life.augmented

STSAFE-TPM

トラステッド・デバイスのための標準化ソリューション

パーソナル・コンピューティングからコネクテッド・デバイスへ信頼を拡張するTCG標準化プラットフォーム

STSAFE-TPMは、広く導入されている標準化されたトラステッド・プラットフォーム・モジュールで、パーソナル・コンピュータやサーバのセキュリティを確保するための鍵となるテクノロジーです。このソリューションは、WindowsおよびLinuxオペレーティング・システム上で構築されたエコシステムに最適です。

STSAFE-TPMセキュア・エレメントは、Common Criteria、TCG、およびFIPS認証を取得済みで、セキュリティおよび規制上の要件を満たします。この製品ファミリはST33ハードウェアをベースとし、民生用、産業用、および車載用アプリケーションに対応した仕様となっています。

利点

- LinuxおよびTCG TPMソフトウェア・スタックとの統合
- Common Criteria、TCG、およびFIPS認証取得
- 長期にわたる製品耐用期間（最大20年）
- 鍵および証明書ロード済みで提供

アプリケーション

- 産業用およびパーソナル・コンピューティング
- PC、サーバ、タブレット
- 周辺機器
- ネットワーク機器
  - ルータ、スイッチ
  - 基地局、アクセス・ポイント
- ホーム & ビル・オートメーション
  - ゲートウェイ
- 医療機器
- 車載用ソリューション

www.st.com/stsafe-tpm

STSAFE-TPMは、WindowsまたはLinuxベースのプラットフォームに最適な、標準化されたトラステッド・コンピューティング・サービス（ISO / IEC 11889）を提供する実績のあるソリューションです。

特徴

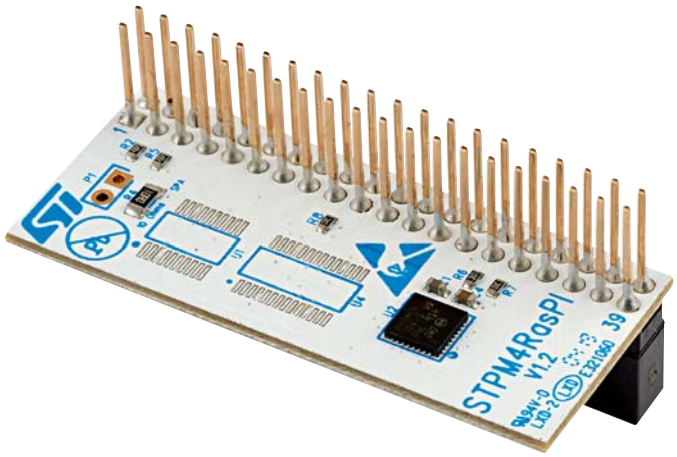
- ライフサイクルの長いデバイスに対応する拡張強化された暗号サポート（ECC384、SHA2-384、SHA3、AES 256）
- 耐障害性に優れたロード・プロセスでTPMファームウェア・アップグレードが可能
- TPMファームウェアと重要データの自己復旧（NIST SP800-193）
- 最高のCC保証レベル（AVA_VAN.5）での侵入テスト実施済み
- TCG準拠のSPIまたはI²Cインタフェース搭載
- 民生用 / AEC-Q100 / 産業用アプリケーションに対応
- 標準化、および小規模実装面積のパッケージ（WLCSPなど）対応
- 広い動作温度範囲（-40°C～105°C）

エコシステム

- 包括的な開発キットが用意され、容易な統合を実現
- Raspberry PI®とSTM32MP1マイクロプロセッサに対応した拡張ボード（STPM4RasPI）、SPIとI²Cの両インタフェース搭載
- ドライバとユーティリティ（通信ドライバおよびファームウェア・アップグレード）を含むソフトウェア・パッケージ
- WindowsとLinuxのサポート、TCGオープンソース、またはサードパーティ製TPMスタックによる円滑なシステム統合

認証

- 高度な攻撃能力に対する耐性（AVA_VAN.5）を備えたトラステッド・コンピューティング・グループのプロテクション・プロファイルに基づく初のCC認証TPM
- FIPS 140-2認証レベル2、物理セキュリティ・レベル3
- TCG認証



STPM4RasPI TPM拡張ボード

製品リスト

品名	アプリケーション分野	OS 対応	インタフェース	認証	パッケージオプション	動作温度範囲
ST33TPHF20/2E	TPM PC / サーバ、ネットワーク、プリンタ、IoT	TPM 1.2 / TPM 2.0	TCG SPI (33MHz) TCG I²C (400KHz)	CC EAL4+、TCG、FIPS 140-2	TSSOP28 VQFN32	-40 ~ +105°C
ST33TPHF2X		TPM 2.0		CC EAL4+ （高攻撃能力に対応）、 TCG、FIPS 140-2	VQFN32	
ST33GTPMA	車載用		TCG SPI (18MHz) TCG I²C (200KHz)		TSSOP20	
ST33GTPMI	産業用				WLCSP	

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: FLSTSAFETPM1120J

詳細は ST ウェブサイトをご覧ください：www.st.com