STSAFE
認証および
組み込みセキュリティ向け

目次

認証の概要

認証製品は、ブランド保護、プラットフォームの整合性、PCおよびITのセキュリティ、クラウドやリモート・サーバへのセキュアな接続に使用されるセキュア・エレメントです。

機密情報を保管して取り扱う優れた能力を持つ認証製品は、複製や盗難に対抗して、企業のイメージ、評判、収益の保護に貢献し、セキュアで信頼性の高いサービスを保証します。

ビジネスとブランドの保護

セキュリティの実装においては、単純なミスや誤ったデータ計測が外部からの攻撃（DoS:Denial of Serviceなど）につながり、ユーザの安全性やプライバシー、および企業のブランド・イメージなどに影響を与えてしまうリスクがあります。このようなリスクに対するブランド保護の実現をサポートするために、STは幅広い製品 / ソリューション・ポートフォリオや、包括的なハードウェア / ソフトウェア開発ツールを提供しています。

STのソリューションがセキュリティの脅威に対処する方法

脅威

- デバイスの複製または偽造
- デバイスの整合性またはデータの破損
- 機密情報の紛失

STのセキュア・エレメント

セキュリティ・サービス

- 認証、ユニークなID
- セキュアな通信
- プラットフォームの整合性
- 使用状況のモニタリング
- セキュア・ストレージ
- キーのプロビジョニング

セキュリティ・サービスの利点

- 収益の保護
- 評判
- サービスの継続性と信頼性
- お客様の資産とプライバシーの保護
- 規制への準拠
- セキュアなインフラストラクチャにおける追加投資の回避

STSECURE

140億以上の
出荷実績

STSAFEポートフォリオおよび市場

ブランド·プロテクションと組み込みシステム向けのスケーラブルなセキュリティ

STSAFEは、認証、機密性、プラットフォームの整合性といったサービスを提供するセキュア·エレメント製品です。製品の複製や偽造、マルウェア注入および無許可の生産を防止します。

最も厳しいセキュリティ認証に準拠したSTSAFEセキュア·エレメントは、事前にプロビジョニングされた機密情報や認証を使用し、信頼できるサプライ·チェーンを通して開発されたターンキー·ソリューションです。セキュアかつシームレスな統合を実現するためのソフトウェア·ライブラリやドライバのセットも併せて提供されています。

STSAFEが実現するエンド·ツー·エンドのセキュリティ

STは、セキュアで信頼性の高いシステムを構築するために、組み込みプラットフォームからゲートウェイやサーバまで、さまざまなアプリケーションに対応する、あらゆるタイプのセキュア·エレメントを提供しています。

デバイス設計に統合され、処理ユニットに接続されたSTSAFEセキュア·エレメントは、デバイスの認証を支援し、エンド·ツー·エンドのセキュリティによりプラットフォームの整合性とデータの機密性を確保します。

製品概要

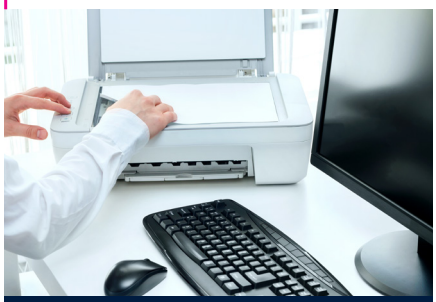
- STSAFE-A: 組み込みシステム向けに最適化
- STSAFE-J: Javaプラットフォームによる高い柔軟性
- STSAFE-TPM: トラステッド·コンピューティング向けに標準化

市場セグメントに対応するSTSAFEの位置付け

標準化されたSTSAFE-TPM
トラステッド·コンピューティングと組み込みシステム向けのTCG標準化プラットフォーム

柔軟性の高いSTSAFE-J
オプションのデフォルト·アプレットを備えた柔軟性の高いJava™プラットフォーム

最適化されたSTSAFE-A
ブランド·プロテクションとセキュアな接続向けに調整



コンスーマ
消耗品、アクセサリ、
プリンタ、コンピュータ

産業機器
環境センサ、アクチュエータ、
ファクトリ·オートメーション

インフラストラクチャ
ゲートウェイ、基地局、
ユーティリティ

STSAFE-A
最適化

CC EAL5+セキュア·エレメント上で動作するSTSAFE-Aは、独立した第三者機関によって認証されたセキュリティ機能を備えた、安全性の高い認証ソリューションです。

そのコマンド·セットは、強力なデバイス認証を確実にし、デバイスの使用状況のモニタリングと、ホストとのセキュアなチャネル確立(TLS)を容易に実現し、ホスト·プラットフォームの整合性を保護します。

利点

- 消耗品および小型プラットフォーム向けに最適化
- パーソナライゼーション·サービス
- STM32およびその他の汎用マイコンと互換性のあるライブラリを使用したシームレスな統合
- eDistributionにより入手可能
- HW CC EAL5+認証済み

STSAFE-A: ビジネスの価値を保護する最適なソリューション

シームレスなセキュリティを実現するSTSAFE-Aエコシステム

STSAFE-A製品ファミリは、純正の周辺機器やIoTデバイスの偽造を防止するための最先端のセキュリティ機能を備えたセキュアなソリューションです。

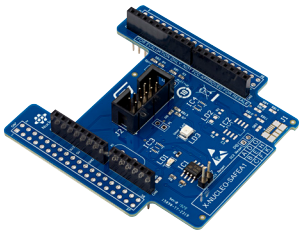
特徴

- 強力な認証(QI V2.0およびMatterに準拠)
- セキュアなチャネル確立(TLS)
- 署名検証
- デクリメント·カウンタ
- セキュアなデータ·ストレージ

エコシステム

STSAFE-Aエコシステムには、シームレスな統合のための以下のような幅広いツールが含まれています。

- ODE STM32拡張ボード (X-NUCLEO-SAFExx)
- STM32 Cube開発エコシステム (X-CUBE-SAFExxソフトウェア·パッケージ)
- 迅速な評価のために、パーソナライズ済みのSTSAFE-Aも利用可能
- STの工場でのお客様の証明書および構成のパーソナライゼーション·サービス(追加費用なし)



詳細はこちらwww.st.com/stsafe-a

製品概要

製品名	機能	インタフェース	セキュリティ認証	パッケージオプション	動作温度範囲	NVMストレージ
STSAFE-A110	• 強力な認証 • セキュアな接続の確立 • 使用状況のモニタリング • ホスト·プラットフォームの整合性検証	I²C	HW CC EAL5+	SO8N DFN8 2 x 3	-40～+105 °C	6 KB

STSAFE-J
柔軟性

STSAFE-Jは、Java Cardオペレーティング・システムに基づく柔軟性の高いソリューションであり、独自のアプレットを実行するお客様に幅広い自由度を提供します。

またSTSAFE-Jでは、ホスト・プラットフォーム上の安全性を確保する（強力な認証、セキュアな接続の確立、使用状況のモニタリング、プラットフォームの整合性）汎用アプレットもご利用いただけます。

利点

- STの汎用アプレットまたはお客様固有のアプレットによる柔軟性の高いJavaソリューション
- 標準的なマイコンおよびMPUと互換性のあるライブラリを使用したシームレスな統合
- HW CC EAL5+認証済み

STSAFE-J：柔軟性の高いJAVAプラットフォーム

認証済みプロテクション・プロファイルを備えたSTSAFE-J100

特徴

- CC EAL5+認証済みプラットフォーム
- Java 3.0.4およびGP 2.1.1認証済みプラットフォーム
- 汎用のSTアプレット：
  - 認証
  - セキュアな接続
  - セキュアなデータ・ストレージ
  - パーソナライゼーション・サービス
- お客様固有のアプレット

開発ツールおよびサービス

- STM32 NucleoボードおよびArduinoボードと互換性のある拡張ボード
- アプリケーション・マイコンに組み込むためのサンプル・コードとライブラリ（PKCS11ソフトウェア・パッケージ）

詳細はこちら**www.st.com/stsafe-j**

製品概要

製品名	OSサポート	インタフェース	セキュリティ認証	パッケージオプション	動作温度範囲	NVMストレージ
STSAFE-J100	GP 2.1.1 / JC 3.0.4	接触型ISO / IEC 7816、I²C	HW CC EAL5+	DFN8 VFQFPN32	-40〜+105 °C	80 KB

STSAFE-TPM
標準化

STSAFE-TPMファミリは、広く使用されて標準化されたTPM（Trusted Platform Module）であり、PCやサーバのセキュリティの基礎として機能します。

TPMはMicrosoft Windowsでは必須であり、Linuxオペレーティング・システムではネイティブにサポートされています。

Common Criteria、TCG、FIPSによる独立したセキュリティ認証は、高いレベルの信頼性を提供しており、規制要件を満たすために活用することができます。

ST33KTPM：コンスーマおよび産業システム向けの新世代TPM

パーソナル・コンピューティングからあらゆるコネクテッドデバイスまで対応する、信頼性が高く将来性のあるTrusted Platform Module

STSAFE-TPMファミリの最新製品であるST33KTPMは、性能の向上、セキュリティの強化、メモリ容量の拡張を実現しており、現在および将来のセキュリティ上の課題に効果的に対応します。ST33KTPMには、異なるインタフェースと製品寿命を持つ3種類の製品があり、あらゆるエコシステム要件に対応します。

利点

- 実績があり標準化されているセキュリティ・ソリューション
- Common Criteria、TCG、FIPS 140認証に基づく高い保証
- Windows、Linux OS、TCG TPMソフトウェア・スタックと簡単に統合可能
- 性能が向上した暗号化サービス
- 今後、新しく有効になる標準化機能および暗号機能にアップグレード可能なファームウェア

アプリケーション

- PC、ワークステーション
- サーバ
- ネットワーク機器
- ホームおよびビル・オートメーション
- POS（Point-Of-Sales）
- EV充電ステーション

ユース・ケース

- プラットフォームの信頼できるID
- デバイスの状態認証
- 偽造防止
- キーおよび重要データの保護
- 暗号化ツールボックス
- セキュアなチャネル通信（TLS）

エコシステム

- Raspberry PI®およびSTM32MPxマイクロプロセッサ用拡張ボード（SPIおよびI²Cインタフェース両方に対応）
- 各種ユース・ケースとユーティリティを備えたソフトウェア・パッケージ（ファームウェア・アップグレード）
- Windows HLK認証および主なLinuxディストリビューションのサポート

認証

ST33KTPM製品は、以下の認証を取得しています。

- TCGプロテクション・プロファイルに準拠したCommon Criteria認証EAL4+ に、潜在的に高い攻撃への耐性を追加（AVA_VAN.5）
- TCG認証

ST33KTPMは、以下の規格にも適合しています。

- FIPS 140-3 physical security level 3

認証状況を確認するには、関連ウェブサイトの認証製品リストを参照してください。

セキュリティ

ST33KTPM製品は、最先端の論理的および物理的攻撃に対する、高度なハードウェアおよびソフトウェアのセキュリティ保護機能を備えています。

アップグレード

ST33KTPM製品は、ファームウェアのアップグレードにより、以下の項目に対応するように設計されています。

- EV充電用標準規格ISO15118-20に対応した暗号化サービス
- 将来のTCG規格
- 耐量子暗号（SP800-108、FIPS 203および204）
- 新たなセキュリティ攻撃を阻止するためのセキュリティ改善

詳細はこちらwww.st.com/stsafe-tpm

特徴

- TCG TPM 2.0規格（リビジョン1.59）の最新仕様に対応
- 拡張暗号に対応（最大RSA 4096、ECC NIST P256およびP384、EC BN256、SHA1、SHA2-256および384、SHA3-256および384、AES 128-192-256）
- TCG準拠のSPIまたはI²Cインタフェースを動的に選択可能
- 不揮発性メモリ（200 KB）
- フォールト・トレラント・ローディング・プロセスによるTPMファームウェア・アップグレード
- TPMファームウェアおよび重要データ自己修復（NIST SP800-193）
- コンスーマおよび産業機器JESD-47認定
- 薄型標準パッケージUFQFPN32および小型フットプリント・パッケージWLCSP24で入手可能
- 拡張動作温度範囲（-40～105 °C）

製品リスト

品名	アプリケーション	TPMバージョン	インタフェース	パッケージ	認証	温度範囲[°C]	寿命
ST33KTPM2XSPI	コンスーマ	2.0 Rev 1.59	SPI	UFQFPN32	CC EAL4+ FIPS 140-3（物理的セキュリティ・レベル3）	-40～+150	10年
ST33KTPM2X	コンスーマ		SPIまたはI²C				
ST33KTPM2I	産業機器（JESD-47準拠）			UFQFPN32 WF WLCSP24			20年

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 052-587-4547
詳細はSTウェブサイトをご覧ください：www.st.com

Order code: BR2401STSAFEJ