローダが必要な場合、これも Flash の一部を消費します。
セキュアサービスのタイプと数は、明らかにメモリ・フットプリントに影響します。
コードのコンパクトさは、コンパイラによって提供される最適化のレベルにも依存します。

以降のスライドでは、次の設定に基づいて指標を示します。
- サイズのアライメントでは、8 KB の Flash メモリのセクタアライメント制約が考慮されます。
- IDE は「-Oz イメージサイズ」オプション付きの Keil® ツールチェーン MDK-ARM 5.31.0 です。

TFM_SBSFU_Boot メモリ・フットプリント

	最小設定	SBSFU の例	TFM_SBSFU の完全な例
設定	SBSFU モードのみ	**SBSFU モードのみ**	**TFM_SBSFU モード**
	TFM セキュアサービスなし	**TFM セキュアサービスなし**	**TFM セキュアサービス**
	量産モード	開発モード	開発モード
	ローカル・ローダとの互換性なし	ローカル・ローダと互換	ローカル・ローダと互換
	ファームウェアスロット x 1 のみ	**ファームウェアスロット x 1 のみ**	**ファームウェアスロット x 2**
	ファームウェアイメージ x 1	**ファームウェアイメージ x 1**	**ファームウェアイメージ x 2**
	上書きモード	上書きモード	上書きモード
	ハードウェアアクセラレーション暗号化	ハードウェアアクセラレーション暗号化	ハードウェアアクセラレーション暗号化
	RSA 2048 暗号化方式	RSA 2048 暗号化方式	RSA 2048 暗号化方式
	ファームウェアの暗号化なし	ファームウェアの暗号化	ファームウェアの暗号化
	耐タンパなし	内部および外部の耐タンパ	内部および外部の耐タンパ
IDE	Keil®(ツールチェーン MDK-ARM 5.31.0、オプション「-Oz イメージサイズ」付き)		
全体サイズ	48KB	72KB	80KB

life.augmented

4

この表は、TFM SBSFU ブートプログラムのサイズを示しています。

TFM_SBSFU_Boot アプリケーションは、Flash メモリの次のセクションで構成されています。
- BL2 NVCNT データ:アンチロールバック機能のファームウェアバージョン情報を格納するために使用される領域。
- SCRATCH 領域:イメージスワップ処理中にイメージデータを一時的に格納するために TFM_SBSFU_Boot によって使用されます(上書きモードでは使用されません)。
- インテグレータの個人データ:SBSFU アプリケーションキーと、TFM セキュアアプリケーションによって使用されるキーと情報を格納するために使用される領域。
- SBSFU コード:「セキュア・ブート」および「セキュアファームウェア更新」機能を管理するコード。
- HDP 有効化コード:アプリケーションを起動する前にすべての SBSFU コードと機密情報を非表示にするコード。

各セクションのフットプリントの詳細については、UM2851 ユーザーズマニュアル「Getting started with STM32CubeU5 TFM application」を参照してください。

この表では、次の 3 つの例を示します。
- 最小設定の例
- STM32CubeU5 MCU パッケージで提供される SBSFU_Boot サンプル
- STM32CubeU5 MCU パッケージで提供される TFM_SBSFU_Boot サンプル

SBSFU のサンプルと TFM のサンプルの違いを太字で示しています。

TFM_Appli_Secure メモリ・フットプリント

設定	空のセキュア アプリケーションテンプレート	制限付き TFM 暗号化 サービスのみ	完全な TFM セキュアサービス
セキュリティインフラ	1 レベルの隔離に対応する非常に基本的なインフラストラクチャ	2 レベルの隔離に対応する TFM セキュリティインフラストラクチャ	2 レベルの隔離に対応する TFM セキュリティインフラストラクチャ
TFM 初期照明サービス	なし	いいえ	はい
TFM セキュア・ストレージ・サービス	なし	いいえ	あり（NV データは 16 KB）
TFM 内部信頼ストレージ サービス	なし	いいえ	あり（NV データは 16 KB）
TFM 暗号化サービス	なし	SHA256	オープンソース TFM リファレンス実装の場合にデフォルトで有効化されるすべての暗号化アルゴリズムで、AES すべてのモード、RSA、ECC、HASH です
		AES GCM	
		ECDSA P256	
暗号の実装	該当なし	使用されるハードウェア暗号化	使用されるハードウェア暗号化
IDE	Keil®（ツールチェーン MDK-ARM 5.31.0、オプション「-Oz イメージサイズ」付き）		
全体サイズ	8 KB	56KB	136KB

life.augmented

5

この表は、TFM セキュアアプリケーションのサイズを示しています。

セキュアアプリケーションは、非セキュアアプリケーションにより実行時に使用できるセキュアサービスを提供します。
- 異なるドメインの隔離とセキュア API メカニズムを備えたセキュリティアーキテクチャの設定
- 非セキュアなユーザアプリケーションで必要となるセキュアなサービスを提供

セキュアアプリケーションのバイナリはファームウェアイメージにカプセル化され、このファームウェアイメージには、「セキュア・ブート」または「セキュアファームウェア更新」機能のコンテキストで使用されるメタデータが含まれています。

セキュアアプリケーションイメージのサイズは、設定の影響を受けます。

この表は、3 つの例を示しています。
- 空のセキュアアプリケーションテンプレート
- 制限付き TFM 暗号化サービスのみ
- 完全な TFM セキュアサービス

TFM_Appli_NonSecure のメモリ・フットプリント

設定	SBSFU の例	TFM の完全な例
ファームウェアスロット数	1	2
セキュアアプリケーション	1 レベルの隔離 基本トグル GPIO	PSA L2 セキュリティインフラストラクチャ 完全な TFM セキュアサービス（オープンソース TFM リファレンス実装ではすべての暗号化アルゴリズムがデフォルトで有効化されています）
ローカル・ローダ	あり（UART/Ymodem プロトコル）	
暗号の実装	ハードウェアアクセラレーション	
IDE	Keil®（ツールチェーン MDK-ARM 5.31.0、オプション「-Oz イメージサイズ」付き）	
アプリケーションで使用可能な最大サイズ	最大 1.9M バイト	最大 750 KB

life.augmented

6

この表は、TFM 非セキュアアプリケーションのサイズを示しています。

内部 Flash メモリが使用される場合、非セキュアアプリケーション領域として使用可能なサイズは設定によって異なります。

この表に、STM32CubeU5 マイクロコントローラパッケージで提供されている 2 つの例を示します。

- SBSFU の例
- TFM の完全な例

TFM_Loader のメモリ·フットプリント

設定	1 つの画像スロット	2 つの画像スロット
ファームウェアスロット数	1（プライマリスロットのみ）	2
IDE	Keil®（ツールチェーン MDK-ARM 5.31.0、オプション「-Oz イメージサイズ」付き）	
インタフェース	UART インタフェース	UART インタフェース
ダウンロードプロトコル	Ymodem プロトコル	Ymodem プロトコル
全体サイズ	セキュア：8 KB 非セキュア：16 KB	セキュア：0 KB 非セキュア：16 KB

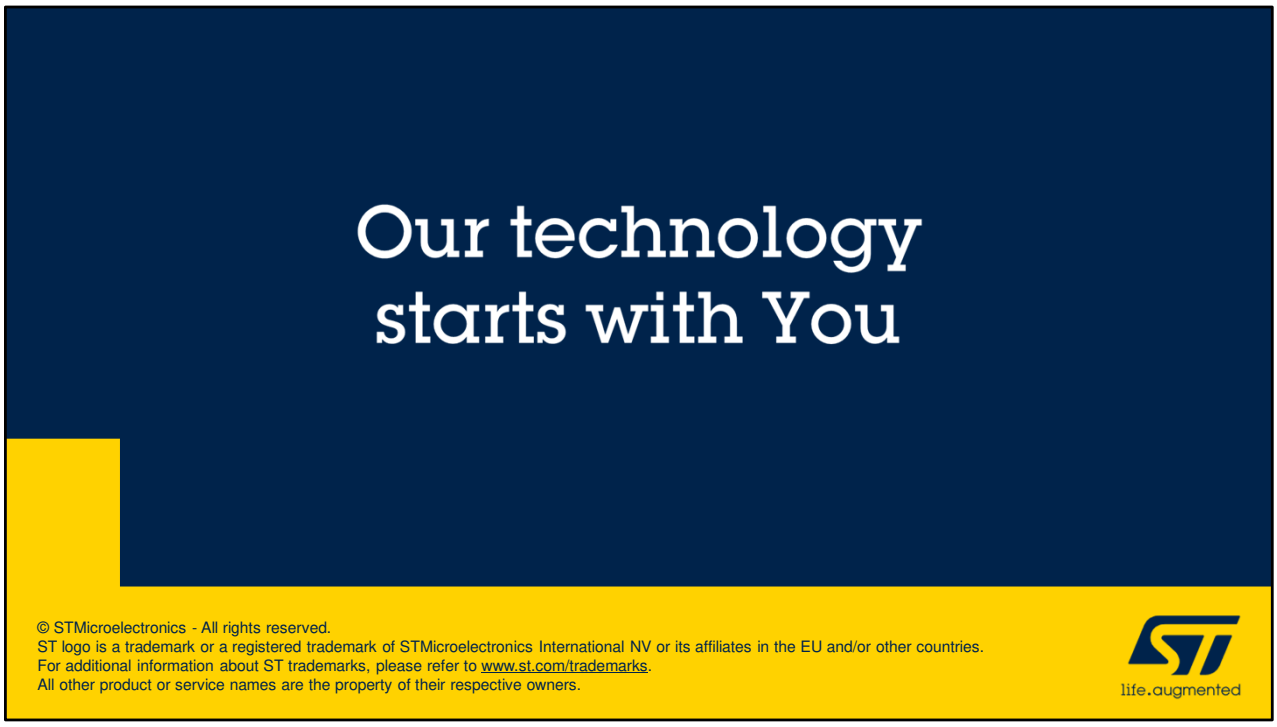
life.augmented

7

この表は、TFM ローダのサイズを示しています。

TFM_Loader アプリケーションでは、Ymodem プロトコルに基づく UART インタフェースを使用して（一例として）、新しいファームウェアバージョンをダウンロードできます。
TFM_Loader アプリケーションはオプションです。必要でない場合は、完全に取り外すことができます。
インテグレータが、製品仕様に従って設定したり、他のハードウェアインタフェースや他のプロトコルをサポートするようにカスタマイズしたりできます。

TFM_Loader アプリケーションのサイズは、設定の影響を受ける可能性があります。
この表は、2 つの例を示しています。
- 1 つの画像スロット
- 2 つの画像スロット



このプレゼンテーションにご参加いただき、ありがとうございました。
TFM の動作を詳しく説明したプレゼンテーションを参照してください。

- STM32U5 の TFM 製品
- TFM ポインタ