STM32U5 セキュリティ認証のプレゼンテーションへようこそ。

STM32U5 PSA L3 および SESIP3 認定済み

- STM32U5 は Arm® Trusted Base System Architecture（TBSA）の要件に準拠し、Arm TrustZone® アーキテクチャを搭載
- STM32U585 は PSA レベル 3 および SESIP 3 の認証を受け、十分なレベルのサイバー保護を確認
- PSA L3 は PSA L2 のみを対象とした物理的攻撃とソフトウェア攻撃から保護する必要のある IoT デバイス用に設計（STM32L5 シリーズの場合）
  - PSA L3/SESIP3 によりキーセキュリティアプリケーションが許可
    - Payment Card Industry Security Standards Council（PCI SSC）に適合
    - すべてのセキュア IoT デバイスとアプリケーション …

life.augmented

STM32U5 は PSA レベル 3 および SESIP レベル 3 の認証を受け、論理的、ボード的、および基本的な物理的耐性のテストに合格し、十分なレベルのサイバー保護を確認しています。

- PSA レベル 3 は、Platform Security Architecture level 3（プラットフォーム・セキュリティ・アーキテクチャ・レベル 3）の略です。信頼を確立するチップのマルチレベル保証プログラムには、信頼できる機能をプラットフォームに提供する PSA 信頼の起点（PSA-RoT）と呼ばれるセキュリティコンポーネントが搭載されています。このマルチレベル方式は、デバイスメーカーと企業がユースケースに必要なセキュリティレベルが得られるように設計されています。
- SESIP レベル 3 は、Security Evaluation Standard for IoT Platforms（IoT プラットフォームのためのセキュリティ評価基準）の略です。GlobalPlatform によって公開された SESIP は、IoT プラットフォームのセキュリティの信頼できる評価の基準を定義したもので、さまざまな商品ドメインの要件を満たす上で再利用できるようになっています。SESIP 保証レベル 3（SESIP3）は、従来のホワイトボックス型脆弱性分析です。評価は、期限付きのソースコード分析と、期限付きの侵入テストを組み合わせて構成されています。

STM32U5 は、ARM Trusted Based System Architecture（TBSA）と呼ばれる ARM V8-M Trustzone テクノロジの要件と機能にも準拠しており、IoT デバイスのあらゆるコストポイントで堅牢なレベルの保護を実現しています。

この技術では、攻撃の可能性を低減するため、重要なセキュリティファームウェア、資産、個人情報をアプリケーションの他の部分から隔離しています。

セキュリティ認証の利点

- セキュリティの評価と認証にはどのような利点があるか?
  - ST の専門性の向上および強化が可能
  - STM32 のセキュリティの堅牢性について、測定可能なインジケータや証拠の提供が可能
  - セキュリティを扱う顧客の信頼および、認証プロセスの簡略化が可能
  - IOT セキュリティ・ワールドで汎用 MCU の基準として STM32 を確立

life.augmented

3

セキュリティ認証には次のような利点があります。

- 標準認証手順を通じて、ST の専門知識を向上させ、強化させることができます
- STM32 のセキュリティの堅牢性を証明します
- セキュリティを扱う顧客の信頼を得て、認証プロセスを容易にします
- STM32 を IoT セキュリティの世界におけるセキュリティ機能の基準として位置付けます。

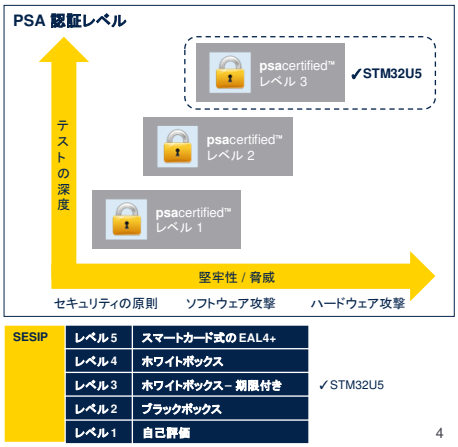
PSA/SESIP L3 セキュリティ機能

10 の PSA L3 セキュリティ機能：9 つの PSA L2 セキュリティ機能 + 物理攻撃への耐性

14 の SESIP3 セキュリティ機能は 9 つの PSA L2 セキュリティ機能に一致

- STM32U5 は PSA/SESIP L3 を実現するフルセットのセキュリティ機能を搭載
  - 暗号化アクセラレータ、セキュアデータストレージ、セキュアファームウェアのインストール、セキュア・ブート、およびセキュアファームウェア更新等の優れた機能
  - サイドチャネル解析（SCA）を使用した、攻撃に対する対称および非対称公開鍵アクセラレータ（AES、PKA）の暗号化の強化
  - セキュアデータストレージ用の独自のハードウェアキーと、内蔵のアクティブタンパ検出
  - 摂動攻撃の際に内部監視（タンパ）により機密データを消去
  - ハードウェア保護メカニズム（RDP、HDP、WRP など）のフルセット

life.augmented



SESIP		
	レベル 5	スマートカード式の EAL4+
	レベル 4	ホワイトボックス
	レベル 3	ホワイトボックス – 期限付き ✓STM32U5
	レベル 2	ブラックボックス
	レベル 1	自己評価

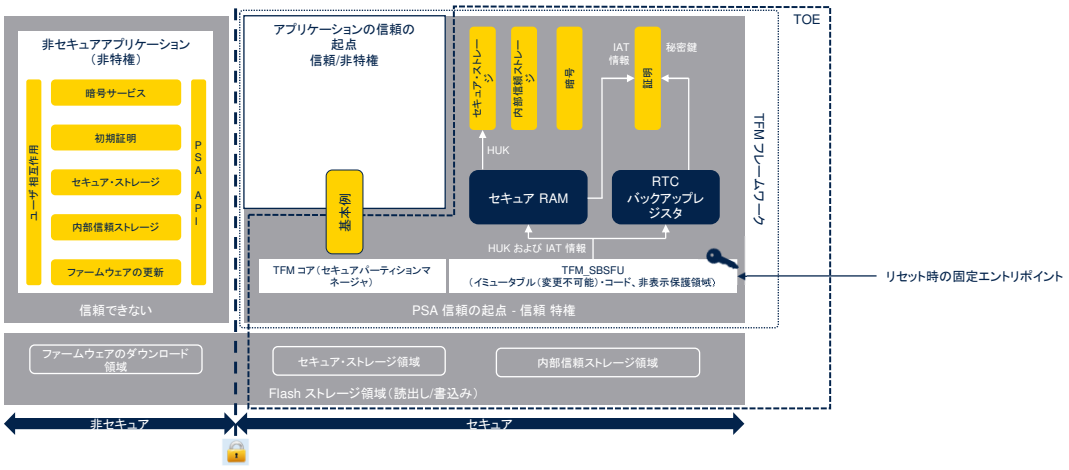
4

PSA レベル 3 および SESIP レベル 3 の認証に合格するため、STM32U5 には複数のセキュリティ機能が組み込まれています。
- 汎用暗号化アクセラレーション
- セキュア・ストレージ
- セキュアファームウェアのインストール
- セキュア・ブート

セキュア AES 256 ビットセキュリティコプロセッサは、サイドチャネルの対策と軽減に対応しています。
STM32U5 は、ハードウェアの不揮発性の固有の秘密鍵と、アプリケーション定義の揮発性ハードウェア秘密鍵を使用するオンチップ強化ストレージ技術を備えています。KEYSTOR というプレゼンテーションを参照できます。
バッテリ駆動式の揮発性セキュア・ストレージは、タンパが発生すると自動的に消去されます。ANTITAMP (アンチタンパー)プレゼンテーションを参照ください。
Flash メモリの内容を保護するために、複数のハードウェア保護メカニズムを利用できます。
- 読出し保護
- セキュア非表示保護
- 書込み保護

認証範囲/評価対象（TOE）

PSA L3 & SESIP3 の TOE：STM32U585 + フル TFM フレームワーク



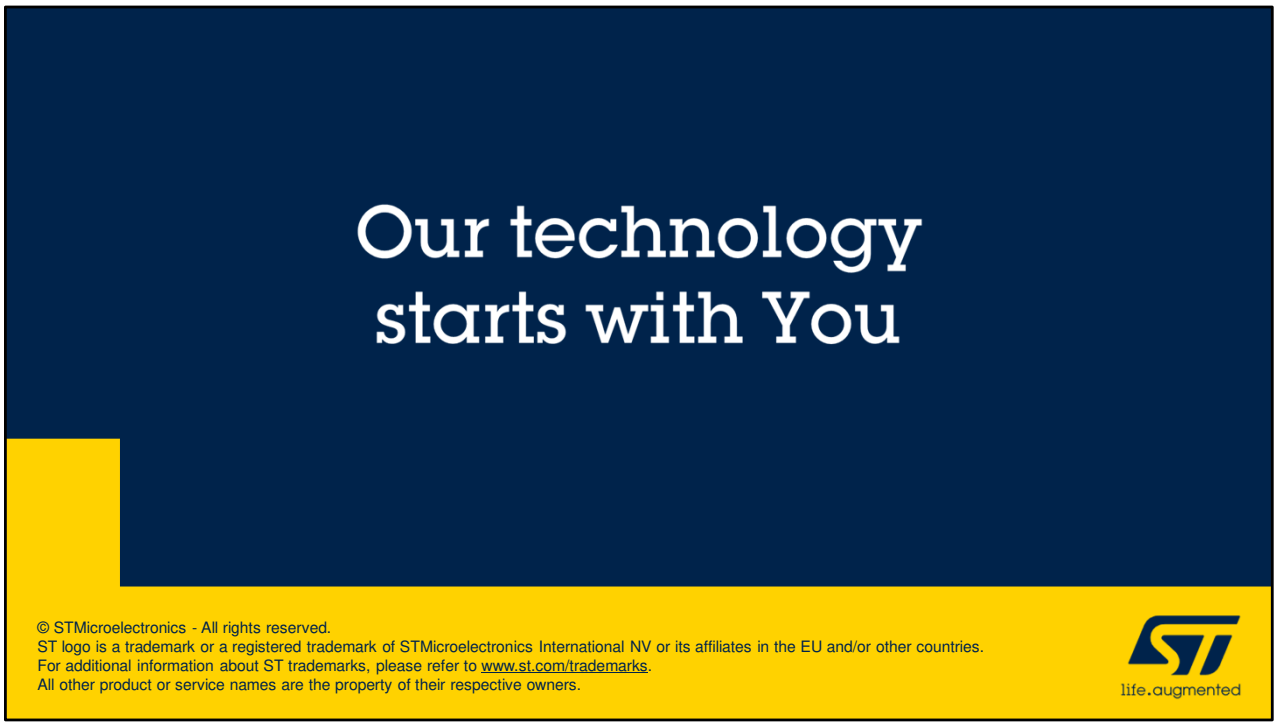
life.augmented

5

PSA 認証レベル 3 セキュリティ評価、または評価対象（TOE）の範囲は、PSA 認証済み仕様に準拠するデバイスをサポートするハードウェアとファームウェアのコンポーネントです。
セキュリティ評価の対象となるプラットフォームコンポーネントは、次のとおりです。

- ソフトウェア分離フレームワークなどの PSA の更新可能な信頼の起点。信頼性の高いソフトウェアを信頼性の低いソフトウェアから保護します。これは、バインディング、初期証明、汎用暗号化サービス、ファームウェア更新の検証などの汎用サービスに基づいています。
- PSA イミュータブルな信頼の起点、たとえばブート ROM、ルート機密情報と ID、隔離ハードウェア、セキュリティライフサイクルの管理と実施など。このコンポーネントは更新できません。
- PSA の信頼の起点で使用される信頼できるサブシステム、たとえばセキュリティサブシステム、信頼できるペリフェラルなど。ハードウェアとソフトウェアの両方のコンポーネントが評価の対象となります。

STM32U5 の認証は、STM32 ハードウェアとソフトウェアのフレームワークに基づきます。
このソフトウェアフレームワークは、CortexM（TFM）用の信頼できるファームウェア、ST セキュア・ブートおよびセキュアファームウェア更新（SBSFU）ソリューションに基づいています。
STM32U5 の TrustZone には、信頼できる環境と特権環境を組み合わせることで、より細かなレベルが用意されています。たとえば、ファームウェアは信頼できる特権環境に位置付けられる可能性が高く、アプリケーションの機密性の高い部分は信頼できるが非特権の領域で実行され、一般的なプログラムは信頼できない非特権システムで実行されます。モジュール性が高いため、安全性の低い環境での侵入があった場合に、機密コードの保護が容易にできます。



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。