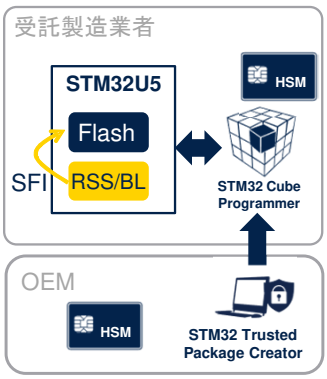
こちらのプレゼンテーションへようこそ。ここでは、ルートセキュリティサービスで提供されるセキュアファームウェアインストール（SFI）機能について説明します。

概要



- **RSS** STM32 イミュータブル（変更不可能）ブートローダ（BL）のセキュア部分であり、TrustZone が有効化されているときに使用可能
- RSS はセキュアファームウェアインストール（**SFI**）ソリューションのためのサービスを提供

適用の利点

- イミュータブル・ルートセキュリティサービス
- セキュアファームウェアインストール（SFI）が利用可能

life.augmented

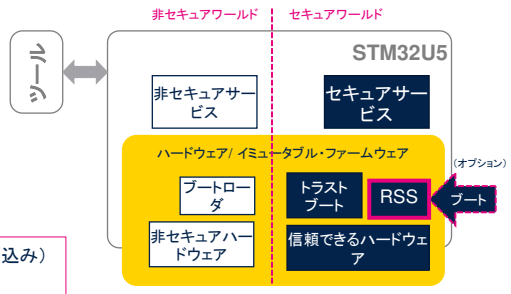
2

ルートセキュリティサービス（RSS）は、STM32U5 イミュータブル・ブートローダのセキュア部分です。デバイスで TrustZone が有効化されている場合にのみ使用できます。
RSS は、イミュータブル・ルートセキュリティサービスを提供し、たとえば、信頼できない環境で STM32 セキュアファームウェアインストール（SFI）ソリューションを実行するために使用されます。
TrustZone と保護されたメモリの詳細については、 オンライントレーニングモジュール「STM32U5 セキュリティの概要」を参照してください。
ハードウェアセキュリティモジュール（HSM）は、以下に対応します。

- OEM AES 秘密鍵の安全な格納
- STM32 デバイスの認証に使用される STM32 デバイス証明書の確認
- 暗号化されたファームウェアを STM32 デバイスにセキュアにインストールするためのライセンスを生成し、セキュアブートローダに提供
- STM32 デバイスの生産数をカウント

RSS の主な機能

- **RSS** はセキュアなイミュータブル・ファームウェアです
  - STM32 **SFI** の実行に必要
  - 固有のエントリポイントとして使用可能
  - RSS には、一連のセキュリティサービスを装備
    - ブート または ランタイム



RSS ブート時サービス

- 非セキュアブートローダのリソース割り当て（SRAM、Flash、ペリフェラル、IO、割込み）
- ブートローダによって使用される Flash セキュアオプションバイトを取得/設定
- STM32U5 デバイス証明書と証明書サイズを取得

RSS ランタイムセキュアサービス

- Flash HDP 領域で実行されているセキュアコードを、保護領域外の指定のアドレスに安全にジャンプ。

life.augmented

3

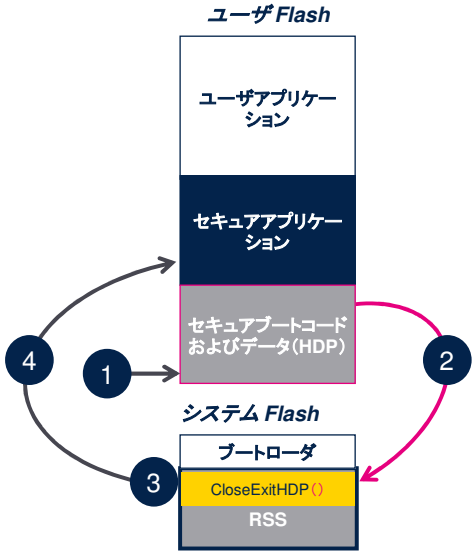
TrustZone が有効化されている場合、RSS はセキュアでイミュータブル・ファームウェアで、STM32U5 の生産時に ST によってデバイス専用の一意のキーペアとともに提供されます。
リセット後、このイミュータブル・ファームウェアは固有のエントリポイントとして使用され、ブート時、場合によってはランタイムでも使用可能な一連のセキュリティサービスを提供します。
RSS には、STM32 セキュアファームウェアインストール（SFI）ソリューションの実行に必要な機能が含まれています。
RSS のブート時サービスには以下が含まれます。

- 非セキュアブートローダのリソース割り当て（SRAM、Flash、ペリフェラル、IO、割込み）
- ブートローダによって使用される Flash セキュアオプションバイトを取得または設定する関数
- STM32U5 デバイス証明書とそのサイズを取得する関数で、ブートローダでも使用されます。

RSS は、セキュア実行および非セキュア実行ファームウェアの両方にもサービスを提供します。
これらのセキュアサービスの 1 つにより、Flash HDP 領域で実行されているセキュアファームウェアは、保護領域外の指定のアドレスに安全にジャンプできます。
次の 3 枚のスライドで、これらのすべてのサービスについて詳しく説明します。

RSS & HDP 領域の終了

- HDP 領域は、HDPEN オプションビットをセットするセキュアコードによって有効化。
- その外にジャンプする一般的なシーケンスは以下
  1. デバイスがブートし、HDP 領域の機密コードの実行
  2. ブートコードにより RSS lib の HDP 終了関数がコール
  3. RSS は、次のリセットまでセキュア HDP 領域を非表示にしてから、(セキュア)アプリケーションコードに分岐
  4. セキュアファームウェアは HDP 領域にアクセス不可
- HDP クローズ & 終了関数の詳細については、**RM0456** を参照



life.augmented

4

セキュア非表示保護（HDP）は、TrustZone セキュアドメイン内の追加の保護メカニズムです。
HDP に組み込まれたコードが最初に実行され、その実行の最後にセキュアユーザアプリケーションにジャンプします。
HDP によって保護されたコードとデータには、次のシステムリセットまでアクセスできなくなります。
HDP 領域は、HDPEN オプションビットをセットするセキュアコードによって有効化されます。
ここで、HDP 領域の外にジャンプするのに RSS がどう役立つかを説明します。
HDP に組み込まれたブートコードが、リセット後に実行されます。図の手順 1 を確認してください。
実行の最後に、RSSLIB_sec_CloseExitHDP をコールします。これが手順 2 です。
次に、この RSSLIB_sec_CloseExitHDP 関数により、Flash HDP セキュアメモリ領域がクローズされます（手順 3）。そして、入力パラメータとしてアドレスが渡されたベクタテーブルで示されるリセットハンドラにジャンプします。
これが手順 4 です。
入力パラメータ値の不良などによる障害が発生した場合、この関数により STM32U5 がリセットされます。

セキュアファームウェアインストール（SFI）

- セキュアファームウェアインストール（SFI）:
  - 信頼できない実稼働環境（OEM 契約製造業者など）での OEM ファームウェアのセキュアなカウント付きインストールが可能
  - SFI は、セキュア RSS と非セキュアでイミュータブル・ブートローダを使用して実装
  - SFI によって保護された OEM ファームウェアは、内蔵Flashに格納したり、外部Flashに暗号化して保存可能
  - ファームウェアがインストールされた STM32 デバイスの数は、HSM によってカウント可能
- 外部Flashメモリが SFI の対象である場合、OEM ファームウェアは外部ファームウェアとデータ AES キーによって暗号化
  - OTFDEC ペリフェラルを使用して暗号の高速化が可能
  - SFI は、OTFDEC ペリフェラル専用の AES キーを使用して、OEM 外部ファームウェアを再暗号化可能
  - キーは（ツールによって）グローバルに管理もしくは、デバイス固有のもの（たとえば、真の RNG ペリフェラルを使用してローカルに計算する）でも可能

life.augmented

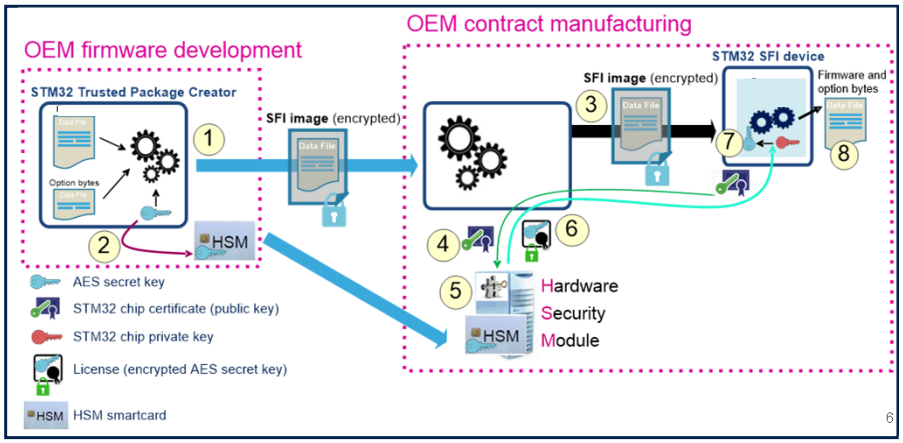
5

セキュアファームウェアインストール（SFI）は、STM32U5 シリーズマイクロコントローラ用のグローバルソリューションで、OEM 契約製造業者などの信頼できない生産環境で OEM ファームウェアのセキュアなカウント付きインストールを行うことができます
SFI は、セキュア RSS と非セキュアでイミュータブル・ブートローダを使用して実装されます。
SFI によって保護された OEM ファームウェアは、デバイスの内蔵 Flash に格納したり、OCTOSPI 経由で接続された外部 Flash 内で暗号化したりできます。
複合化されたファームウェア（およびオプションバイト）により内蔵 Flash をプログラムする前に、OEM 内部ファームウェア（およびオプションバイト）の信頼性、完全性、機密性がチェックされます。
STM32U5 SFI ソリューションには STM32 Trusted Package Creator ツールが用意されていて、AES 秘密鍵を使用して OEM ファームウェアとオプションバイト全体が暗号化されます。
これは、OEM ファームウェアの開発中に行われます。
この AES 秘密鍵の機密性は、RSS によってのみ読み出しが可能な秘密鍵を使用し、STM32 デバイス専用の固有のキーペアによって保証されます。
詳細については、AN5391 の「STM32L5/U5 SFI ツール、ブートローダ、および RSS インタフェース」 を参照してください。
OCTOSPI を介して接続された外部 Flash メモリが SFI の対象となる場合、OEM ファームウェアコードを外部ファームウェアとデータ AES キーで暗号化する必要があります。
このキーは次のいずれかとすることができます。
- すべてのデバイスに共通（この場合、ツールで暗号化を実行できます）
- デバイスごとに一意（この場合、ファームウェアはデバイス内で暗号化されます）

SPI Flash メモリに格納された暗号化ファームウェアのオンザフライ復号は、STM32U5 デバイスでのみ使用できることに注意してください。
詳細については、このモジュールの最後を参照してください。セキュアファームウェアインストール（SFI）ソリューションについてはアプリケーションノート AN4992 を参照してください。

SFI から内部 Flash へ

1. SFI イメージ(暗号化)は *STM32 Trusted Package Creator* から入手可能
2. OEM が AES 秘密鍵を使用して HSM をプログラム
3. SFI プロセスの開始
4. デバイス証明書の取得
5. HSM での STM32 デバイス認証
6. HSM から STM32 にライセンスを提供
7. RSS が、ライセンスで暗号化された OEM AES 秘密鍵を取得
8. 暗号化済ファームウェアとオプション・バイトが復号化され、プログラムされる

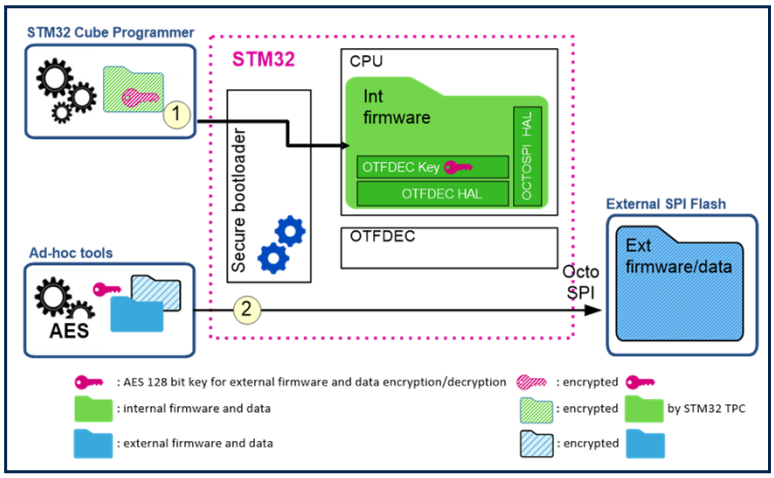


life.augmented

内部 Flash メモリにセキュアファームウェアをインストールする手順は、次のとおりです（図の番号に対応）。
（1）（暗号化された）SFI イメージは STM32 Trusted Package Creator から入手できます。
（2）OEM が AES 秘密鍵を使用して HSM をプログラムします。
（3）SFI プロセスの開始。
（4）デバイス証明書の取得。
（5）HSM での STM32 デバイス認証。
（6）HSM から STM32 デバイスにライセンスを提供します。
（7）RSS が、ライセンスで暗号化された OEM AES 秘密鍵を取得します。
（8）暗号化済ファームウェアおよびオプション・バイトが転送され、復号化されてからプログラムされます。

SFI から内部および外部 Flash へ（1）

1. SFI を使用した内部 Flash メモリのセキュアプログラミング
2. 外部ファームウェアおよびデータの暗号化とプログラミング
   - ✓ 詳細については、次のスライドを参照。



注：OTFDEC ペリフェラルは、STM32U5 デバイスでのみ使用可能です

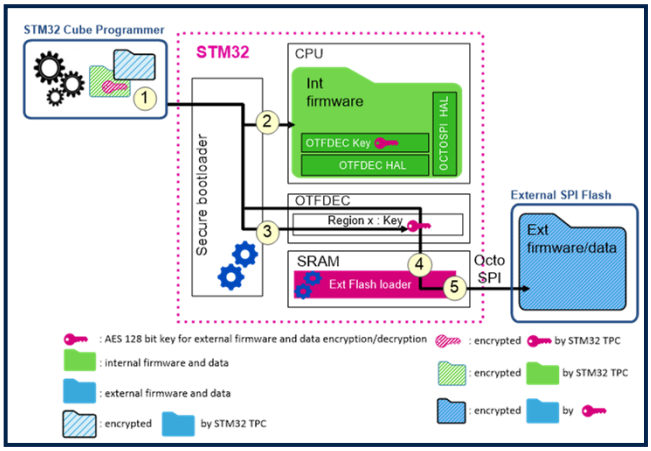
life.augmented

7

外部 Flash メモリのオンザフライ復号化（OTFDEC）を担当する暗号化エンジンは、AES 標準暗号化アルゴリズムに対応しています。
この標準アルゴリズムにより、OEM は外部 Flash メモリにプログラムする前に、STM32 セキュアブートローダを使用せずに、ホスト上の外部ファームウェアとデータを暗号化できます。
このスライドは、内部 Flash メモリのセキュアプログラミング（1）と、外部ファームウェアとデータの暗号化およびプログラミング（2）が、2 つの個別のフローで実行できることを示しています。
最初のフローではセキュアブートローダを使用し、2 番目のフローでは OEM ホストを使用して外部 Flash メモリをプログラムします。
その後、各セキュア・ブート中に、セキュア内部ファームウェアにより、最初に AES ファームウェアとデータキーが書込み専用 OTFDEC キーレジスタにコピーされ、次に、これらのキーに関連付けられた OTFDEC 領域が有効化されます。
OCTOSPI ドライバが初期化されると、この時点で、CPU ではデータの読出しと外部 Flash メモリからのコードのフェッチをシームレスに行うことができます。

SFI から内部および外部 Flash へ（2）

1. 以下を使用して、SFI イメージを作成し
   - 内部ファームウェアとデータ（外部 Flash メモリドライバを含む）
   - 外部ファームウェアとデータ *AES キー*
   - 外部なファームウェアとデータ
2. 内部 Flash メモリのプログラミング
3. OTFDEC ペリフェラルでの外部ファームウェアとデータ *AES キー*のプログラミング
   - またはそのようなキーを、フラッシュ・ツールでグローバルな管理以外に、デバイス内でローカルに管理可能
4. 外部 Flash メモリのチャンクの暗号化
   - イメージが AES キーですでに暗号化されている場合は不要
5. ユーザのファームウェアによる外部 Flash メモリのプログラミング



TPC : Trusted Package Creator

注：OTFDEC ペリフェラルは、STM32U5 デバイスでのみ使用可能です

このスライドは、STM32 セキュアブートローダにより、内部ファームウェアのインストールと、グローバル外部 Flash メモリの AES キーと外部 Flash メモリローダを利用した外部ファームウェアのインストールの両方を処理するシーケンスを表しています。以下の番号は図の番号に対応しています。
（1） a) 内部ファームウェアとデータ（外部 Flash メモリドライバを含む）、b) 外部ファームウェアとデータ AES キー、c) 外部ファームウェアとデータで SFI イメージを作成します。
（2）内部 Flash メモリのプログラミング（前のスライドの説明を参照）。
（3）OTFDEC ペリフェラルでの外部ファームウェアとデータ AES キーのプログラミング。スライドに描画されるように、このキーは、フラッシュ・ツールでグローバル管理以外にも　、デバイス内でローカルに管理することもできます。
（4）外部 Flash メモリのチャンクの暗号化。イメージが STM32 Trusted Package Creator によって暗号化されなかった場合に必要です。
（5）ユーザのファームウェアによる外部 Flash メモリのプログラミング。
その後、各セキュア・ブート中に、セキュア内部ファームウェアにより、最初に AES ファームウェアとデータキーが書込み専用 OTFDEC キーレジスタにコピーされ、次に、これらのキーに関連付けられた OTFDEC 領域が有効化されます。
OCTOSPI ドライバが初期化されると、この時点で、CPU ではデータの読出しと外部 Flash メモリからのコードのフェッチをシームレスに行うことができます。

参照

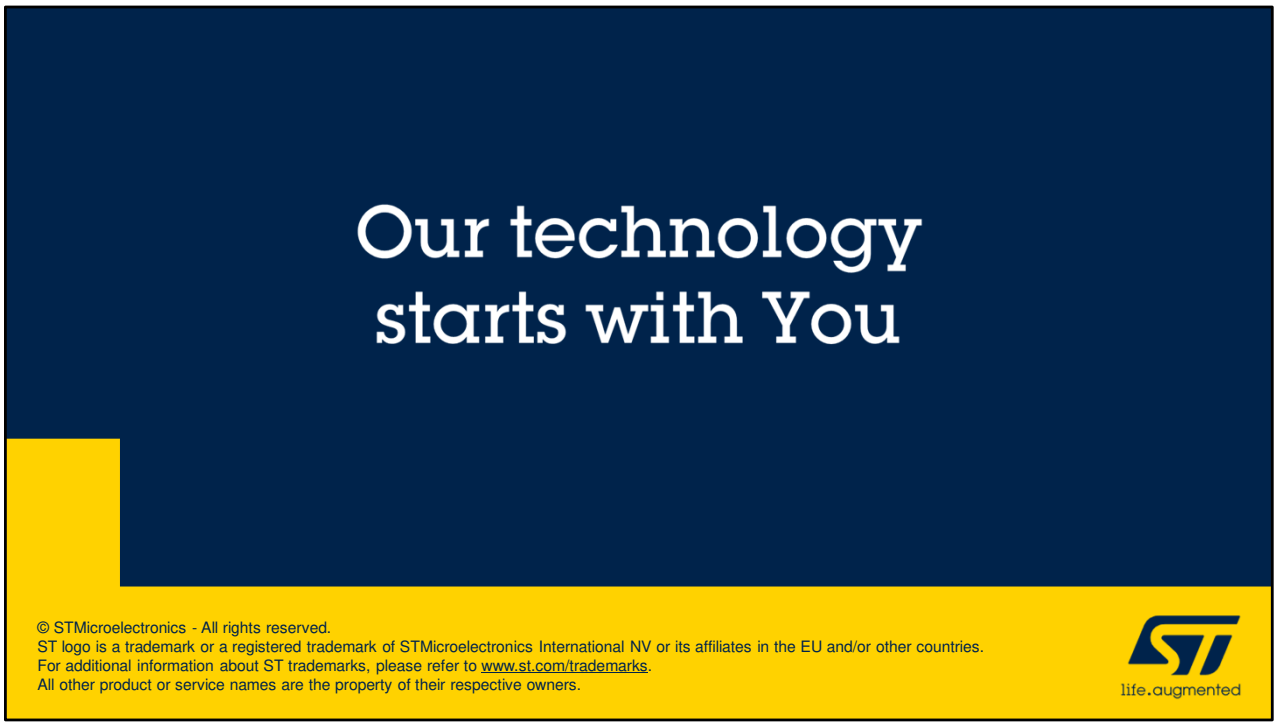
- 詳細および追加情報については、以下を参照してください。
  - RM0456：STM32585x および STM32U575x リファレンスマニュアル
  - AN2606：STM32 マイクロコントローラシステム・メモリ・ブート・モード
  - AN4992：STM32 MCU セキュア・ファームウェア・インストール（SFI）の概要
  - UM2237：STM32CubeProgrammer software description
  - UM2238：STM32 Trusted Package Creator tool software description
  - AN5391：STM32L5/U5 SFI tools, bootloader and RSS interface（要NDA）

life.augmented

9

詳細については、以下を参照してください。

- STM32 マイクロコントローラシステム・メモリ・ブート・モードに関するアプリケーションノート AN2606
- セキュアファームウェアインストール（SFI）の概要に関するアプリケーションノート AN4992
- STM32CubeProgrammer と STM32 Trusted Package Creator のユーザマニュアルも、ST の Web サイトから入手できます。



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。
STM32U5 のセキュリティ機能については、次のプレゼンテーションも参照してください。

- セキュリティの概要
- 強化耐タンパ
- 強化キーストレージ
- ハッシュと乱数
- 対称暗号
- 非対称暗号
- 暗号ライブラリ
- セキュリティ認証