Security Partner

MACNICA

Partner Use Case

Security lifecycle management of IoT

Remote key management and seamless environment integration between IoT terminals and the cloud.

Products

OPTIGA™ Trust P

Security Partner

Use case

Application context and security requirement

IoT (Internet of Things) devices are commonly used at the customers' site, and as such, the time needed for an attacker to compromise a device can be quite high. If the attacker can manage to steal the device key, this time needed is substantially reduced. In such an event, if a mechanism existed to deactivate this compromised key, the potential risk and attack could be mitigated.

Challenge

The first point of action is to build a server that can manage keys and certifications from remote locations. As a result, even if there is a sudden incident, you can revoke or discard the key remotely and reduce the security risk more by renewing the key periodically. The second point is that the key management server needs to be built in a high security environment to securely manage the keys.

Implementation

By integrating embedded development experience with OPTIGA™ solutions and secured IC (integrated circuit) chips technology to distribute and manage confidential data through the network, our solution provides key lifecycle management with a high security server to protect IoT terminals in factories from threats such as interception, tampering, and taking over.

Benefits for the user:

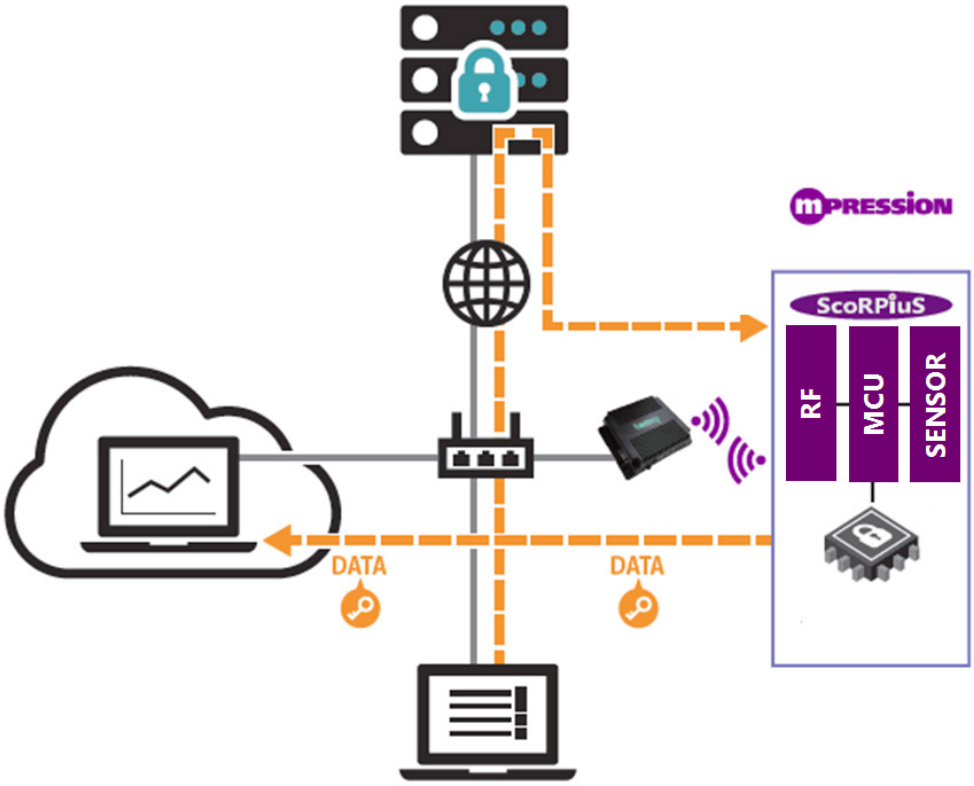
› Secured and reliable cloud for IoT and data collection
› Turnkey key lifecycle management solution
› Terminal platform and key management server combination allows fast and seamless environment integration

Security Partner

Solution

An OPTIGA™ product is embedded in the IoT terminal storing the keys and certificates. The key management server's task is to allow only legitimately authenticated IoT devices to access the cloud, preventing access from impersonator and counterfeit devices, as well as protecting end-to-end data communication between the IoT terminal and the cloud. Using the know-how accumulated in the development and operation of financial systems, it becomes possible to generate, revoke and update keys for remote IoT terminals with a highly secured key management server.

Even when the IoT terminals have been distributed to the market, keys can still be managed remotely due to the advantage of the OPTIGA™ solution, enabling a flexible response to sudden security incidents.



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.

Macnica

Macnica, employing 2600 worldwide, provides services and high-value products, including semiconductor components, electronic devices, network equipment and software to Japanese and foreign electrical and electronics manufacturers who lead the automotive, industrial and telecommunication industries.

Macnica's outstanding engineering capabilities are considered unique. Through business development with promising ventures worldwide, Macnica has gained the ability to identify and cultivate new products and technologies. The company has the planning capabilities to discover true needs and to create optimal solutions, and by making the best use of the customer's potential strengths, Macnica works to maximize value for its customers.

Macnica's contribution to the Infineon Security Partner Network

Macnica provides license based system level turn key secure solutions including applets, APIs for Infineon's OPTIGA™ product family, middleware with Certification Authorities (CA), software stacks related to key management systems and maintenance services for the Industrial IoT market working with our cutting edge partners.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 06 / 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.