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

Ubiquitous
TPM Secure Boot

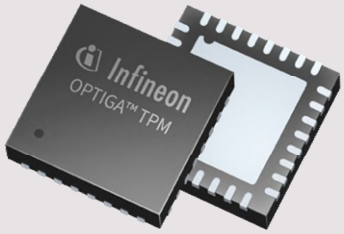
Ubiquitous AI Corporation

Ubiquitous TPM Secure Bootをお使いになれば、ブートおよびOSのソフトウェアが改ざんされていないこと、メーカー検証済みのソフトウェアバージョンであることが保証されます。

Ubiquitous
TPM Security

製品

OPTIGA™ TPM



www.infineon.com/ispn

Ubiquitous AI Corporation

ユースケース

アプリケーション・コンテキストとセキュリティ要件

今までネットワーク対応でなかった機器がネットワーク接続機能を備えるようになると、プロセス内では、さまざまなセキュリティリスクへの対策が必要になります。

特に自動車業界では、セキュリティ対策へのニーズが増加しています。Over The Air (OTA) による電子制御ユニット(ECU)のファームウェア更新では、ファームウェア更新が適切か、更新ファームウェアが信頼できるかを評価する必要がますます高まってきています。さらに、自動運転、ADAS（先進運転支援システム）、コネクテッドカーの普及に伴って、サイバーセキュリティに対する脅威が増大しています。

走行を安全に制御するためにセンサーデータの安全な処理、送受信データの真正性の保証、ハッキングの脅威への対処、ECU相互間のメッセージの認証など、さまざまなプロセスをセキュアに実行することがますます重要になっています。

このようなアプリケーションのセキュリティは、車載用途だけでなく、あらゆるIoT機器について、きわめて重要になってきています。

課題

ファームウェアの完全性を検証し、データの真正性を保証するにあたっては、車載用ECUやIoTデバイスの限られた資源を使いながらも、厳密なタイミングで要求に応答して、高い性能を実現しなければなりません。車載ECUの起動時には、ファームウェアの完全性を迅速かつ安全に検証する必要があります。

また、自動運転用のセンサーデータの処理には、データの認証ときわめて厳しいタイミング要件への対応が必要です。

実装

Ubiquitous TPM Securityは、IoT機器など、組み込み機器用のOPTIGA™ TPMの性能を最適化する、「小型」「軽量」「高速」なSecure Bootおよびトラステッド・コンピューティング・グループ (TCG) およびTCG Software Stackを利用したソリューションを提供します。

Ubiquitous TPM SecurityのSecure Bootソリューションは、IoT機器で利用されるOSレス環境あるいはRTOSをサポートするように設計されており、使用環境に応じたセキュリティと性能を両立する柔軟なカスタマイズ性を備えています。株式会社ユビキタスAIコーポレーションは、セキュリティの実装に不慣れな開発者でも対応しやすい、秘密鍵および公開鍵の管理、先進的暗号処理など、最適なセキュリティソリューションを提案しています。

電子認証局が発行する公開鍵基盤 (PKI) 証明書と組み合わせ、株式会社ユビキタスAIコーポレーションは、高度なコード署名、サービス認証などのソリューションも提案しています。

ユーザーにとってのメリット：

- リッチOSのみでなく、OSレス環境やRTOS IoT機器にも対応
- CPU 資源 (ROM、 RAM容量など) が要件に応じてカスタマイズ可能
- 機器単独、あるいはサーバと連携して使用
- Automotive Thin Profileのユースケースに対応

Ubiquitous AI Corporation

ソリューション

Ubiquitous TPM Security Secure Boot ソリューションは、リッチOSだけでなく、OSレスやRTOS IoT機器にも対応しています。
Ubiquitous TPM Securityは、要件に応じてCPU資源（ROMやRAMの容量など）のカスタマイズが可能です。
また、Ubiquitous TPM Securityは、機器単独、あるいはサーバと連携させて使用できます。

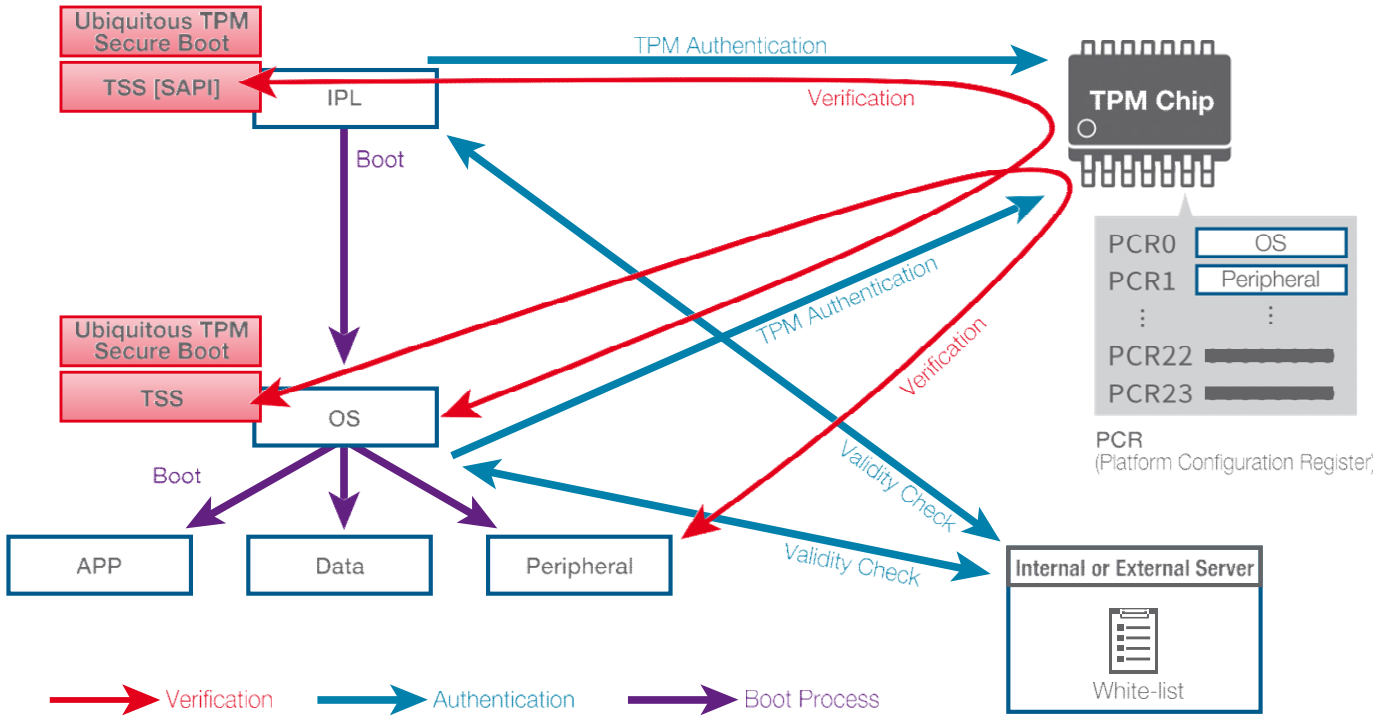
また、Ubiquitous TPM Security Secure Bootソリューションは、OPTIGA™ TPM のAutomotive Thin Profileのユースケースにも対応予定です。

さらに、Ubiquitous TPM SecurityのSecure Bootソリューションは、FIPS 140-2に加えて、FIPS 140-3にも準拠した設計になっています。FIPS 140-3は、今のところ草案の段階ですが、長期間にわたって使用できるように安全を考慮して設計されています。

OPTIGA™ TPM は、車載用アプリケーションに利用可能です。Ubiquitous TPM Security Secure Bootソリューションは、OPTIGA™ TPM のAutomotive Thin Profileのユースケースに対応予定です。

インフィニオンのOPTIGA™ TPM の主要なメリット：
OPTIGA™ TPM (Trusted Platform Module) は、標準化されたセキュリティコントローラの幅広いラインナップを取り揃え、組み込み機器およびシステムの完全性と信頼性を保護します。OPTIGA™ TPM セキュリティチップは、セキュリティ保護されたキーストアとさまざまな暗号化アルゴリズムへの対応により、豊富な機能で重要なデータやプロセスを強力に保護します。

ブート・シーケンス概要



パートナー

Ubiquitous AI Corporation

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。

株式会社ユビキタスAIコーポレーション

日本を拠点とする株式会社ユビキタスAIコーポレーションは、コンパクトで効率的で高速なソフトウェアソリューションで有名な車載系組込みソリューションの大手プロバイダーです。ソフトウェアソリューションの1つに、TPMソフトウェアセキュリティソリューションのUbiquitous TPM Securityがあります。

他の主要ユビキタスソリューションには、LinuxやAndroid用の高速ブートソリューション QuickBootと、IoT分野向けのコンパクトなネットワークスタックであるUbiquitous Network Framework があります。

株式会社ユビキタスAIコーポレーションは、人と人、人と物、そして物と物を「つなぐ」ことにより、ネットワークの利便性を享受できる「ユビキタス時代」の到来を加速する、そのようなソフトウェアの提供をお約束します。

株式会社ユビキタスAIコーポレーションのインフィニオン セキュリティ パートナー ネットワークへの貢献

株式会社ユビキタスAIコーポレーションは、InfineonのOPTIGA™ TPMのすべてのユーザーに、TPMソフトウェアソリューション Ubiquitous TPM Securityを提供しています。このソフトウェアソリューションは、他のソリューション同様に、安全で高速なブート機能など、セキュアブート機能やTCGソフトウェアスタックを提供し、多くのアプリケーションでご使用できます。株式会社ユビキタスAIコーポレーションは、IoT市場のみならず、自動車やPCのセキュリティにも注力しています。

株式会社ユビキタスAIコーポレーションは、近日中にV2Xソリューションの提供を開始予定です。

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 01 / 2018

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.