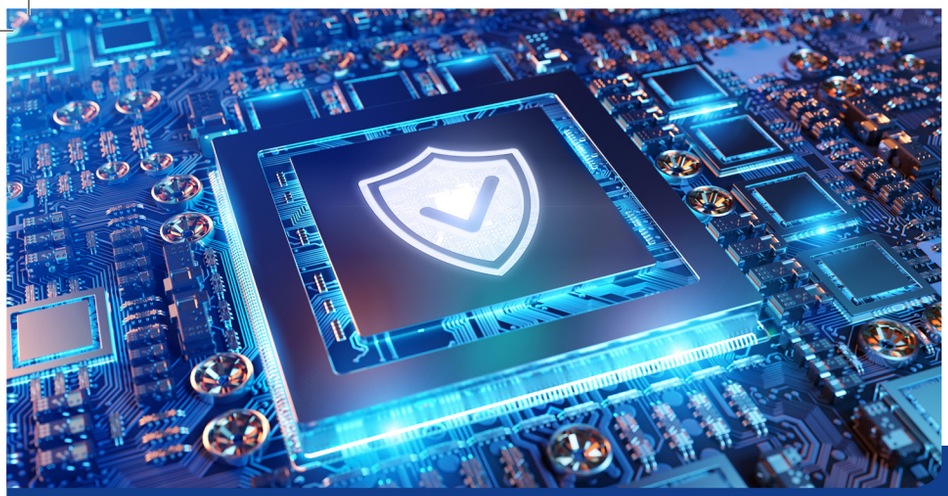

NXP EdgeLock™
SE050

ユース・ケース:
トラステッド・プラットフォーム・モジュール (TPM) を超える

リソースに制約のあるエッジ・デバイスが、軽量な実装で柔軟な暗号化機能を必要とする IoT では、パワフルな PC やタブレット・デバイスのアーキテクチャとライフサイクル向けに設計された従来の TPM は最良の選択とはならないかもしれません。TPM 機能を備えたセキュア・エレメントを採用することで、IoT の運用により適した方法で高レベルの保護を追加することができます。

アプリケーション

産業用 PLC

ロボット

センサ / アクチュエータ

課題

10 年以上にわたり、コンピューティング業界は、PC、ラップトップ、ネットワーク機器およびその他のコンピューティング・デバイスにハードウェア・ベースの保護を提供する「トラステッド・プラットフォーム・モジュール (TPM)」と呼ばれる特殊なタイプのセキュア暗号プロセッサに依存してきました。

コンピューティングでは、TPM は主に、ユーザーのパスワード保護、ディスク暗号化、および信頼できる実行に必要となる認証資格情報を安全に保存するために使用されます。実際、TPM チップにはプロダクト構成レジスタ (PCR) が含まれており、インストールされているソフトウェアとシステム構成の追跡が可能で、コンピューティング・プラットフォームの信頼性を長期にわたって確保するのに役立ちます。TPM 機能は ISO/IEC 118889 として規定されており、TPM の動作は、主要なコンピューター・プラットフォーム企業によって形成された業界団体である Trusted Computing Group (TCG) によって認定されています。

PLUG &TRUST

NXP

明日のIoTを保護するのは今です。

モノのインターネット (IoT) で動作するデバイスは、ネットワークに接続されたコンピュータと同様のリスクに直面しています。とはいえ、IoT の観点から見ると、たとえコンパクトであっても TPM を設計に追加すると、TPM の駆動に必要となる SW スタックとプラットフォーム・リソースのサイズの点で、過剰なオーバーヘッドが生じる可能性があります。また追加したとしても、セキュアなネットワーク接続の作成、複数のクラウドでのオンボーディング、データ認証用の複数のキーの保存、複数の他のデバイスへのセキュアな接続など、IoT に固有のタスクに必要とされる柔軟性と暗号化機能は得られません。こういったユース・ケースは、従来のコンピューティング TPM では予期されなかったものです。さらに、IoT デバイスにはさまざまな脅威モデルとフォーム・ファクタが関連しているため、IoT デバイスには、ホスト・コントローラとのセキュアなバインディング (例えば、Global Platform が標準化した Secure Channel Protocol 03 (SCP03) を活用するなど)、小型デバイスに適合する小型フットプリント、IoT デバイスのタイプにセキュリティ・ロジックを適合させるためのプログラマビリティなど、従来の TPM では通常提供されない機能も必要になります。

IoT に特有のニーズに対処するには、IoT 運用に特化して構築されたセキュア・エレメントを使用して TPM 機能を提供することができます。

ソリューション

EdgeLock SE050 は、IoT ユース・ケース向けに最適化されたアプレットがプリインストール済みの改ざん防止セキュア・エレメントであり、IoT アプリケーションに TPM 機能をもたらします。EdgeLock SE050 セキュア・エレメント・ファミリのエントリー・レベルからハイエンドにいたるまで全製品で、セキュアな暗号化処理、セキュアなキー・ストレージ、一意の ID 生成およびストレージなどの TPM に類似した機能を提供しています。また、デバイスの健全性をリモートで検証し、信頼性を確保するための証明機能と PCR も含まれています。従来の TPM と比較した場合に EdgeLock SE050 が持つ大きなメリットとしては、IoT 関連機能に対するサポートの増加、幅広い開発および使用モデル、小型センサやエッジ・コンピューティング・プラットフォームなどのパワフルな IoT 機器でも使用できることなどが挙げられます。

EdgeLock SE050 は TPM 動作のベース・ラインとなるだけでなく、認証資格情報やユーザー・ポリシーを管理するためのより柔軟なアプローチを含む IoT 動作に対して、特化されたサポートを提供します。各認証資格情報オブジェクトに対してのユーザー / ポリシーの組み合わせが増えており、IC はホスト MCU へのセキュア・バインディング (標準 SCP03 プロトコルを使用) をサポートします。この IC は、キーを凍結する機能 (これにより他者による削除を回避) と、大量オンチップ・メモリ上でアクセス権ポリシーを構成する機能をサポートしており、NXP EdgeLock 2GO サービスと組み合わせることで、フィールドで無線経由でキーとデジタル証明書を管理できるようになります。この IC はマルチ・テナントもサポートしており、複数の関係者 (機器メーカー、メンテナンス担当者、インフラストラクチャ・オペレータなど) が同じ EdgeLock SE050 のセキュア・エレメントを使用して、機密データと認証資格情報を安全に保存することができます。

統合を簡素化し、開発にかかる期間を削減するために、EdgeLock SE050 は、プラットフォーム・レベルとアプリケーション・レベルの両方で、プロセッサへのセキュア・バインドをサポートしています。メモリの占有面積が小さいため、IoT フォーマットとうまく連携し、実装のコスト効率が高くなります。

リソースの少ない IoT ノードに対応するため、ホストのマイクロプロセッサまたはマイクロコントローラ上で実行される軽量 Plug & Trust ミドルウェアのサイズは最適化されています。また、従来の TPM から EdgeLock SE050 への迅速な移行を可能にするために、Plug & Trust ミドルウェアでは、TPM ソフトウェア・スタック (TSS) に簡単に統合できる TSS アダプテーション・レイヤーを提供しています。OpenSSL や mbedTLS などの複数のコントローラ、プロセッサ、暗号ライブラリも事前に統合済みで、開発時の労力と時間を節約することができます。

EdgeLock SE050 は NXP EdgeLock Assurance Program の一部であり、ハードウェアだけでなくオペレーティング・システム・レベルでも、EAL6+ AVA_VAN.5 耐性レベルのコモン・クライテリア・フレームワークに従って、認証済みのセキュリティを提供します。EdgeLock SE05x セキュア・エレメントは拡張性も考慮して設計されており、スマート・ホーム用の CHIP (Connected Home over IP)、スマート・メータリング用の DLMS-COSEM、インダストリアル制御セキュリティ用の ISA/IEC 62443、インダストリアル通信のデータ交換規格を定義する Open Platform Communication United Architecture (OPC UA) などの、既存および今後の基準をサポートするように構成することも容易です。

詳細な情報

NXP のデザイン・コミュニティ・サイトでは、EdgeLock SE050 で使用するための役立つヒント、わかりやすいハウツー、詳細なアプリケーション ノートを提供しています。EdgeLock SE050 製品ページには、詳細な仕様、設計ツールおよびソフトウェア、トレーニングおよびサポートなどへのリンクが掲載されています。

- **NXPデザイン・コミュニティ**
  https://community.nxp.com/community/identification-security/secure-authentication/overview
- **EdgeLock SE050製品ページ**
  https://www.nxp.jp/SE050

より詳細な情報はこちら : **www.nxp.jp/SE050**

リリース日 : 2021 年 4 月