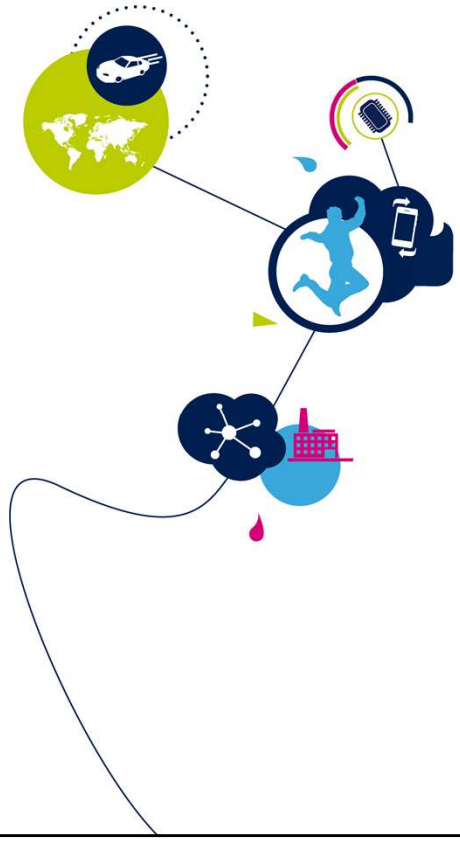
STM32WB - RSS

ルートセキュリティサービス

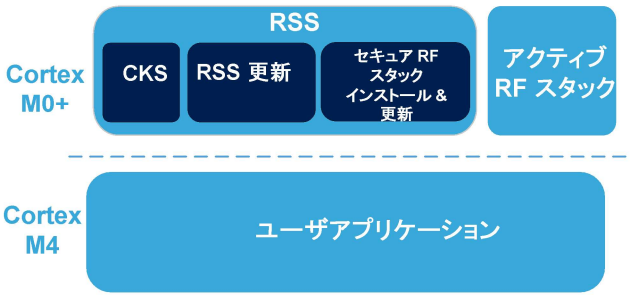
1.0 版



life.augmented

STM32WB ルートセキュリティサービス機能のプレゼンテーションにようこそ。

概要



- RSS サービス
  - ワイヤレススタックのセキュアなインストールと更新
    - ST とユーザによるデュアル認証
  - セキュアな RSS 更新
  - 暗号鍵ストレージ
    - セキュアなメモリに最大 100 個までの AES キーを格納
    - ユーザファームウェアによるキーの直接操作を防止

アプリケーション側の利点

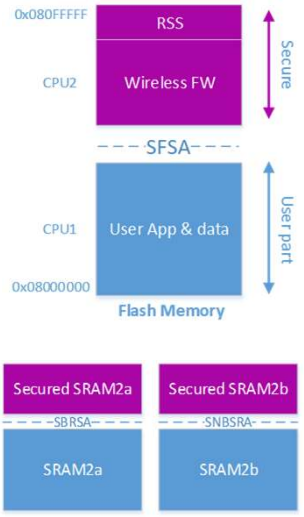
- デバイス寿命の間、最高のワイヤレス性能と最新のセキュリティレベルを維持可能
- セキュア CM0+ 側のアプリケーションキーのストレージ

life.augmented

ルートセキュリティサービス（RSS）とは、Cortex®M0+ コアによって実行される保護されたファームウェアのことです。ワイヤレススタックのインストールと更新を暗号メカニズムを用いてセキュアに行い、その完全性と認証を保証するために用いられます。ワイヤレススタックの更新は、デバイスの寿命全体を通じて最高の性能とセキュリティレベルを保証する鍵です。
ワイヤレスワームウェアの認証は、デフォルトで STMicroelectronics によって取得されます。ただし、ユーザによって二重認証を追加できます。
RSS ファームウェア自体は更新可能です。
RSS によって、暗号鍵を格納するセキュアなスロットが得られます。そうすることで、値に直接アクセスすることなく、ユーザによる秘密鍵の提供と使用が可能となります。

Cortex® M0+ コード保護

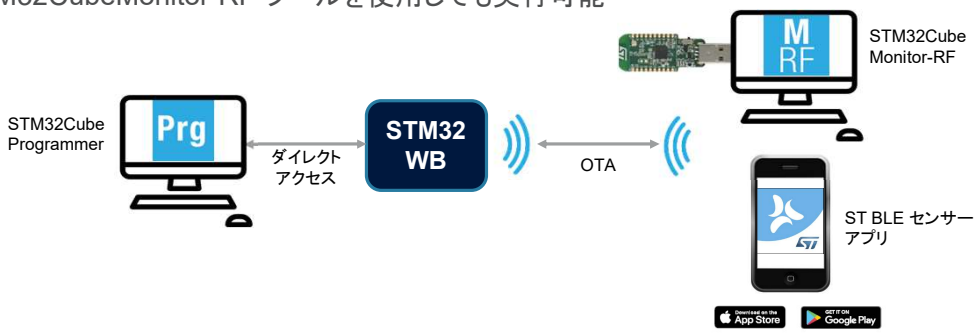
- RSS とアクティブワイヤレススタックは、セキュア Flash メモリの一部
  - それらのコードとデータは Cortex M4（CPU1）とデバッグポートからアクセス不可。
  - 実行データは SRAM2 の保護部分に格納。
  - そのデータは Cortex M0+（CPU2）のみによって実行。
- RSS とワイヤレススタックは排他的
  - ワイヤレススタックが存在しない場合、RSS はデフォルトで アクティブ。
  - そうではない場合、ワイヤレススタックが実行中。
  - 以下のいずれかによってリクエストされたときに CPU2 が RSS をオン。
    - ブートローダコマンドから
    - IPCC メッセージ（メールボックス）経由でユーザアプリケーションから



RSS ファームウェアとワイヤレススタックは、暗号化データが組み込まれた機密コードです。したがって、CortexM0+ コアのみがアクセス可能な Flash メモリのセキュア部分に格納されます。
このメモリ部分に格納されているコードとデータは、Cortex M4 コア上で動作するどのアプリケーションからもアクセスできません。さらに、デバッグポートからもアクセスできません。実行に必要な揮発性データも、SRAM2 メモリのセキュア部分に保護されます。
RSS ファームウェアとワイヤレススタックは排他的です。Cortex M0+ コアはどちらか一方を実行可能です。デフォルトで、ワイヤレススタックがインストールされていない場合には RSS がアクティブとなります。初回のインストールの後、ワイヤレススタックがアクティブになります。RSS への新規アクセスは、ブートローダコマンドか、プロセッサ間通信コントローラ（IPCC）を通じたアプリケーションメッセージかによって与えられます。

ダイレクトアクセスと OTA

- ワイヤレススタックは 2 つの方法で更新可能
  - ダイレクトアクセス
    - ユーザメモリ空間を節約：新しいスタックをインストールする前に現在のスタックを削除
    - ダイレクトアクセスはブートローダと STM32CubeProgrammer ツールから行われる
  - 無線通信でのアップデート(Over-the-Air: OTA)
    - デバイスへの物理アクセスが可能ではない場合にワイヤレス更新が可能
    - 更新クライアントとしてモバイルアプリの使用が可能ST BLE センサーアプリ
    - STM32CubeMonitor-RF ツールを使用しても実行可能



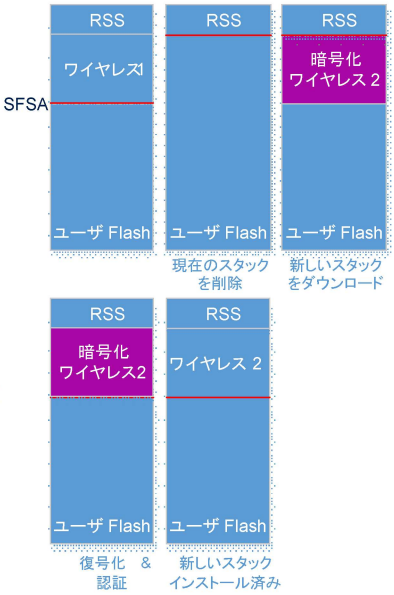
life.augmented

ワイヤレススタックは、デバイスへの物理的（有線）リンクの有無に応じて、2 種類の方法で更新できます。
ブートローダを使用するための物理的リンク経由のダイレクトアクセスによって、ワイヤレススタックの初回インストールが可能です。
その後は、現在のスタックを最初に削除することでスタックの更新が可能ですので、操作に必要なメモリ量が削減されます。
Flash メモリには、スタック 1 つ分に足りる空間しかありません。
STM32CubeProgrammer ツールを使用すると、ブートローダと専用コマンドにダイレクトアクセスできます。
ワイヤレススタックを更新する 2 番目の方法は、OTA で行うものです。これには、新しいワイヤレススタックのダウンロードに、現在のスタックを使う必要があります。すなわち、更新のために Flash メモリ境域が余分に使用可能である必要があります。
STM32Cube ファームウェアパッケージの中には、OTA アプリケーションの例が格納されています。新しいファームウェアは、ST BLE センサーモバイルアプリか、STM32CubeMonitor-RF ツールと BLE ドングルかどちらかを使ってダウンロードできます。

ワイヤレススタックの更新

ダイレクトアクセス

- 更新手順
  1. 現在のスタックは RSS コマンドによって削除。
     - 現在のスタックの空間は、次のダウンロードのために開放。
     - ワイヤレス接続はこれ以上不可。
  2. 暗号化されたスタックが使用可能なユーザ領域にダウンロード。
     - CPU1 アプリケーション、SWD/JTAGまたはブートローダによる
  3. 保護がワイヤレススタックまで拡張。
  4. 暗号化されたスタックが復号化され、RSS によって認証。
  5. 新しいスタックヘッダに応じて、セキュリティオプションバイトが RSS によりセット。
  6. CPU2 は新しいワイヤレススタックを実行する準備OK。

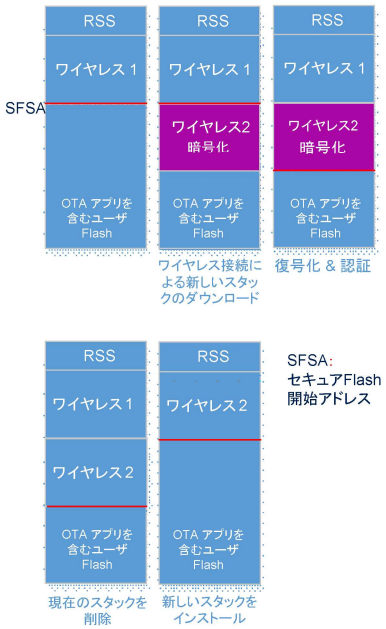


このスライドには、ワイヤレススタックを更新するダイレクトアクセスの手順が示されています。
この手順は、ブートローダから更新コマンドが送信されると、RSS ファームウェアによって自動的に実行されます。
最初に、現在のワイヤレススタックが削除されます。次に、暗号化と署名が行われた新しいワイヤレススタックが Flash メモリにダウンロードされます。
機密性のある操作である復号化、完全性および認証性チェックは、保護された Flash メモリ領域内部の RSS ファームウェアによって実行されます。
手順の最終ステップにおいて、ワイヤレス実行設定に関連したオプションバイトが適切な値にセットされます。
手順の最後で、ワイヤレススタックがアクティブとなります。

ワイヤレススタックの更新

- 更新手順
  1. 新しいワイヤレススタックのダウンロードには次のものが必要。
     - OTA サービスを含むユーザアプリケーション
     - 現在アクティブなスタック（ワイヤレス 1）
     - 新しいスタック（ワイヤレス 2）の格納に使用できる十分なユーザメモリ
  2. 保護が新しいスタックまで拡張。
  3. 暗号化されたスタックが復号化され、RSS によって認証。
  4. 認証および整合性チェックの後、現在のスタックが削除され、新しいスタックと入れ替え。
  5. 新しいスタックヘッダに応じて、セキュリティオプションバイトが RSS によりセット。
  6. CPU2 は新しいワイヤレススタックを実行する準備OK。

OTA

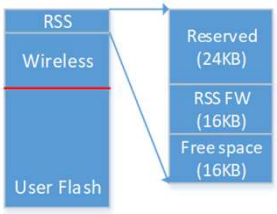


life.augmented

このスライドには、ワイヤレススタックを更新するOTAの手順が示されています。
この手順には、ユーザ側からリモートクライアントにダウンロードサービスを提供可能なワイヤレスアプリケーションが必要です。
このクライアントからのリクエストにより、ユーザアプリケーションは、新しいワイヤレススタックをデバイスの Flash メモリにダウンロードします。次に、RSS にメッセージを送信して更新手順を開始します。
暗号化と署名が行われた新しいワイヤレススタックが、復号化と認証が行われる前に Flash メモリにダウンロードされます。
チェックに合格したら、現在のスタックが削除され、新しいスタックと入れ替えられます。
手順の最終ステップにおいて、ワイヤレス実行設定に関連したオプションバイトが適切な値にセットされます。
手順の最後で、新しいワイヤレススタックがアクティブとなります。

RSS 更新

- RSS は以下の要素で構成。
  - 予約データ（最大 24KB）
  - RSS ファームウェア（最大 16KB）
  - RSS ファームウェア更新用空き空間（16KB）
    - この領域によって、ロールバック機能付きの RSS 更新可能。
- 更新手順
  - 現在の RSS ファームウェアは更新の間アクティブ。
  - 新しい RSS ファームウェアのダウンロードは、ダイレクトアクセスまたは OTA で実行可能。
  - 以前の RSS メモリ空間は将来の更新に利用可能。

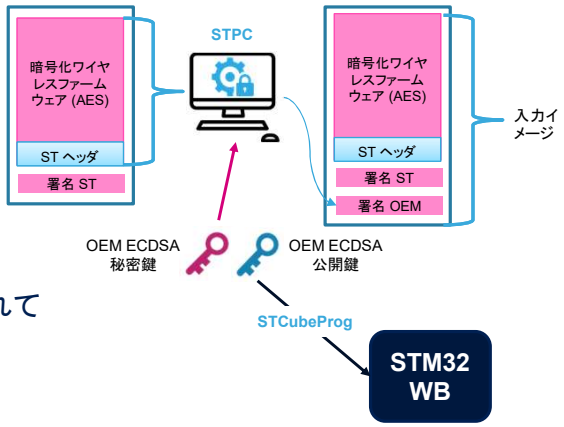


life.augmented

このスライドには、RSS ファームウェア更新手順が示されています。
RSS ファームウェア自体は更新可能です。RSS ファームウェア用として 2 つのスロットが利用可能です。1 つはアクティブな RSS コード用、もう 1 つは新しいコードのインストール用です。
有線接続経由か OTA によって、暗号化と署名が行われた新しい RSS ファームウェアがダウンロードされます。復号化と認証が行われると、新しい RSS がアクティブとなります。その後、古いものが削除され、そのスロットは将来の更新のために開放されます。

OEM ワイヤレススタック認証

- RSS 暗号化スキーム
  1. 暗号化
     - ワイヤレススタックは、ST によって AES アルゴリズムで暗号化。
  2. 認証
     - 第 1 レベル：ST 認証
     - オプションの第 2 レベル：OEM 認証
- ツール
  - ワイヤレススタックは、ST によって暗号化と署名が行われて配信。
  - 以下のものにより追加認証が提供。
    - 署名とイメージ作成のための STM32TrustedPackageCreator ツール
    - デバイス内部のセキュア領域に公開鍵をダウンロードするための STM32CubeProgrammer



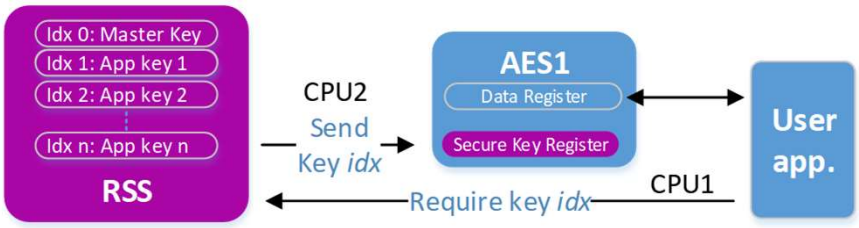
life.augmented

ワイヤレススタックは、ST によって開発と暗号化と署名が行われます。その暗号化は AES アルゴリズムによって保証されており、署名は楕円曲線アルゴリズムに依拠しています。2 番目の認証レベルをユーザが追加できます。特定のバージョンのワイヤレススタックのみをダウンロードできるようにするために、第2レベルの認証が必要になる場合があります。ユーザ認証では、同じ楕円曲線アルゴリズムが使われます。秘密鍵と公開鍵のペアが用いられます。秘密鍵は、STM32TrustedPackageCreator を用いてスタックイメージに署名するために使用されます。公開鍵は、STM32CubeProgrammer と特定の RSS サービスを用いて Flash メモリのセキュア部分に格納されます。

暗号化キーストレージ - CKS

AES1 HW IP を用いた方法

- AES 暗号鍵のセキュアストレージ
  - AES1 ハードウェア IP にはセキュアキーレジスタが存在。
    - Cortex M0（CPU2）のみがキー値にアクセス（読出し／書込み）可能。
    - AES データは、Cortex M4（CPU1）によってユーザアプリケーションに供給。
  - アプリケーションキー（128 または 256bit の AES）がセキュア Flash メモリ内部の RSS 領域に格納。
  - プロビジョニング後、アプリケーションキーはユーザの観点から単純インデックスで参照。

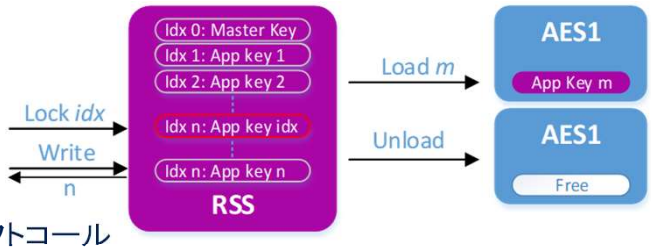


RSS によって、AES 暗号鍵を格納するセキュアなスロットが提供されます。
これらのキーは、AES1 IP とともに使用するためのものです。
このハードウェアブロックのキーレジスタは、セキュアな設定の Cortex M0+ のみがアクセス可能です。
データの AES1 ブロックが送信され、ユーザアプリケーションによってフェッチされる一方で、ユーザリクエストに応じて RSS によってキーレジスタがロードまたはアンロードされます。
ユーザの観点から、RSS 内部のインデックスでキーが参照され、その値には二度とアクセスできなくなります。

暗号化キーストレージ - CKS

プロビジョニングとコマンド

- キープロビジョニング
  - デバイス外：STM32CubeProgrammer
    - 平文フォーマット
    - 暗号フォーマット
      - マスタキーを最初にプロビジョニングする必要あり。
  - デバイス内：ユーザコードから RSS へのダイレクトコール



- CKS ランタイムサービス

CKS 機能	使用方法	引数
書込み	RSS 内部にキーを格納	入力： キータイプ 出力：キーインデックス
ロード	AES1 キーレジスタ内部の特定キーをロード	入力： キーインデックス
アンロード	AES1 キーレジスタから現在のキーを削除	なし
ロック	次回リセットまでキーの再使用を防止	入力： キーインデックス

life.augmented

STM32CubeProgrammer ツールを用いてデバイスブートローダにより、キーのプロビジョニングが可能です。
キーは、平文で送ることも、マスタ暗号鍵で最初に暗号化してから送ることもできます。このマスタキーは、安全な場所ですでにプロビジョニングされています。
アプリケーションの実行時に、プロビジョニングを含むすべてのルートセキュアサービスが使用可能です。キー管理には、以下の 4 つのサービスがユーザアプリケーションに提供されています。

- 追加のキーを格納するための書込みサービス
- AES1 キーレジスタをプログラミングするためのロードサービス
- AES1 をクリアするためのアンロードサービス
- 次回リセットまである特定のキーの別プロセスによる再使用を防止するロックサービスこのサービスは、ユーザセキュアブートアプリケーションなどによって使用できます。

関連資料

- この機能に関連した以下のトレーニングとアプリケーションノートを参照してください。
  - オンライントレーニングモジュール
    - 「STM32WB-システム-CM0+ セキュリティ」モジュール
    - 「STM32WB-セキュリティ-メモリ保護」モジュール
  - アプリケーションノート
    - AN5185 “STM32WB ST Firmware Upgrade Services”
    - AN5247 “STM32WB: application and wireless firmware update on-the-air (OTA)”

life.augmented

このトレーニングに加えて、Flash メモリインタフェースとシステム設定トレーニングが役に立つことがわかるでしょう。