Security Partner Preferred

Partner Use Case

Ubiquitous TPM Secure Boot

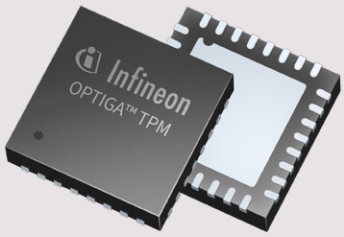
Ubiquitous

Ubiquitous TPM Secure Boot verifies both the Boot and Operating System (OS) software has not been tampered with, and is the manufacturer's verified version of the software

TP Ubiquitous TPM Security

Products

OPTIGA™ TPM



Infineon Security Partner Preferred

Use case

Ubiquitous

Application context and security requirement
Measures against various security risks are needed in processes where devices, that were not network compliant so far, now have network connection functions available.

Specifically the automotive industry has an increasing need of such security measures. Over The Air (OTA) updates of Electronic Control Units (ECU) firmware make it more and more necessary to verify the integrity of this firmware in order to evaluate whether these firmware updates are appropriate and whether the updated firmware can be trusted.
In addition, the importance of cyber security is increasing because of the spread of self-driving, Advanced Driver Assistance Systems (ADAS) and connected cars.

In order to safely process various sensing data and to carry out safe control of the vehicle, it becomes necessary to securely perform various processes such as checking the data authenticity to be transmitted and received, coping with the threat of attacks, and authenticating messages between ECUs.

And security in such applications is becoming extremely important not only for automobiles but all IoT devices.

Challenge
To verify the firmware integrity and to confirm the data authenticity, it is required to be able to respond to requests at severe timing and to demonstrate high performance by using limited hardware resources of automotive ECUs and IoT devices.
When ECUs in an automotive are started up, the firmware integrity has to be verified fast and safely.

Also, when handling sensing data for automatic driving, data authentication and responding to extremely severe timing requirements are necessary.

Implementation
Ubiquitous TPM Security provides solutions that utilize “small”, “light”, “fast” secured boot and Trusted Computing Group (TCG) Software Stack that optimize the performance of OPTIGATM TPM for embedded devices such as IoT devices.

Ubiquitous TPM Security’s Secure Boot solution is designed to support OS-less or RTOS assuming IoT devices, and also has flexible customizability to simultaneously achieve security and performance according to customer’s usage environment.
Ubiquitous proposes optimal security solutions such as private and public keys management and advanced cryptographic processing, even for developers who are new to security implementation.

In combination with the Public Key Infrastructure (PKI) certificate issued by the electronic certificate authority, Ubiquitous can also propose solutions such as advanced code signing, service authentication and others.

User benefits:
› Supports not only Rich OS but also OS-less or RTOS IoT devices
› CPU resources (ROM, RAM size etc.) are customizable according to requirements
› Can be used only with the device or in conjunction with the server
› Supports use-cases in Automotive Thin Profile

Infineon Security Partner Preferred

Solution

Ubiquitous

Ubiquitous TPM Security Secure Boot solution can support not only Rich OS but also OS-less or RTOS assuming IoT device. In Ubiquitous TPM Security, CPU resources (ROM, RAM size etc.) are customizable according to requirements. Also, Ubiquitous TPM Security can be used only with the device or in conjunction with the server.

And, Ubiquitous TPM Security Secure Boot solution is planned to support the use-cases in Automotive Thin profile with OPTIGA™ TPM.

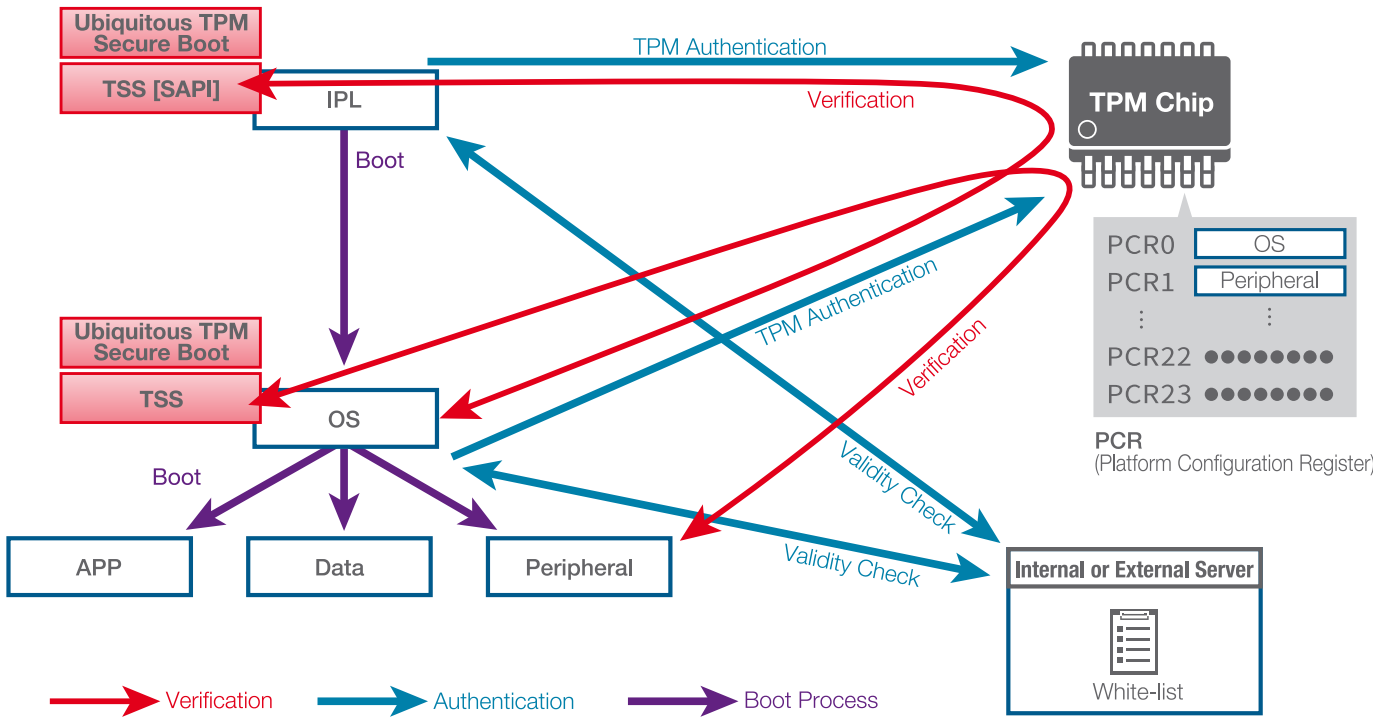
In addition, the Ubiquitous TPM Security Secure Boot solution is designed in compliance with not only FIPS 140-2 but also FIPS 140-3. FIPS 140-3 is currently in draft, and it is designed with consideration of safety that can be used for a long time.

OPTIGA™ TPM is applicable as automotive solution. Ubiquitous TPM Security Secure Boot solution is planned to support the use-cases in Automotive Thin Profile recommended by TCG.

Main benefits of Infineon product

OPTIGA™ TPM (Trusted Platform Module) offers a broad portfolio of standardized security controllers to protect the integrity and authenticity of embedded devices and systems. With a secured key store and support for a variety of encryption algorithms, OPTIGA™ TPM security chips provide robust protection for critical data and processes through their rich functionality.

General Outline of Boot Sequence



Security Partner Preferred

Partner

Ubiquitous

Partners from the Infineon Security Partner Network help you secure your devices and applications: understand which threats can undermine your business, propose solutions that will protect your business, build and implement such security solutions and, when relevant manage their operation. They have been selected by Infineon on the basis of their system security competence and ability to design and deliver strong and trustworthy security solutions. Their activities are diverse and include security consulting, security solution provision, electronic design, systems integration and trust services management. For some, offers are off-the-shelf; while for others, offers are custom-built.

Ubiquitous Corporation

Ubiquitous Corporation, based in Japan, is a publicly traded, leading Embedded and Automotive Technology Solution Provider famous for its compact, efficient and fast software solutions. One of the software solutions is a TPM software security solution, called Ubiquitous TPM Security.

Other main Ubiquitous solutions are QuickBoot - a fast boot solution for Linux and Android, and Ubiquitous Network Framework – a compact network stack for the IoT world.

Ubiquitous Corporation is committed to the provision of software that will accelerate the advent of the “ubiquitous age”, in which all the convenience of networks will be enjoyed through the connection of people to people, people to devices, and devices to devices.

Ubiquitous Corporation’s contribution to the Infineon Security Partner Network

Ubiquitous Corporation provides a TPM software solution called Ubiquitous TPM Security for all users of Infineon’s OPTIGA™ TPM. This software solution provides a secured boot function and a TCG software stack as well as other solutions, e.g. secured “fast” boot, and can be used in many applications. Ubiquitous Corporation specially focuses on the IoT market but also on the automotive and PC security.

In the near future, Ubiquitous Corporation will provide also a V2X solution.

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.