SHC RISC-V ルートオブトラストデモ

FreeRTOS と Amazon IoT Core を搭載した Andes RISC-V SoC

2020 年 11 月 4 日　SH コンサルティンググループ

SHC が作成したデモ：　AWS IoTCore を使用した AndesCorvette F1 RoT

このデモは、Corvette-F1 ボードを使用したセキュアな IoT ソリューション、32 ビットの AndesCoreN25 と AndeShape AE250 プラットフォームをサポートする評価キット使い、Amazon Web Services のマイクロコントローラー用のオープンソースオペレーティングシステムである Amazon FreeRTOS（ AWS）を実行します。 ESP32-WROOM ボードを外部 Wi-Fi モジュールとして使用しています。 ATECC608A-MAHDA チップは、トラステッドプラットフォームモジュール（TPM）などに統合されており、ハードウェアベースのエンドポイントデバイスセキュリティを提供します。この統合により、デバイス ID の確立に使用される秘密鍵を改ざん防止ハードウェアデバイスに安全に保存して、なりすましやその他の悪意のあるアクティビティのためにデバイスから秘密鍵が取り出されるのを防ぐことができます。

IoT ソリューションの展開では、メッセージングゲートウェイと通信しているデバイスの ID を確認することが重要です。初めてデモを実行すると、TPM はデバイスのキーペアを生成し、トラフィックの認証と暗号化に使用されます。キーは TPM 自体の内部で生成されるため、外部プログラムによる取得から保護されます。実際、ハードウェアの信頼のルートとセキュアブートの機能を利用しなくても、TPM はハードウェアのキーストアとしても価値があります。秘密鍵はハードウェアによって保護されており、ソフトウェア鍵よりもはるかに優れた保護を提供します。この統合では、TPM へのインターフェイスとして PKCS＃11 プロトコルを使用します。

キーペアを生成した後、このデモでは FreeRTOSMQTT ライブラリを使用して AWSCloud に接続し、AWS IoTMQTT ブローカーによってホストされている MQTT トピックにメッセージを定期的に公開します。 SHC によって開発された特定の Android アプリケーションも、このトピックを使用して Corvette-F1 ボードと通信し、オンボード LED を制御します。

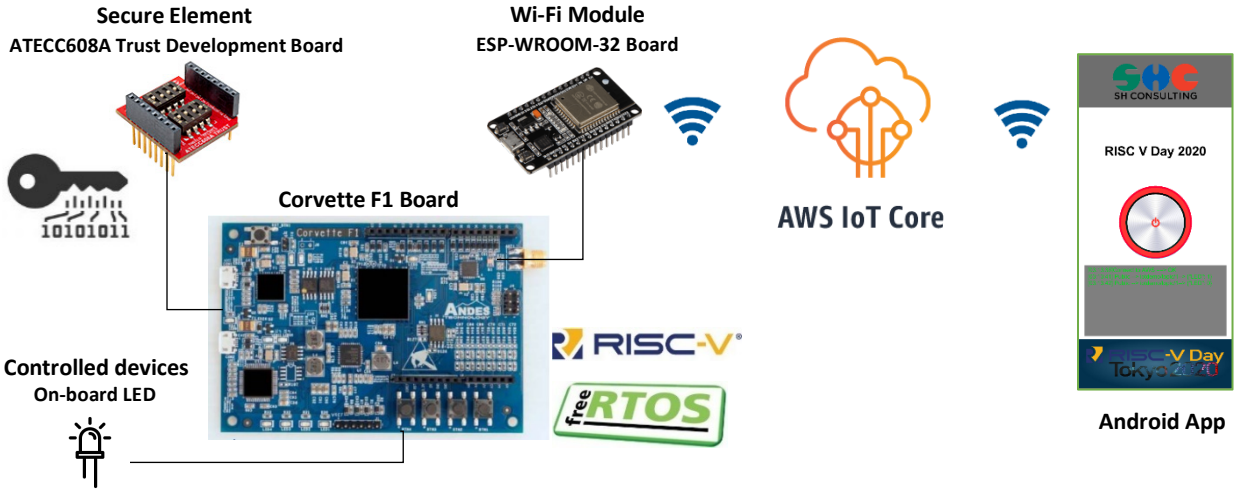


図 1：コルベット F1 の信頼のルートと AWS IoT デモ

アンデステクノロジ社 Corvette F1 ボード

概要

Andes Technology は、高性能で低電力のコンパクトな 32/64 ビット RISC-V CPU コアの大手サプライヤーであり、RISC-VFoundation の創設メンバーです。その Corvette-F1N25 プラットフォームは、AmazonFreeRTOS に認定された最初の RISC-V プラットフォームの 1 つです。 Amazon FreeRTOS は、Amazon Web Services（AWS）のマイクロコントローラー用のオープンソースオペレーティングシステムであり、小型で低電力のエッジデバイスのプログラミング、デプロイ、セキュリティ保護、接続、および管理を容易にします。開発者は、Andes Technology の RISC-V プラットフォームを使用することで、AmazonFreeRTOS の機能と利点を活用できます。

ますます多くのテクノロジーがインターネットに導入されるにつれて、IoT 市場は多種多様なアプリケーションで成長しています。 RISC-V 命令セットアーキテクチャ（ISA）は、柔軟性、拡張性、スケーラビリティを強化し、IoT の新しい可能性を生み出し、この成長する市場を活用するためのコンパクトな IoT ハードウェアの設計を容易にします。 Andes Technology は、RISC-V プラットフォームを Amazon FreeRTOS、AWS IoT Greengrass、AWS IoT Core などのソリューションと組み合わせることで、開発者が包括的で競争力のある RISC-V ベースの IoT システムを作成できるよう支援します。

Corvette-F1 N25 プラットフォームは、AmazonFreeRTOS に認定された最初の RISC-V プラットフォームの 1 つです。 Corvette-F1 N25 プラットフォームは、FPGA ベースの Arduino 互換の評価プラットフォームです。 60MHz で動作する 32 ビット RISC-VAndesCore™N25、4MB フラッシュ、256KB 命令 SRAM および 128KB データ SRAM、および GPIO、I2C、PWM、SPI、およびを含む豊富な周辺機器を備えた AndeShape™AE250 プラットフォーム IP が付属しています。 UART。ユーザーは、Arduino 標準 IDE とフル機能の AndeSight™IDE の下で IoT デバイスのプロトタイプとアプリケーションを簡単に構築できます。

マイクロチップ社 ATECC608A チップ

特長

• ハードウェアベースの安全なキーストレージを備えた暗号化コプロセッサ：
–最大 16 個のキー、証明書、またはデータを格納できる堅牢化されたストレージ
•非対称署名、検証、鍵共有のハードウェアサポート：
– ECDSA：FIPS186-3 楕円曲線デジタル署名
– ECDH：FIPSSP800-56A 楕円曲線ディフィーヘルマン
–NIST 標準 P256 楕円曲線のサポート
•対称アルゴリズムのハードウェアサポート：
–オフチップコンテキストの保存/復元を含む SHA-256 および HMAC ハッシュ
– AES-128：暗号化/復号化、GCM のガロア体乗算
• ネットワーキングキー管理サポート：
– TLS1.2 および 1.3 のターンキー PRF / HKDF 計算
–SRAM での一時的なキー生成とキー合意
–キーが完全に保護された小さなメッセージの暗号化
•セキュアブートのサポート：
–完全な ECDSA コード署名検証、オプションの保存されたダイジェスト/署名
–セキュアブート前のオプションの通信キーの無効化
–オンボード攻撃を防ぐためのメッセージの暗号化/認証
•内部高品質 NISTSP 800-90A / B / C 乱数ジェネレーター（RNG）
•2 つの高耐久性単調カウンター
•保証された一意の 72 ビットシリアル番号
•利用可能な 2 つのインターフェイスオプション：
–1 つの GPIO ピンを備えた高速シングルピンインターフェイス
– 1MHz 標準 I2C インターフェース
• 1.8V～5.5V IO レベル、2.0V～5.5V 供給電圧
•<150nA スリープ電流
•8 パッド UDFN および 8 リード SOIC パッケージ

アプリケーション

- ネットワーク/ IoT ノードエンドポイントセキュリティ

ノード ID 認証とセッションキーの作成と管理を管理します。 TLS 1.2（およびそれ以前）および TLS1.3 を含む複数のプロトコルのエフェメラルセッションキー生成フロー全体をサポートします

- セキュアブート

コードダイジェストを検証し、オプションで成功時に通信キーを有効にすることで、MCU ホストをサポートします。パフォーマンスを向上させるためのさまざまな構成が利用可能です。

- スモールメッセージ暗号化

PII 情報などの小さなメッセージやデータを暗号化および/または復号化するためのハードウェア AES エンジン。AES-ECB モードを直接サポートします。他のモードは、ホストマイクロコントローラーの助けを借りて実装することができます。 AES-GCM をサポートするための追加の GFM 計算機能。

- ソフトウェアダウンロードの鍵生成

ダウンロードした画像のローカル保護キー生成をサポートします。それぞれが同じ復号化キーを持つ多くのシステムへの 1 つのイメージのブロードキャスト、またはシステムごとの一意のイメージのポイントツーポイントダウンロードの両方がサポートされています。

- 生態系制御と偽造防止

システムまたはコンポーネントが本物であり、銘板に示されている OEM からのものであることを検証します。

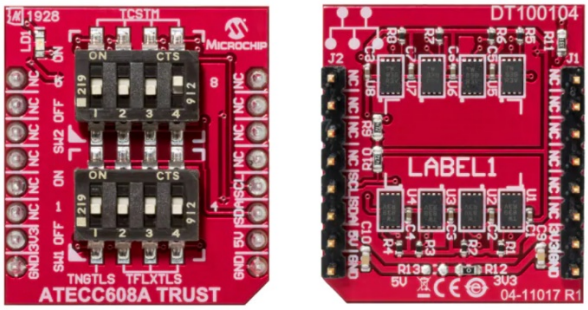


図 2：ATECC608A トラストボード（上面図と底面図）

暗号処理機能

ATECC608A は、楕円曲線暗号と ECDSA 署名プロトコルに基づく完全な非対称（公開/秘密）鍵暗号署名ソリューションを実装します。このデバイスは、NIST 標準 P256 プライムカーブのハードウェアアクセラレーションを備えており、高品質の秘密鍵生成から ECDSA 署名生成、ECDH 鍵合意、および ECDSA 公開鍵署名検証までの完全な鍵ライフサイクルをサポートします。

このデバイスは、複数の秘密鍵とそれに関連する公開鍵および証明書を安全に保存するように設計されています。

ランダムな秘密鍵の生成はデバイスの内部でサポートされており、秘密鍵がデバイスの外部で認識されないようになっています。保存された秘密鍵に対応する公開鍵は、鍵が生成されるときに常に返され、オプションで後で計算される場合があります。

ATECC608A は、NIST 800-90A、800-90B、および 800-90C のドキュメントに記載されている要件を満たすように設計された、内部乱数ジェネレーターを使用して高品質の乱数を生成できます。

これらの乱数は、デバイスの暗号プロトコルの一部としての使用を含め、あらゆる目的に使用できます。各乱数は、このデバイスまたは他のデバイスでこれまでに生成されたすべての番号から本質的に一意であることが保証されているため、プロトコル計算に含めることで、リプレイ攻撃（つまり、以前に成功したトランザクションの再送信）が常に失敗します。

マイクロチップの信頼プラットフォームによるルートオブトラスト

IoT の時代では、ハードウェアベースのセキュリティは、物理的な攻撃やリモート抽出から秘密鍵を保護する唯一の方法です。ただし、各デバイスを構成およびプロビジョニングするには、セキュリティに関する幅広い専門知識、開発時間、およびコストが必要です。 Microchip は、CryptoAuthentication ファミリ用に Microchip の Trust Platform と呼ばれる主要なセキュリティサービスを開発しました。これは、小規模または大規模の OEM がハードウェアデバイスに安全な認証を実装するための簡単な方法を提供します。このサービスは、デバイスキーを製造するための安全なシステムと、カスタム部品番号を生成するためのサプライチェーンを提供します。

ATECC608A の安全な要素に基づいて、Trust Platform は、すぐに使用できる事前プロビジョニングから完全にカスタマイズ可能なものまで、ユーザーのニーズを満たすために 3 つの層で利用できます。 ATECC608A は、Common Criteria Joint Interpretation Library（JIL）の「高」評価のセキュアキーストレージを提供し、デバイスが業界で実証済みのセキュリティプラクティスと最高レベルのセキュアキーストレージを実装していることをお客様に確信させます。ハードウェアベースの信頼のルートストレージと暗号化対策は、既知の物理的攻撃の最も幅広いクラスからデバイスを保護します。

3 つのレベルは、Trust＆GO、TrustFLEX、および TrustCUSTOM です。

• マスマーケット向けの Trust＆GO（ATECC608A-TNGTLS）は、最小注文数量（MOQ）が 10 ユニットという、ゼロタッチの事前プロビジョニングされた安全な要素を提供します。デバイスの資格情報は、自動クラウドまたは LoRa WAN 認証のオンボーディングのために、事前にプログラムされ、出荷され、ATECC608A 内でロックされます。

•TrustFLEX（ATECC608A-TFLXTLS）は、事前構成されたユースケースの恩恵を受けながら、顧客の認証局を使用する柔軟性を提供します。これらのユースケースには、任意の証明書チェーンを使用して任意の IP ベースのネットワークに接続するためのトランスポート層セキュリティ（TLS）強化認証、LoRaWAN 認証、セキュアブート、無線（OTA）更新、IP 保護、ユーザーなどのベースラインセキュリティ対策が含まれます。データ保護、およびキーローテーション。

•TrustCUSTOM（ATECC608A-MAHDA）は、完全なカスタマイズを可能にし、顧客固有の構成機能とカスタム資格情報のプロビジョニングを提供します。

Microchip は Amazon Web Services（AWS）と連携して、Microchip Trust Platform のすべてのバリアントで設計された製品の AWS IoT サービスへの簡単で簡素化されたオンボードプロセスを可能にしました。 ATECC608A セキュアエレメントは、任意のマイクロコントローラおよびマイクロプロセッサと組み合わせることができます。

Amazon IoT コア

デバイスをクラウドに簡単かつ安全に接続します。 数十億のデバイスと数兆のメッセージに確実に拡張できます。

AWS IoT Core とは何ですか？

AWS IoT Core は、接続されたデバイスがクラウドアプリケーションや他のデバイスと簡単かつ安全に対話できるようにするマネージドクラウドサービスです。 AWS IoT Core は、数十億のデバイスと数兆のメッセージをサポートし、それらのメッセージを処理して AWS エンドポイントや他のデバイスに確実かつ安全にルーティングできます。 AWS IoT Core を使用すると、アプリケーションは、接続されていない場合でも、すべてのデバイスを常に追跡して通信できます。

AWS IoT Core を使用すると、AWS Lambda、Amazon Kinesis、Amazon S3、Amazon SageMaker、Amazon DynamoDB、Amazon CloudWatch、AWS CloudTrail、Amazon QuickSight、Alexa Voice Service などの AWS および Amazon サービスを簡単に使用して、収集、処理する IoT アプリケーションを構築できます。 、インフラストラクチャを管理することなく、接続されたデバイスによって生成されたデータを分析して処理します。

AWS IoT Core はどのような機能を持っていますか？

デバイスを接続し管理します

AWS IoT Core を使用すると、任意の数のデバイスをクラウドや他のデバイスに簡単に接続できます。

デバイスのパブリッシュおよびサブスクライブ
何十億もの IoT デバイスをパブリッシュし、サブスクライブさせることができます。

AWS IoT コア
メッセージは MQTT プロトコルを使用して送受信します。これにより、IoT デバイスのコードのフットプリントが最小限に抑えられ、さらに、必要となるネットワーク帯域幅仕様要件が軽減されます。

デバイス通信機能
AWS IoT Core により、デバイスは AWS サービスおよび相互に通信できます

安全にデバイスを接続し IoT データを護ります

AWS IoT Core は、AWS IoT Core にデバイスが最初に接続したときに自動構成と自動認証を提供します。すべての接続ポイントでエンドツーエンドの暗号化を提供します。また、証明された ID(サティフィケート)がないとデバイスと AWS IoT Core 間でデータが交換することはありません。 さらに、きめ細かい権限を持つポリシーを適用することで、IoT デバイスや IoT アプリへのアクセスを保護します。

入力
温度センサーの配列がデータを送信します

認証する
AWS IoTCore への接続が認証されます

AWS IoT コア
センサーが温度がしきい値を超えていることに同意すると、ファンがオンになります。 認証されたユーザーのみがファンを制御できます

認証する
ファンへの接続が認証されます

制御信号出力
ファンはコマンドを受信してオンになります

いつでもデバイスの状態を読み取り状態を設定できます

AWS IoT Core は、接続されたデバイスの最新状態を保存し、いつでも読み取りまたは設定できるように維持します。これにより、デバイスは常にオンラインであるかのようにアプリケーションに表示されます。

入力
接続された質量分析計は、数時間のサイクルでその状態と読み取り値を報告します

断続的な接続

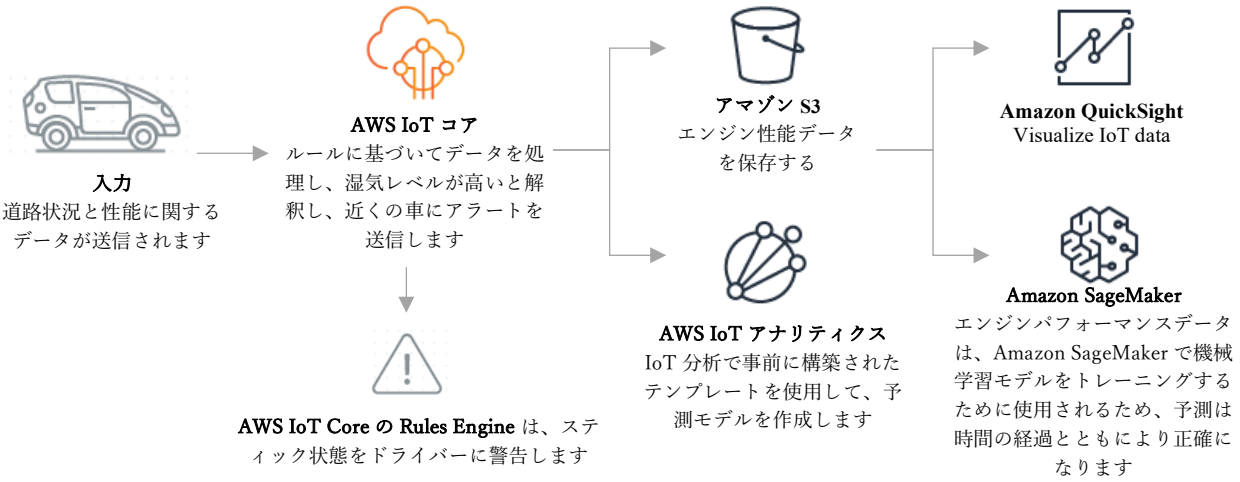
AWS IoT コア
分光計はサイクルが完了するとオフラインになりますが、最後に報告された状態は AWS IoT Core に残ります

REST APIs

出力
技術者は、モバイルアプリを使用して、新しい望ましい状態を設定したり（たとえば、サイクルを一時停止したり）、分光計の最後に報告された状態を照会したりできます。

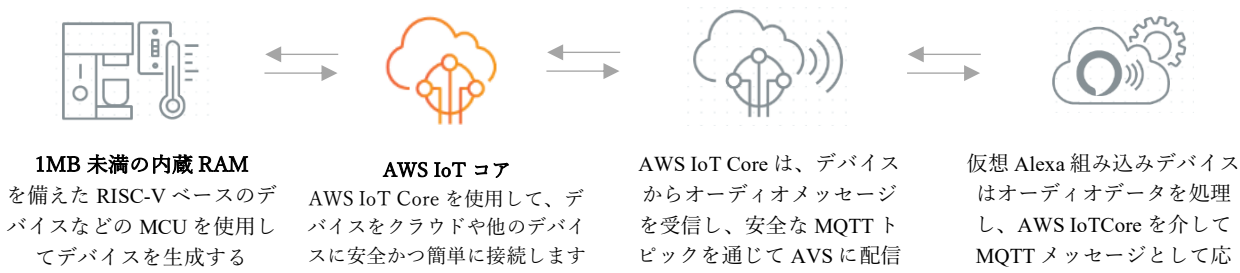
デバイスデータを解析して処理します

AWS IoT Core を使用すると、定義したビジネスルールに基づき、デバイスデータをオンザフライでフィルタリング、変換、処理できます。



費用対効果の高い方法で数億の Alexa ビルトインデバイスに拡張することができます

AWS IoTCore の AlexaVoice Service（AVS）統合により、クラウドに新しい仮想 Alexa ビルトインデバイスが導入されます。 これにより、お客様は、予約済みの MQTT トピックを介してオーディオメッセージを送受信し、デバイスのマイクとスピーカーとインターフェイスし、同じ安全な IoT Core 接続を使用しながらデバイス側の状態を管理できます。



SH コンサルティンググループについて

SH コンサルティンググループ（SHC）には、米国、ベトナム、および日本のエンジニアがいて、RTOS、デバイスドライバー、および H8、SH、ARM、RISC-V などの MCU のワイヤレス接続に安定性を提供することを専門としています。 長年にわたり、MCU 用の QNX、.NETMF、Linux、Windows などの OS と、Lora、WiFi、Bluetooth などのワイヤレスソリューションを統合してきました。 彼らは Windows、Android、iOS プラットフォームで動作しました。 近年、SHC エンジニアは ARM プラットフォーム上の大規模な半導体企業向けに FreeRTOS をエネーブルし、最近は、この取り組みを RISC-V に向けています。

SH コンサルティング株式会社
- 東京本社
〒104-0061 東京都中央区銀座 7 丁目 18 番 13-502 号
TEL: 03-3833-3717

- 東京国分寺設計センタ
〒185-0021 国分寺市南町 3 丁目 23-12 山元ビル 5 階

SH CONSULTING VIETNAM COMPANY LTD.（ベトナム）
(Local Name: CÔNG TY TNHH SH CONSULTING VIỆT NAM)

Quang Trung Software park, Tan Chanh Hiep Ward,
District 12 Ho Chi Minh City
Phone: 84-8-3715-0060

SOFTWARE HARDWARE & CONSULTING LLC (USA)
San Francisco Bay Area USA:
Software Hardware & Consulting LLC
1325A Church St, San Francisco, CA 94114-3900
Phone: +1-(408) 510-8221