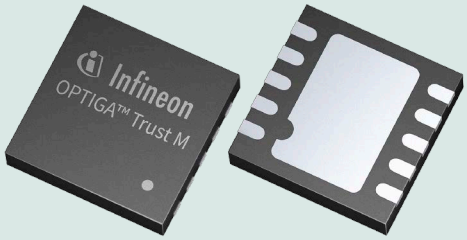

Open source

製品概要

OPTIGA™ Trust M

セキュアなクラウドサービスのプロビジョニング - 容易に実現可能！

クラウドサービスとAIが、革新的なアプリケーションの波を引き起こしています。こうしたアプリケーションに接続されるデバイスの数も増加しており、大きなチャンスがある一方で、セキュリティリスクも高まっています。

インフィニオンは、攻撃者の間で組込みシステムへの注目が高まっていることに対応して、コネクテッドデバイスに最適化されたハイエンドのセキュリティコントローラであるOPTIGA™ Trust Mソリューションを提供しています。OPTIGA™ Trust Mソリューションは、産業用、ビルディングオートメーション、スマートホーム、コンシューマーアプリケーション向けに、主要なクラウドプロバイダーへの極めて柔軟で高性能なセキュアアクセスを提供します。

ゼロタッチプロビジョニング

OPTIGA™ Trust Mは、クラウドへのセキュアな接続性を次のレベルへと引き上げます。事前にカスタマイズされた証明書により、あらゆる主要なクラウドサービスプロバイダーへの安全で高速かつ容易なアクセスを提供します。また、性能が大幅に向上することで、最高のユーザーエクスペリエンスを実現しています。

容易な実装

集積を迅速かつ容易に - 完全なシステム集積によるターンキーセットアップにより、設計、統合、導入の労力を最小限に抑えることができます。暗号化ツールボックスや保護されたI2Cインターフェースは、お客様の作業を簡素化するためのほんの一例です。

将来性のあるセキュリティ

有効期限を過ぎた証明書は無効にしなければなりません。OPTIGA™ Trust Mの証明書は、現場で安全に更新することができます。OPTIGA™ Trust Mは、すべてのIoTデバイスに独自のアイデンティティを与えます。証明書とキー ペアは最初からOPTIGA™ Trust Mに安全に保管されており、キー ペアはInfineonの安全な工場で安全に注入されます。

性能

お使いのデバイスの性能を向上させる必要がありますか？OPTIGA™ Trust Mは、ソフトウェアのみのソリューションに比べ、お客様のデバイスを最大10倍の速さでクラウドに接続します。

MITライセンスソフトウェア

オープンソースの利点：OPTIGA™ Trust Mのホストソフトウェアとドキュメントは GitHubで公開されています。開発者から直接サポートを受けたり、新バージョンや新機能のアップデートを受けることができます。

OPTIGA™ Trust Mは、簡単に実装でき、幅広いセキュリティ機能を備えているため、お客様のすべての組み込みプロジェクトに最適なソリューションです。

主な特長 [1)]

- CC EAL6+ (high) 認証済みのハイエンドセキュリティコントローラ
  - ECC：NIST推奨曲線のP-521まで対応、Brainpool楕円曲線暗号r1の512ビットまで対応
  - RSA® 暗号化キーは2048ビットまで対応
  - AES暗号化キーは256ビットまで対応、HMAC SHA-512に対応
  - TLS v1.2 PRFとHKDF、SHA-512まで対応
  - TRNG/DRNG
- シールドコネクション付きI2Cインターフェース
- 消費電力ゼロのハイバネートモード
- USON-10 パッケージ (3 x 3mm)
- 標準および拡張温度範囲：-40°C～+105°C
- 最大10 kBのユーザメモリー
  - 安全性が保護されたアップデート
  - アクセス回数カウンター
  - 動的オブジェクト (クレデンシャルなど) のロック
- 設定が可能なデバイスセキュリティ監視
- 産業用およびインフラ用アプリケーション向けとして最大20年の寿命
- SHA-256, ECC, RSA® , AES, HMACおよび鍵の導出用の暗号ツールボックスコマンド
- GitHub上のMIT認証ソフトウェアフレームワーク
  github.com/Infineon/optiga-trust-m

1) 最新の製品に適用される機能です

OPTIGA™ Trust M

セキュアなクラウドサービスのプロビジョニング - 容易に実現可能！

簡単に実装可能	› 短時間で簡単に実装できるターンキーソリューション › ゼロタッチプロビジョニング：チップごとにプログラムされている独自の認証情報 › GitHubから入手できるオープンソースコード
性能	› クラウドへの接続が、ソフトウェアのみのソリューションに比べて10倍以上高速
強化されたセキュリティ	› CC EAL6+ (high) 認証ハイエンド セキュリティ コントローラー › 高度な非対称暗号化 (ECC & RSA) をシングルチップソリューションで実現 › ホストとセキュリティコントローラー間でAES128-CCM暗号化通信
柔軟性	› あらかじめパーソナライズされた証明書により、あらゆるクラウドプロバイダーに迅速かつ容易にアクセス可能

製品概要

タイプ	説明	温度範囲 [°C]	パッケージ
SLS32AIA010MK	コネクテッドデバイス向け組み込みセキュリティ ソリューション	-25 ... +85	USON-10
SLS32AIA010ML	コネクテッドデバイス向け組み込みセキュリティ ソリューション	-40 ... +105	USON-10
評価キット	OPTIGA™ Trust M搭載XMC4800 IoT Connectivity Kit	–	ボード

OPTIGA™ Trustファミリーの製品

OPTIGA™ Trust Mは、インフィニオンのOPTIGA™ Trustファミリーの製品で、コネクテッドデバイスをターゲットにした幅広い組み込みセキュリティソリューションです。OPTIGA™ Trustファミリーには下記のような製品もあります。

- OPTIGA™ Trust B,は、デバイス認証やブランド保護に適した製品です。
- OPTIGA™ Trust Eは、デバイス認証とブランド保護向け強化されたセキュリティソリューションです。
- OPTIGA™ Trust Pは、Java Cardを使用したプログラムが可能なソリューションで、幅広いユースケースに対応します。
- OPTIGA™ Trust Xは、コネクテッドデバイス向けの拡張セキュリティソリューションです。

インフィニオンのOPTIGA™ファミリーは、組み込みシステムのセキュリティを確保するための製品とソリューションで構成されています。全製品がセキュリティ保護されたハードウェアとソフトウェアをベースにしています。この包括的な製品ファミリーには、トラステッド コンピューティング グループ (TCG) コンプライアンスを必要とする組み込み設計を対象としたOPTIGA™ TPM (Trusted Platform Module)などの製品があります。

約30年にわたりセキュリティ市場をリードし、全世界で270億個以上のセキュリティコントローラを出荷してきたインフィニオンは、その豊富な専門知識で、お客様のビジネスの成功要因にセキュリティを役立たせるため努力を続けています。

Published by
Infineon Technologies AG
81726 Munich, Germany

Document number: B189-I0824-V2-7600-EU-EC-P
Date: 11 / 2020