こんにちは。このプレゼンテーションでは、STM32U5 への TF-M の実装に関連するドキュメントや URL へのリファレンスについて説明します。

U5 TFM ポインタ

- ドキュメント
  - [AN5156]：アプリケーションノート - Introduction to STM32 microcontrollers security
  - [AN4992]：アプリケーションノート - STM32 MCU セキュア・ファームウェア・インストール（SFI）の概要
  - [UM2851]：ユーザ マニュアル - Getting started with STM32CubeU5 TFM application
  - [UM2852]：ユーザ マニュアル - STM32U585xx security guidance for PSA Certified™ Level 3 with SESIP Profile
- STM32CubeU5 で使用可能な B-U585I-IOT02A ディスカバリ・ボードのアプリケーション例が利用可能
  - TFM の例
  - SBSFU の例

life.augmented

ST は、STM32U5 への TF-M の実装について記載のあるいくつかのドキュメントをリリースしています。
アプリケーションノート 5156 では、STM32 マイクロコントローラのセキュリティの基本について説明します。
アプリケーションノート 4995 では、STM32U5 で使用可能なセキュアファームウェアインストール（SFI）機能について記載があります。
ユーザマニュアル UM 2851 では、STM32CubeU5 マイクロコントローラ・パッケージの一部として提供される STM32CubeU5 TFM アプリケーションの使用開始方法について説明しています。
ユーザマニュアル UM 2852 では、STM32CubeU5 マイクロコントローラ・パッケージに含まれている STM32Cube_FW_U585_Security_certification_V1.0.0 ソフトウェア・パッケージを使用して、PSA レベル 3 用の SESIP プロファイルに準拠したセキュアシステムソリューションを構築するために、STM32U5 マイクロコントローラを準備する方法について説明しています。
STM32U585AI マイクロコントローラが統合された B-U585I-IOT02A ボードは、セキュアサービスを使用して非セキュアアプリケーションを実装およびテストするためのハードウェア媒体として使用されますが、追加のセキュリティメカニズムをもたらすわけではありません。
B-U585I-IOT02A ボード用の STM32CubeU5 TFM アプリケーションと SBSFU アプリケーションの例が提供されています。
TFM ベースのアプリケーション例は、4 つの主要なソフトウェア・コンポーネントで構成されており、これらはインテグレータによってそれぞれのニーズに応じて設定できます。

- TFM_SBSFU_Boot：セキュア・ブートおよびセキュアファームウェア更新アプリケーション
- TFM_Loader：USART の Ymodem プロトコルに基づいたアプリケーションローダアプリケーション
- TFM_Appli_Secure：非セキュアユーザアプリケーションにセキュアサービスを提供するセキュアアプリケーション（実行時）
- TFM_Appli_NonSecure：非セキュアユーザアプリケーション

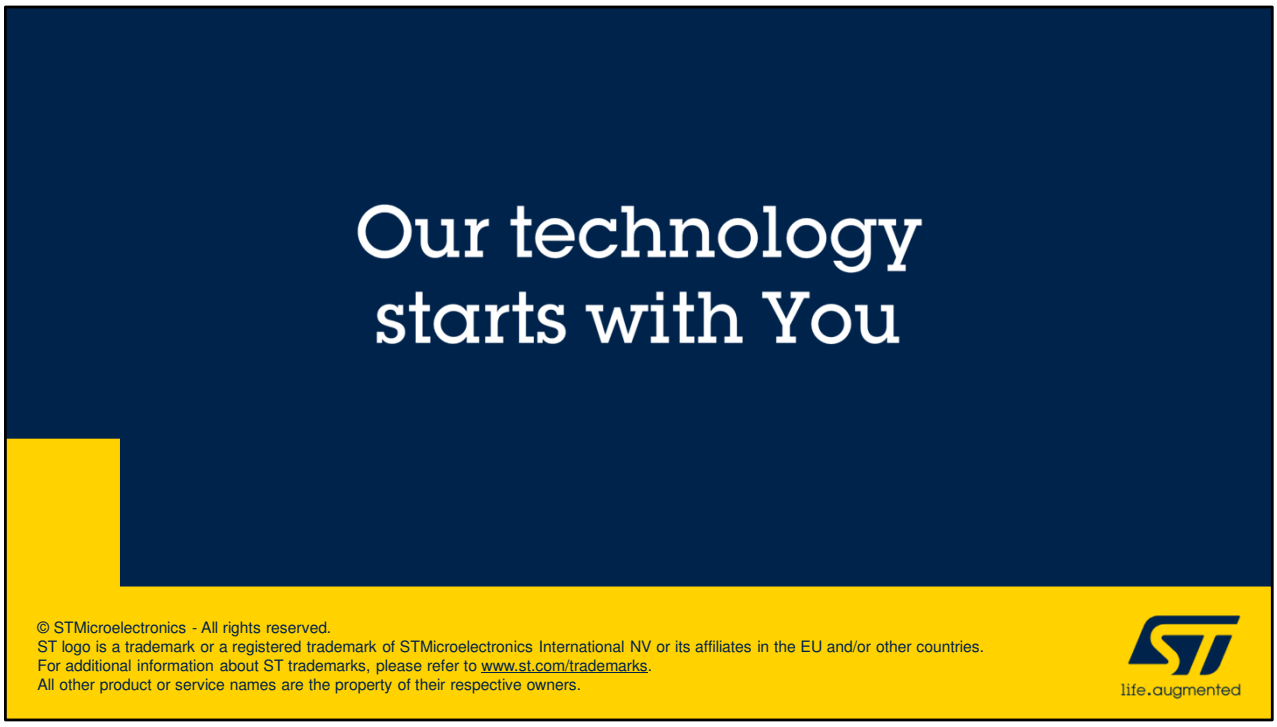
SBSFU アプリケーションは最小限で、TF-M のセキュア・ブートおよびセキュアファームウェア更新サービスのみを備えています。

U5 TFM ポインタ

- 公開されているドキュメントは、Trusted Firmware コミュニティのウェブサイト（www.trustedfirmware.org）からオンラインで入手可能
  - TF-M ユーザガイド v1.0：
    - リリース — Trusted Firmware-M 1.4.0+（gdcfab8ab）のドキュメント
- PSA 開発者向け API：
  - https://developer.arm.com/architectures/security-architectures/platform-security-architecture#implement

life.augmented

セキュリティ標準に関する知識を得るには、次のようなより一般的なドキュメントも役立ちます。
- TF-M User Guide for v1.0 およびすべてのリリース
- PSA 開発者向け API



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。
以降、TFM の仕組みについて詳しく説明した他のプレゼンテーションを参照できます。

- TFM Flash メモリのフットプリント
- STM32U5 での TFM のご提案