STM32U5 のセキュリティ機能の概要へようこそ。

STM32L5 から更新

主なセキュリティ機能

このモジュールの内容

- 独自のブートエントリと非表示保護領域(HDP)機能によるセキュア・ブート
- TrustZone を使用したリソースの隔離の改善と特権モード
- 読出し保護(RDP)により強化されたライフサイクル管理
  - デバッグ保護 & オプションのパスワードベースの RDP の回帰
- 複数開発者ファームウェア配布方式
- 外部 Flash メモリに格納された暗号化イメージのオンザフライ復号

別のトレーニングモジュールの内容

- 強化されたセキュア・ストレージ
  - STM32U5 セキュリティ 強化されたキーストレージ
- 暗号化アクセラレーション(機密情報操作時のサイドチャネル保護を含む)
  - STM32U5 セキュリティ 暗号
- アクティブタンパと、温度、電圧、周波数攻撃からの保護
  - STM32U5 セキュリティ 強化された耐タンパ
- セキュアファームウェアインストール(SFI)
  - STM32U5 セキュリティ セキュアファームウェアのインストール
- 認証 SESIP レベル 3/PSA レベル 3
  - STM32U5 セキュリティ セキュリティ認証

life.augmented

2

STM32U575/585 ファミリのデバイスは、包括的なセキュリティ機能セットを使用して設計されており、その一部は標準 Arm TrustZone テクノロジに基づいています。これらのセキュリティ機能により、セキュリティ標準に照らして IoT デバイスを評価するプロセスが簡素化されます。また、再利用が容易になり、相互運用性が向上し、API のフラグメンテーションが最小化されているため、OEM およびサードパーティ開発者のソフトウェア開発のコストと複雑さが大幅に低減されます。
このモジュールでは、次の主要なセキュリティ機能について説明します。

- 独自のブートエントリと非表示保護領域(HDP)機能によるセキュア・ブート
- TrustZone と特権モードを使用したリソースの隔離の向上、セキュリティ保護可能な I/O、メモリ、ペリフェラルへの拡張
- 読出し保護(RDP)により強化されたライフサイクル管理。ここには、デバッグ保護とオプションのパスワードベースの RDP の回帰が含まれます。
- TrustZone、オンザフライ復号、RDP0.5 を使用した複数開発者ファームウェア配布方式
- 外部 Flash メモリに格納された暗号化イメージのオンザフライ復号(および関連するセキュアファームウェアのインストール)

他のモジュールには、次の情報が含まれます。

- 強化されたセキュア・ストレージ
- 暗号化アクセラレーション(機密情報操作時のサイドチャネル保護を含む)
- アクティブタンパと、温度、電圧、周波数攻撃からの保護
- セキュアファームウェアのインストール
- 認証 SESIP レベル 3/PSA レベル 3

STM32L5 から更新

セキュア・ブートの主な機能

TrustZone が有効な場合のブートモード

BOOT_LOCK	RSSCMDR	リセット解除時にラッチ				ブート領域（セキュア Flash 領域にある必要があります）
		nBOOT0 Flash_OPTR [27]	BOOT0 ピンの PH3	nSWBOOT0 Flash_OPTR [26]	Flash セキュアブートアドレス	
0	0	-	0	1	SECBOOTADD0	ユーザ定義 (1)（セキュアのみ）
		-	1		*n/a*	RSS：0x0FF8_0000
		1	-	0	SECBOOTADD0	ユーザ定義 (1)（セキュアのみ）
		0	-		*n/a*	RSS：0x0FF8_0000
	≠0	-	-	-	*n/a*	RSS：0x0FF8_0000
1	-	-	-		SECBOOTADD0	ユーザ定義 (1) (2)（セキュアのみ）

RDP 保護レベルに対するブート領域

RDP	ブート領域（TZEN=1）
0	任意のブートアドレス
0.5	許可されたブートアドレス：RSS のみまたはセキュア Flash メモリ（0x0C00_0000 ～ 0x0C1F_FFFF）内のみ セキュア Flash メモリのプログラミングに問題があると、RSS で強制的にブートが行われます
1	
2	

(1) セキュアユーザオプションバイト SECBOOTADD0 で定義されています オプションバイトのデフォルト値は 0x0C00_0000 です
(2) アプリケーションによる変更ができなくなります（一意なブートエントリの強制）

life.augmented

3

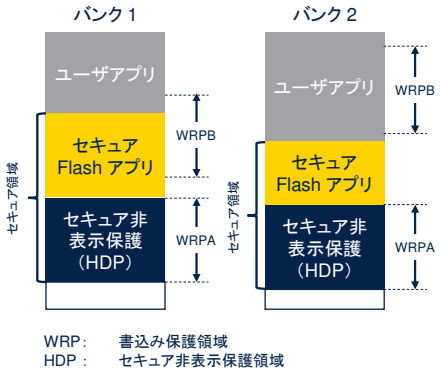
このスライドは、TrustZone が有効な場合のブートオプションをまとめたものです。
- BOOT_LOCK=1 の場合、他のパラメータに関係なく、ブートアドレスは固有であり、セキュアユーザオプション SECBOOTADD0 によって定義されます。
- RSSCMDR が非ヌルであり、BOOT_LOCK=0 の場合、ルートセキュリティサービス（RSS）でのブートが実行されます。
- RDP が 0 より大きい場合、ブートコードをセキュア領域に配置する必要があります。

TrustZone が無効化された場合、表の中央のみが関連し、SECBOOTADD0 の代わりに非セキュア NSBOOTADD0 が使用され、RSS 固定アドレスに代わりに非セキュア NSBOOTADD1 が使用されます。

STM32L5 から更新

内蔵 Flash の主なセキュリティ機能

- Flash がデュアルバンクアーキテクチャでのみ設定されています
- STM32L5 と同様に、バンクごとに 2 つの書込み保護領域があります（不揮発性設定）
  - 不揮発性書込み保護ロック を使用して、U5 では不変メモリ（ROM）をエミュレートできます
    - L5 は HDP 領域のみに依存しています
  - RDP の回帰後は書込み保護がアンロックされるため、アプリケーションではそのような回帰を防止してその領域を不変に保つ必要があります（たとえば、ランダムな OEM キーパスワードをプロビジョニングすることによって）
- Flash の 8 KB の各ページを S/NS や P/NP とすることができます（揮発性の設定）



life.augmented

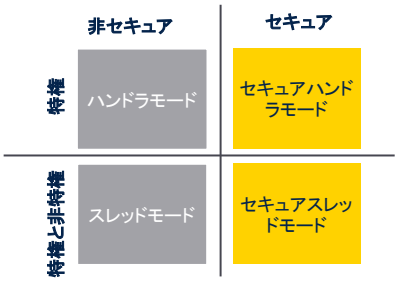
内蔵 Flash には、バンクごとに 2 つの書込み保護領域があり、不揮発性設定ビットによって制御されます。対応する UNLOCK 設定ビットがゼロのとき、これらのビットは変更できません。
UNLOCK ビットをセットできるのは、RDP レベル 1 からレベル 0 に回帰するときのみです。
デバイスで TrustZone が有効になっている場合、内蔵 Flash には次の保護が適用されます。

- ユーザ Flash バンクごとに 1 つのセキュア領域をセキュアな不揮発性ユーザオプションバイトで定義。デフォルトのプログラミングは、すべてセキュアです
- バンクごとに 1 つのセキュア非表示保護（HDP）領域を、アプリケーションによるブート後に必ず非表示
- 8 キロバイトのユーザページを、動作中にアプリケーションによって揮発性セキュアレジスタを使用してセキュアとして定義。リセット後のデフォルト設定は非セキュアです

また、8 キロバイトの各ユーザページを動作中に特権として定義するには、揮発性特権レジスタを使用する必要があります。
ページをセキュアと定義すると、セキュアなアプリケーションでのみこのプロパティを変更できます。

リソースの隔離の向上（1）

- SESIP レベル 3 – PSA レベル 3 認証を取得するために、アプリケーションでシステムペリフェラルとメモリ用に 4 つの隔離状態を使用することができます
  - セキュア / 特権（S/P）
  - セキュア / 非特権（S/NP）
  - 非セキュア / 特権（SN/P）
  - 非セキュア / 非特権（NS/NP）



life.augmented

5

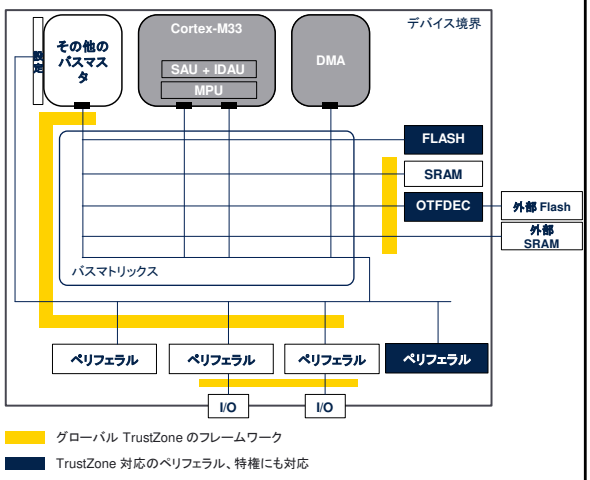
TrustZone が有効になっている場合、セキュアワールドを使用して、非セキュアワールドで実行されている露出の高いコードによる意図的または偶発的な改ざんから重要なコードを保護できます。
TrustZone が有効化されているかどうかに関係なく、Cortex 特権モードを使用すると、露出の高い非特権コードによる意図的または非意図的な改ざんから重要なコードやデータを保護できます。
これらのリソース分離機能は、SESIP レベル 3 – PSA レベル 3 認証を取得するのに役立ちます。
SESIP は Security Evaluation Standard for IoT Platforms（IoT プラットフォームのセキュリティ評価標準）の略で、PSA は Platform Security Architecture（プラットフォームセキュリティアーキテクチャ）の略です。

STM32L5 から更新

リソースの隔離の向上（2）

グローバル TrustZone コントローラ（GTZC）

- ペリフェラルのセキュリティ保護（TZSC を使用）
  - ペリフェラルごとのセキュアな特権設定
- メモリのセキュリティ保護（MPCBB と TZSC を使用）
  - 内部 SRAM 用のブロックベースセキュアな特権設定
  - ウォーターマークによる外部メモリ OCTOSPI / FSMC とバックアップ SRAMサブ領域のセキュアな特権設定
- MPU とは異なり、GTZC では、Cortex-M33 以外のマスタによる非特権トランザクションに対してレガシーメモリとペリフェラルを保護できます
  - レガシーマスタごとのセキュアな特権設定
- GTZC の特権分離の粒度により、Cortex コアで使用可能な粗い特権分離が補足されます（8x MPU 領域）



life.augmented

6

Cortex-M33 の Armv8-M TrustZone セキュリティ拡張機能に加え、これらのデバイスにはグローバル TrustZone コントローラ（GTZC）と呼ばれる補助セキュリティ機能が内蔵されており、セキュアワールド/非セキュアワールド間、および特権ワールド/非特権ワールド間の隔離が柔軟に強化されています。
GTZC では、TrustZone セキュリティコントローラ（TZSC）のレジスタを使用してペリフェラルを保護します。メモリの保護は、ブロックベースのメモリ保護コントローラ（MPCBB）と TZSC レジスタを使用して行われます。
GTZC では、Cortex-M33 以外のマスタによって開始された非セキュアなトランザクション、またオプションで非特権のトランザクションに対する保護ができます。
ペリフェラルによっては、ネイティブに TrustZone 対応および特権対応を備えているため、GTZC によってセキュア保護または特権保護を行う必要がないものもあることに注意してください。

STM32L5 から更新

強化されたライフサイクル管理（1）

RDP の保護レベル		デバッグ	ライフサイクルの概要
レベル 0	デバイスオープン	セキュア[1] および非セキュア	**TZEN=1 の場合、ブートアドレスはセキュア領域を対象とする必要があります（セキュア SRAM、セキュア Flash メモリ、システム Flash メモリ内の RSS）**
レベル 0.5[2]	デバイスが部分的にクローズ	非セキュアのみ	**ブートアドレスはセキュア領域を対象とする必要があります（セキュア・ユーザまたはシステム Flash メモリ）** ➢ SRAM でのブートは許可されていません ➢ デバッグが接続されている場合、非セキュア Flash メモリへのアクセスが可能です ➢ レベル 0 への回帰を防ぐために OEM1 キーをプロビジョニングできます
レベル 1	デバイスメモリの保護	非セキュアのみ（条件付き）	**ブートアドレスはユーザまたはシステム Flash メモリを対象とする必要があります（TZEN = 1 の場合はセキュア）** ➢ デバッグが接続されている場合、非セキュア Flash メモリ、暗号化 Flash メモリ[3]、SRAM2、およびバックアップレジスタへのアクセスは**できません** ➢ レベル 0 への回帰を防ぐために OEM1 キーをプロビジョニングできます ➢ レベル 0.5 への回帰を防ぐために OEM2 キーをプロビジョニングできます
レベル 2	デバイスがクローズ	なし（JTAG ヒューズ）	**ブートアドレスはユーザ Flash メモリを対象とする必要があります（TZEN = 1 の場合はセキュア）** ➢ オプションバイトは読出し専用であるため、OEM2 キーがプロビジョニングされてロックされている場合を除いて RDP レベル 2 は変更できません

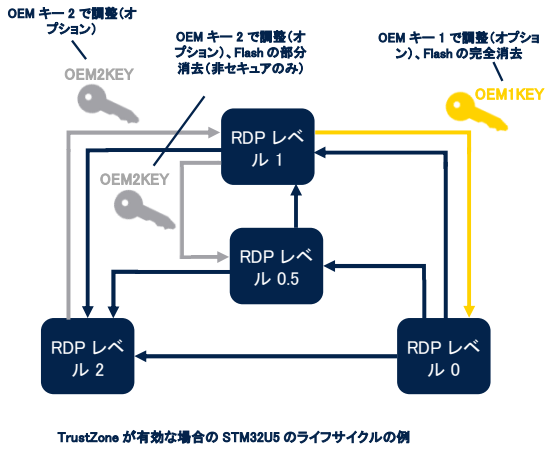
1. RSS コードの実行中、デバッグは使用できません
2. 製品で TrustZone セキュリティが有効化されている場合にのみ適用できます（TZEN=1）
3. OTFDEC によって動作中に復号化される外部 Flash メモリ領域

life.augmented

デバイスのライフサイクルは、読出し保護オプションバイト（RDP）によって管理されます。
この RDP メカニズムは、この表にまとめられているように、デバイスのデバッグ、テスト、およびプロビジョニングされた機密情報へのアクセスを制御するハードウェア機能です。
次のスライドで、キーのアンロックに関連する新機能について説明します。

強化されたライフサイクル管理（1）

パスワードキーベースの RDP の回帰（STM32L5 にない新機能）



TrustZone が有効な場合の STM32U5 のライフサイクルの例

- パスワードキーは **OEM1KEY**、**OEM2KEY** の 2 つがあります
  - 両方 64 ビット、書込み専用、読出し不可
  - プログラムしない場合、デバイスの動作は STM32L5 と同様になります
- OEM1KEY は、**レベル 1** から **レベル 0** への RDP レベルの回帰を管理するために使用されます
- OEM2KEY は、**レベル 2** から **レベル 1**、また**レベル 1** から**レベル 0.5** への RDP レベルの回帰を管理するために使用されます
- アンロックするには、また RDP を回帰するには、**リセット中に** JTAG / SWD ピンを介して正しいキーをシフトする必要があります
- パスワードによるデバイスのアンロックは、**電源サイクルごとに 1 回**のみ可能です

life.augmented

8

パスワードキーベースの RDP の回帰は、デバッグインタフェースまたはシステムブートローダから利用できます。

デバイスに不可逆的にロックをかけたくない場合に理想的です。

図のように、セキュア（OEM1）および非セキュア（OEM2）のアプリケーションコードを個別に保護するために、2 つの 64 ビットキーが内蔵 Flash に定義されています。

この使用法の 1 つを、「複数開発者ファームウェア配布方式」のスライドに示します。

パスワードによるデバイスのアンロックは、電源サイクルごとに 1 回のみ可能であることに注意してください。

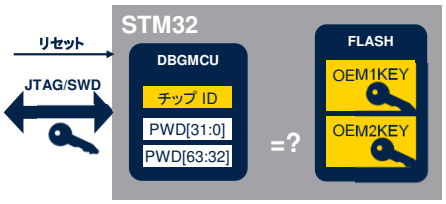
RDP = 0 の場合、OEM1KEY は常に変更できます。RDP = 0.5 または 1 の場合は、OEM1LOCK = 0 であれば変更ができます。

RDP = 0 または 0.5 の場合、OEM2KEY は常に変更できます。RDP = 1 の場合は、OEM2LOCK = 0 であれば変更ができます。

強化されたライフサイクル管理(2)

パスワードキーとチップ ID の関連付け(STM32L5 にない新機能)

- 32 ビットデバイス固有の量のデータを常に JTAG/SWD ポートから読み出すことができますが、RDP レガシー方式が適用され(OEM2LOCK=0)、レベル 2 がセットされている場合(JTAG なし)は例外となります
- OEM ではこのチップ ID と秘密マスタキーを使用して、OEM1/2KEY オプションバイトでデバイス固有のパスワードをプロビジョニングできます
  - Flash で OEM キーがプロビジョニングされると、OEM ツールではチップ ID を読み出して、デバイスのアンロックのために注入すると思われるキーを導出することができます
- パスワードを取得してもデータの機密性が損なわれることはありません
  - RDP 保護の回帰のみが許可されます



life.augmented

9

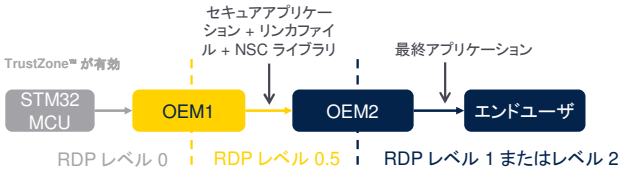
デバッグインタフェースを通じて、32 ビットデバイス固有の量のデータを読み出して、デバイス固有のパスワードを計算できます。
この方法は、RDP レベルが 2 で、OEM2LOCK=0 である場合は適用されません。
パスワードを取得してもデータの機密性が損なわれることはありません。
RDP 保護の回帰のみが許可されます。

複数開発者ファームウェア配布方式

1 人の開発者によるアプローチ

- 1 人の開発者（OEM）が、セキュアアプリケーションと非セキュアアプリケーションの両方を開発できます
  - 製品ファームウェアは RDP レベル 1 または 2 を使用して保護されます
  - TrustZone が無効になっている場合、セキュアなアプリケーションはありません

複数開発者によるアプローチ



- 最初の開発者（OEM1）が、セキュアアプリケーションとそれに関連する非セキュアな呼び出し可能（NSC）ライブラリ（.lib および .h）を開発します
- 2 番目の開発者（OEM2）が、OEM1 によって作成されたリンカファイルを使用して、非セキュアアプリケーションを開発します
  - セキュアアプリケーションは RDP レベル 0.5 に基づいて保護されます。
  - 非セキュアアプリケーションは RDP レベル 1 または RDP レベル 2 に基づいて保護されます。

life.augmented

10

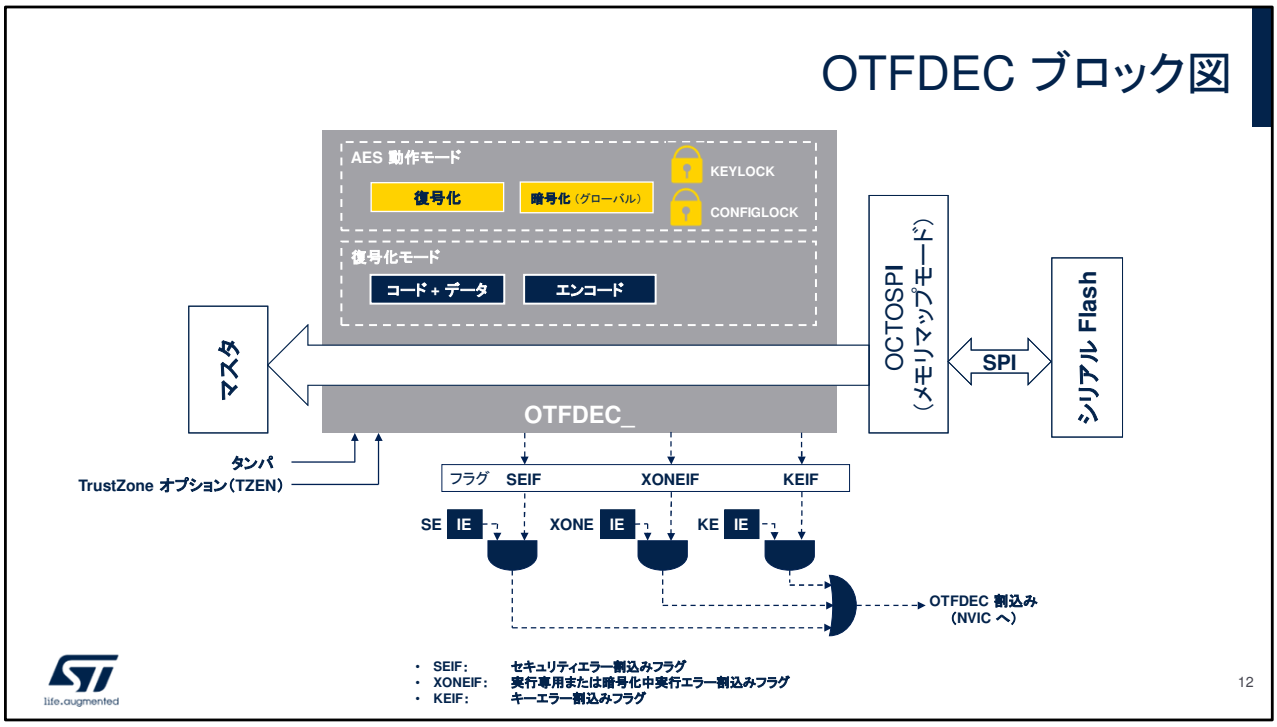
このデバイスはSTM32 の複数開発者ファームウェア配布方式に対応しています。
– 1 人の開発者方式では、1 人の OEM がセキュアアプリケーションと非セキュアアプリケーションを開発します。両方のアプリケーションは、RDP レベル 1 または RDP レベル 2 に基づいて保護する必要があります。
– 複数開発者方式では、最初の OEM がセキュアアプリケーションとそれに関連する非セキュアの呼び出し可能ライブラリを開発し、非セキュアアプリケーションを開発する 2 番目の OEM に事前定義リンカファイルを提供します。
複数開発者方式では、セキュアアプリケーションはインストール後に RDP レベル 0.5 に基づいて保護する必要があります。最後の非セキュアアプリケーションは、RDP レベル 1 または RDP レベル 2 に基づいて保護する必要があります。

オンザフライ復号エンジン（OTFDEC）特徴

- 外部 SPI Flashで暗号化された読出し専用情報を動作中に復号化します
  - 4 つの領域を定義でき、それぞれに専用のキーと公開の多様化データがあります
- カウンタモードで標準 AES-128 を使用し、オプションの強化暗号化オプション（命令のみ）も使用できます
- 書込み専用のキーレジスタ、次のリセットまで書込み保護（KEYLOCK & CONFIGLOCK）
- グローバルセキュリティメカニズム
  - 侵入、RDP の回帰、または MODE 変更が発生した場合にキーを消去
  - TrustZone 対応ペリフェラル（TZEN=1 の場合、レジスタ書込みは常にセキュア）
  - OTFDEC_PRIVCFGR の PRIV ビットがセットされている場合は特権専用アクセス
- 暗号化モード（セキュアのみ）

life.augmented

OTFDEC モジュールでは、外部 SPI Flashで暗号化された読出し専用情報が動作中に復号化されます。
カウンタモードの AES 128 ビット暗号を使用して、遅延を最小限に抑えます。
独立したオーバーラップしない暗号化領域を 4 つ定義できます。領域ごとに、標準 AES 暗号化アルゴリズムの上に保護レイヤを追加することができ、オンチップで暗号化を行う必要があります。
このような強化保護が選択された場合、この領域には命令のみを格納できます。
OTFDEC は暗号化モードにも対応しており、復号化が行われていない場合に使用できます。
キーレジスタはすべて書込み専用で、タンパまたは RDP の回帰の発生時に自動的に消去されます。
OTFDEC は TrustZone 対応ペリフェラルです。
製品でセキュリティが有効化されているとき（TZEN = 1）、レジスタへのすべての書込みはセキュアである必要があります。
OTFDEC の PRIV ビットがセットされている場合、大部分の OTFDEC レジスタへのアクセスでは特権アクセスのみが許可されます。



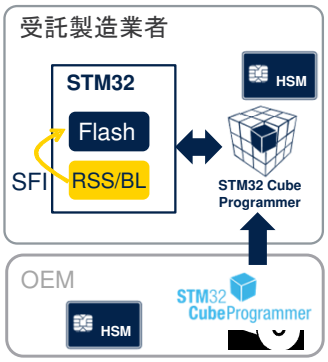
OTFDEC では関連する AHB バスの AHB 読出し転送すべてが解析されます。読出しリクエストがプログラムされた 4 つの領域のいずれかにある場合、カウンタモードの AES アルゴリズムに基づき、制御ロジックによってキーストリームの計算がトリガされます。
このキーストリームは、OCTOSPI AHB マスタからの読出し転送で、存在するデータを動作中に復号化するために使用されます。
有効化された OTFDEC 領域以外へのアクセスは、すべて非暗号化領域に属します。
OTFDEC を OCTOSPI と一緒に使用する場合、Flash コントローラのメモリマップモードで Flash メモリにアクセスする必要があります。
OTFDEC で NVIC への割込みをアサートする原因として、次の 3 つが考えられます。

- セキュリティエラー
- キーエラー
- 実行専用または暗号化中実行エラー

これらのエラーには、それぞれ専用のフラグと割込みイネーブルビットがあります。

OTFDEC を使用したセキュアファームウェアインストール

- セキュアファームウェアインストール（SFI）を使用すると、信頼できない実稼働環境（OEM 契約製造業者など）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
- 外部 Flash メモリが SFI の対象である場合、OEM ファームウェアは専用の AES キーで暗号化されます
- OTFDEC を使用すると、たとえば固有のデバイスキーでこの外部ファームウェアを暗号化できます
  - 領域に対して強化暗号化が選択された場合、このオプションは必須です
- SFI の詳細については、AN4992 を参照してください

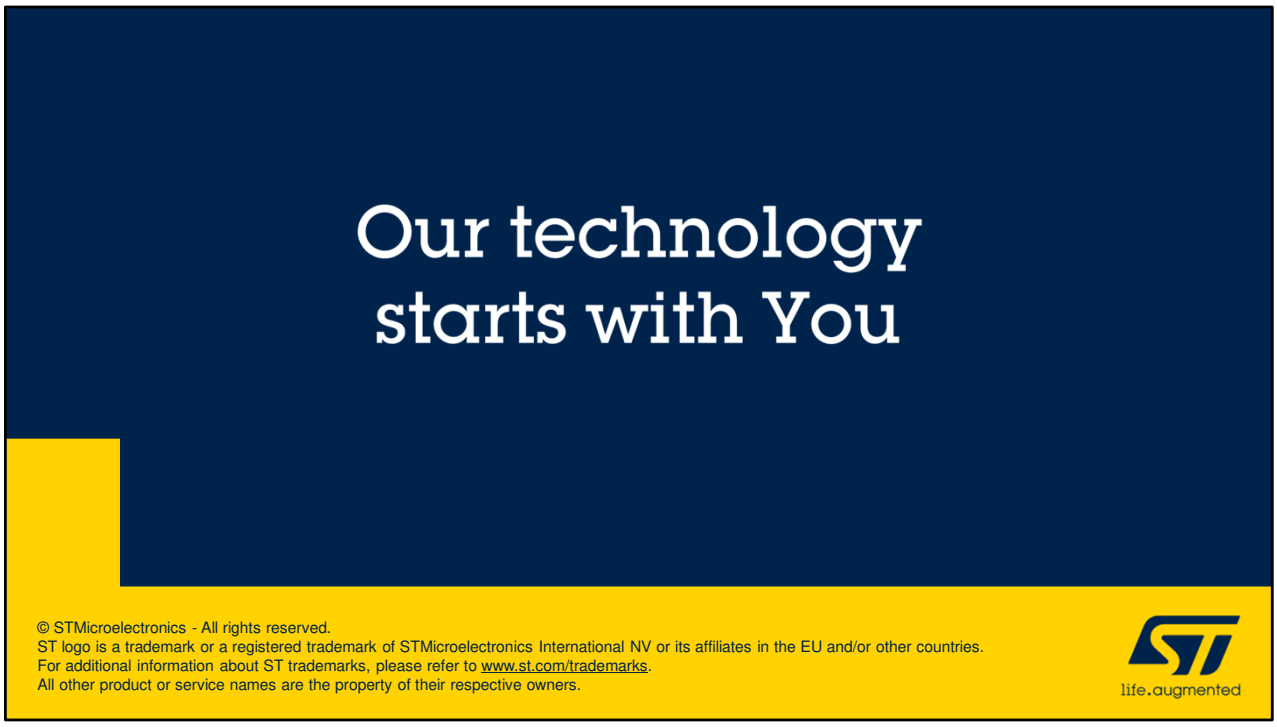


life.augmented

セキュアファームウェアインストール（SFI）は、この STM32 シリーズの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あり、信頼できない実稼働環境（OEM 契約製造業者など）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。
外部 Flash メモリが SFI の対象である場合、OEM ファームウェアコードは、専用の AES キーで暗号化する必要があります。
このキーは次のように使用できます。

- 製品ファミリに共通とし、OEM ツールで暗号化を実行
- デバイスごとに一意とし、ファームウェアをデバイス内で暗号化

OTFDEC 強化暗号化が選択されている場合、オンチップ暗号化は必須です。
詳細については、セキュアファームウェアインストール（SFI）ソリューションのアプリケーションノート AN4992 を参照してください。



プレゼンテーションをご覧いただき、ありがとうございます。
STM32U5 のセキュリティモジュール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。

- 対称暗号化
- 非対称暗号化
- ハッシュと乱数の生成
- 強化耐タンパ
- 強化キーストレージ