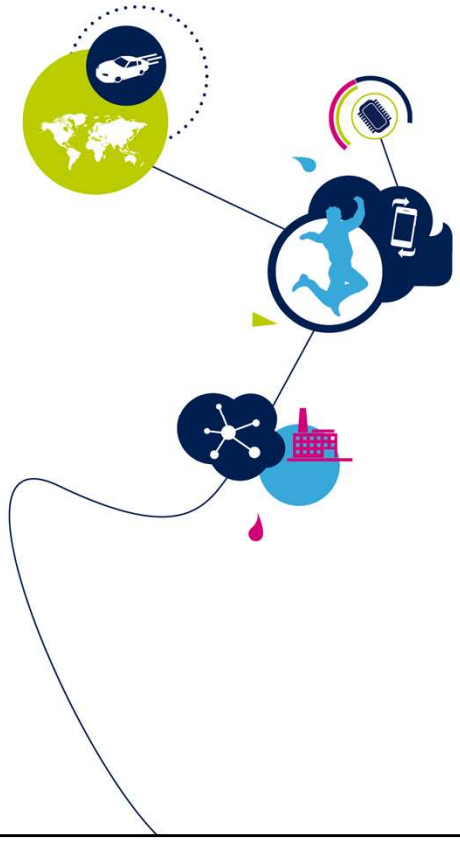
STM32H7 - RSS

ルート･セキュリティ･サービス
1.0版



life.augmented

このオンライン･トレーニング･モジュールでは，STM32H7の高度なセキュリティ機能であるルート･セキュリティ･サービス(RSS)について説明します。
オンライン･トレーニング･モジュール「メモリ保護」をすでにご覧になっていることをお勧めします。

概要

- ルート･セキュリティ･サービス(RSS)
  - セキュリティ管理に特化したST ROMコード
    セキュアなファームウェア / モジュール･インストール･
    アプリケーションのための非対称キー･ペアを内蔵
    STM32H7の**セキュア･アクセス･モード**が提供する高
    度なセキュリティ機能の一部
- セキュアサービス
  - ファームウェアやモジュールの安全なインストール
    (SFI/SMI)
    - OEMファームウェアの機密性保護ファームウェアの過剰
      生産の防止(カウントインストール)サードパーティ･モジュール
      の知的財産の保護
  - 保護エリアの管理

アプリケーション側の利点

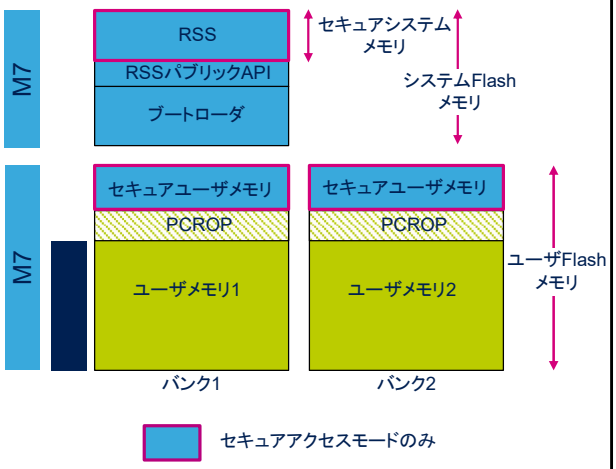
- 秘密鍵によるセキュアなチップ
  パーソナライゼーション
- 安全でない環境でのファームウェアや
  モジュールの知的財産の保護

life.augmented

ルート･セキュア･サービス（RSS）は，STM32H7のセキュリティ機能の一部であるST ROMコードです。これらのファームウェア･サービスは，STM32H7シリーズで導入された新しいセキュリティ･デバイス構成であるセキュア･アクセス･モードで利用できます。セキュア･アクセス･モードの定義および設定方法については、オンライン･トレーニング･モジュール「STM32H7メモリ保護」をご参照ください。RSSが提供する主なセキュアサービスは，セキュア･ファームウェア･インストール（SFI）です。このサービスは、データをフラッシュに転送する際のファームウェアの機密性を確保し、機密性の低い製造環境での過剰生産を防ぎます。高いレベルの保護を実現するために、STのソリューションは、STM32H7デバイスごとに固有の秘密鍵を持つ非対称暗号に依存しています。SFIの手順については、次のスライドで詳しく説明します。RSSは、PCROPやセキュアユーザーメモリなどの保護領域の管理にも使用されます。これらの保護機能については、オンライン･トレーニング･モジュール「STM32H7メモリ保護」で詳しく説明しています。

メモリ·アーキテクチャ

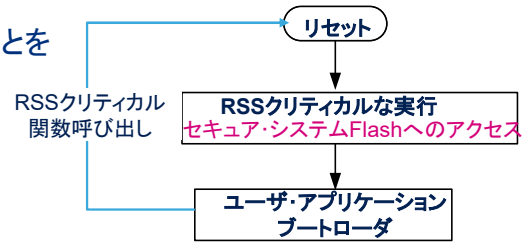
- システムFlashメモリ
  - STのファームウェア専用のFlashメモリ領域:
    ブートローダ、RSS
  - RSSのセンシティブなコードやデータは、システムFlash
    メモリ内のセキュアな部分に保護されており、特定のアクセス
    メカニズムを備えている
    RSSのパブリックAPIは標準のシステムFlashに格納される
  - システムFlashにアクセスできるのはCortex M7のみ
- セキュアなシステム·メモリ·アクセス
  - セキュア·アクセス·モードでのみ使用可能
  - Cortex-M7によるRSS実行のためにシステムがリセットされた
    後に、アクセスが1回許可される
    - RSSはデバイス上の他のすべての処理を優先し、Cortex-M4は
      その実行中に保持
    - RSSの選択されたサービスが完了すると、セキュアシステム
      メモリへのアクセスは出来なくなる



RSSは、このスライドで紹介する特定のメモリ保護メカニズムに依存しています。
他のSTM32製品と同様に、STM32H7はFlashメモリ内に読取り専用の領域を持っています。この領域はシステムFlashメモリと呼ばれ、ブートローダやRSS機能などのSTのファームウェアが組み込まれています。
なお、システムFlashメモリにアクセスできるのは、Cortex-M7コアだけがシステムFlashメモリにアクセスでき、Cortex-M4コアは読出しも実行もできません。機密性の高いアルゴリズムや暗号鍵を持つRSS機能は、システムFlashメモリの特定の部分に組み込まれています。
セキュアシステムメモリ:
このメモリには特定のアクセスルールが設定されており、デバイスを非常に高いレベルで保護します。
このメモリは、セキュア·アクセス·モードでのみ利用可能です。RSSサービスにアクセスするには、デバイスがこのモードに設定されている必要があります。
ほとんどのRSSサービスへのアクセスは、システムリセット後に許可されます。その後、Cortex-M7コアは、いずれかのコア上で実行されている他のすべてのプロセスを先取りして、必要なサービスを安全に実行することができます。
RSSの実行が完了すると、デバイスはユーザアプリケーションにジャンプし、次のシステムリセットが行われるまでセキュアシステムメモリにはアクセスできなくなります。

サービスの種類

- RSSサービスとは
  - 直接的なAPIファンクションコールによるもの
  - または、ブートローダ拡張コマンドセットによる
- クリティカルサービス
  - 機密データや保護されたコードを操作
  - セキュアシステムのメモリからシステム・リセットを実行することを要求
    - セキュア・ファームウェア・インストール
    - セキュア・ユーザ・メモリの初期化
- クリティカルでないサービス
  - 秘密ではないデータやステータス（証明書、RSSバージョンなど）へのアクセス
  - 暗号化されたデータのみを操作
  - リセットの実行を必要としない



RSSサービスは、アプリケーション・プログラミング・インターフェース(API)の機能を使って直接呼び出すことも、ブートローダの特定のコマンドを使って呼び出すこともできます。次のスライドでは、RSSの機能とブートローダのコマンドセットを紹介します。
RSSサービスは、機密データまたはコードによって、2種類に分割できます。
クリティカルなサービスとは、暗号鍵などの機密データを操作するものや、他のプロセスからの安全な実行を必要とするものです。これらのサービスを実行する前には、システムリセットがかかります。
クリティカルなRSSサービスには、次のものがあります。
•安全なファームウェアまたはモジュールのインストール
•セキュア・ユーザー・メモリおよびPCROPエリアの除去の初期化
クリティカルでないサービスは、機密データへのアクセスを必要とせず、リセットなしで実行できます。

RSSコール

- ユーザ・アプリケーションからの直接APIコールによる

API名	説明
RSS_resetAndInitializeSecureAreas	セキュア・ユーザ・メモリ（バンク1およびバンク2）の開始および終了アドレスの設定
RSS_exitSecureArea	セキュア・ユーザ・メモリからの安全な終了 この保護された領域への将来のアクセスを防ぐ

- STM32CubeProgrammerを使ったセキュア・プログラミングを通して
  - セキュア・ファームウエアのインストールに使用(SFI)
  - 次を参照
    - SFIの概要については、AN4992
    - セキュア・プログラミングの説明はAN5054

life.augmented

このスライドでは、利用可能なRSSサービスとその呼び出し方法を紹介しています。ダイレクトAPIで呼び出されるサービスは、デバイス管理用ファームウェアで呼び出すことができるものです。これらのサービスは、セキュアな領域管理を可能にします。SFI(セキュアファームウェアインストール)で使用されるRSSサービスは、STM32CubeProgrammerツールでアクセスします。詳細は、専用のアプリケーションノートをご参照ください。

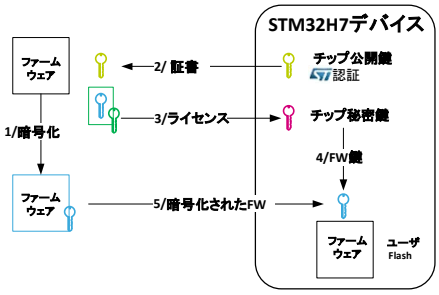
保護エリアのマネジメント

- 保護されたメモリの管理に特化したセキュアなサービス
  - ユーザ·ファームウエアからの直接呼び出しでのみアクセス可能(ブートローダ·コマンドなし)
  - RSS関数
    - セキュア·エリアの初期化
      - システム·リセットのトリガ(重要なサービス)
      - セキュア·ユーザ·メモリ·エリアの開始および終了アドレスの設定
      - この関数は、ST-Linkユーティリティ·ツールから呼び出すことが可能
    - 安全なエリアを終了
      - ユーザのセキュリティで保護されたアプリケーションで、メインアプリケーションにジャンプする前に、ユーザのセキュリティで保護されたユーザ·メモリを閉じるために使用される

このスライドでは、デバイスの保護領域を管理するために使用されるRSSサービスを示します。
これらのサービスでは、セキュリティで保護されたユーザメモリの設定と管理が可能になります。
このメモリは、安全な環境で実行される重要なユーザーファームウェア用です。このような重要なファームウェアの典型的なアプリケーションは、「セキュアファームウェアアップデート」(SFU)とセキュアブートローダです。
セキュアユーザメモリ機能の詳細については、STM32H7トレーニングモジュール「メモリ保護」およびアプリケーションノートAN4925をご参照ください。

セキュア・ファームウェアのインストール(1/4)

- 手順の説明
  - 原則
    - SFIは、安全でない製造段階でのファームウェアのコピーを防ぐために、暗号化されたファームウェアをデバイスに転送
    - 各STM32H7デバイスは、STMicroelectronicsによって、デバイス認証用のチップ非対称キー・ペアと証明書が提供
    - 暗号化キーおよびファームウェア復号化フローへのアクセスはRSSによって提供
      - 暗号鍵は、SFI/SMIアプリケーション専用であり、ユーザアプリケーションでは使用できない
  - SFI暗号フロー
    1. ファームウェアはAES-GCMアルゴリズムによりファームウェア所有者の鍵で暗号化
    2. チップの公開鍵は、STが認証した証明書によって取得
    3. ファームウェアの鍵は、チップの公開鍵(ライセンス)によって暗号化され、デバイスに転送
    4. ファームウェアキーがデバイス内で秘密鍵を用いて復号化
    5. ファームウェアが復号化され、ユーザ・フラッシュに格納

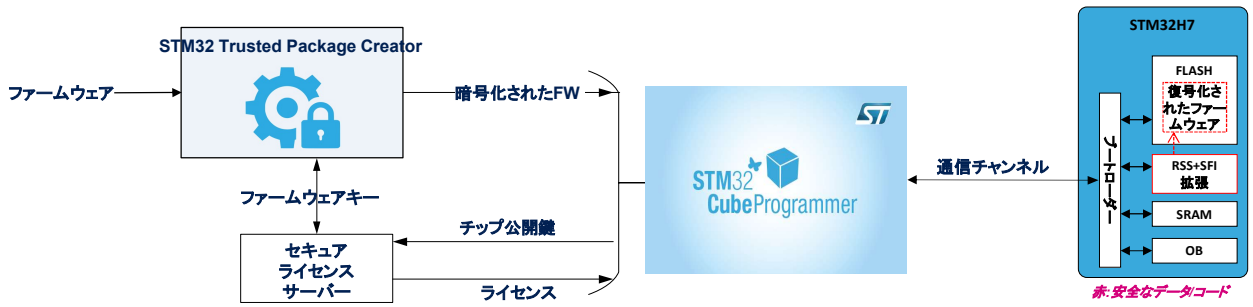


life.augmented

このスライドでは、セキュア・ファームウェア・インストール(SFI)である主なRSSサービスについて説明します。
SFIは、安全でない製造段階において、ファームウェアをデバイスに安全に転送するために使用されます。ファームウェアは、暗号アルゴリズムによってコピーや過剰生産から保護されます。
各STM32H7デバイスは、デバイスの認証とファームウェアの機密性のために、STMicroelectronicsによってチップ非対称キー・ペアと証明書が提供されます。
デバイスの秘密キーはセキュアシステムフラッシュに埋め込まれ、ST RSSサービスのみがアクセスできます。
SFI暗号化フローについては、このイメージで説明します。
まず、ファームウェアは、Galoisカウンターモード(AES-GCM)で高度暗号化標準で暗号化されます。
次に、ファームウェアの暗号化鍵とデバイスの公開鍵から、デバイスのファームウェアライセンスが生成されます。このライセンスは、対象のデバイスでのみ使用できます。
最後に、暗号化されたファームウェアはデバイスに転送され、ユーザのFlashメモリに格納される前に復号化されます。

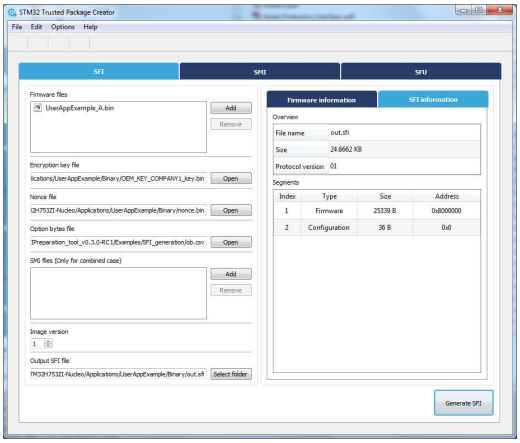
セキュア·ファームウェアのインストール(2/4)

- SFIの手順:
  - ファームウェア暗号化ツール:**STM32 Trusted Package Creator**
  - ファームウェア·ライセンス用のセキュアなサーバまたはハードウェア·セキュア·マシン(HSM)
  - SFIサービスのRSSと通信するためのフラッシャ·ツール:**STM32CubeProgrammer**



前のスライドで紹介した暗号化データの流れには、ファームウェアの暗号化ツール、デバイスに関連付けられたファームウェアライセンスを生成するライセンスサーバー、デバイスのブートローダーを介してSFIシーケンスを実行するフラッシャーツールなど、特定のツールが必要です。

セキュア・ファームウェアのインストール(3/4)



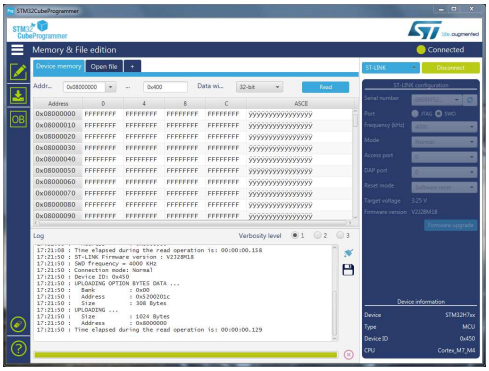
- STM32 Trusted Package Creator
  - AES-GCMアルゴリズムによるファームウェア・イメージの暗号化
    - AES-GCMはイメージを暗号化し、認証
    - ツール出力:暗号化されたFW、FWタグ、ヘッダMAC
  - SFIとSMIの同じツール / アルゴリズム
  - セキュア・ライセンス・サーバ
    - このツールはOEMの責任下で使用
    - 信頼されていない製造環境からOEMの秘密を保護（ファームウェア・キー、ダウンロード・カウンタ...）
    - OEMのファームウェア・キーとチップの公開鍵からファームウェア・ライセンスを生成

life.augmented

STM32 Trusted Package Creatorは、AES-GCMアルゴリズムを実装し、正しいヘッダとオプション・バイトの記述を持つ暗号化されたファームウェア・イメージを生成します。
また、ファームウェアアップデート用のサードパーティモジュールにも使用できます。
デバイス証明書とファームウェアキーからライセンスを生成するには、セキュアライセンスサーバーが必要です。このサーバーは製品の所有者の責任下にあり、製品メーカーがアクセスします。

セキュア･ファームウェアのインストール(4/4)

- STM32CubeProgrammer
  - UART、USB（ブートローダ経由）、JTAGおよびSWDインタフェースを介してSTM32デバイスのプログラミングを可能にする新しいSTツール（ST-Linkユーティリティの置き換え）
  - SFI/SMI手順
    - SFIシーケンスのデータとコマンドの取得と送信
    - STM32CubeProgrammerのコマンドライン･インタフェース（CLI）で利用可能



プログラミングツールは、デバイスのブートローダとそのRSS拡張機能を使用して、SFIシーケンスを駆動します。このツールは、デバイス証明書を取得し、ライセンスサーバーからファームウェアライセンスを取得し、暗号化されたファームウェアをデバイスに転送します。
STのプログラミングツール「STM32CubeProgrammer」をST.comで入手するか、当社のパートナーのものをご利用ください。

関連ペリフェラル

- このペリフェラルに関連するトレーニングをご参照ください:
  - メモリ保護

メモリアーキテクチャ、オプションバイト、Flashの操作方法については、Flashメモリ保護トレーニングをご参照ください。

参照

- 詳細は、以下のリソースをご参照ください
  - アプリケーションノートAN2606: STM32 microcontroller system memory boot mode
  - アプリケーションノートAN4992: STM32H753xI secure firmware install (SFI) overview.
  - アプリケーションノートAN5156: Introduction to STM32 microcontrollers security
  - ユーザマニュアルUM2237: STM32CubeProgrammer software description
  - ユーザマニュアルUM2238: STM32 Trusted Package Creator software description

life.augmented

RSSの概念については、以下のアプリケーションノートや取扱説明書で詳しく説明されています。
•アプリケーションノートAN2606は、ブートローダ機能について説明しています。
•アプリケーションノートAN4992は、SFI手順について詳しく説明しています。
STM32CubeProgrammerおよびSTM32 Trusted Package Creatorのユーザ・マニュアルは、STのウェブサイトでもご覧いただけます。