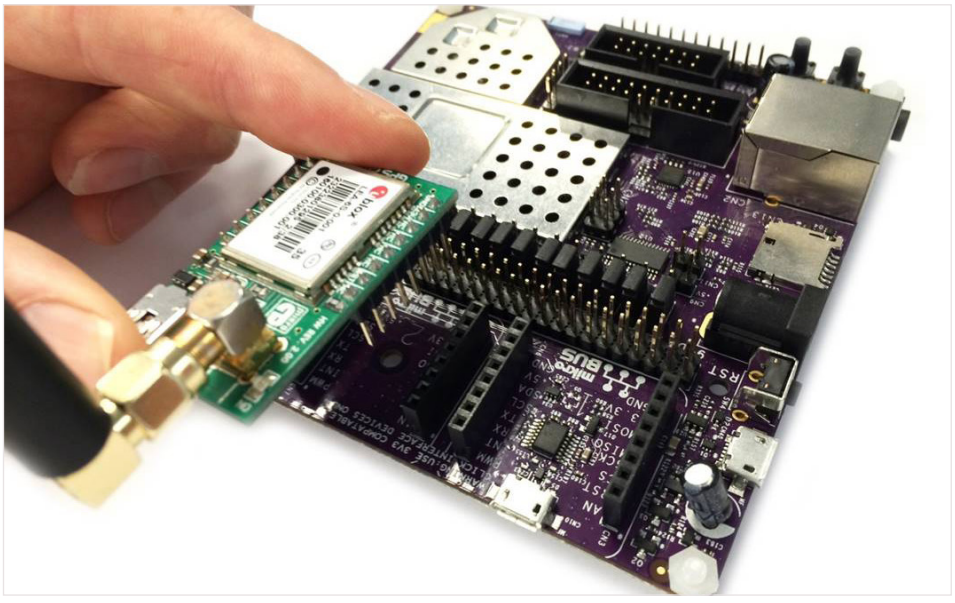
Security Partner

Partner Use Case

Create your own IoT Security

Infineon's OPTIGA™ TPM is integrated on a MIPS based IoT development platform.



Products

OPTIGA™ TPM

Security Partner

Use case

Application context and security requirement

The Creator Ci40 is an IoT development platform created in-house by Imagination Technologies. The Ci40 acts as an IoT hub aggregating data from multiple sensors and is capable of running the applications locally or in the cloud. Based on a 550MHz dual core, multi-threaded MIPS interAptiv CPU, the platform is more than capable of running Linux distributions such as OpenWRT while offering Wi-Fi, 802.15.4 and Bluetooth connectivity with embedded security enabled.

Challenge

Enterprise level IoT developers wishing to design a system with the Infineon OPTIGA™ TPM (Trusted Platform Module) solution have a ready made development platform that they can pick up on the open market which will help them to improve their time-to-market.

Implementation

To help accelerate security solutions with the Infineon OPTIGA™ TPM, developers are able to use open source examples with Creator Ci40. Specific examples of the TPM running with both the Universal Boot Loader (U-Boot) and the Linux platform are available on Github now:
https://github.com/CreatorDev/u-boot
https://github.com/openwrt/openwrt/pull/131
https://github.com/CreatorDev/Ci40-platform-feed/pull/69

The system can be used by default for a verified boot and with additional development can open the way for features such as measured boot, secret handling and rollback protection. Integrated TPM drivers in the Open-Wrt build system supported with the Creator Ci40, allow developers to use standard Linux interfaces for accessing the TPM for rapid development. A number of useful packages such as TPM-tools and TrouSerS have also been ported to the Creator platform.

User benefits

› Ready made IoT hub platform to accelerate development
› Platform is available in the open market place
› Open source reference examples are available
› Great for developing cloud, embedded device authenticated and trusted solutions
› Allows for scalable solutions
› TPM tools and TrouSerS ported to Ci40
› Standard Linux interfaces can be used to access TPM

Infineon Security Partner

Solution

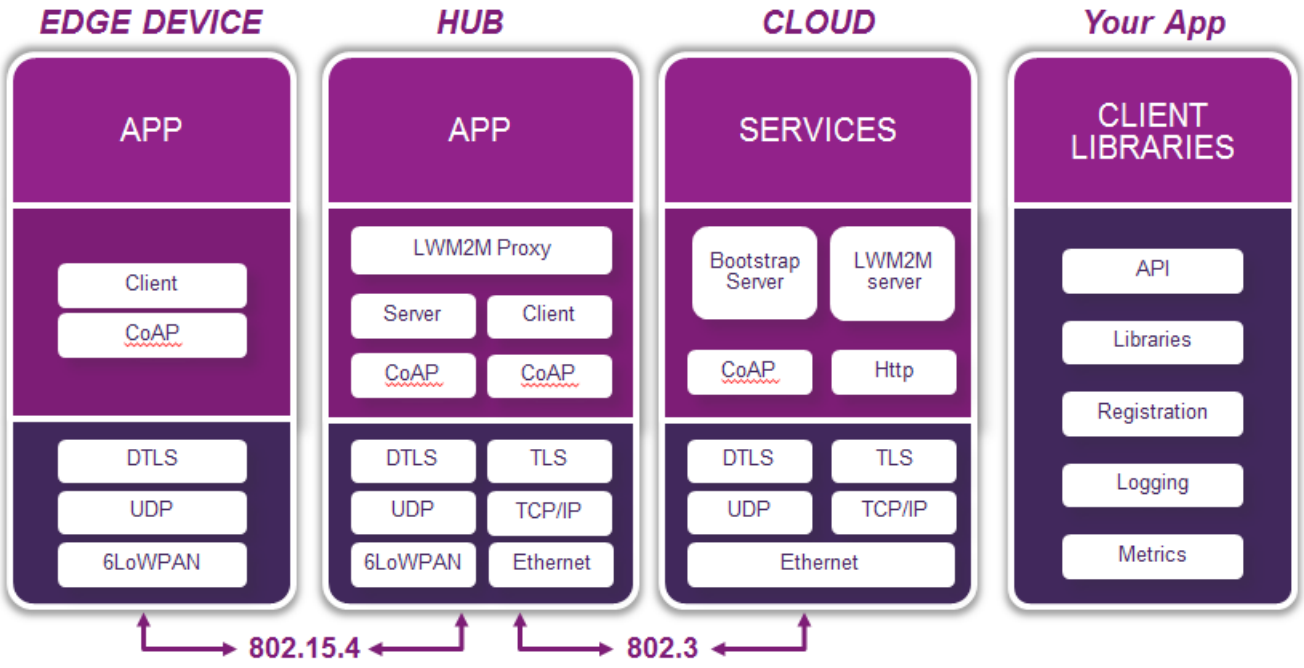
Imagination

Security proves itself again and again as a critical element in IoT development. This board allows developers to independently test and improve their security solution. An Infineon OPTIGA™ TPM v1.2 device is used as the verified boot solution implemented on the platform. Open source code is provided using standard Linux interfaces to access the TPM device. Certificates and keys can be stored and accessed in the TPM, building a development system that can show secured interaction with the cloud. The TPM tools and TrouSerS are ported to the Ci40 to help accelerate development work. Developers can also prove out roll-back protection.

Beyond the OPTIGA™ device, the platform also provides a multi-threaded dual core MIPS interAptiv CPU with 2 32/32kb L1 caches, a 512kb L2 cache and a range of off-chip memories that includes a 16 Mbit NOR Flash, 4Gbit NAND Flash, 2Gbit DDR3 SDRAM and an SD card slot for additional storage.

Powered off an external 9volt DC power supply or 5v USB source, the board acts as an IoT hub providing 802.11 AC 2x2 Wi-Fi 2.4 & 5G, 802.15.4 and Bluetooth Classic & LE wireless functionality for a mix of different IoT developments.

The development platform comes with a complete open source software stack to establish communication from the cloud, via the Ci40 IoT hub and the Constrained Edge Device to show an end-to-end system with end-to-end security.



Infineon Security Partner

Solution

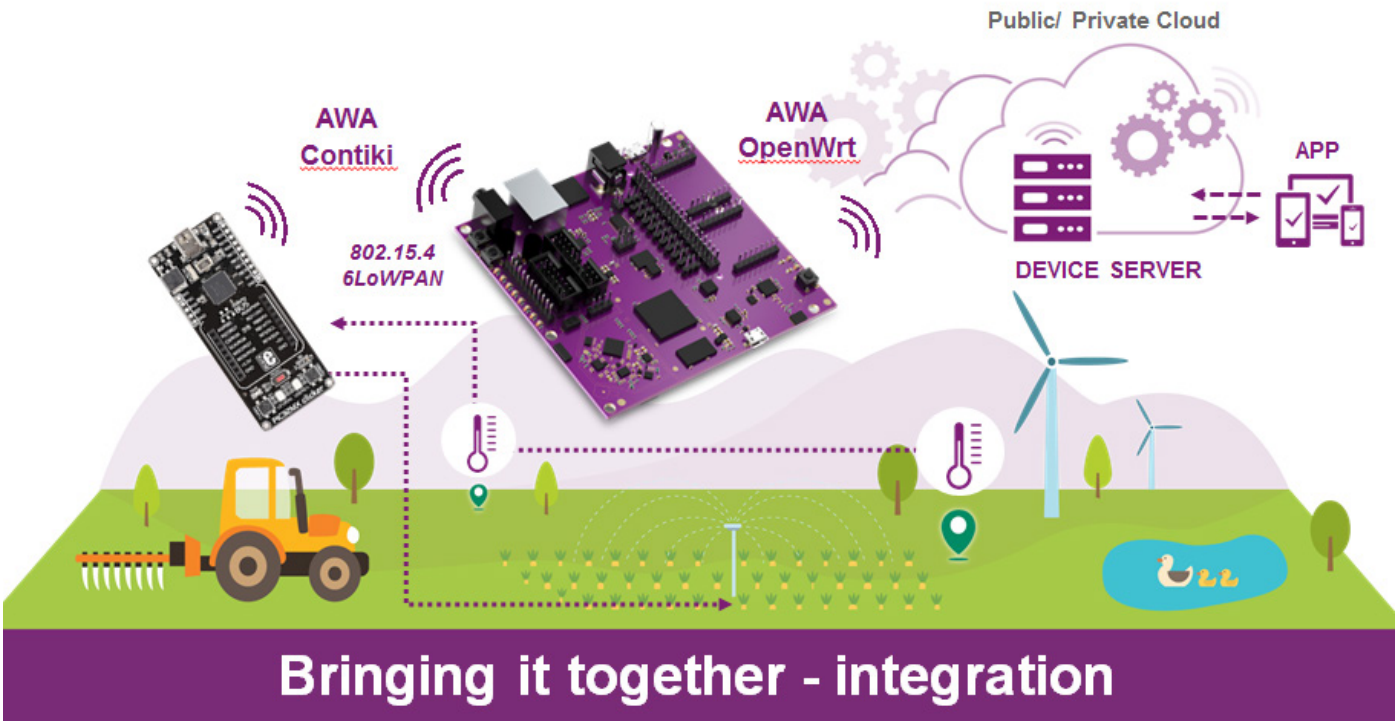
Imagination

Main benefits of the Infineon product

The Infineon OPTIGA™ TPM reduces operational risk. it enables developers to use firmware roll back protection; in order to prevent an attacker replacing newer securer software with older vulnerable software. It also supports measured boot; providing a log of platform configuration at boot for determination of trustworthiness.

This protects data flows in an IoT system such as on a “smart farm”, where data might be manipulated for financial gain.

http://creatordev.io/ci40-iot-dev-kit.html



Security Partner

Partner

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.

Imagination Technologies

Imagination is a global technology leader whose products touch the lives of billions of people across the globe. The company's broad range of silicon IP (intellectual property) includes the key processing blocks needed to create the SoCs (Systems on Chips) that power all mobile, consumer and embedded electronics. Its unique software IP, infrastructure technologies and system solutions enable its customers to get to market quickly with complete and highly differentiated SoC platforms. Imagination's licensees include many of the world's leading semiconductor manufacturers, network operators and OEMs/ODMs who are creating some of the world's most iconic products. Listed on the London Stock Exchange, with revenues of £120M Imagination employs around 1400 people globally.

Imagination Technologies contribution to the Infineon Security Partner Network

The Creator Ci40 IoT-in-a-box development kit offers a development platform that stretches from constrained devices to IoT hub and onto the cloud allowing developers to quickly and easily come up to speed with the security requirements of each stage. The open source main board, Ci40 IoT hub, contains an Infineon Optiga™ TPM device for key storage, verified boot and many other security features. The low cost development kit can be bought on the open market from worldwide distributors such as Mouser & RS. Along with the Infineon Optiga™ TPM the board also offers three common IoT radio standards soldered directly to the board, namely Wi-Fi 802.11 2x2 AC, Bluetooth Classic & LE and n 802.15.4 radio for 6loWPAN. If that's not enough the board also offers expansion ports for the addition of other radios, sensors and actuators. The kit is suitable for development in a wide range of markets from IoT to consumer.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 01 / 2017

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).