STM32Trust

STM32のセキュリティを大幅に強化

STM32向け包括的なセキュリティ・エコシステム

STM32Trustは、STSAFEセキュア・エレメントで強化したSTM32マイコンおよびマイクロプロセッサ・ベースのシステムにおいて堅牢な多重構造のセキュリティを実現します。

また、STM32Trustは、STのノウハウやエコシステム、およびセキュリティ・サービスを組み合わせたセキュリティ・フレームワークです。

このソリューションは、コード・プロテクションおよび実行プロテクション用の包括的なツールセットの提供によりソフトウェアIPおよびデータの保護、および検証済みの認証情報の使用、ファームウェアの真正性確保とファームウェア更新のセキュリティ保護などを可能にします。

セキュリティ機能

STM32Trustは、ユーザ事例の精密な分析結果に基づき、そのニーズに必要とされる12のセキュリティ機能を提供します。

- セキュア・ブート
- セキュア・インストール/アップデート
- セキュア・ストレージ
- 分離
- 異常状況処理
- 暗号エンジン
- 監査 / ログ
- ID / 認証 / 証明書
- シリコン・デバイス・ライフサイクル
- ソフトウェアIP保護
- セキュア・マニュファクチャリング
- アプリケーション・ライフサイクル

www.st.com/stm32trust

1 セキュア・ブート
デバイスに内蔵されたアプリケーションの真正性と完全性を確保することが可能

2 セキュア・インストール / アップデート
ファームウェアのインストールやアップデートにおいて、プログラミングおよび実行前に完全性と真正性の初期チェックを実施

3 セキュア・ストレージ
データや鍵などの機密情報をセキュアに保存することが可能

4 分離
アプリケーションの中で信頼性の高い部分と低い部分を分離

5 異常状況処理
異常な状況（ハードウェアとソフトウェアの双方）を検出し、機密情報の削除など適切な対応をとることが可能

6 暗号エンジン
セキュリティ保証レベルの指針に従い、暗号アルゴリズムを処理することが可能

7 監査 / ログ
セキュリティ・イベントの記録を変更不可能な形で保持

8 ID / 認証 / 証明書
デバイスやソフトウェアの固有IDとその真正性を確認する機能をデバイスの内外に実装

9 シリコン・デバイス・ライフサイクル
状態を管理し、条件付き経路でシリコン・デバイス資産をセキュアに保護

10 ソフトウェアIP保護
特定のセクションやソフトウェア全体をチップ内外から保護する機能で、マルチテナント構成が可能

11 セキュア・マニュファクチャリング
セキュリティ保護されていない環境におけるデバイスの初期プロビジョニングに対応。不正な過剰生産を防止し、セキュアなパーソナライズが可能

12 アプリケーション・ライフサイクル
変更不可能な漸進的状態を定義し、アプリケーションの状態および資産をセキュアに保護

これら12のセキュリティ機能は、ハードウェアやソフトウェア・ツール、およびサービスの組合せにより、STが提供するソリューションにおいて包括的または部分的にサポートされます。

セキュリティ機能	STM32F4/F7/L1/WB/G0/G4/H7/L0/L4		STM32MP1		STM32L5 WITH TRUSTZONE		+ STSAFE-A/TPM
	デバイス	ファームウェア	デバイス	ファームウェア	デバイス	ファームウェア	デバイス
セキュア・ブート	✓	SBSFU	✓	TF-A	✓	TFM_SBSFU	✓
セキュア・インストール / アップデート	✓		✓	OPTEE	✓		✓
セキュア・ストレージ	(L0/L4/H7/G0/G4)	(WB) SBSFU KMS (L4)	✓	OPTEE	✓	TFM SPE	✓
分離	✓		✓	OPTEE	✓	TFM	✓
異常状況処理	✓		✓		✓		
暗号エンジン	✓	暗号ライブラリ	✓	OPTEE	✓	暗号ライブラリ TFM	✓
監査 / ログ					✓	TFM	
ID / 認証 / 証明書	✓		✓		✓	TFM 認証	✓
シリコン・デバイス・ライフサイクル	✓		✓		✓		
ソフトウェアIP保護	✓		✓	OPTEE	✓	TFM	
セキュア・マニュファクチャリング	SFI (H7/L4) with STM32HSM		SSP with STM32HSM		SFI with STM32HSM		✓
アプリケーション・ライフサイクル	✓		✓		✓		✓

* ソリューションの詳細はSTウェブサイトをご覧ください。www.st.com/stm32trust

ST製リファレンス・ファームウェア
ユーザにより開発されるファームウェア

認証

STは提供するソリューションについて、専門独立機関による認証の取得を実施しています。

詳細については、STウェブサイトをご覧ください。www.st.com/stm32trust

製品			
認定			評価
ARM PSA	共通基準	SESIP	PCI
• **レベル1** STM32L4 STM32L5 • **レベル2** STM32L5 (TFM) • **APIコンポーネント** STM32L5 (TFM)	• **CC EAL5+** STSAFE-A110 STSAFE-TPM	• **レベル1** STM32L4 (SBSFU) •**レベル3** STM32L4 (SBSFU)	• **POSアプリケーション** STM32L4

STマイクロエレクトロニクス株式会社 ■東京 TEL 03-5783-8200 ■大阪 TEL 06-6397-4130 ■名古屋 TEL 052-259-2725

life.augmented

Order code: FLSTM32TRUST0320J

詳細はSTウェブサイトをご覧ください：www.st.com/stm32trust