インフィニオン セキュリティ パートナー ネットワーク (ISPN)

セキュリティ
パートナー
プリファード

パートナー ユースケース

公開鍵認証基盤(PKI)と OPTIGA™ TPMによる 強力なデバイスID

クラウドベース・インフラのメリットと、クラス最高のハードウェア＆ソフトウェアベースのセキュリティ技術を組み合わせることで、製造から事前設定まで、お客様のIoTを保護します。

製品

OPTIGA™

ユースケース

アプリケーション・コンテキストおよびセキュリティ要件

産業用のエンドポイントや機械におけるインターネット対応機器が増加するにつれて、セキュリティや機器に対する強力な認識機能の必要性が、サイバーセキュリティの観点からもっとも重要となっています。これは従来の運用技術では困難です。

課題

堅牢で信頼性高いメカニズムを構築するのに必要なシンプルで強力なセキュリティソリューションを見つけるのが、デバイスメーカーにとって難しいことがあります。多くの場合、機能環境に制限が設けられていることによりますが、製造環境における信頼性やセキュリティ制御が不十分であることが原因のこともあります。こうした問題の解決として、OEMメーカーが情報セキュリティを製品の新たな売りにすることが多く、こうした企業はサイバー攻撃に対する保護が必要であることをよく理解しています。

実装

OEMメーカーは、ハードウェアベースのTPMとソフトウェアベースの公開鍵認証基盤 (PKI) を組み合わせることで、信頼性の高い製造環境に、デバイスの強力な完全性証明および検証の機能を導入でき、頑強で信頼性の高いIDを持つデバイスを工場出荷できます。性能が実証されているPKI技術とハードウェア・ベースの「信頼のルート（root of trust）」アプローチを使用し、GlobalSignのアイデンティティ・セキュリティ・ソリューションは、相互に確実な通信を行うデバイスの信頼性の高いエコシステムを、効果的に確立することができます。

ユーザーにとってのメリット：

› ユーザーは、正規製品の1つであるとしているデバイスが、本当にその企業もしくはそのパートナーによって製造されたのか確認できます

› ユーザーは偽造品がシステムに接続されるのを防止し、ブラックマーケットやグレーマーケットのデバイスを減らすことができます。

› ユーザーは、このソリューションによって確認されたデバイス識別情報を活用して、対応するサブスクリプション/合意レベルに基づき、顧客が利用できる機能セットを選択的に制御できます。

ソリューション

セキュリティソリューションは、GlobalSign証明書を製造されたデバイスに提供するために使用されます。このステップは、生産サイクルの終盤にかけて行われることがありますが、品質評価もしくはファームウェア初期化過程において行うことが好ましく、または現場で基板実装工程でも行うことができます。

生産ライン・インフラは、GlobalSignクラウドまたはオンプレミスのホスティングサービスに接続・統合し、ソリューションを有効にする必要があります。

インフィニオンの OPTIGA™ TPM は、物理的に実装するチップで、製造装置の設計に組み込む必要があります。

アーキテクチャ上は、システムのサブコンポーネントがプロビジョニングデバイスとして機能します。このサブコンポーネントは、デバイスにインストールされたTPMの下流にあるアップストリーム、および前述のGlobalSign証明書プロビジョニングサービスの2つのコンポーネントと統合するソフトウェアを実行します。

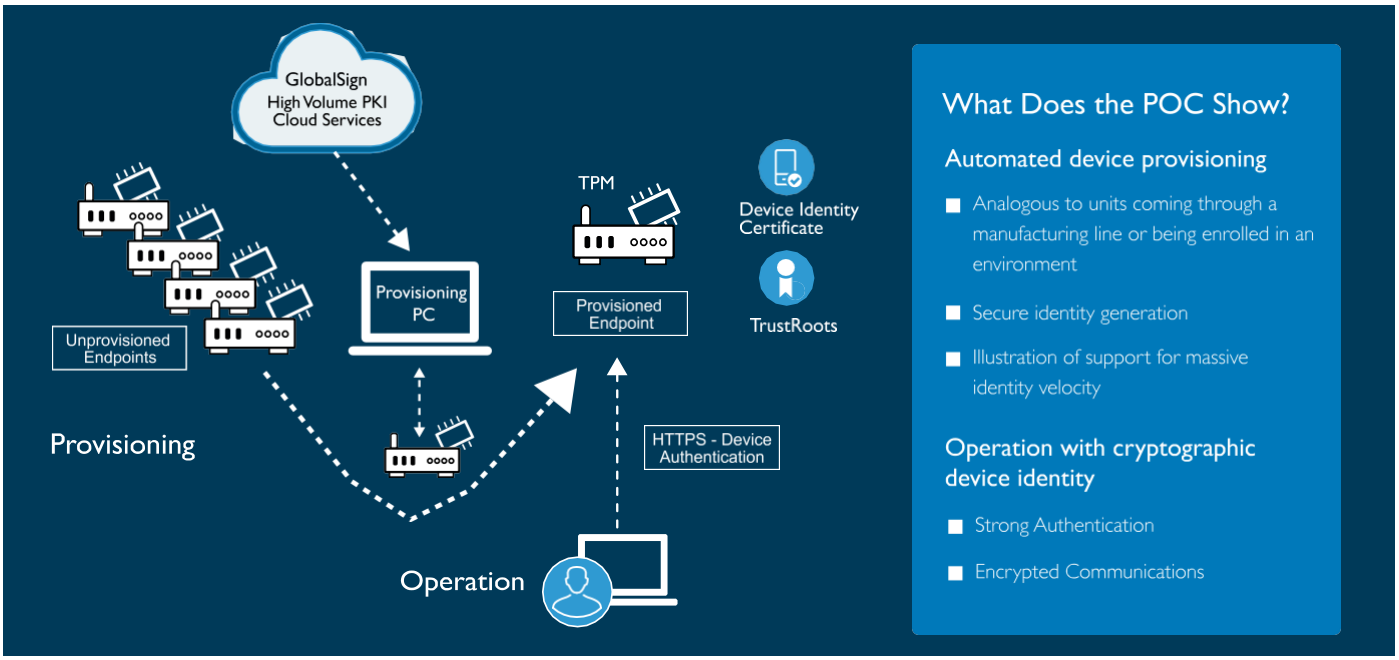
OEM. ソリューションは、プロビジョニングソフトウェアがコールを行うことができ、証明書の発行に先立ちハードウェアコンポーネントの信頼性検証を実行するREST API (Representational State Transfer Application Programming Interface) で構成されます。実際のプロビジョニングデバイスのアーキテクチャは、ケースバイケースで、OEMごとに決定・開発されます。

オンプレミス機器の物理的なセキュリティは、場合によってOEMによって確保する必要があります。

ソリューションについての詳細は、YouTubeの動画をご覧ください。：http://youtu.be/j8scQ_atQBg

インフィニオン製品の主な利点

インフィニオンの OPTIGA™ TPM は、強固なデバイスID (Strong Device Identity)ソリューション に不可欠です。暗号コプロセッサがデバイスの秘密鍵を安全に保存することができ、前述のハードウェアの指紋同等のIDの証明を支援できるからです。



セキュリティ パートナー プリファード

パートナー

インフィニオン セキュリティ パートナー ネットワークのパートナーは、お客様のビジネスを揺るがせかねない脅威を理解し、ビジネスを守るためのソリューションを提案・構築し、実装します。 インフィニオンは、システムセキュリティに対する能力と、強固で信頼性の高いセキュリティソリューションを設計・提供できるかどうかに基づき、パートナーを選んでいます。パートナーのビジネス内容は、セキュリティコンサルティング、セキュリティソリューションの提供、電子設計、システムインテグレーション、トラストサービス管理など多岐にわたっています。そのうちのいくつかは市販品ですが、それ以外のものはカスタム品です。

GMOグローバルサイン株式会社

GMOグローバルサイン株式会社は、トラステッドIDおよびセキュリティソリューションの大手プロバイダーとして、世界中の店舗、大企業、クラウドサービス・プロバイダー、およびIoTイノベータが安全なオンライン通信を行い、無数の検証済みIDや、自動承認、暗号化を管理できるようサポートしています。大規模な公開鍵暗号基盤 (PKI) およびIdentity and Access Management (IAM)ソリューションにより、IoE (Internet of Everything) を構成する何十億ものサービス、デバイス、人、モノを保護します。同社はアメリカ、ヨーロッパ、アジアにオフィスを構え、世界各地に300人以上の従業員と5,000人のグローバルパートナーがいます。

インフィニオン セキュリティ パートナー ネットワークにおけるGMOグローバルサイン株式会社の役割

GMOグローバルサイン株式会社は、OPTIGA™ TPMなどのインフィニオン製品を活用したデバイスIDおよびセキュリティソリューションを提供しています。これらのセキュリティソリューションの対象分野は、スマートな製造、車載、産業オートメーションなど、さまざまなIoT分野です。

共同技術パートナーシップは、IoT開発者が、PKIを活用してハードウェアを保護し、スケーラブルな方法で通信に強力な認証、暗号化やプライバシーを実装するのをお手伝いします。

GMOグローバルサイン株式会社は、PKIおよびSSL(Secure Sockets Layer)技術を使用する上での経験と専門知識と、包括的な製品ラインアップにより、小規模および大規模なビジネス環境におけるサイバーセキュリティ問題を解決します。

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 05 / 2016

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (www.infineon.com).

Please note!
THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND ANY INFORMATION GIVEN HEREIN SHALL IN NO EVENT BE REGARDED AS A WARRANTY, GUARANTEE OR DESCRIPTION OF ANY FUNCTIONALITY, CONDITIONS AND/OR QUALITY OF OUR PRODUCTS OR ANY SUITABILITY FOR A PARTICULAR PURPOSE. WITH REGARD TO THE TECHNICAL SPECIFICATIONS OF OUR PRODUCTS, WE KINDLY ASK YOU TO REFER TO THE RELEVANT PRODUCT DATA SHEETS PROVIDED BY US. OUR CUSTOMERS AND THEIR TECHNICAL DEPARTMENTS ARE REQUIRED TO EVALUATE THE SUITABILITY OF OUR PRODUCTS FOR THE INTENDED APPLICATION.

WE RESERVE THE RIGHT TO CHANGE THIS DOCUMENT AND/OR THE INFORMATION GIVEN HEREIN AT ANY TIME.

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life endangering applications, including but not limited to medical, nuclear, military, life critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.