NXP EdgeLock™ SE050

使用事例：
Wi-Fi使用時の認証情報の保護

Wi-Fi を使って無線接続するデバイス、ゲートウェイ、またはルータにセキュア・エレメントを追加すると、ネットワーク・オンボーディングが容易になるうえ、証明書ベースの認証と行政組織グレードの暗号化を行うことで、ネットワークを攻撃から保護することができます。

アプリケーション

ルータ

ゲートウェイ

課題

IEEE 802.11 規格に基づく Wi-Fi 技術は、IoT 全体で使用されており、eLock やスピーカーなどの個々のエッジ・デバイスとゲートウェイやルータとの間、そしてゲートウェイやルータとより広いネットワークやクラウドとの間を接続しています。

Wi-Fi は、あらゆるデバイスをネットワークに接続する家庭用アプリケーションでも産業用アプリケーションでも、すでに IoT 接続の重要な部分を占めています。

そのうえ、性能とバッテリ寿命が大幅に向上した Wi-Fi 6 の登場により、IoT における Wi-Fi の重要性がいっそう高まることが予想されます。

Wi-Fi 接続する IoT デバイスの導入が進むと、エンド・ユーザーが簡単に設置できるようにするために、デバイス・メーカーには、迅速で簡単な実装を望む声が強まります。特に、新しいデバイスをネットワークに接続するプロセスは、オンボーディングと呼ばれ、できる限り簡単であることが求められます。しかしまた、Wi-Fi 接続の数が増えるにつれて、セキュリティ・リスクも高まります。

ハッカーが、DDoS 攻撃の土台や他のデバイスの悪意のある制御、プライバシーの侵害など、ネットワークに何らかの危害を加えるための入口を探して、Wi-Fi 接続のデバイスを標的にすることがよくあるからです。

IoT デバイスとその接続先のゲートウェイやルータの保護に使用できる Wi-Fi プロトコルは複数あります。

最善の方法の一つを、業界で知られているベスト・プラクティスに基づいた認証制度を運用する独立組織、Wi-Fi Alliance が定義しています。

その方法は、EAP（Extensible Authentication Protocol）を使用した証明書ベースの認証に加えて、WPA（Wi-Fi Protected Access）の最新版と行政組織グレードの AES 暗号化を用いるものです。

EAP-TLS フレームワークでは、トランザクションのクライアント側とサーバ側の両方で証明書を使用し、ユーザ・ベースおよびセッション・ベースのセキュリティ・キーを動的に生成することで、認証後の Wi-Fi クライアントとアクセス・ポイントの間の通信をセキュリティで保護できるため、このフレームワークが最も安全な認証方法と考えられています。

ユーザがネットワーク・サービスに接続して利用する場合、認証、許可、アカウンティング（AAA またはトリプル A）管理には、クライアント／

PLUG&TRUST

NXP

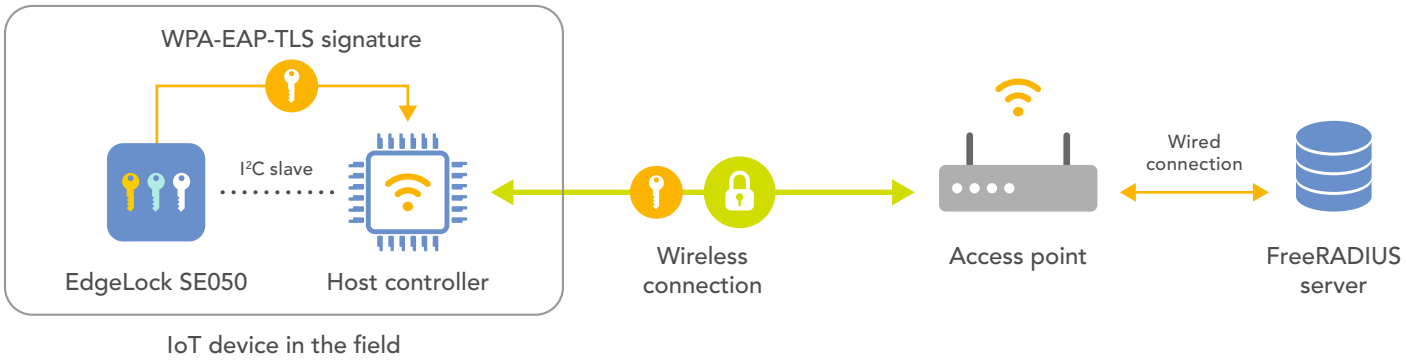
Securing tomorrow's IoT. *Today.*

サーバ・ネットワーク・プロトコルとして、一般に RADIUS（Remote Authentication Dial-In User Service）が使用されます。
ただし、設計で使用するプロトコルの組み合わせに関係なく、セキュリティ・キーをハードウェアに保存するのが最善です。
シリコン・ベースのセキュリティの場合、高レベルの保護を提供できるため、Wi-Fi デバイスがネットワークに接続する際のリスクを最小限に抑えることができるからです。

ソリューション

EdgeLock SE050 は、耐タンパ性を備えたプラットフォームであり、セキュリティ・キーと証明書による強固な保護に基づいた、IoT セキュリティのさまざまな使用事例を想定して設計されています。
また、最新の WPA-EAP-TLS セキュリティ・プロトコルに加えて、HKDF、PBKDF2、セキュア SCP チャネル保護などの暗号関数もサポートしています。
EdgeLock SE050 は、製造時または販売店からの出荷前にセキュリティ・コードのプリインストールおよび認証情報の事前設定が行われるため、開発時間の短縮を実現します。認証情報を事前設定することにより、IoT デバイスに個別情報が提供されるため、ネットワーク・オンボーディングが容易になり、セキュリティも向上します。
デバイスが Wi-Fi ルータに接続する際の認証プロセスでは、この認証情報が使用されるため、ネットワークを不正なアクセスから保護することができます。認証情報が IC から切り離されることはないため、製品のライフサイクル全体にわたって信頼のチェーンが保持されます。
その結果、Wi-Fi を使用するデバイスのルート・オブ・トラストに基づいて真にエンド・ツー・エンドのセキュリティが実現されます。
ブロック図に示したように、EdgeLock SE050 は IoT デバイスにセキュアな個別情報を提供し、Wi-Fi ルータに接続する際の認証には必ずその情報が使用されます。
ホスト・コントローラには I^2C スレーブ・インターフェースを使用して接続します。
Wi-Fi ネットワークとの接続は、認証プロセスの一環で EdgeLock SE050 の事前設定済みの認証情報を使用するミドルウェアによって確立されます。

ブロック図



関連情報

NXP デザイン・コミュニティのサイトでは、EdgeLock SE050 用の役立つヒント、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 製品ページでは、詳細な仕様、設計ツールおよびソフトウェア、トレーニングとサポートなどのリンクを提供しています。

▶ **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**
www.nxp.com/SE050

Find all information on www.nxp.com/SE050

SE050UCWiFiCredentialProtectionWPJP rev 0, December 2020 （原本：June 2020）

PLUG&TRUST