# IoTデバイスにおける セキュアなSSL通信を最小限の手間で実現する

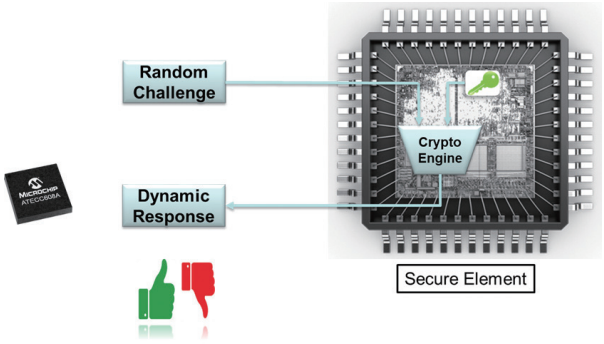
## —— Microchip「Provisioning Service」

昨今、ちょっとしたIoTデバイスであっても、セキュリティが要件として含まれることがごく一般的になりつつある。新規開発だけでなく、すでに納入したシステムに後付けでセキュリティ機能を追加してほしい、なんてケースもあり得るわけで、セキュリティ対策は避けては通れない要件となっている。

こうしたケースで役に立つのが、Secure Elementと呼ばれるデバイスである。以前にも紹介したMicrochipのATECC608Aは、その代表例ともいえる製品だ。

ハイパフォーマンスな32bit MCUならともかく、8/16bit MCUでは通信のセキュア化に必要な暗号化/復号化の処理もかなりの負担となるが、Secure Elementを併用することでこうした問題も簡単に解決する。

しかし、セキュリティ要件についてはもうひとつ注意すべき点がある。特に32bit MCUでConnected Deviceを構築したい、という場合、通信にはSSL(Secure Sockets Layer)を利用することが増えてきた、というかそれが要求されるシーンが増えている。つまり、このSSL通信の利用をセキュアにすることが求められているということだ。




### Microchip「ATECC608A」の特徴

- 通信の暗号化/復号化で利用されるアルゴリズムを高速に実行できるアクセラレータを内蔵
- 暗号を利用する際に必須となるキーを最大16個格納可能
- 乱数発生器(RNG)や、セキュアブート対応のメカニズムも搭載

### クラウド接続に必要な証明書発行と登録の手間を省くMicrochipのProvisioning Service

組み込み向けでSSLというと、WolfSSLが利用されるケースが少なくない。Microchipの場合、同社から無償提供されているMPLAB Harmony V3このWolfSSLを商用利用できる無償ライセンスが提供されている。さらにビルドオプションで、このWolfSSLがATECC608Aを利用するように設定することで、高速なSSL通信をCPUの負荷を最小にしたまま可能にできる。

ではSecure Elementを利用すればそれでOKか?というと、実はそうではない。主要なクラウドサービス、たとえばAWS IoTとかAzure IoT、あるいはGoogle Cloud Platformなど、こうしたクラウドサービスと接続するためには、事前に「証明書の登録」という作業が必要になる。

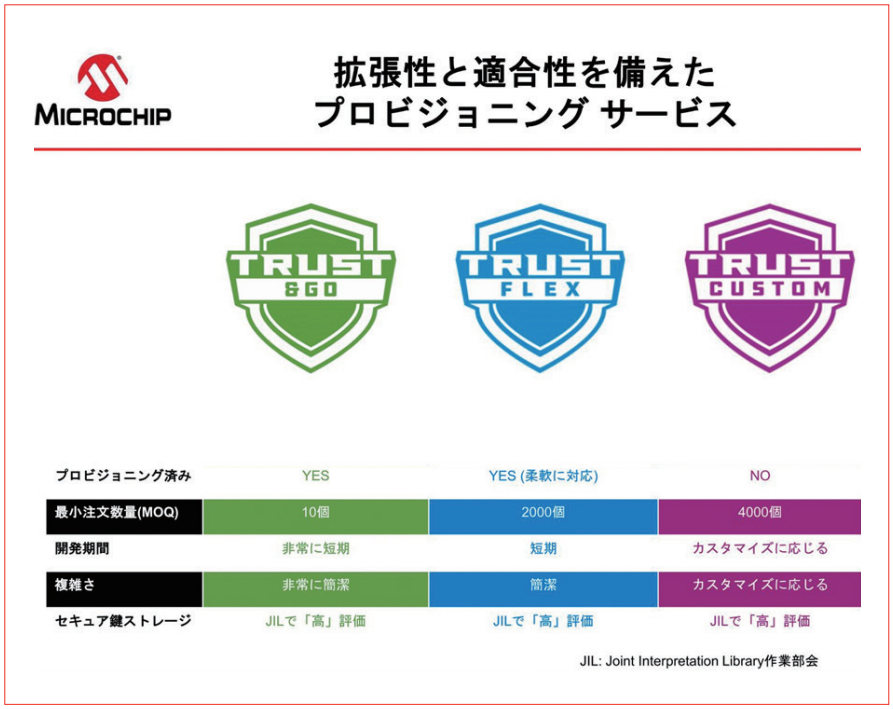
当たり前の話で、こうしたクラウドサービスはどんな相手とも無制限で繋がるわけではなく、事前に接続申請を行う必要がある。そしてその接続申請のためには、自身のデバイス情報を伝える必要がある。問題はそのデバイス情報が、他人に改ざんされたりしたものではないことをきちんと保証する証明書のかたちになっていないといけないことだ。これは、安全に自分のデバイスがクラウドサービスと通信できることを担保するために必要な手続きではあるのだが、言うまでもなくこれは大変に面倒である。基本、証明書は第三者機関に発行してもらわないといけないからで、申請の手続きも大変だし、時間もかかる。特に量産段階に入った場合はまだしも、試作の段階でとりあえず繋いでみたいという場合にもこの手間は省けないから、開発時間が無駄に伸びる要因になりかねない。

こうした証明書発行と登録の手間を最小限に抑えるためのサービスが、MicrochipのProvisioning Serviceである。これはSecurity ElementにATECC608Aを使うことを前提に、利用するクラウドサービスに対応した証明書を、ATECC608Aと一緒に提供してくれるというものだ。開発者は、ATECC608Aを入手したら、そこに付属している証明書をWeb経由でクラウドサービスに登録するだけで、目的のクラウドサービスを利用することが可能になる。

### 用途に応じたカスタマイズ性を持つラインアップ構成

Provisioning Serviceには、3種類のラインアップが存在する。Trust&Goは、言ってみれば試作向けのサービスに近く、最も簡単に利用できるもので、個々の機能を使う際に発生する認証手続きの手間も必要ないうえ、そもそもセキュリティの概念を理解しなくても利用できるほど簡単化されている。また、最小発注数量はわずか10個という、通常のカスタム発注(最低10万個オーダー)では考えられない少量発注が可能なのも、開発費の抑制という観点ではうれしいだろう。

その一方でTrust&Goは、制約も多い。Trust&Goで提供されるものは、特定(AWS IoT/Azure IoT/Google IoT Coreのいずれかひとつ、もしくはLoRaWAN Network/3rd Party TLSのどちらか)のクラウドサービスとの接続「だけ」をサポートしており、また通信方法もTLSベースに限られている。ここまで割り切ったからこそ簡単に利用できるかたちで提供可能になったわけだが、逆に例えばAWS IoTにLoRaWAN経由で接続したいなんてケースでは、AWS IoT接続用のATECC608Aと




LoRaWAN接続用のATECC608Aのふたつを MCUに繋げる必要がある。ATECC608Aの機能そのものはひとつのデバイスで両方の用途に十分対応可能であるが、Trust&Goでは複雑なカスタマイズができないのでこうした制約がつくことになる。なので、PoCあるいは試作段階ではこれで十分であるが、量産を前提とした製品には使いにくい。

逆に、フルカスタマイズ可能なのがTrustCUSTOMである。こちらはどんな相手(クラウドサービス以外も含む)に、どんな暗号化方式/通信手順で通信を行うか、というレベルで完全にカスタマイズ可能になっており、自社で全く新しいサービスを提供し始めるので、それ向けのデバイスを作成する、なんて場合にも利用できる。当然こうなるとセキュリティの知識は相応に必要になるし、その暗号化方式/通信手順を実現するためのソフトウェアもユーザーの側で開発する必要がある。ただそれでも量産に当たっては、やはり大手クラウドサービスと同様に証明書付きでデバイスの登録を必要とするのが普通だし、これを最小発注個数4000個で請け負ってくれるサービスはほかには類を見ない。

さて、このTrust&GoとTrustCustomの中間に位置するのがTrustFlexである。特徴としては、基本的にはTrust&Goと同様の機能を提供できるが、個々にその機能を使う/使わないのカスタマイズが可能である。またTrust&Goには無い機能(たとえばOTA Updateの検証機能)などもあらかじめ用意されており、ほとんどの用途はTrustFlexで提供される機能の組み合わせで構成可能である。

先にTrust&Goのところで挙げた、AWS IoTにLoRaWANで接続するといったケースでも、TrustFlexを利用すればひとつのATECC608Aでまかなうことが可能になる。Trust&GoがPoCや試作向けであるのに対し、その意味でTrustFlexは量産向けのサービスということになる。

## 必要となるノウハウやテクニカルなサポートを提供するAvnet

ただカスタマイズが可能、ということは逆にそのカスタマイズ可能な項目のことをきちんと理解している必要がある。これには相応のセキュリティに関する知識が必要だ。

TrustFlexではサンプルコードとして、AWS IoT/Azure IoTと3rd Party TLS(WolfSSL/mBED TLS/Linux)の3種類が提供されているが、このサンプルコードを読むだけでこと足りるのであれば、そもそもTrustFlexである必要性が薄い(Trust&Goでもまかなえる可能性が高い)のが正直なところである。

こうした場合に頼りになるのがAvnetである。Avnetは単にTrust&Go/TrustFlex/TrustCustomの購入手続きを行ってくれるだけではなく、カスタマイズに必要なテクニカルサポートやコンサルティングも提供してくれる。加えて、セキュリティの知識をもっと得たいという場合には、トレーニングを含めた包括的なサービスも提供してくれる。

セキュリティ対応に必要な事柄や知識を十分に理解し、実装の経験もあるユーザーであれば、ATECC608Aだけを手に入れれば迅速に対応ができるだろう。しかしながら、そこまでの知識や経験が無いにも関わらず、要件としてセキュリティ対応を求められているのであれば、MicrochipのProvisioning Serviceと、これをカバーするAvnetのサービスを検討してみることをおすすめしたい。

急がば回れではないが、結果としてこうしたサービスを受けることが、きちんとセキュリティ対策を行った製品を出荷するための一番の近道になることは珍しくないからだ。




■お問合せ先
AVNET
アヴネット株式会社
〒150-6023 東京都渋谷区恵比寿4丁目20-3 恵比寿ガーデンプレイスタワー23F
TEL：03-5792-9820　FAX：03-5792-9703
http://avnet.me/MCHP-security