life.augmented

STM32U5

TFM の概要

Rev 1.0

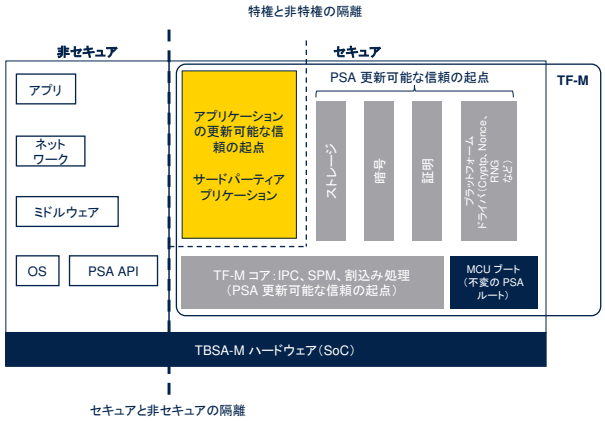
Trusted Firmware for Cortex-M（TFM）の概要へようこそ。

ARM TF-M の概要

PSA 標準の ARM オープンソースリファレンス実装 / セキュア OS の種類

- **TF-M（Trusted Firmware-M）：ARM の提供するオープンソース・ソフトウェアフレームワークは、ARM-CM33（TrustZone）コアでの PSA 標準のリファレンス実装を提供**
  - セキュアパーツ
    - PSA 不変 RoT（信頼の起点）：セキュア・ブート & セキュアファームウェア更新
    - PSA 更新可能な RoT：
      - セキュアな隔離設定、セキュアな IT 管理…
      - 不透明キー API に基づいたセキュアな暗号化サービス
      - ストレージ：NV Flash ストレージのデータの機密性/真正性/完全性を保護
      - 内部信頼ストレージサービス：NV セキュア/特権 Flash ストレージサービス
      - 証明：エンティティ認証トークンを介して製品の ID を証明します
    - アプリケーション 更新可能な RoT：サードパーティセキュアサービス
  - 非セキュア部分：セキュアサービスにアクセスするために PSA API を使用するユーザアプリケーション

TF-M TRUSTED FIRMWARE（https://www.trustedfirmware.org ）



life.augmented

TFM フレームワークは、セキュア・ブート、リセット後に実行されるセキュアファームウェア更新アプリケーション、および実行時に使用可能な一連のセキュアサービスで構成されています。
MCU-boot は信頼の起点で、不変であり、各リセット後に最初に実行されるコードです。
非セキュアアプリケーションと、セキュアアプリケーションの一部は、mcu_boot アプリケーションを介して更新できます。
TFM-core は、セキュアアプリケーション内の PSA レベル 2 の隔離を管理し、PSA API を介した非セキュアアプリケーションからセキュアサービスへのアクセスを制御します。
IoT アプリケーションからは、以下のセキュアサービスをリクエストできます。

- 暗号サービス
- セキュア・ストレージ
- 証明サービス

TFM はモジュール構成になっています。

- 灰色の各ボックスは（コンパイルスイッチを介して）個別に無効化できるため、MCU ブート部分のみが保持されるようにセキュアサービスを容易に削減できます。
- アプリケーションに必要な暗号化アルゴリズムのみがサポートされるように、セキュア暗号化サービスを設定できます。

TFM コアおよび TFM セキュアサービスは、PSA レベル 2 の認証要件に加え、物理的な攻撃に対する耐性を含む STM32U5 PSA レベル 3 の認証に使用されます。
これらは、STM32U5 シリーズで提供されるハードウェア保護（図では TBSA-M ハードウェア）に基づいています。

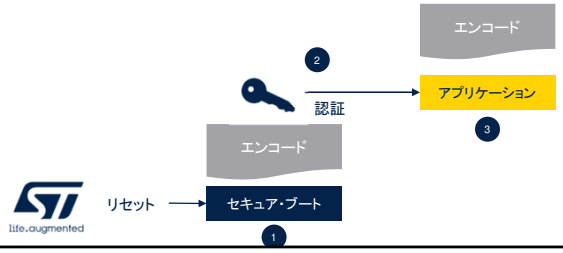
SBSFU サービス（PSA 不変 RoT）

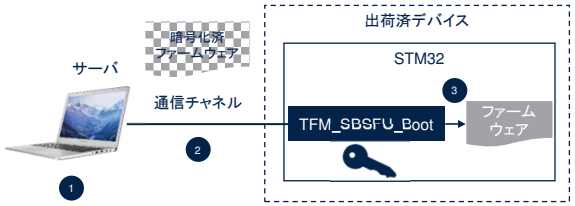
セキュア・ブート（SB）

- 暗号チェックに基づいて実行されるユーザ・アプリケーション・イメージの完全性と認証性を確認します
- Step1：SB により、最初の信頼できるコンポーネントとして信頼の起点を実装します。
- Step2：それ以外のすべてのコンポーネントが認証されます。
- Step3：信頼できる環境でユーザアプリケーションが実行されます

セキュアファームウェア更新（SFU）

- インフィールドファームウェア更新のセキュアな実装を提供します
- 新しいファームウェアイメージを安全な方法でデバイスにダウンロードします
- デバイスで新しいファームウェアイメージを認証、復号化、インストールし、実行します





3

実際の現場にあるデバイスは信頼できない環境で動作するため、脅威や攻撃の影響を受けます。
攻撃のリスクを低減させるために、認証されたファームウェアだけをマイクロコントローラ上で動作させることが目標となります。
セキュアファームウェア更新は、マイクロコントローラで使用可能な暗号化ファームウェアと SBSFU サービスを提供するサーバに依存します。
OEM サーバと Web サービスは、次の処理を行います。

- 新しいバージョンのデバイスファームウェアの格納
- デバイスとの通信、暗号化された状態での新しいイメージバージョンの送信

STM32U5 がフィールドに配備されます。ここには、ファームウェア更新プロセスを実行するコードが組み込まれています。
サーバと通信して新しいファームウェアイメージを受信し、認証と復号化を行い、実行前に新しいファームウェアイメージをインストールします。

実行時のセキュアサービス

SST：セキュア・ストレージ・サービス

- PSA 保護ストレージ API を実装します
- 非セキュア領域アクセスからの HW Flash の隔離に依存
- AES-GCM ベースの AEAD ポリシーに基づいてデータを暗号化
- 高レベル要件により以下に対応します
  - 機密性：HW/SW 攻撃に対する耐性
  - アクセス認証によりリクエスタの ID を確認
  - 完全性 - 耐タンパ性により悪質な HW/SW 攻撃を検出
  - 信頼性 - 電力障害シナリオおよび不完全な書込みサイクルへの耐性
  - 設定能力：モジュラ設定
  - 性能：リソースの制約に合わせた最適化

内部信頼ストレージサービス（ITS）

- PSA 内部信頼ストレージ API を実装します
- 非セキュア領域アクセスおよびアプリケーション更新可能な RoT からの HW Flash の隔離に依存
- 暗号化なし、最もセキュアな Flash 領域に配置
- 高レベル要件により以下に対応します
  - 機密性：HW/SW 攻撃に対する耐性
  - アクセス認証によりリクエスタの ID を確認
  - 完全性 - HW 隔離メカニズムによる、物理的なアクセスに基づく攻撃者からの改ざんへの耐性
  - 信頼性 - 電力障害シナリオおよび不完全な書込みサイクルへの耐性
  - 設定能力に基づいて、メモリ・フットプリントのスケールアップ/スケールダウン

life.augmented

4

TF-M セキュア・ストレージ（SST）サービスでは、PSA 保護ストレージ API を実装します。
このサービスは、Flash アクセスドメインのハードウェア隔離によってサポートされ、ハードウェアを利用して非セキュアアクセスから Flash 領域を隔離します。
SST サービスの現在の設計は、TF-M により提供されるハードウェア抽象化レベルに依存しています。
SST サービスでは、データの完全性と信頼性を保護するため、基準として、AES-GCM に基づく AEAD 暗号化ポリシーを実装します。
この設計は、次の高レベルの要件も満たしています。

- 機密性：ハードウェア/ソフトウェア攻撃による不正アクセスに対する耐性。
- アクセス認証：リクエスタ（非セキュアなエンティティ、セキュアなエンティティ、またはリモートサーバ）の ID を確立するためのメカニズム。
- 完全性：製品、パッケージ、またはシステムの通常ユーザや、これらに物理的にアクセスできる他の人による改ざんに対する耐性。セキュア・ストレージの内容が意図的に変更された場合、サービスにより検出できます。
- 信頼性：電源障害のシナリオおよび不完全な書込みサイクルに対する耐性。
- 設定能力：メモリ・フットプリントを増減する高度な設定能力により、さまざまなセキュリティ要件を持つさまざまなデバイスに対応します。
- 性能：シリコン・フットプリントが非常に小さく、リソースに制約のあるデバイスでの使用に最適化されているため、PPA（電力、性能、面積）は最適です。

TF-M 内部信頼ストレージ（ITS）サービスは、PSA 内部信頼ストレージ API を実装しており、ハードウェアセキュリティ保護メカニズムによって非セキュアまたは非特権アプリケーションから隔離された Flash メモリ領域に内蔵されたマイクロコントローラにデータを書き込むことができます。
この設計は、次の高レベルの要件も満たしています。

- 機密性：Flash アクセスドメインのハードウェア隔離に基づく、ハードウェア/ソフトウェア攻撃による不正アクセスへの耐性。
- アクセス認証：リクエスタ（非セキュアなエンティティ、セキュアなエンティティ、またはリモートサーバ）の ID を確立するためのメカニズム。
- 完全性：物理的にアクセスする攻撃者による改ざんへの耐性は、内部 Flash デバイス自体によって得られますが、非セキュアまたはアプリケーション更新可能な RoT の攻撃者による改ざんへの耐性は、ハードウェア隔離メカニズムによって得られます。
- 信頼性：電源障害のシナリオおよび不完全な書込みサイクルに対する耐性。
- 設定能力：メモリ・フットプリントを増減する高度な設定能力により、さまざまな要件を持つさまざまなデバイスに対応します。

実行時のセキュアサービス (2)

セキュア暗号サービス

- TF-M の PSA 更新可能な RoT セキュアパーティションで PSA 暗号化 API を提供します
- mbed-crypto に基づきます*。PSA 暗号化 API を参照
- セキュア処理環境（SPE）で実行されている他のサービスによって使用可能
- 非セキュア処理環境（NSPE）で実行されているアプリケーションによって使用可能

初期証明サービス（IAT）

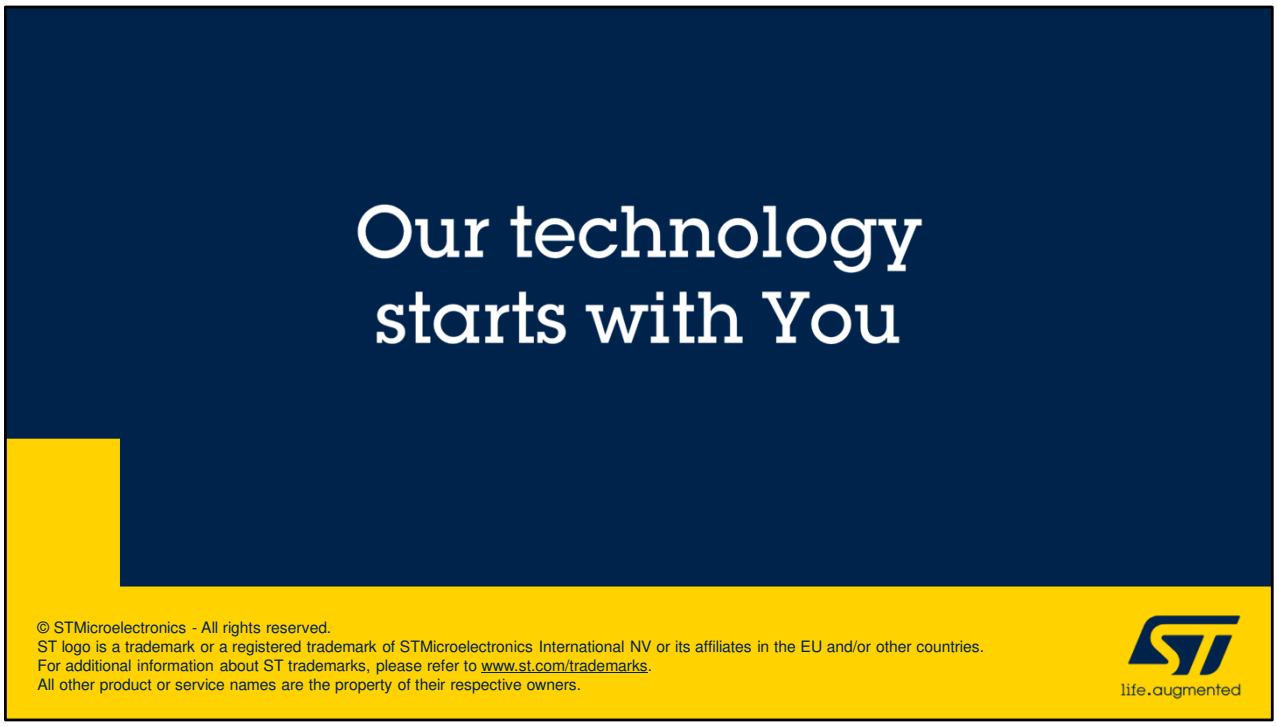
- TF-M 初期証明サービスにより、アプリケーションでは、認証プロセス中に、検証エンティティに対してデバイスの ID を証明できます
- 要求に応じて、デバイス固有データの固定セットを含むエンティティ証明トークン（EAT）を作成できます

* github.com/ARMmbed/mbed-crypto

life.augmented

5

TF-M 暗号化サービスでは、TF-M の PSA 更新可能な RoT セキュアパーティションにおける PSA 暗号化 API の実装を提供します。
これは、PSA 暗号化 API のリファレンス実装である mbed-crypto に基づいています。
PSA 暗号化 API または mbed-crypto 実装の詳細については、MbedCrypto GitHub リポジトリを直接参照してください。
暗号化の機能を提供するため、セキュア処理環境（SPE）で実行中の他のサービスや、非セキュア処理環境（NSPE）で実行中のアプリケーションでこのサービスを使用することができます。
TF-M 初期証明サービスにより、アプリケーションでは、認証プロセス中に、検証エンティティに対してデバイスの ID を証明できます。
初期証明サービスでは、要求に応じてエンティティ証明トークン（EAT）を作成できます。ここには、デバイス固有データの固定セットを含めることができます。
デバイスには、デバイス固有の証明キーペアが格納されている必要があります。
トークンは、証明キーペアの秘密部分を使用して署名されます。
キーペアの公開部分は、検証エンティティによって知られています。公開鍵は、トークンの信頼性を確認するために使用されます。
トークン内のデータ項目は、デバイスの完全性を確認し、信頼性を評価するために使用されます。証明キーの提供は、証明サービスの範囲を超えており、製品の製造中に行う必要があります。



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。
TFM の機能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。

- TFM Flash メモリのフットプリント
- STM32U5 の TFM 製品
- TFM ポインタ