Security Partner

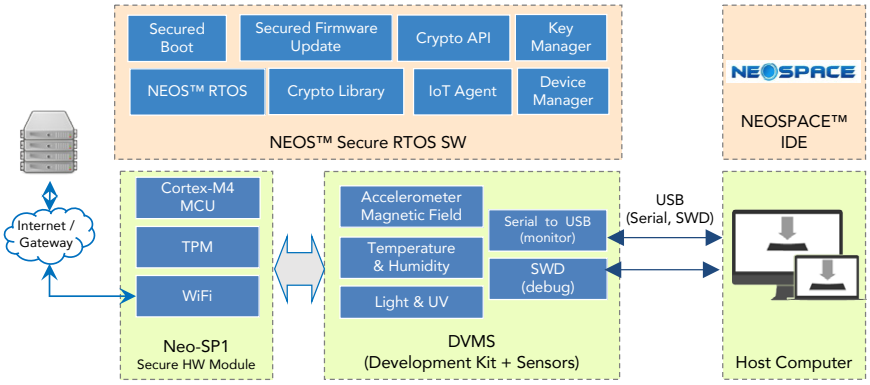
mds technology

Partner Use Case

NEOS™ RTOS based Security Platform for IoT Devices

The NEOS™ RTOS based IoT security solution offers ready-to-go device management & key management system integration.

NEOS IoT Security Platform



Products

OPTIGA™ TPM

Security Partner

Use case

Application context and security requirement
NEOS™ IoT Security Platform provides NEOS™ RTOS (Real Time Operating System) based security solution with cryptography library, device management solution, crypto-key management solution and Trusted Platform Module (TPM) library for resource constrained and unmanned IoT device environment.

Challenge
Today's IoT devices face two major challenges: constrained resources (e.g. limited CPU performance, memory size and battery capacitance) and remote operation (i.e. no direct human input). Given these conditions, hardware-based solutions can enable remote device management that is far more secure than that typically provided by general purpose operating systems, like Linux or Windows.

Implementation
The NEOS™ IoT Security Platform is a real-time operating system that enables secured device and key management solutions remotely, including secured booting and firmware updates and its own crypto-library.

The platform drives an OPTIGA™ TPM chip which generates locally secured Public Key Infrastructure (PKI) keys. These provide security throughout the boot and firmware update processes via signature verification. The Operating System (OS) image and Firmware image are signed with the crypto-keys, thus protecting the device from executing or updating malicious code.

Controlling and monitoring IoT devices remotely is straightforward thanks to the integrated Neo-IDM™ function, based on international standard protocol LwM2M for device management. Furthermore, iKMS, the Key Management System for IoT, is also integrated; key generation and distribution to both device and server are handled through the iKMS, which satisfies international standards.

NEOS™ RTOS is a small sized, robust, and field proven real-time operating system, which is strictly verified and certifiable for DO-178B Level A system.

The benefits of the NEOS™ IoT Security Platform are as follows:
- Combined hardware- and software-based approach enables IoT service providers or integrators to deploy reliable and secured IoT services for remote and resource-constrained devices and servers
- Ready-to-use, real-time operating system with integrated remote device and key management solutions for secured IoT services
- OPTIGA™ TPM offers cost effective, robust security which can be easily managed via the platform's TPM driver interface library

Security Partner

Solution

In order to secure reliable IoT service, the following functions must be provided.

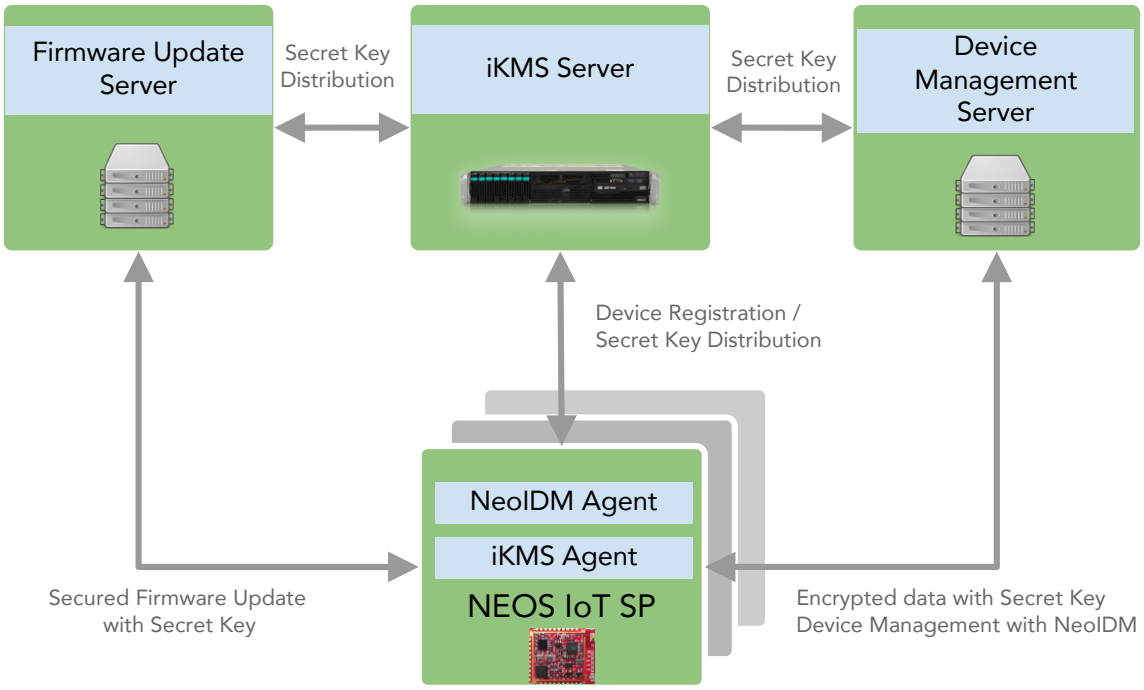
› Mechanism to securely generate secret keys
› Ability to distribute generated secret key between IoT server and IoT device
› Secured storage of the generated security key with additional hardware-based protection against external attacks.
› Standard encryption / decryption algorithm for encrypted communication for end-to-end security
› Verification function to protect against malicious firmware updates to IoT device
› Verification function to provide secured boot of IoT device
› IoT device management and monitoring function

The NEOS™ IoT Security Platform provides cryptographic algorithms for data encryption/decryption, such as AES and TDES. It uses an Infineon OPTIGA™ TPM to securely generate and store the secret key required for encryption. The robust, hardware-based security the TPM provides not only allows reliable and secured device-to-device and device-to-IoT server data communication for remote device management but provides protection from attackers, via signature verification, during the otherwise vulnerable booting and firmware update process.

The keys are distributed to the registered IoT devices and servers via the platform's integrated key management system, iKMS, and its integrated Neo-IDM™ device management system (based on international standard LwM2M), facilitates remote controlling and monitoring of devices from the IoT server.

Main benefits of the Infineon product

The Infineon OPTIGA™ TPM reduces operational risk and is a hardware-based security solution for resource-constrained IoT devices. A device management and key management solution are integrated for ready-to-go fast development and service deployment.



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.

MDS Technology

MDS Technology, a leader in embedded solutions in Korea, has been focusing on the embedded solutions industry for more than 20 years, having served over 1,500 clients, including Samsung, LG, Hyundai, and SK. We provide customers with global cutting-edge embedded solutions and aim to help customers reduce time-to-market while improving quality by providing the most effective total solutions for embedded industries, such as industrial IoT, automotive, defense/aerospace, mobile, digital device, etc. By integrating existing industrial systems with sensors, wired and wireless communications and network infrastructure, security, big data and cloud technology, we are providing more efficient and intelligent end-to-end solutions for IoT realization throughout the industry. In addition, we are the Microsoft Strategic Partner and Cloud Solution Partner (CSP) in Korea as well as South East Asia, India, and Oceania. We have utilized that experience transforming to provision of IoT solutions and services that extends the value of the device through integration with Microsoft Azure cloud platform.

MDS' contribution to the Infineon Security Partner Network

The NEOS™ IoT Security Platform is a real-time operating system that enables secured device and key management solutions remotely, including secured booting and firmware updates and its own crypto-library which is driven by OPTIGA™ TPM chip that generates locally secured PKI keys. By integrating OPTIGA™ TPM, it provides security throughout the boot and firmware update process via signature verification. The OS and firmware image are signed with the crypto-keys, thus protecting the device from executing or updating malicious code. The NEOS™ IoT Security Platform can be widely used in various IoT industrial applications including smart grid and water cleaning facility.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 05 / 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).

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.