ECC608 TrustMANAGER と Kudelski IoT 社が提供する SaaS の役割を理解する

Xavier Bignalet (Microchip 社　プロダクトマーケティングマネージャー)

本ブログ記事では、Microchip 社の ECC608 TrustMANAGER と Kudelski IoT 社の keySTREAM™ SaaS (Software as a Service)を組み合わせた意義とその機能、IoT 環境においてセキュリティと信頼性を確立するために果たす役割について説明します。

IoT 時代における動的な信頼管理

テクノロジーとモノのインターネット（IoT）システムが主流の時代において、信頼の概念は新たな次元を迎えています。IoT デバイスがオンライン取引（Alexa が次の製品を注文する場合など）を処理している時も、機密情報を共有する場合(Alexa 経由の注文がクレジットカードに請求される場合）でも、仮想空間内で他のデバイスと連携している場合（注文によって荷物の配達のためにガレージが開く場合）でも、信頼は我々のデジタルエクスペリエンスの形成において極めて重要な役割を果たします。今までのところ、IoT デバイスは静的な信頼に依存してきました。しかし、システムをリモートで更新する必要がある場合や、そのシステムの所有権が侵害されたり、頻繁に変更する必要がある場合はどうなるでしょうか。例えば、短期契約の賃貸住宅が備えるインターネット接続のスマートドアロックを想像してみてください。賃借人が変わるたびにドアロックの認証と信頼を更新する必要があるはずです。この場合、ドアロックのライフサイクルを通して信頼のチェーン(Chain of trust)を動的に管理する必要があります。このようなデジタル信頼エコシステムの陰の立役者が、Kudelski IoT 社の keySTREAM™ SaaS と組み合わせた ECC608 TrustMANAGER の役割なのです。本ブログ記事では、この製品の重要性、その機能、そして安全で信頼性の高い IoT 環境を確保する上での重要な役割について説明します。

IoT の信頼に関する課題

生活の様々な局面でデジタル プラットフォームへの依存度が高まるにつれ、信頼の必要性はますます明らかになっています。コンシューマ向け、産業用、車載、医療用を含む様々な市場において、IoT デバイスは常に潜在的脅威に晒されながらの複雑なネットワークの中を渡り歩いています。様々な問題が IoT の世界で信頼を確立、維持、管理する事の重要性を示しており、サイバーセキュリティの侵害、個人情報の窃盗、データの漏洩はそのような課題のほんの一部に過ぎません。ほとんどの IoT 製品は、製品のデバイス証明書に関連付けられた秘密鍵の保護も、製造側（証明書の発行元）の保護も、ルート認証局が存在するはずの製品会社レベルの保護も行われないまま、静的な証明書チェーンのままで設計されています。そのような IoT デバイスが世界中に出回っている現在、セキュリティ専門家はそれらのデバイスがフィールドで使われた時に IoT セキュリティモデルに何が起こるのか疑問を持ち始めています。セキュリティはどのように維持され、最新状態に保たれているでしょうか。そして今、セキュリティの更新可能性の義務化を目指す規格および法規制が増えつつあります。この課題に対する Microchip 社の答えが「クラウド管理された TrustMANAGER セキュア認証 IC」なのです。

keySTREAM SaaS とは

keySTREAM SaaS は Kudelski IoT 社の製品であり、デジタルトラストのクラウドの守護神として機能します。このソフトウェアは IoT デバイスに実装された ECC608 TrustMANAGER セキュア認証 IC により暗号認証操作を監視します。keySTREAM の役割は以下の場合に特に重要です。

- **カスタム ルート CA と関連付けられた PKI(公開鍵基盤)のセットアップ**が複雑または高コストであり、企業がそれに必要な時間も専門知識もほとんどまたは全く持たない場合

- そのような場合でもルート CA は非常に基本的なセキュリティ基盤であり、製品内で構築する必要があります。加えて、規格と法規制さらに企業の IT ポリシーが将来それを義務付けるでしょう。

- フィールドにおいて IoT デバイス内部のセキュリティ認証情報を**セキュアに更新および管理する**必要がある場合
- IoT デバイスのライフサイクルを通してカスタム PKI を**動的に管理する必要がある**場合
- 製品のライフサイクルを通してその**所有権を複数の所有者の間で移転する**必要がある場合
- 鍵の一意性を維持する上で、カスタム・セキュリティ IC を扱うサプライチェーン・ロジスティクスが、**在庫**管理上の課題となる場合
- **PKI と暗号の健全状態を良好に維持する**事が規格または将来の法規制を遵守し続けるための基本的取り組みであると認識される場合

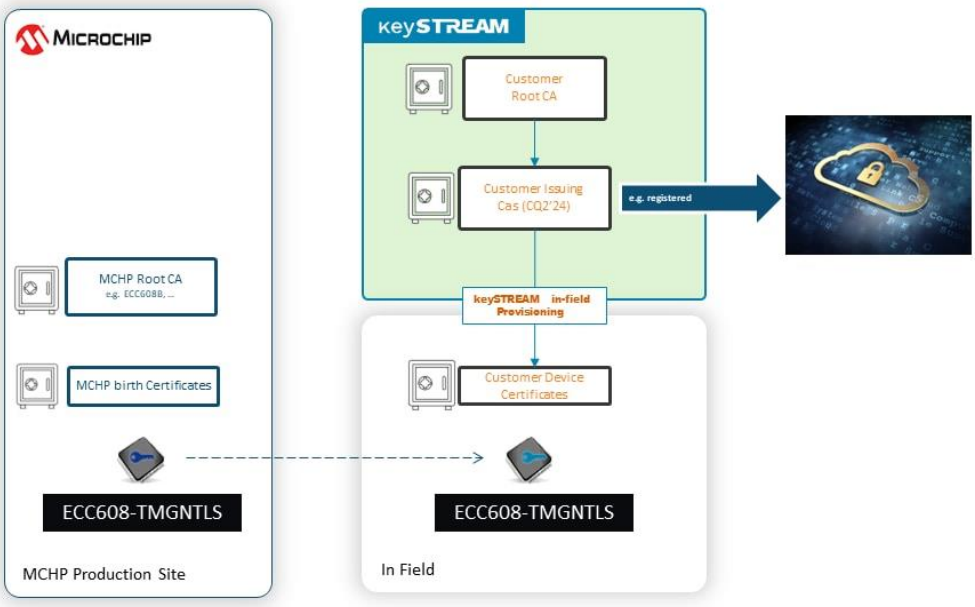
ECC608 TrustMANAGER とは

Microchip 社の ECC608 TrustMANAGER は CryptoAuthentication™ファミリのセキュア認証 IC であり、keySTREAM SaaS によって管理される暗号鍵をセキュアに保存します。

本デバイスはプロビジョニング済みの鍵セットが書き込まれた状態で納入され、これらの鍵は IoT デバイスが最初に接続された時に keySTREAM によって制御されます。この動作はフィールド上で発生し、「PKI のインフィールド プロビジョニング」と呼ばれます。インフィールド プロビジョニングが発生すると、ECC608 TrustMANAGER を実装した IoT デバイス群（フリート）はユーザの keySTREAM アカウント内で「クレーム」された後に「アクティベート」されます。

- 「クレーム済み」デバイス: 購入済みの ECC608 のバッチが keySTREAM アカウント内に表示されますが、それらは未接続です。
- 「アクティベート」されたデバイス: 購入された ECC608 のバッチは keySTREAM に接続されてインフィールドプロビジョニングが実行済みです。

請負製造業者のプロビジョニング操作だけでも一連の操作となり、プログラミング時間が消費され、製造コストが増加します。さらに、Trust Platform ソリューションを使わない場合、製造中にセキュリティの脆弱性が露呈します。例えば、鍵が工場から漏洩して模倣される可能性があります。



舞台裏では何が起こっているのでしょうか？

スケーラブルな認証 SaaS と特定のセキュア認証 IC 向けに動的かつセキュアな鍵プロビジョニング サービスの両方を開発して維持/サポートするには何年もかかります。数千ユニットから数百万ユニットの間で従来の IoT 製品開発を考えた場合、企業が単独でそのような開発に投資してもスケールメリット(規模の経済性)は意味を持ちません。しかし必要である事は明らかです。各種セキュリティ規格、法規制、推奨される基本的セキュリティプラクティスに従うには、マネージド認証が鍵となります。

keySTREAM SaaS と ECC608 TrustMANAGER を使うと、以下の処理がわずか数分で実現可能になります。

- HSM (Hardware Security Module)空間がマルチテナント機能を備えた keySTREAM アカウント内で作成されます。
- この HSM 空間内で、カスタム ルート CA 証明書とそれに関連付けられた秘密鍵が HSM の保護された環境内で作成されます。
- ルート CA 証明書の作成中に固有の企業情報がルート CA 内でキャプチャされ、それがその企業とデバイス群に対するカスタム ルート CA とされます。
- PKI カスタマイズ プロセス中は、keySTREAM へのユーザ入力を除けば、人間との操作は発生しません。
- 購入された数量の「既成品」のセキュア認証 IC が数秒以内に「クレーム」されます。

請負製造業者には、デバイスの「クレーム」処理に関して、その検査時間や製品メーカーとのやりとりも一切必要としません。IoT デバイスが現場に配備されると、製品会社はエンドユーザに快適な管理および PKI メンテナンスエクスペリエンスを提供する事ができます。

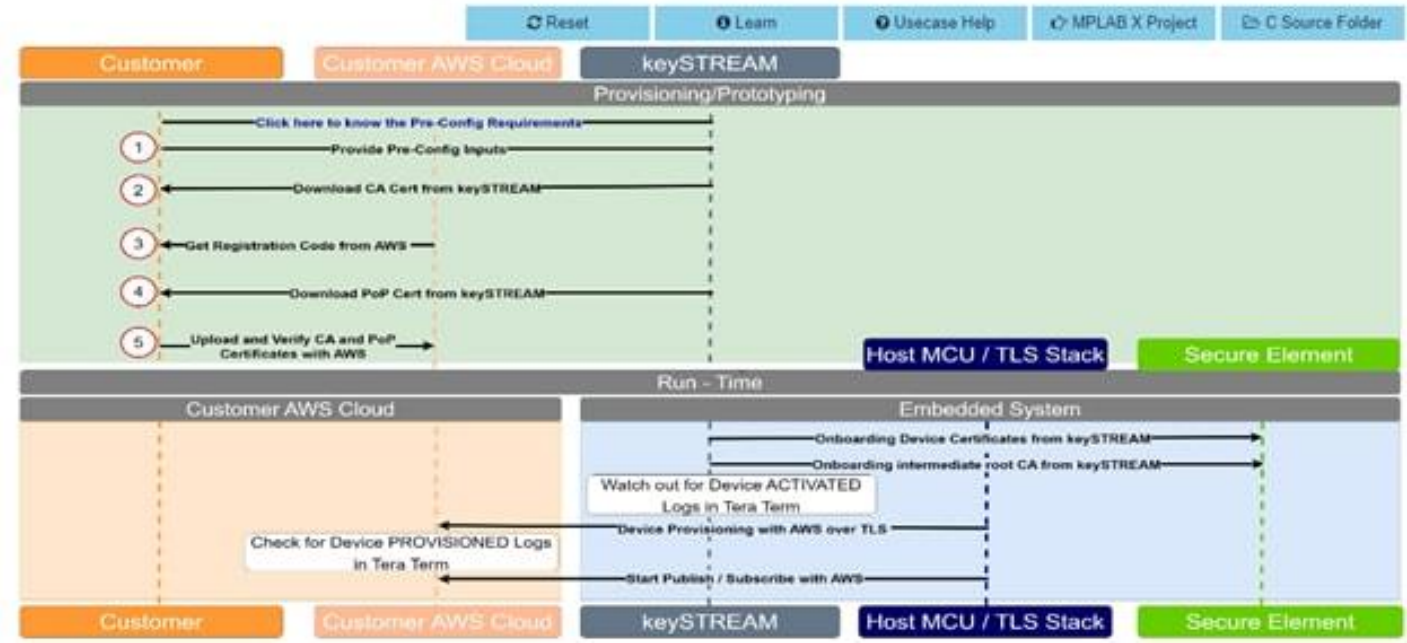
- デバイス証明書の有効期限が切れた時、keySTREAM プラットフォームは新しい証明書チェーンを再初期化し、それを自動的に ECC608 TrustMANAGER に結び付けます。
- デバイス内で信頼が損なわれた場合、リモートでそれを無効にし、最終的に完全に再生できます。再生により、低コストでデバイスをエンドユーザの手に戻す事ができます。

TrustMANAGER と keySTREAM の主な特長

1. ルート CA を含むセルフサービス カスタム PKI を設定するにあたって、Microchip 社およびサードパーティとのやりとりを必要としません
2. ルート CA を含む全ての証明書レベルで、ライフサイクルを通して、HSM 内で証明書チェーンとその秘密鍵の保護および可用性を長期にわたって維持します
3. 自社が使用しているあらゆるクラウドプラットフォームに IoT デバイスをオンボードでき、フリートの規模や、クラウドプラットフォームに大量の証明書やその他の暗号化認証情報をアップロードするのにかかる時間を心配する必要はありません
4. クラウド プラットフォームに実際に接続された IoT デバイスに対しては、使用した分だけ費用が発生します。
   - エンドユーザが IoT 製品を決してインターネットに接続しない場合、クラウド プラットフォーム内でそのデバイスをアクティベートするためのコストは不要です。
5. 証明書チェーンの健康状態の管理
   - 証明書の有効期限が切れた時または証明書チェーンを変更する必要が生じた場合、keySTREAM はチェーン内の各証明書レベルを管理し、破損したチェーンを無効にして修理し、有効期限の更新を調整します。

開発を始める

Trust Platform Design Suite をダウンロードし、ECC608 TrustMANAGER 内の keySTREAM のユースケースをテストします。



最初のステップをガイドする入門編 Chiptorial YouTube ビデオ①と②もご覧になれます。

keySTREAM と ECC608 TrustMANAGER が、ビル入退室管理業界におけるコンシューマアプリケーションの拡張にどのように役立つかについてのケーススタディもご覧ください。

信頼管理の将来

技術革新が進むにつれ、keySTREAM と ECC608 TrustMANAGER の役割も進化します。データプライバシーと規則遵守の重要性が高まる中、TrustMANAGER は企業等の組織に要求されるセキュリティプラクティスを確実に遵守するために極めて重要な役割を果たします。

まとめ

デジタル技術に様々な課題が突きつけられる中、TrustMANAGER と keySTREAM は IoT デバイスのセキュリティを守る陰の守護神として機能します。その多面的な役割には、潜在的脅威の先を行く堅固なセキュリティ対策の実装とインシデントへの迅速な対応が含まれます。個人および組織レベルで IoT 化が進む中、TrustMANAGER の役割を正しく理解し評価する事がセキュアで信頼できる IoT エコシステムの発展において最も重要になります。