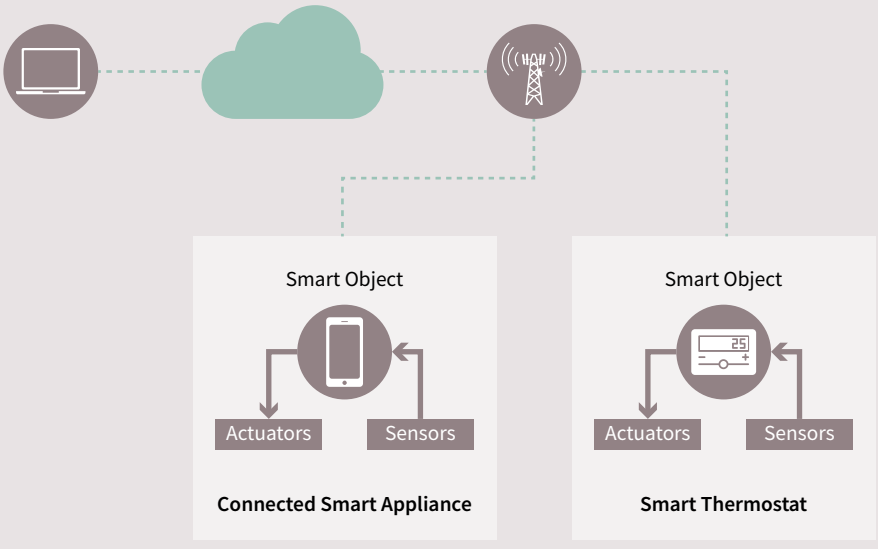
Security Partner

Partner Use Case

# Securing connected IoT with Java

Javelin-SC: intelligent and efficient IP-addressable security building blocks for connected devices and network nodes.




## Products

SLE 78

Security Partner

# Use case

**Application context and security requirement**

Internet of Things is the network of connected devices which collect and store data, share it within the network and eventually execute functions related to this data. However, unattended and remote peripherals connected to Internet are targets of malware and can be taken over as a platform for further attacks, posing serious risks in the context of cyber-physical devices.

**Challenge**

Securing Internet connected devices poses several challenges:

› Secure content loading, storage and execution, as well as secret keys and certificates storage must be realized
› Defensive software design is costly and security experts are scarce

**Implementation**

The solution is intelligent and efficient IP-addressable security for connected devices and network nodes. Efficiency is realized by leveraging proven JavaCard and GlobalPlatform architecture that secures billions of SIM cards, ePassports and EMV payment cards worldwide. As device business logic is written in Java language, the learning curve and software defects are minimized. Devices' operating system and applets are field upgradable, maximizing flexibility and security lifecycle. Easy In/Out interfaces allow for multiple sensors, actuators and I/O lines.

**User benefits**

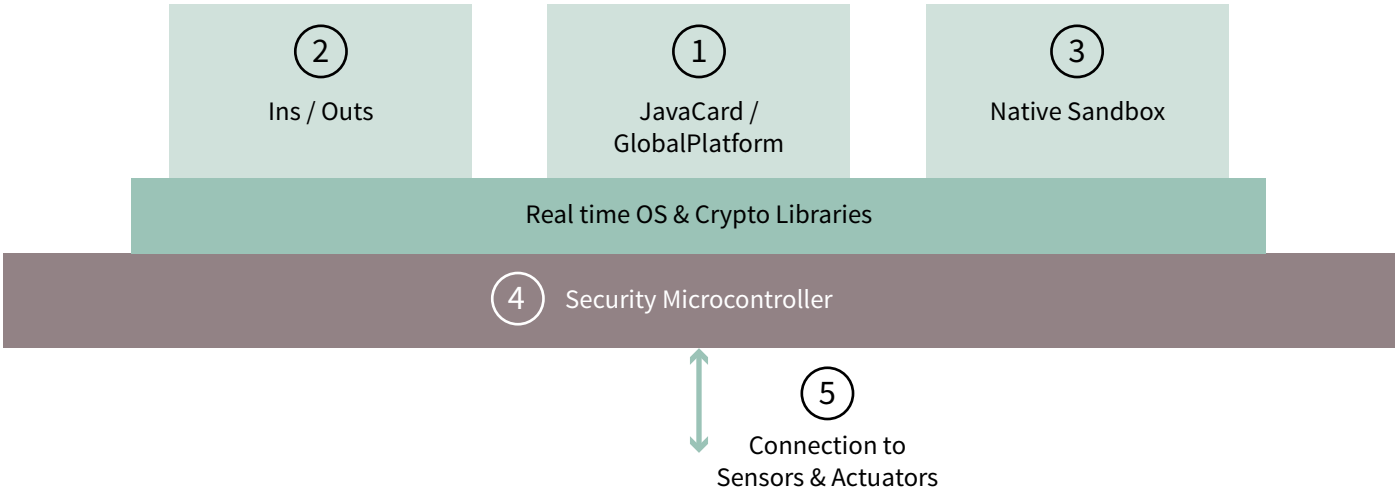
› Cost effective, security solution leveraging mass-produced hardened security components, defending against physical and logical attacks
› Convenient and efficient Java-based programming combined with a flexible yet secure executable applet management into the remote devices
› Unique identification of the secure nodes on the Internet or on private data networks and communication over standard Java sockets using regular browsers
› Time-critical applications programming in sandboxed native "C" to fulfill industrial automation's requirements for real time execution
› Simple interfacing with LCD and keypad peripherals for hands-on monitoring and control

Security Partner

# Solution

Javelin-SC is composed of a set of building blocks, whose combination creates a comprehensive, solid and convenient security platform for Internet of Things.

1) jNet's JavaCard and GlobalPlatform core smart object operating system is built on several key technologies:
   - Proven security and robustness using the latest JavaCard v3.0.4 specification with most GlobalPlatform v2.2.1 features already supported
   - Ability to securely load and manage applets over remote links and validate their integrity prior to execution
   - Programming in Java language that encapsulates the hardware platform and uses a built-in memory manager, hence eliminating learning curve for chip and tools, reducing number of software defects as compared to standard "C" programming
   - JavaCard Protection Profile suitable for Common Criteria certification up to EAL5+
   - Powerful Java crypto APIs (application program interface) accelerated with hardware co-processor and secure key storage inside the chip
2) An integrated micro-TCP/IP stack, based on the new IPv6 standard is suitable to address IoT's billions of devices and enables the setup of micro Virtual Private Networks.
3) The JavaCard secure kernel has been merged with a real time operating system (RTOS) along with related trigger mechanisms. Native tasks sensing alarms and abnormal conditions can trigger Java applets registered for such triggers. Reciprocally, Java applets can trigger execution of native tasks upon request.
4) The host solution is based on a cost effective, security hardened device derived from ePassport chips already in mass production.
5) Connection with wireless networks and interfaces with sensors and actuators allow controlling relays and switches as well as controlling or monitoring smart objects from Android or iOS smart phones. Interfaces include USB, SPI, I2C and GPIO, and serial I/O.




**Main benefits of the Infineon product**

- Quality and stability, due to the SLE 78's pure digital security features
- Long-lasting and solid security level thanks to the SLE 78's dual CPUs checking each other's flawless operation
- Easy implementation of applications on top of the secure hardware platform

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.

**jNet ThingX Corp.**
jNet ThingX is in the business of securing the Internet of Things by bringing connected JavaCard and GlobalPlatform implementations into embedded (non-smartcard) form factor products. SmartObject, connected, IP-addressable and Java-programmable System-on-Chip, is one such product. The building blocks jNet ThingX has developed are based on proven IP licensed from jNet Technology.

jNet's customers come from a variety of segments such as industrial automation, instrumentation and secure payments. The company is based in Silicon Valley, California.

**jNet ThingX contribution to the Infineon Security Partner Network**
jNet's SmartObjects provide unique identifiers for IoT devices. They allow for programmability and remote configuration capabilities. They form a security backbone for Internet of Things.

The Javelin-SC is a specially designed and optimized JavaCard Virtual Machine that has been created for independent operation in a remote, IP-connected environment to collect data, report alarm conditions, monitor sensors and actuate relays or switches. It is built on Infineon's security component that is flash-based, allowing field upgrades for the operating system and its Java applets.

Javelin-SC can be configured as primary device controller or as secondary crypto/security co-processor depending on system design. As primary controller it can monitor sensors, process data, perform signal filtering tasks and make logic decisions, programmed entirely in Java language and downloaded over the Internet to a specific, IP-addressable node on a network.

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.