Security Partner

Partner Use Case

Device identity management solution for smart homes

IKV's iBadge solution uses a cryptographic authentication chip to offer IoT service providers a hardware-based security management platform. The device authentication and counterfeit protection of this platform will secure business model and profitability.

Products

OPTIGA™ Trust SLS 10ERE

Infineon
Security
Partner

Use case

Application context and security requirement

IoT devices possess special characteristics of easy connection and sustainable security. The IoT assets and architecture require the effective protection from threats such as counterfeiting.

Challenge

A zero security solution will bring risk of potential business loss. A software-based security solution is better than no security, but easily accessible, reproducible and reversible. IoT devices need a cost effective security solution to make connected devices with unique identification and trustworthy authenticity, and good countermeasure to counterfeit and device hacking.

Implementation

iBadge device identity management offers a hardware-based security solution for authentication and management. Devices equipped with the iBadge solution are easy to implement, with the following capabilities:

- No manual work is required during the production process
- A unique chip identifier and authentication key
- No need for complicated cryptographic algorithms in the firmware
- Device management via web-browser or smart-phone app
- Easy management of device ID and other data, through our back-end module

User benefits

- Cost effective hardware-based turnkey security solution for IoT devices
- Shorter time to market and faster deployment for device providers
- Business model and profitability is secured

Smart-home device manufacturers in China have adopted the iBadge solution and commented “...iBadge helped our engineers to quickly implement security mechanisms on our devices. And we didn’t need to consider the complex cloud protocols for the protection on device messages back and forth between our server and the devices....”

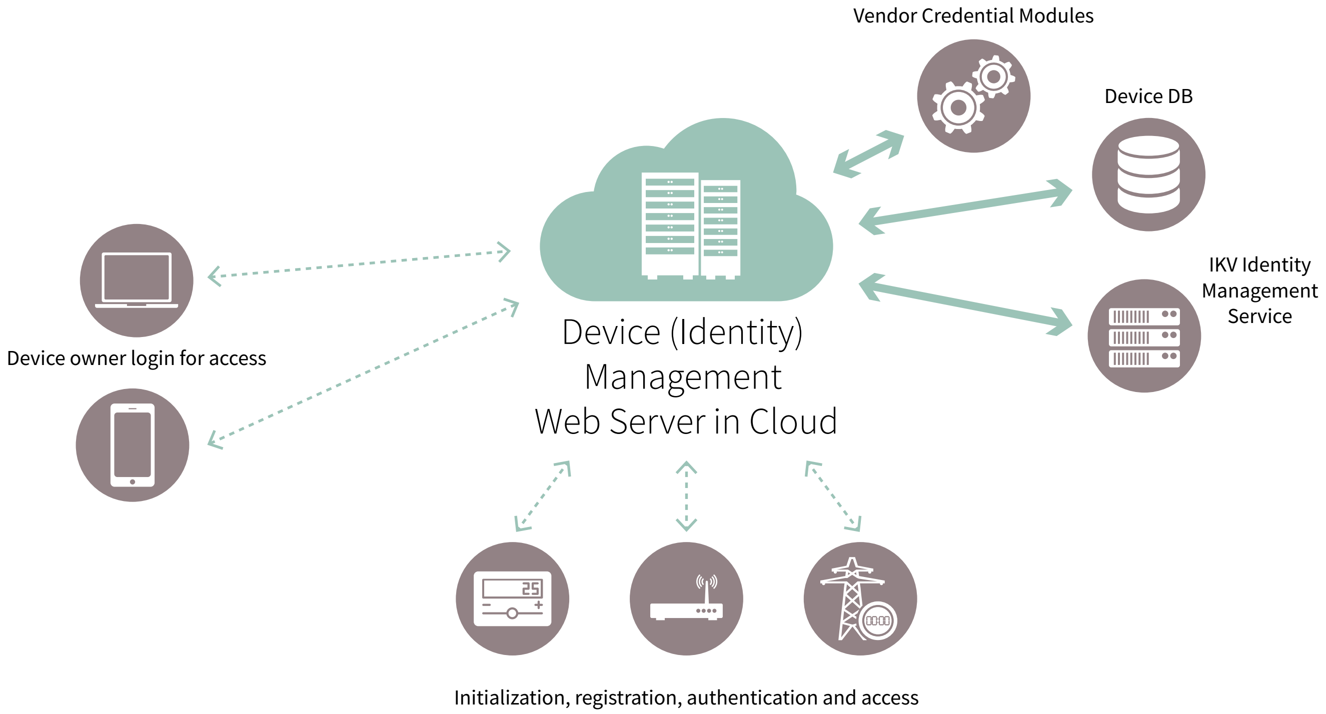
Infineon Security Partner

Solution

Most of the IoT devices do not design any security mechanisms, or the security mechanism is very weak, which means the hackers can control the devices easily and retrieve data for unauthorized activities. To avoid these kind of threats, the devices' security mechanism must design within and run effectively.
iBadge Device Identity Management provides the total solution for IoT device security. iBadge security solution consists of three function blocks:

1) Cloud applications and data server with iBadge cloud modules in it, including device database, vendor credential modules, and IKV identity management service.
2) IoT devices with iBadge device application protocol interface and Infineon OPTIGA™ Trust security chip mount on it.
3) PC or mobile applications with iBadge security protocols in it. Infineon OPTIGA™ Trust supports elliptic curve cryptography cryptographic, plays the key role in iBadge solution. IoT device providers own unique sets of root keys associated with chips at Infineon production line.

Through the IoT gateway and cloud network service, the application and data server generates a challenge and then sends to OPTIGA™ Trust chip to trigger ECC computation in it. After ECC computation is complete, the server will read a response code from OPTIGA™ Trust and confirm its validity. Once the validity confirmation is received, the connections between IoT devices and IoT device user, and applications data server are set up securely.


Vendor Credential Modules
Device DB
IKV Identity Management Service
Device owner login for access
Device (Identity) Management Web Server in Cloud
25
00:00
Initialization, registration, authentication and access

Main benefits of the Infineon product

- The unique identifier and root key are burned into the device automatically during packaging and testing stage, and is convenient for mass production and reduces cost.
- Strong hardware-based security using ECC asymmetric cryptographic algorism to protect unique ID and root key
- Turnkey support for both host and device side, including authentication libraries and application protocol interface for device management

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.

IKV (InfoKeyVault Technology)
IKV was founded in August 2006, and ever since has persisted in their modus operandi to "protect our customers' digital assets through professionalism and creativity."

Although the major customers locate at the Greater China area, their products by the help of IKV are pervasively adopted worldwide because of the global logistic model. In the past few years, IKV has successfully delivered the hardware-based security products and solutions to some security-aware industries, such as gaming, military-grade devices and mobile computing applications. Noway, IKV staffs devoted themselves to develop the security solutions for the IoT customers. "iBadge" is the most remarkable. The company has US$600K capital and US$1,000K revenue in 2015.

IKV's contribution to the Infineon Security Partner Network
As an independent design house of Infineon, IKV helps the customers of the security chips to efficiently and effectively optimize the protection on their own products. IKV leverages SLE 97, OPTIGA™ TPM, OPTIGA™ Trust product series and create the value of these chips by providing the customer's systems with the customized firmware API and COS (Chip Operating System). With IKV's support, the development cycles can be reduced and the results are more reliable in security. The most significant references of IKV include the first SLE 97 -equipped BitCoin wallet in the world, "CoolWallet", and "iBadge" solution based on OPTIGA™ Trust authentication chips. IKV has also implmented a leading "secure boot" solution by integrating SLE 97 with the most secure field programmable gate array of the world to help the cutomers to protect the sensitive firmware codes in the commerical System on Chips.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 05 / 2016

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.