STSAFE™-TPM
標準化されたソリューションにより高い信頼性を実現

パーソナル・コンピューティングから接続型機器まで高い信頼性を幅広く提供

コンピューティング・プラットフォームのセキュリティとユーザの資産の保護は、接続型機器を設計するOEMだけでなく、個人のプライバシーやデータ保護に対する懸念を強めているエンド・ユーザにとっても非常に大きな課題になっています。
接続型コンスーマ機器や産業用IoT機器の普及が拡大するにつれて、この課題はさらに重要性を増します。
STSAFE-TPMは、STのセキュア・マイクロコントローラ・ハードウェアを使用して、トラステッド・コンピューティングにとって最も包括的でコスト効率の良いシステム・オン・チップ・ソリューションを提供します。

特徴

- TPM 1.2 & TPM 2.0ライブラリ
- TPM 1.2 & TPM 2.0スイッチ機能
- TPMファームウェア用のセキュア・フィールド・アップグレード・モード
- Common Criteria (CC) EAL4+、TCG、FIPS 140-2認定
- Windows 10 Redstone (RS) 認定
- Linux TPMドライバと互換
- 広い温度範囲 : -40°C ~ +105°C

利点

- ハイエンド・セキュア・マイコンが基盤
- 認定ハードウェア・ベースの信頼の根幹
- 大容量でセキュアなユーザ不揮発性メモリ
- 独立系認証局 (CA) によりルート署名されたTPM証明書
- シームレスな統合 (ISO / IEC 11889準拠)

アプリケーション

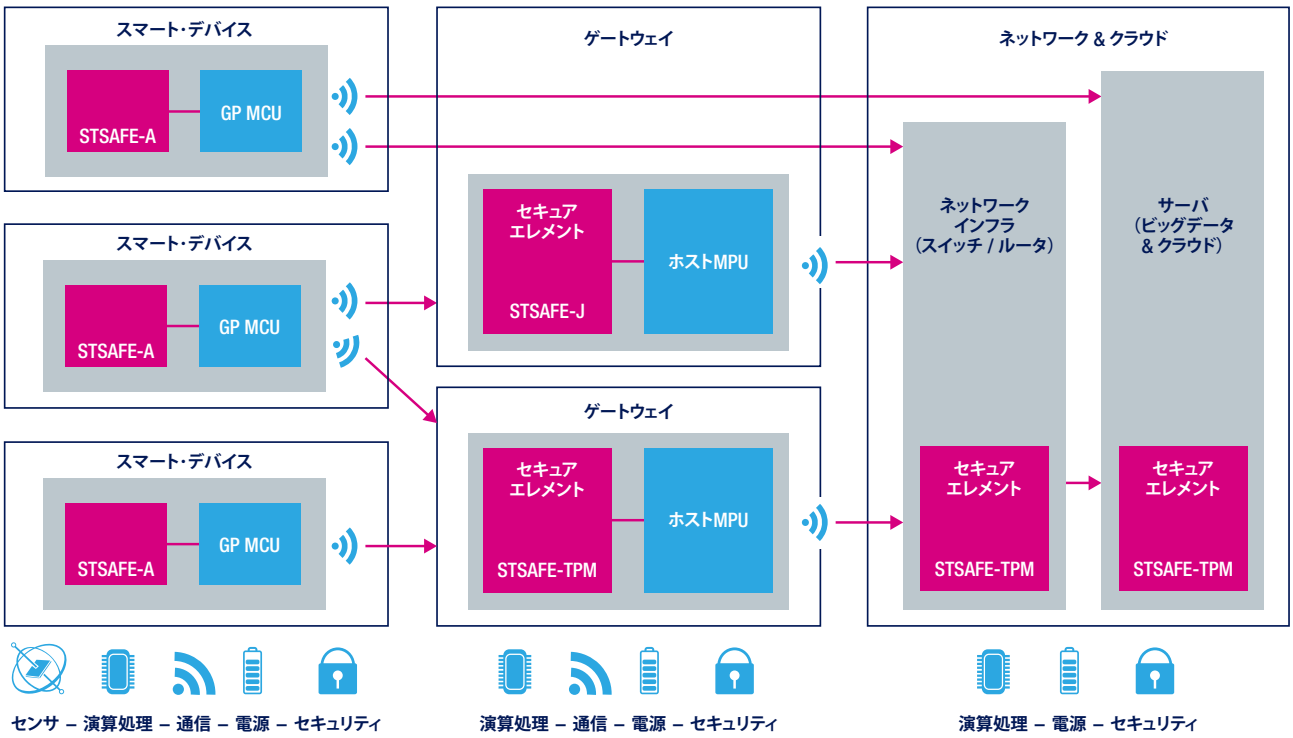
- パーソナル・コンピューティング
- パソコン、サーバ、タブレット
- 周辺機器
- 産業用コンピューティング
  - シングル・ボード・コンピュータ
  - プログラマブル・ロジック・コントローラ
- ネットワーク機器
  - ルータ、スイッチ
  - 基地局、アクセス・ポイント
- ホーム / ビル・オートメーション
  - ゲートウェイ
- 医療機器
- 車載ソリューション

STSAFE-TPM

トラステッド・コンピューティングのための標準化された認定ソリューション

コンピューティングは、もはや従来の単なるパーソナル・コンピュータだけの話ではありません。
今では、コネクティビティ機能をシステムに統合した新しいタイプの機器を含む形で市場は拡張しています。
その結果、これらの技術により普及率が高くなっていることも、セキュリティに対する新たな懸念をもたらしています。
100以上の業界リーダーで構成された国際的な標準化団体であるトラステッド・コンピューティング・グループ（TCG）は、機器の完全性や健全度チェック、強力なユーザ認証、セキュア・ネットワーク・アクセス、データと資産の保護等のセキュリティ課題などに対応するオープンな規格と仕様を提供しています。
STSAFE-TPM製品はTCGのトラステッド・プラットフォーム・モジュール（TPM）仕様に完全に準拠しており、Common Criteria EAL4+およびFIPS 140-2認証も取得しています。
このコスト効率に優れたシステム・オン・チップは様々なパッケージおよびインタフェースで提供され、あらゆる接続型機器に適合するために柔軟性の高いソリューションを提供します。STSAFE-TPM製品は広い産業用温度範囲での動作が認定されているため、市場で最も適切で包括的なTPM製品です。

STSAFE-TPMによる信頼点（トラスト・アンカー）の搭載例



製品ポートフォリオ

品　名*	TPM対応	TCGインタフェース	パッケージ	動作温度範囲	NVMサイズ
ST33TPHF2ESPI	TPM 1.2 / TPM 2.0	TCG SPI	TSSOP28、VFQFPN 32	-40 ~ +105°C	16KB/32KB
ST33TPHF20SPI	TPM 2.0	TCG SPI	TSSOP28、VFQFPN 32	-40 ~ +105°C	110KB
ST33TPHF2EI2C	TPM 1.2 / TPM 2.0	TCG I2C	TSSOP28、VFQFPN 32	-40 ~ +105°C	16KB/32KB
ST33TPHF20I2C	TPM 2.0	TCG I2C	TSSOP28、VFQFPN 32	-40 ~ +105°C	110KB

* 注記：この製品リストの品名は、注文用コードとは異なります。正式なオーダー・コードは各製品のデータシートをご確認いただくか、セールスオフィスまでお問い合わせください。

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