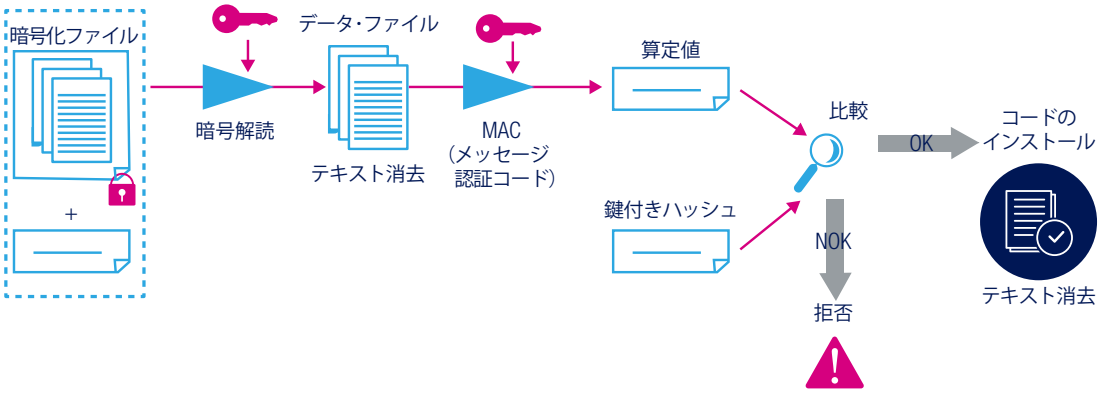
STM32でRoot of Trustを実現
セキュリティ・ソフトウェア・パッケージ

組込みアプリケーションのセキュア・ファームウェア・インストールおよびアップブレードを可能にするソリューション

X-CUBE-SBSFUセキュア・ブート & セキュア・ファームウェア・アップデート・ソリューションは、STM32マイクロコントローラの組込みプログラムをフィールドで新しいファームウェア・バージョンにアップデートし、新しい機能の追加やファームウェアの潜在的な問題の修正を可能にします。
アップデートのプロセスはセキュアな方法で実行され、不正なアップデートやデバイス内の機密データへの不正なアクセスを防ぎます。

特徴

- セキュア・ブート・モジュール
  - Root of Trustサービスによる実行
  - 実行前のアプリケーション認証と完全性チェック
- セキュア・ファームウェア・アップデート・モジュール
  - インストールする新しいFWバージョンの検出
  - FWバージョンの管理(不正なアップデートや不正なインストールのチェック)
- セキュア・エンジン・モジュール
  - ユーザ・アプリケーション・ソフトウェアの実行から隔離されたコード
  - 暗号アルゴリズムの実行専用
  - セキュア鍵ストレージの管理

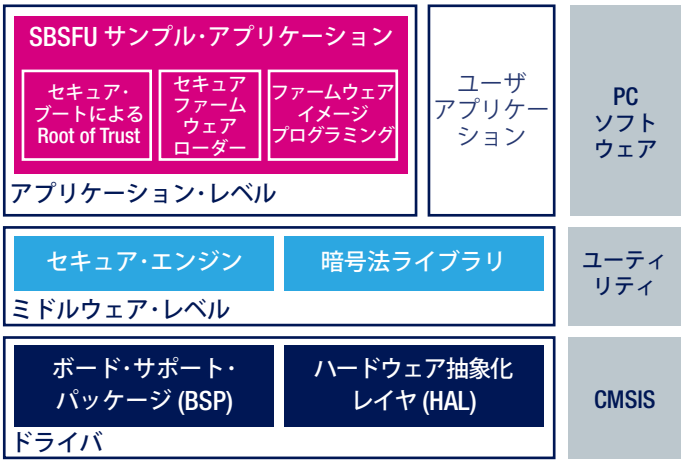


STM32Cube用セキュア・ブート & セキュア・ファームウェア・アップデート拡張パッケージ

セキュア・ブートによるRoot of Trustサービスは、STM32のセキュリティ・メカニズムをチェックおよびアクティベートし、実行前に毎回ユーザ・アプリケーション・コードの真正性と完全性をチェックして、無効または悪意のあるコードが実行される可能性がないことを保証します。
セキュア・ファームウェア・アップデート・アプリケーションは、暗号化されたファームウェア・イメージを受け取り、その真正性をチェックし、復号した後に、コードの完全性をチェックしてからインストールします。
X-CUBE-SBSFUはSTM32Cubeソフトウェア技術を基盤としているため、異なるSTM32マイコン間の移植が容易です。
このソフトウェア拡張パッケージは、STM32セキュリティ保護を実行するためのリファレンス・コードとして提供されます。
X-CUBE-SBSFU拡張パッケージには、STM32F4シリーズ、STM32F7シリーズ、STM32G0シリーズ、STM32G4シリーズ、STM32H7シリーズ、STM32L0シリーズ、STM32L4シリーズ、STM32WBシリーズで動作するサンプルが付随します。

詳細はこちら

アーキテクチャ概要



セキュリティ・レイヤ

アプリケーション
特徴 / サービス
通信 (TLS)

セキュリティ・サービス
セキュア・ブート、セキュア・ファームウェア更新

暗号機能
秘密性、安全性、可用性

マイコンの安全機能
ファイアウォール、PCROP、RDP、WRP、MPU

STM32対応表

X-CUBE-SBSFU STM32Cube 用 拡張ソフトウェア	STM32F4	STM32F7	STM32H7 デュアル シングル	STM32L0	STM32L1	STM32L4 STM32L4+	STM32G0	STM32G4	STM32WB
	ハイパフォーマンス・マイコン			超低消費電力マイコン			メインストリーム・マイコン		ワイヤレス・マイコン
セキュア・ブート	√	√	√	√	√	√	√	√	√ (M4)
セキュアFW更新	√	√	√	√	√	√	√	√	√ (M4)
セキュア・エンジン	√	√		√	√	√			
セキュア・キーストレージ						√			√ (Sec-M0)

ST コミュニティ

STM32ユーザ向けコミュニティで、質問したり、議論したり、色んなアイデアをシェアして、皆で一緒に取組みましょう。community.st.com/stm32

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