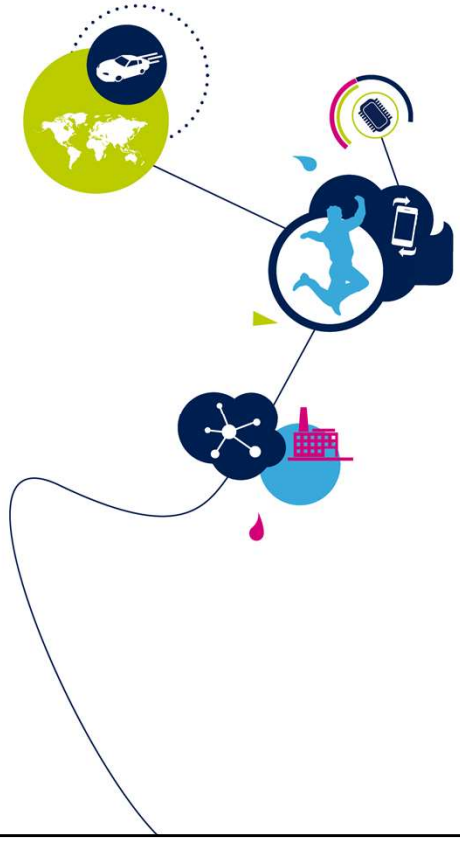
STM32H7B - OTFDEC

オンザフライ復号化エンジン

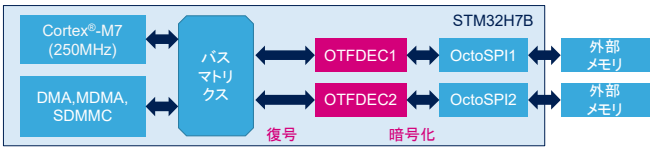
1.0版



こんにちは、STM32H7Bマイクロコントローラに内蔵される
OTFDECのプレゼンテーションへようこそ。

概要

- OctoSPIのメモリマップ読出し操作（単一または複数）中にオンザフライで復号化を実行
  - カウンタ(CTR)モードでのAESの使用により、最小の遅延時間を実現
- OTFDECのロケーション:



アプリケーション側の利点

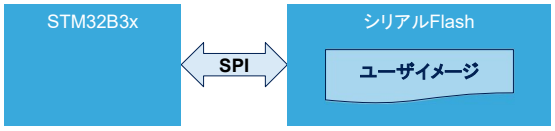
- 外部Flashの保護
- 最大8つの独立した暗号化領域(OTFDECあたり4つ)
- 領域設定書込みロック機構

OTFDECの本来の目的は、外部のSPI NOR Flashデバイスに格納された読み取り専用のファームウェアライブラリの機密性を保護することです。
OTFDECは、OCTOSPIのメモリマップにおけるリード動作中に、オンザフライで復号化を行います。また、1バイト単位での読み出しにも対応しています。
2つのOTFDECインスタンスは、AXIバスマトリックスと、外部シリアルFlashへのアクセスを制御する1つのOctoSPIペリフェラルの間に配置されています。
カウンタモードでの高度な暗号化標準(AES)-128ビットアルゴリズムが実装され、最小の待機時間を実現します。

そのため、暗号化された領域の内容を変更するたびに、領域全体を異なる暗号コンテキスト（鍵や初期化ベクトル）で再暗号化する必要があります。
最大8つの独立した暗号化領域（OTFDECごとに4つ）を定義でき、それぞれに128ビットの鍵と初期化ベクター情報（64ビットのアプリケーションノンスと16ビットの暗号化ライブラリバージョン）を持たせることができます。
書込みロックメカニズムにより、各領域のパラメータの再設定ができないようになっています。

外部Flashの保護

- 外部Flashに保存されたコードやデータを保護したい場合
  - 外部Flashは、新しいボード上で再びはんだ付することが可能
  - 外部Flash標準のSPIバスをプローブで覗くことも可能



- ユーザはパフォーマンスへの影響を最小限に抑えた保護を望む
  - AESアルゴリズムは、データのブロックを処理するために多くのサイクルを消費

OTFDECペリフェラルの目的は、外部のシリアルFlashメモリに保存されているユーザーコードやデータを保護することです。
イメージが暗号化されずに保存されている場合、Flashデバイスのはんだを取り除いて別のボードに再はんだ付けするか、ロジックアナライザやオシロスコープを使ってSPIバスのトラフィックを監視することで、イメージを簡単に読み取ることができます。
そのため、Flashメモリに保存されたイメージは暗号化され、ランタイムリードの際にその場で復号化される必要があります。
復号化によるレイテンシーを最小限に抑える必要があります。
OTFDECは、これらの目的に取り組むために設計されました。

OTFDECによる外部Flashの保護

- OTFDECは、STM32H7Bのペリフェラルで、外部SPI Flashに格納されたコードやデータを低遅延で復号することが可能
  - OTFDECは、グローバル暗号化モードにもサポート
- コードとデータは、STM32H7Bマスタへの OTFDEC出力まで、外部Flash内で保護
- 各OTFDECは、STM32マスタから見て1つのOctoSPIの前に立ち、外部Flash（メモリマップド･モード）を対象としたすべてのデータ読出しおよび命令フェッチトランザクションをインターセプトする
- OTFDECセットアップ後、OTFDECを介した外部Flashへのリード / フェッチ・トランザクションは、STM32マスタから見て透過的である（復号化の必要はない）

life.augmented

OTFDECは、STM32H7Bラインに実装されたペリフェラルで、外部Flashに格納されたコードやデータを低遅延で復号することができます。また、暗号化モードもサポートしています。
暗号化プロセスは、リファレンスマニュアルに記載されている順序に従う必要があります。暗号化モードを選択すると、すべてのリージョンのオンザフライ復号化は解除されます。
復号化はマイクロコントローラの内部で行われるため、OctoSPIバスで転送されるデータは暗号化されます。これは、Flashのはんだ除去やバスのスパイ対策になります。
OTFDECは、OctoSPIペリフェラルのコンパニオンIPです。
OTFDECは、外部Flashをターゲットにしたデータリードや命令フェッチを遮断します。
復号化はCortex-M7コアに対して透過的です。プロセッサーが受け取るデータおよび/または命令は、OTFDECペリフェラルによってハードウェアで暗号化解除されています。

OTFDEC機能(1/2)

- 外部の機密性を保護:
  - 読出し専用のコード、読出し専用のデータ、または読出し専用のコード + データエリア、すべてがオンザフライで復号化
  - OTFDECユニットごとに、4つの独立したオーバーラップしない暗号化領域を定義可能
- カウンタ·モード(CTR)のAES128ビット暗号を採用し、最小の遅延を実現
  - アクセス最小粒度:8ビット
- 各領域は以下のように定義
  - 秘密鍵とその公開8ビットCRC
  - 公開されている多様なデータ: 64ビット·アプリケーション情報＋16ビット·ライブラリ·バージョン
- レジスタ·プログラミング用AHBインタフェース

life.augmented

OTFDECは、外部の読出し専用コード、読み出し専用データ、または読出し専用{コード＋データ}領域の機密性を保護します。
それらはその場で復号化されます。
4つの独立したオーバーラップしない暗号化領域を定義できます。
カウンタモードのAES128ビット暗号を採用し、最小のレイテンシを実現しています。
アクセスの最小粒度は8ビットです。
各リージョンは、128ビットの秘密鍵と、8ビットの公開CRCで定義されます。
各リージョンの初期化ベクトルは、64ビットのアプリケーション情報と16ビットのライブラリバージョンを用いてOTFDECユニットが構築されます。ユーザはこの情報を公開多様化データとして定義することができます。
OTFDECユニットにはAHBスレーブインタフェースがあり、制御レジスタやステータスレジスタにアクセスするために使用されます。

OTFDEC機能(2/2)

- 領域ごとのOTFDECの動作モード:
  - MODE = 00 (*): 命令アクセスのみ暗号化される
  - MODE = 01 (*): データアクセスのみ暗号化される
  - MODE = 10 (*): すべてのリードアクセスが命令、データともに復号化される
  - MODE=11 (**):拡張暗号化による命令フェッチのみ可能

(*) 標準的なAES-CTR暗号、ツールやアプリケーションのファームウェアへの組み込みが可能

(**) 標準のAES-CTRに追加の保護レイヤ（独自）を加えたもの、オンチップでの暗号化が必要

- リージョンごとのセキュリティ・メカニズム
  - 書込み可能なキーレジスタ、次回リセット時まで書き込み禁止 (KEYLOCK&CONFIGLOCK)
- グローバル・セキュリティ・メカニズム
  - 侵入、RDP回帰、モード変更の場合のキー消去
  - 暗号化モード、不変のRSSコードへの予約

各領域ごとに、動作モードを選択する必要があります。具体的には:

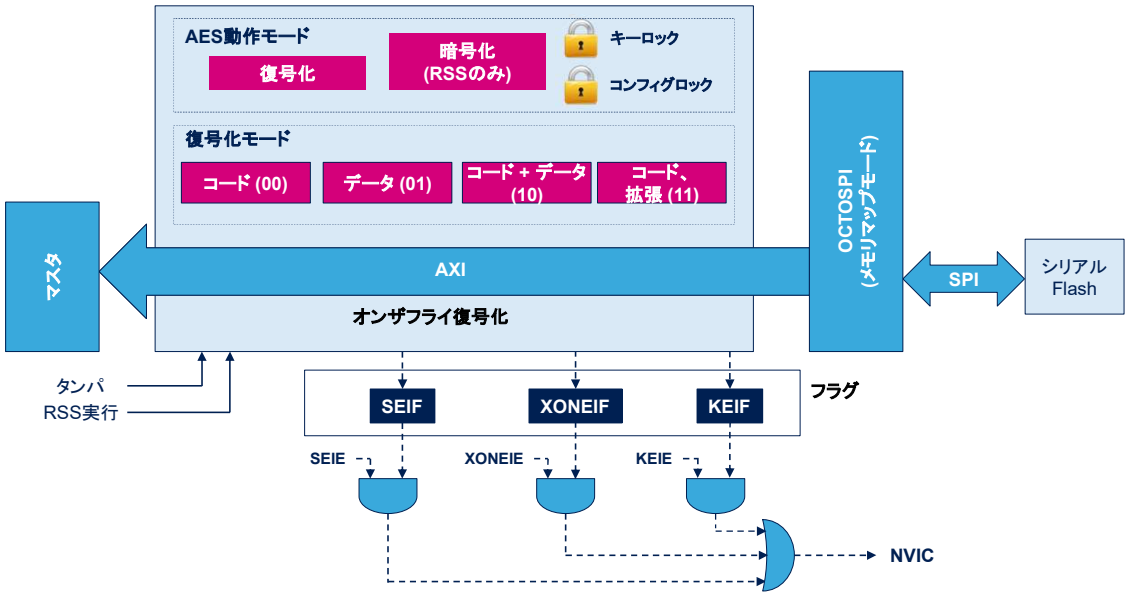
- 領域内にコードとデータの両方が含まれている場合は、リージョン・コンフィギュレーション・レジスタのMODEフィールドをバイナリ値10に設定する必要があります。
- 領域がデータのみを含む場合は、リージョン・コンフィギュレーション・レジスタのMODEフィールドをバイナリ値01に設定する必要があります。
- 領域に外部から暗号化できるコードのみが含まれている場合は、リージョン・コンフィギュレーション・レジスタのMODEフィールドをバイナリ値00に設定する必要があります。

この3つのモードでは、標準的なAES暗号化アルゴリズムを使用しているため、コード生成ツールやアプリケーションのファームウェアに暗号化処理を組み込み、ランタイム暗号化を行うことができます。

領域に命令のみ含まれている場合は、リージョンコンフィギュレーションレジスタのMODEフィールドをバイナリ値11に設定することができます。この場合，標準的なAES暗号化アルゴリズムの上にさらに保護レイヤが追加されるため，ソフトウェアツールに暗号化処理を組み込むことはできません。（専用のRSS関数を使用して暗号化を実行するには，OTFDECを使用する必要があります）

各リージョンの設定を独立してロックすることで、それ以上の変更を防ぐことができます。128ビットの鍵と設定パラメータの両方をロックすることができます。すべてのキーレジスタは書込み専用であり、改ざん、読出し保護(RDP)の回帰、またはMODEフィールドの変更によって侵入が検出された場合には自動的に消去されます。

OTFDECブロック図

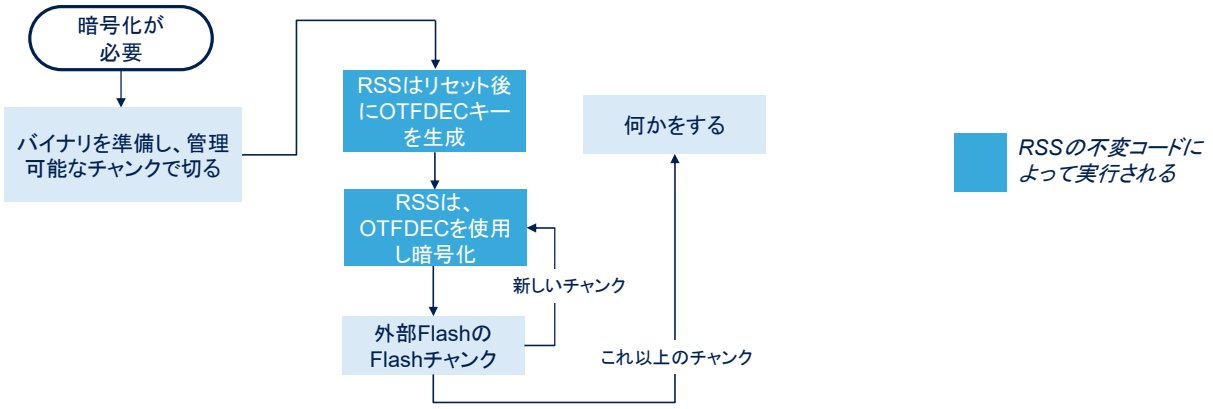


OTFDECの原則は、関連するAXIバス上のすべてのAXI読取り転送を分析します。
読出し要求がOTFDECでプログラムされた4つの領域のいずれかに含まれる場合、制御ロジックはカウンタモードのAESアルゴリズムに基づいてキーストリームの計算を開始します。
このキーストリームは、OCTOSPI AXIマスタからのリード転送に含まれるデータをオンザフライで復号するために使用されます。キーストリーム情報が計算されている間、このマスタのRREADY信号はLowに保たれます。(これには最大11サイクルかかります)
有効化されたOTFDEC領域外へのアクセスは、暗号化されていない領域に属します。
OTFDECはOCTOSPIと組み合わせて使用するため、Flashコントローラのメモリーマップモードを使用してFlashメモリにアクセスすることが必須となります。
リージョンコンフィギュレーションレジスタのMODEビットは，OTFDECの動作モード(標準暗号化または拡張暗号化)を定義します。
RSSでは、OTFDECを使って、標準のAESアルゴリズムまたは拡張された暗号化アルゴリズムのいずれかを使ってデータを暗号化することができます。
タンパ検出、RDP回帰、またはMODEビットの変更は、キーを自動的に消去します。

OTFDECは、3つの可能性のある原因に対して、NVICに割込みをアサートすることができます。OTFDECは，次の3つの原因でNVICに割込みをかけることができる。これらの原因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暗号化

- ユーザまたはSTのファームウェアは、OTFDEC RSSサービスresetAndEncrypt()でOTFDECの暗号化を管理することが可能
  ユーザのファームウェアは、外部Flashプログラミングを行う
  - 詳細はアプリケーションノートAN5281を参照



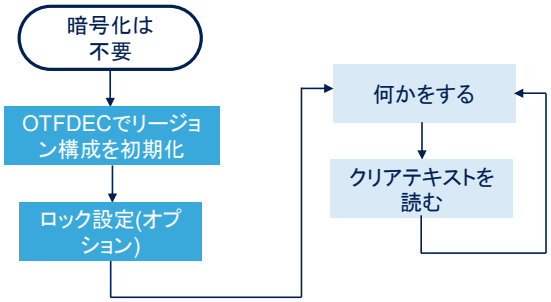
life.augmented

アプリケーション（STまたはユーザ）へのRSS resetAndEncrypt()サービスは，専用SRAM領域にロードされたコードを暗号化するものです。暗号化するコードのサイズに応じて、このサービスへの複数のコールを要求できます。
ユーザファームウェアは、外部Flashプログラミングを担当します。

注意：RSSサービスのresetAndEncrypt()は、常にシステムリセットのトリガとなります。

OTFDEC復号化

- STM32H7Bのリセット時、ブート･シーケンス中に、ユーザ･ファームウェアは:
  - OTFDECキーレジスタ内の各OTFDECリージョンのキーを読込む
    - 2つのOTFDECインスタンスを持つ8つの利用可能なリージョン（OTFDECごとに4つ）
  - OTFDECの設定をロックする（キーなど）
- その後、オンザフライでの復号が可能になる



セキュリティで保護されたユーザコードで実行される(推奨)

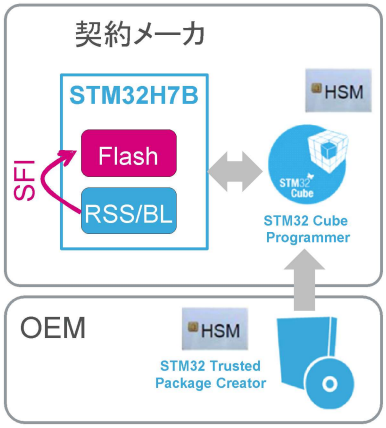
ユーザファームウェアは、ブートシーケンスにおいて以下の初期化を担当します。:

- 各OTFDECリージョンのOTFDECキーレジスタ内のキーの読込み
- 各OTFDEC領域のノンセ、バージョン、アドレス開始、アドレス終了情報の読込み
- REG_ENビットの設定
- 上記のOTFDECの構成をロックする（推奨）

これにより、オンザフライでの復号化が可能です。

OTFDECを使用した セキュア·ファームウェア·インストール(1)

- セキュア·ファームウェア·インストール(SFI)は、STM32H7xシリーズ·マイコン向けのグローバル·ソリューションで、信頼できない生産環境(OEM契約メーカなど)で、OEMファームウェアを安全にカウントしてインストールすることが可能
- 外部FlashメモリがSFIの対象となる場合、OEMファームウェアは外部ファームウェアとデータのAESキーで暗号化される
- OTFDECは、デバイス固有のキーなどを用いて外部ファームウェアを暗号化するために使用可能
  - このオプションは、リージョンに対してMODE=11(拡張)が選択されている場合は必須(次スライドに図示)
- 詳細については、AN4992を参照



セキュア・ファームウェア・インストール(SFI)は、STM32H7Bシリーズ・マイクロコントローラのためのグローバルソリューションで、信頼できない生産環境(OEM契約メーカなど)において、OEMファームウェアを安全かつ計数的にインストールすることができます。SFIで保護されたOEMファームウェアは、デバイスの内部Flashに保存するか、OCTOSPI経由で接続された外部Flashに暗号化して保存することができます。

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は外部ファームウェアおよびデータのAESキーで暗号化する必要があります。このキーは

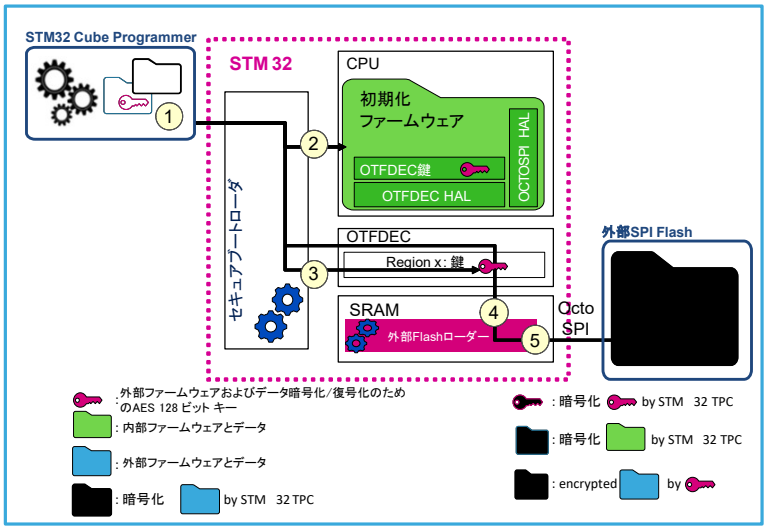
- 全デバイス共通(この場合、OFTDEC MODE=10であればツールで暗号化が可能)、または
- デバイスごと固有(この場合、ファームウェアはデバイス内で暗号化され、OTFDEC MODE=11の場合は必須)

OTFDECを使ったオンチップ暗号化は次のスライドで説明します。

詳細については、アプリケーションノートAN4992のSFI(Secure Firmware Install)ソリューションをご参照ください。

OTFDECを使用した セキュア・ファームウェア・インストール(2)

1. STM32 Trusted Package Creator (TPC) によるSFIイメージの作成
   - 内部のファームウェアとデータ（外部Flashメモリドライバーを含む）
   - 外部ファームウェアとデータのAESキー
   - 外部ファームウェアとデータ
2. 内蔵Flashメモリのプログラミング
3. 外部ファームウェアとデータOTFDEC ペリフェラルでのAESキープログラミング
   - また、このような鍵は、Flashツールでグローバルに管理するのではなく、デバイスにローカルに管理することも可能
4. 外部Flashメモリのチャンク暗号化
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



life.augmented

このスライドは、STM32のセキュアブートローダが、内部ファームウェアのインストールと、グローバルな外部Flashメモリ用のAESキーと外部Flashメモリ・ローダの助けを借り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。数字のステップは、回路図で表されています。
(1)STM32 Trusted Package Creator (TPC)を用いて、a)内部のファームウェアとデータ（外部Flashメモリのドライバを含む）、b)外部のファームウェアとデータのAESキー、c)外部のファームウェアとデータを含むSFIイメージを作成します。
(2)STM32H7B RSSトレーニングで説明されている内部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のAESキーのプログラミング。スライドに描かれているのとは異なり、このキーはフラッシングツールでグローバルに管理するのではなく、デバイスにローカルに管理することができます。
(4)外付けFlashメモリのチャンク暗号化
(5)ユーザのファームウェアによる外部Flashメモリの書込み

その後、起動のたびに、RSSのセキュアな内部ファームウェアが、まずAESのファームウェアとデータキーを書込み可能なOTFDECキーレジスタにコピーし、それらのキーに関連付けられたOTFDEC領域をアクティブにします。この時点で、OCTOSPIドライバが初期化されていれば、CPUは外部Flashメモリ（暗号化されていてもいなくても）からデータやコードをシームレスにリード/フェッチすることができます。

割込み

割込みイベント	説明
セキュリティエラー	キーレジスタへの読取りが不正 KEYLOCK=1の間にキーレジスタへの不正な書込み CONFIGLOCK=1の間にリージョンの構成に対する不正な書込み
実行のみ 実行しない	実行専用領域への読取りアクセス(MODE[1:0]=00または11) 実行しないデータ領域(MODE[1:0]=01)へのアクセスを実行
キーエラー	キーレジスタがNULLであるか、または正しく初期化されていない間に、暗号化領域への読み取り要求(KEYCRC=0x0) ➢ エラーの原因は、不正なキー読込みシーケンス(OTFDEC_RxCFGRのKEYCRCを参照)、または改ざん、読み出し保護(RDP)の回帰またはMODEフィールドの変更によって検出された侵入の場合に消去される可能性がある このような読取りリクエストは、バスエラーなしで0x0返す

OTFDECには3つの割込みソースがあります。
セキュリティエラーは、KEYLOCKビットが設定されている状態で、キーレジスタの読出しを試みたり、キーの書込みを試みたり、CONFIGLOCKビットが設定されている状態で、リージョンの再構成を試みたりした場合に発生します。
実行専用モード(MODE=00)または暗号化強化モード(MODE=11)が選択されている場合、この保護領域にリードアクセスしようとすると、実行専用エラーが発生します。
データオンリーモード(MODE=01)を選択した場合、このプロテクト領域に実行アクセスしようとすると、”実行しないエラー”が発生します。
キーエラーは、キーレジスタがNULLであったり、正しくプログラムされていない(KEYCRC=0x0)領域にリードリクエストを試みたときに発生します。キーエラーは、キーレジスタの書き込みシーケンスが正しくない場合に発生します。また、タンパ、リードアウトプロテクション（RDP）の回帰、MODEフィールドの変更などにより侵入が検知された場合にも発生します。

低電力モード

モード	説明
DRUN	アクティブ
DSTOP	停止 ペリフェラル·レジスタの内容は保持
DSTOP2	
STANDBY	パワーダウン STANDBYモードを終了した後、ペリフェラルを再初期化する必要がある
SHUTDOWN	パワーダウン SHUTDOWNモードを終了した後、ペリフェラルを再初期化する必要がある

OTFDECは、DRUNモードでアクティブです。
DSTOPモードまたはDSTOP2モードでは、OTFDECは停止され、そのレジスタの内容は保持されます。
STANDBYモードまたはSHUTDOWNモードでは、OTFDECは電源をオフにして、後で再初期化する必要があります。

関連ペリフェラル

- 詳細については、このペリフェラルにリンクされている以下のトレーニングをご参照ください
  - OctoSPIインタフェース(OCTOSPI)
  - ネスト化されたベクト割込み(NVIC)
  - セキュア･ファームウェア･インストール(SFI)
  - ルート･セキュリティ･サービス(RSS)

- 詳細および追加情報については、以下をご参照ください
  - AN4992: Overview of secure firmware install (SFI)
  - AN5281: How to use OTFDEC for encryption/decryption in trusted environment on STM32 MCUs

life.augmented

OTFDECモジュールは、以下の他のモジュールと関係があります。

- OctoSPIインタフェース
- ネスト化されたベクト割込みコントローラ
- セキュアファームウェアインストール（SFI）
- ルートセキュリティサービス(SFI情報を含む)

SFIの詳細については、セキュアファームウェアインストール(SFI)の概要に関するアプリケーションノートAN4992をご参照ください。
暗号化および復号化におけるOTFDECの使用法の詳細(およびコード例)については、アプリケーションノートAN5281をご参照ください。