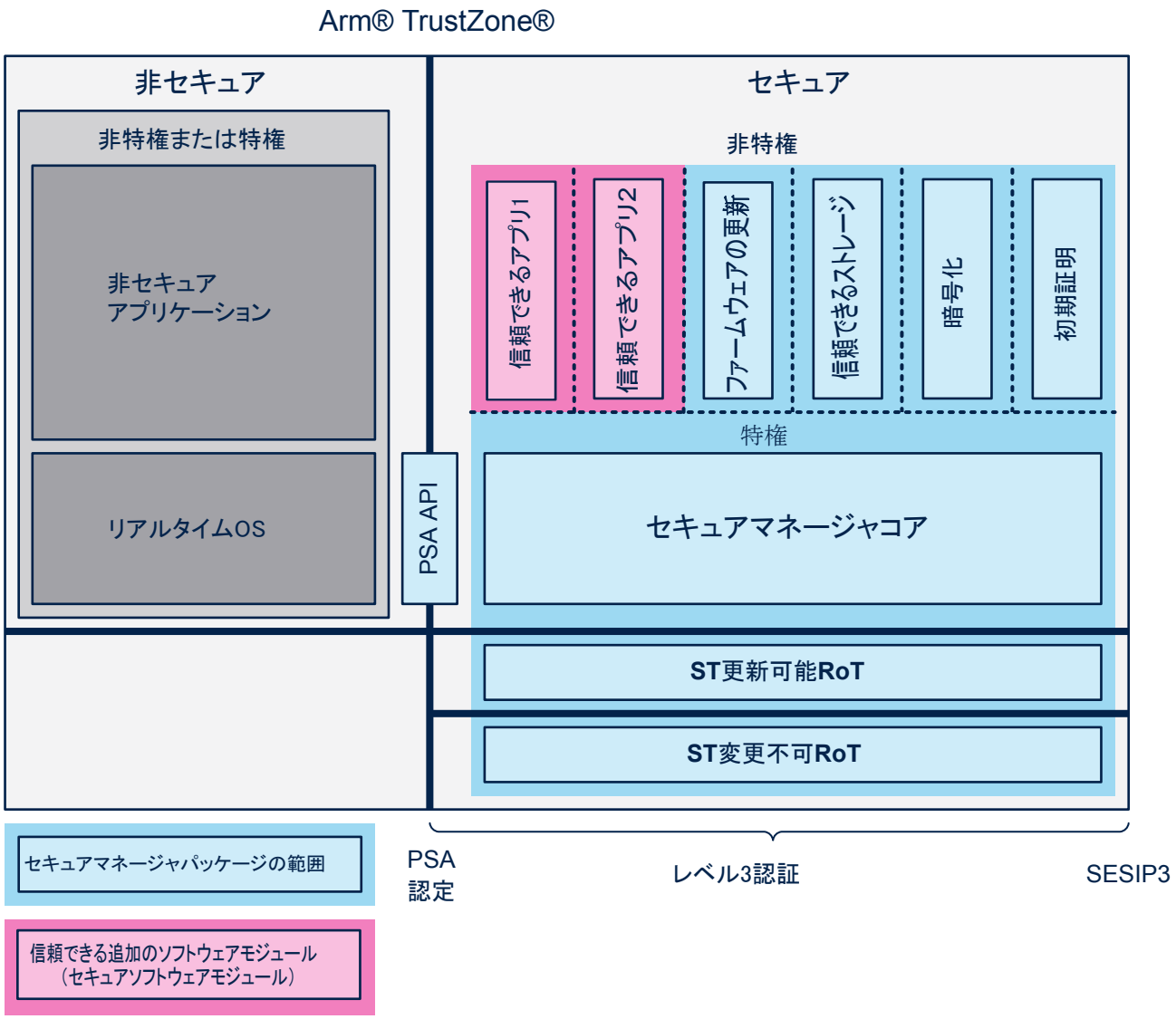
STM32TRUSTEE-SM

データ・ブリーフ

STM32Cube 組込みソフトウェア・セキュアマネージャ



製品ステータスのリンク
STM32TRUSTEE-SM

機能

- Arm® PSA 標準と API の準拠
- Arm® PSA サービス
  - セキュア·ブート
  - 信頼の基点 チップ分散型キーによる(RoT)
  - 暗号化機能
  - 信頼できる内蔵ストレージ (IT)
  - 初期証明 (IAT)
  - ファームウェア更新(FWU)
- ソフトウェア IP 保護(PSA の隔離レベル 3)
  - サンドボックスセキュアサービス
- セキュリティハードウェア
  - Arm® Cortex®-Arm® TrustZone®を備えた Arm® Cortex®-M33 Arm® TrustZone®
  - オプションバイト OB-Key セキュアシステム·キーストレージ(STiRoT、STuRoT、および証明キー)
  - 耐サイドチャネル暗号化アクセラレータ SAES および SPKA
  - 内部および外部イベントタンパ検出
  - TRNG NIST SP800-90B
  - 証明書によるデバッグ認証
- セキュリティ認証(ターゲット)
  - PSA Certified™レベル 3
  - GlobalPlatform SESIP3

説明

セキュリティはマイクロコントローラ市場の中心的な推進要因で、ユーザーにとっては複雑と感じられることがよくあります。

STM32Trust TEE セキュアマネージャ(STM32TRUSTEE-SM)は、組込みアプリケーションの開発を簡素化してセキュリティサービスがいつでも利用できるようにするための、システムオンチップ·セキュリティソリューションのスイートです。STM32 マイクロコントローラでは、STM32Trust TEE セキュアマネージャにより、ベストプラクティスに従って開発されたセキュリティサービスが提供され、開発者は独自のコードを記述したり検証したりすることから解放されます。

STM32Trust TEE セキュアマネージャでは、STM32Trust TEE セキュアマネージャ·アクセスキット(SMAK)と STM32Trust TEE セキュアモジュール開発キット(SMDK)という 2 種類のパッケージが提供されています。

STM32Trust TEE セキュアマネージャ·アクセスキット(SMAK)は STM32 製品へのインストールが製造ラインで容易にできます。いつでも使用できる高性能の認定済ソリューションで、Arm® PSA 仕様で定義された、セキュア·ブート、信頼の基点、暗号化、信頼できる内蔵ストレージ、初期証明、ファームウェア更新の機能に対応しています。

STM32Trust TEE SMAK バイナリコードは Arm® TrustZone®ハードウェアによって隔離され、その機能と、そこで管理／格納されるすべての OEM が利用可能なセキュア資格情報が保護されます。OEM では通常通り、アプリケーション·ファームウェアを開発、デバッグ、保護し、ST マイクロエレクトロニクスが提供する STM32Trust TEE SMAK 非セキュアリファレンスセキュアコードで定義された STM32Trust TEE SMAK セキュア関数をコールします(データ概要の開発キットセクションを参照してください)。

STM32Trust TEE セキュアマネージャソリューションは、STM32CubeMX 初期化コード発生ツール、STM32CubeIDE 統合開発環境、STM32CubeProgrammer(STM32CubeProg)プログラマを備えたグローバル STM32 エコシステムツールによってサポートされています。

STM32H573xx マイクロコントローラは STM32Trust TEE セキュアマネージャソリューションに対応する最初の製品です。ドキュメントとソフトウェアパッケージは STM32TRUSTEE-SM ウェブページからダウンロードしてください。操作と機能の追加説明が必要な場合、ST マイクロエレクトロニクス wiki セキュリティページ(wiki.st.com)から取得してください。STM32H573xx マイクロコントローラ用の STM32Trust TEE セキュアマネージャ·アクセスキット(SMAK)バイナリソフトウェアパッケージのリファレンスは X-CUBE-SEC-M-H5 です。このソフトウェアパッケージは輸出規制条件の対象になっています。ダウンロードする前に、「ソフトウェアの取得」の説明を確認してください。

STM32Trust TEE SMAK バイナリは、セキュアソフトウェアモジュールと呼ばれる、新しいセキュア関数によって補完でき、ST マイクロエレクトロニクスおよび、ソフトウェア知的財産の販売と保護を求める OEM、ST のパートナーによる開発が可能です。

STM32Trust TEE セキュアモジュール開発キット（SMDK）は、この新しい セキュアソフトウェアモジュールの開発を目的としています。ソフトウェアモジュールはシンプルな機能の場合もあれば複雑な機能の場合もあり、STM32 ペリフェラルおよびインタフェースへのアクセスが可能で、コードサイズが制限されています。OEM と ST のパートナーは、STM32Trust TEE SMDK を使用して、独自のソフトウェアモジュールを開発し、トレース付きでデバッグし、配布して、STM32Trust TEE SMAK のルールと隔離のもとでインストール、更新、実行することができます（データ概要の開発キットセクションを参照してください）。

STM32H573xx マイクロコントローラ用の STM32Trust TEE セキュアモジュール開発キット（SMDK）は、マスマーケットでは使用できません。特定のソフトウェア使用許諾契約に基づいて提供されます。詳細については、ST マイクロエレクトロニクスの代理店までお問い合わせください。使用に関する詳細は、ST マイクロエレクトロニクス wiki（wiki.st.com）のセキュリティセクションを参照してください。

該当する製品のリストは、データ概要の対応するセクションに記載されています。

1 一般情報

STM32Trust TEE セキュアマネージャ（STM32TRUSTEE-SM）に対応した STM32 32-bit マイクロコントローラは、Arm® TrustZone®を備えた Arm® Cortex®-M プロセッサに基づいています。

注 Arm および TrustZone は、米国内およびその他の地域にある Arm Limited 社（またはその子会社）の登録商標です。

arm

1.1 注文情報

STM32H573xx マイクロコントローラ用の STM32Trust TEE セキュアマネージャ・アクセスキット（SMAK）（X-CUBE-SEC-M-H5）は、www.st.com ウェブサイトの STM32TRUSTEE-SM ウェブページから無料でダウンロードできます。

注 X-CUBE-SEC-M-H5 は輸出規制条件の対象になっています。www.st.com からダウンロードする前に、「ソフトウェアの取得」の説明を確認してください。

STM32H573xx マイクロコントローラ用の STM32Trust TEE セキュアモジュール開発キット（SMDK）は、マスマーケットでは使用できません。特定のソフトウェア使用許諾契約に基づいて提供されます。詳細については、ST マイクロエレクトロニクスの代理店までお問い合わせください。

1.2 対象とする製品

表 1. 対象とする製品

セキュアマネージャ	マイクロコントローラ	組込み ソフトウェア
STM32Trust TEE SMAK パッケージ(1)	STM32H573xx	STM32CubeH5 X-CUBE-SEC-M-H5

1. 詳細は、ST マイクロエレクトロニクス wiki（wiki.st.com）のセキュリティセクションを参照してください。

1.3 ライセンス

STM32Trust TEE セキュアマネージャ・アクセスキット X-CUBE-SEC-M-H5 パッケージは SLA0048 ソフトウェア使用許諾契約に基づいて提供されます。セキュアマネージャバイナリは SLA0044 ソフトウェア使用許諾契約に基づいて提供されます。

1.4 開発キット

図 1 に、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開発するためのセキュアマネージャ・アクセスキットを示します。

図 1. 非セキュアアプリケーション用のセキュアマネージャ・アクセスキット

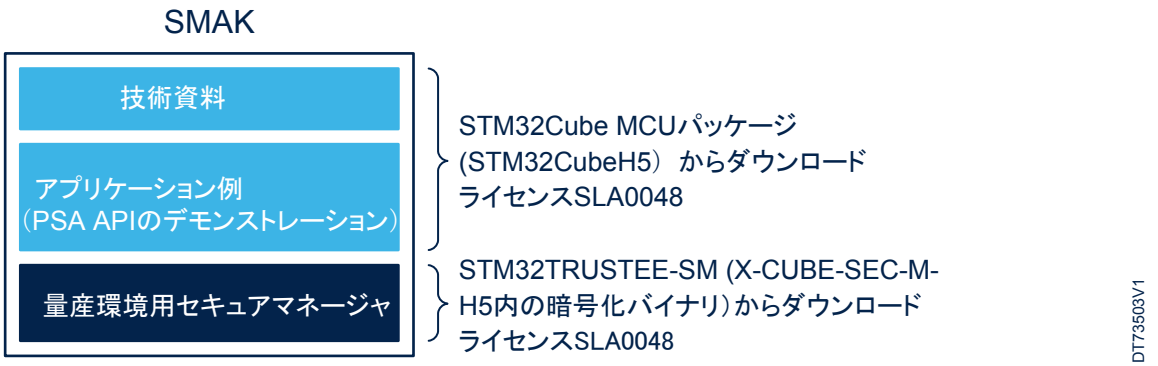
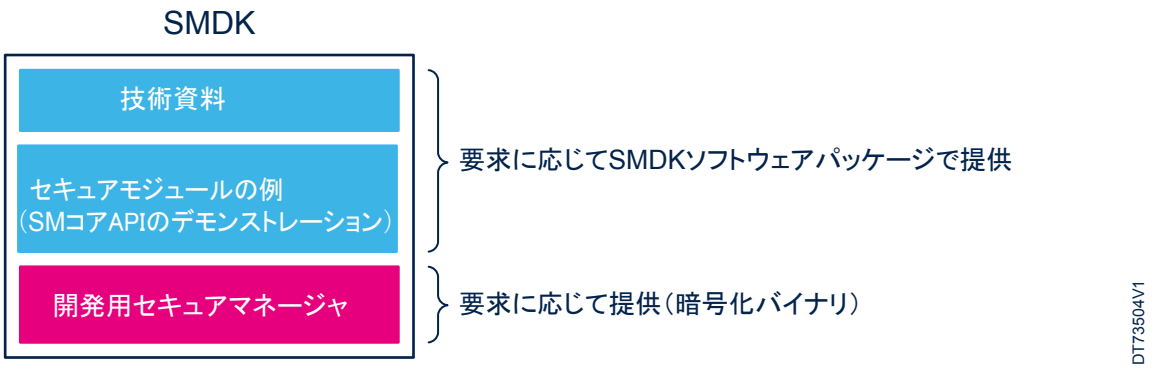


図 2 に、信頼できるアプリケーションを開発するためのセキュアモジュール開発キットを示します。

図 2. 信頼できるアプリケーション用のセキュアモジュール開発キット



1.5 STM32Cube とは

STM32Cube は開発の工数、時間、コストを削減して設計者の生産性を大幅に向上させるために STMicroelectronics が独自に提唱している取り組みです。STM32Cube は、STM32 のポートフォリオ全体に対応しています。

STM32Cube には、次の内容が含まれます。

- コンセプトから実現までのプロジェクト開発をカバーする扱いやすいソフトウェア開発ツール群:
  - STM32CubeMX:グラフィックウィザードにより初期化 C コードを自動的に生成する、グラフィックインタフェースを備えたソフトウェア設定ツール
  - STM32CubeIDE:ペリフェラル設定、コード生成、コードコンパイル、デバッグの機能を備えたオールインワンの開発ツール
  - STM32CubeProgrammer(STM32CubeProg):グラフィックバージョンとコマンドラインバージョンで使用できるプログラミングツール
  - STM32CubeMonitor(STM32CubeMonitor、STM32CubeMonPwr、stm32cubemonrf、STM32CubeMonUCPD):STM32 アプリケーションの挙動と性能をリアルタイムで微調整する強力な監視ツール
- STM32Cube MCU パッケージおよび MPU パッケージ:マイクロコントローラおよびマイクロプロセッサの各シリーズに特化した包括的な組込みソフトウェアプラットフォーム(STM32H5 シリーズの STM32CubeH5 など):
  - STM32Cube ハードウェア抽象化レイヤ(HAL):STM32 ポートフォリオの製品間で最大限の移植性を実現
  - STM32Cube 低階層 API:ユーザがハードウェアを高度に制御して最高のパフォーマンスとフットプリントを実現
  - ThreadX、FileX / LevelX、NetX Duo、USBX、USB PD、mbed-crypto、secure manager API、mcuboot、OpenBL などの一貫性のあるミドルウェアコンポーネント群
  - すべてのペリフェラル群と実用的なサンプルを備えた組込みソフトウェアユーティリティ
- STM32Cube MCU パッケージおよび MPU パッケージ の機能性を補完する組込みソフトウェアコンポーネントを含んだ STM32Cube 拡張パッケージ:
  - ミドルウェア拡張および実用的なレイヤ
  - 一部の STMicroelectronics 開発ボードで動作するサンプル

改版履歴

表 2. 文書改版履歴

日付	版	変更内容
2023 年 3 月 6 日	1	初版発行
2023 年 8 月 22 日	2	表紙の写真、説明、対象とする製品、およびライセンスを更新。 開発キットを追加。