Spotlight on IoT Security
Choose the right security for the Internet of Things

www.infineon.com/IoT-security
Rising concerns about IoT Security

With trends such as the Internet of Things (IoT) and machine-to-machine communication (M2M) mean that the number of connected devices and machines is increasing. Many of these – from small household appliances through large communication networks to complex, industrial automation systems – are controlled by special-purpose, embedded computing systems.

As it continues to gather pace, the networking trend promises greater convenience and comfort for users, plus new business and service models for companies. However, security in this embedded world often lags far behind. Security vulnerabilities are rising dramatically as the attack surface widens and manufacturers struggle to protect sensitive data, intellectual property (IP) and process integrity.

Why do we need IoT Security?

A successful attack on an embedded system can expose confidential information such as know-how, intellectual property, customer data and process intelligence. In addition, it can interrupt operations, compromise business continuity and even endanger a company’s brand image, success and very existence.

Challenges

› Protect systems against increasingly sophisticated and determined hacker attacks
› Balance financial constraints with the value of protected assets
› Find reliable, trustworthy functionality that is easy to implement
› Increase system security without compromising usability

Opportunities

› Develop new business and service models
› Carve out an image-building competitive differentiator
› Reduce security investment by building on partner know-how
› Increase production site flexibility through improved control across the supply chain

The answer

With its OPTIGA™ family, Infineon offers easy-to-integrate, scalable and customizable turnkey solutions to meet your IoT Security challenges. As a trusted advisor, we help you reduce complexity and implementation costs. Rather than investing in security know-how and infrastructure yourself, you can build on our vast and proven expertise in hardware-based security solutions.
Software alone is not enough to protect embedded systems as it can be read, copied and distributed with relative ease. Secured hardware is needed to reliably store data and software code, detect manipulation and encrypt data for safe storage and processing. You can rely on our solutions to establish a hardware-based root of trust that renders embedded software trustworthy.

Our OPTIGA™ portfolio achieves this by supporting the following three key security-critical functions:

› **Authentication**
   Our OPTIGA™ security ICs authenticate people and devices so information is exchanged between authorized individuals and devices only

› **Encryption**
   Our security controllers protect sensitive information by encrypting it and securely storing the secret keys

› **Integrity**
   Our security chips check platform, machine and device integrity to identify manipulation and detecting unauthorized changes

By building a root of trust in security architectures, our semiconductor-based solutions create immense value for consumers and enterprises – giving all stakeholders the peace of mind needed to fully leverage the potential offered by the Internet of Things.

Protection against digital threats

Reaching beyond product-based security

Drawing on our 30-year, proven track record in security, our mission extends beyond inspiring our customers with reliable, tangible security products.

We build trust beyond product-based security in a number of ways. Firstly, we focus on process security. Concrete measures include security-certified design environments, dedicated security infrastructure with biometric access and a secured production environment to protect key programming in particular.

Secondly, our security experts put our market-leading products through rigorous testing. This allows us to keep track of attack trends, continuously adapt our product concepts and proactively manage the product lifecycle.

And last but not least, we have our products as well as our development and manufacturing processes certified by third parties. Most of our products have successfully completed the strict Common Criteria certification process with the German authorities.

These measures combine to give our customers easy-to-grasp proof points that empower them, in turn, to build trust among their customers.
We understand that security needs are as varied as they are complex. Scaling from basic, single-function authentication solutions to robust certified security controllers for advanced platform integrity checks, we have developed the market’s widest portfolio to support individual security needs across a broad market spectrum.

**Broad market spectrum**

We add value to today’s smart home by offering flexibility and cost savings for all implementations, building trust in new applications with ground-up, proven security capabilities and thus paving the way for new business and service models.

**Automotive security**

We are making cars safer and protecting sensitive user data – for example by:
- Securing communication over telematics systems
- Authenticating infotainment systems to enable media service models
- Securing remote maintenance information and firmware updates

We build confidence in the connected car with optimized security solutions that synergize our long-standing automotive expertise with our extensive security know-how. This also gives you the chance to capture new business and service models.

**ICT security**

Our scalable portfolio safeguards communications and access across everything from small network switches up to enterprise-scale networks – for example by:
- Protecting data through secured communication between networking devices
- Securing software updates and protecting software
- Checking integrity of devices with router-enabled network access

As a trusted partner in the ICT field, we keep our customers ahead with easy access to the latest security solutions, backed by integration and device management support delivered through our wide partner network. With our trustworthy security solutions, you can develop new business and service models.

**Industrial security**

We are helping manufacturers to safeguard long-term success by securing everything from machine sensors to control systems – for example by:
- Securing communication between the automation system and IT platform to protect sensitive data and IP
- Authenticating sensors and devices in the automation network
- Securing software or firmware updates to protect IP and prevent operational interruptions

Our synergized industrial and security expertise builds confidence in the modern smart factory with a scalable portfolio to match individual requirements. Easy access to our established security know-how and infrastructure allows you to rein in your security investment.

**Iot Security**

Here we enable protection of everything from the toaster sensor to the overarching control system – for example by:
- Securing communication between the smart home gateway and the server
- Authenticating home automation components
- Protecting against counterfeit home automation components

We add value to today’s smart home by offering flexibility and cost savings for all implementations, building trust in new applications with ground-up, proven security capabilities and thus paving the way for new business and service models.
Our OPTIGA™ family of security solutions is designed for easy integration into embedded systems. These hardware-based security solutions scale from basic authentication functionality to complex implementations to meet your individual and changing needs, while maximizing the return on your investment. Both our OPTIGA™ Trust and OPTIGA™ TPM product families provide proven and reliable IoT Security performance.

Meeting today’s and tomorrow’s security challenges with OPTIGA™

Security level
- High
- Low

OPTIGA™ Trust E
  - Turnkey
  - Common Criteria Certified

OPTIGA™ Trust P
  - Programmable
  - Common Criteria Certified

OPTIGA™ Trust X
  - High-end security solution for IoT
  - Easy to integrate

OPTIGA™ TPM
  - Turnkey
  - Common Criteria Certified

Use cases in focus

Device authentication
Authentication is the process of identifying users, computers, devices and machines in networks, and restricting access to authorized persons and non-manipulated devices. Hardware-based security can support authentication by providing secured storage for a device’s credentials (cryptographic keys or passwords). We have developed a broad portfolio of OPTIGA™ products that build a root of trust in hardware devices to allow the secured authentication of devices and systems looking to connect to clouds, servers and other devices.

Boot process and device integrity protection
To secure embedded devices, the integrity of the device needs to be protected in order to prevent unauthorized changes. Protecting the boot process of the device is a key factor here. Also known as secured, verified or trusted boot, boot access protection blocks unauthorized booting of computing devices to stop compromised devices from exchanging data over the Internet of Things. With the OPTIGA™ family, we deliver a range of security ICs to enhance boot protection and take the complexity out of integrity metrics management.

Secured communication
In typical embedded system architectures, devices and systems are connected across heterogeneous networks employing various standard and proprietary protocols. To protect communication against eavesdropping and message falsification, for instance, it must be secured between these systems. Our OPTIGA™ family enables secured communications by storing the keys and certificates used in communication protocols as well as supporting cryptographic operations.

Secured software and firmware updates
Software and firmware in embedded systems need to be updated on a regular basis. However, it can be challenging to protect both the software itself as well as the system that is being updated. Updates protected by software only are at risk as software can typically be read, analyzed and modified to compromise the update or system. However, software can become trustworthy by combining it with secured hardware. Secured hardware from our OPTIGA™ family protects the processing and storage of code by means of encryption, fault and manipulation detection, and secured code and data storage.

Secured data protection
Embedded devices often store sensitive user data. The confidentiality of this data can be protected by encrypting it and storing it in a secured location. The challenge lies in securely storing cryptographic keys. Data can be easily decrypted if an attacker manages to read out the keys. Our OPTIGA™ Trust and OPTIGA™ TPM families overcome this problem by encrypting data and storing cryptographic keys securely.

With a proven portfolio of exceptional depth and breadth, we cover just about every conceivable use case scenario. The following outlines the most typical scenarios that can benefit from our tailored offering.
**OPTIGA™ Trust family**

**Authentication solution for improved security and reduced system costs**

Easy, cost-effective security solution for high-value goods

**OPTIGA™ Trust B**
- OPTIGA™ Trust B (SLE 95250) is a robust cryptographic solution for embedded systems requiring medical & diagnostic equipment, medical devices & consumer electronics, industrial control and automation, embedded systems networked over the IoT, protection of IP and data, consumer electronics, industrial control systems, PC and embedded computing.
- Medical & diagnostic equipment
- Medical devices & consumer electronics
- Industrial control and automation
- Embedded systems networked over the IoT
- Protection of IP and data
- Consumer electronics
- Industrial control systems
- PC and embedded computing

**Key features**
- Size-optimized TSNP-6-9 package (1.1 x 1.5 mm)
- Easy-to-implement single-wire host interface
- 512 bit user NVM
- Turnkey solution including host-side software for personalization (unique key pair per chip)
- Strong cost efficient asymmetric cryptography with personalization

**Key benefits**
- Easy to integrate with wide range of open source support
- Extended temperature range (-40° to +85°C)
- LPC interface
- SPI interface
- Secure storage for keys, certificates and passwords as well as dedicated key management
- Easy integration into all platform architectures and operating systems
- Easy to integrate with wide range space over en support

**Applications**
- Smart home
- Consumer electronics
- Industrial control and automation
- Enabling new features & business models
- Cost-effective deployment
- Enhanced security for connected devices (IoT)

**OPTIGA™ Trust E**

Easy, cost-effective security solution for high-value goods

**OPTIGA™ Trust E (SLE 95550)** is a single module security solution with full system integration support for easy and cost efficient deployment. It supports a broad range of use cases based on the product and process requirements of your business model. Easy to use authentication mechanisms uniquely identify clients and protect POS terminals.

**Key features**
- Low cost efficient symmetric key cryptography with 128-256 bit key lengths
- OPTIGA™ Digital Signature (ECC256) with a strong message authentication code
- Standard and extended temperature ranges (-40° to +85°C)
- Compliant in USB Type-C security

**Key benefits**
- Protection of data and IT
- Protection of all aspects and compute imaging
- Full system integrity and confidentiality
- Easy to integrate with wide range space over en support

**Applications**
- Smart home
- Consumer electronics
- Industrial control and automation
- Enabling new features & business models
- Cost-effective deployment
- Enhanced security for connected devices (IoT)

**OPTIGA™ Trust T**

High security microcontroller with advanced cryptographic algorithms implemented in hardware (e.g. RSA 2048, ECC 256), Common Criteria EAL4+ and FIPS security validation

**OPTIGA™ Trust P**
- OPTIGA™ Trust P (SLJ 52ACA) is a high-security, feature-rich solution. As a fully programmable security microcontroller, it provides advanced and efficient protection against side-channel, back door attacks, and physical attacks.
- High security microcontroller with advanced cryptographic algorithms implemented in hardware (e.g. RSA 2048, ECC 256), Common Criteria EAL4+ and FIPS security validation
- Protection of systems integrity, communication and data confidentiality

**Applications**
- Operational end of systems
- Healthcare and remote medical
- Secure storage for keys, certificates and passwords as well as dedicated key management
- Easy to integrate with wide range space over en support

**OPTIGA™ Trust X**

Programmable trust anchor for embedded systems

**OPTIGA™ Trust X (SLS 32AIA)** is a turnkey security solution for industrial automation systems, smart home and home security systems.

**Key features**
- High security microcontroller with advanced cryptographic algorithms implemented in hardware (e.g. RSA 2048, ECC 256), Common Criteria EAL4+ and FIPS security validation
- Protection of systems integrity, communication and data confidentiality

**Applications**
- Operational end of systems
- Healthcare and remote medical
- Secure storage for keys, certificates and passwords as well as dedicated key management
- Easy to integrate with wide range space over en support

**OPTIGA™ TPM**

Standardized, feature-rich security solution

**OPTIGA™ TPM (SLS 32AIA)** is a standard security anchor that protects the integrity and authenticity of devices and systems in embedded worlds. Based on proven microcontroller technology for the Trusted Computing Group (TCG) standard, it offers a broad portfolio of certified OPTIGA™ TPM security controllers based on the Trusted Computing Group (TCG) standard and all-encompassing.

**Key features**
- High security microcontroller with advanced cryptographic algorithms implemented in hardware (e.g. RSA 2048, ECC 256), Common Criteria EAL4+ and FIPS security validation
- Protection of systems integrity, communication and data confidentiality

**Applications**
- Operational end of systems
- Healthcare and remote medical
- Secure storage for keys, certificates and passwords as well as dedicated key management
- Easy to integrate with wide range space over en support

**Overview of OPTIGA™ TPM family**

<table>
<thead>
<tr>
<th><strong>OPTIGA™ TPM</strong></th>
<th><strong>Overview</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SLB 9645</strong></td>
<td>TPM 1.2</td>
</tr>
<tr>
<td><strong>SLB 9665</strong></td>
<td>TPM 1.2</td>
</tr>
<tr>
<td><strong>SLB 9670</strong></td>
<td>TPM 2.0</td>
</tr>
</tbody>
</table>

**Key benefits**
- Increased flexibility based on programmable solution with reference keys to comply commonality and scalability
- Protection of systems integrity, communication and data confidentiality
- Increased flexibility based on programmable solution with reference keys to comply commonality and scalability
- Protection of systems integrity, communication and data confidentiality
Security is evolving from a business imperative into a business advantage. Deployed correctly, it offers a genuine competitive differentiator:

- Security can protect your business model and your IP, helping to avoid service disruptions and quality issues e.g. due to counterfeit products, manipulated updates or stolen data. This, in turn, builds trust in your brand and reputation, fueling growth and profitability.

- Certified security capabilities and the promise of smooth, predictable operations can even pave the way for new business models.

- The latest security technologies can save you deployment costs and benefit your bottom line by avoiding unplanned downtime.

Hardware-based security solutions clearly outperform software-only approaches through dedicated, protected features. In addition, certified hardware solutions accelerate time-to-solution with the added acknowledgement of independent evaluations. Discrete solutions not only offer strong tamper resistance, scalability and dynamic innovation cycles, they also facilitate implementation by reducing design and production complexity as they e.g. do not require a secured production environment. This translates into cost savings as you do not need to invest in a dedicated infrastructure and specialist know-how to deliver the highest levels of standards-compliant security to your customers.

Infineon has been pioneering the security market for more than 30 years. Every year, we ship more than 2 billion security controller ICs – proof positive that we have the expertise, experience and problem-solving capabilities to meet and exceed our customers’ expectations over time. A strong R&D and quality commitment, a rich support and partner network spanning a wide ecosystem, and active industry engagement make us the partner of choice across the widest range of industries. Customers the world over know they can rely on us to take the complexity out of today’s security challenges with solutions combining convenience with ease of implementation.

Why security?

Why hardware-based security?

Why choose Infineon?
Service Hotline

Infineon offers its toll-free 0800/4001 service hotline as one central number, available 24/7 in English, Mandarin and German.

› Germany .................... 0800 951 951 951 (German/English)
› China, mainland .......... 4001 200 951 (Mandarin/English)
› India ......................... 000 800 4402 951 (English)
› USA ............................ 1-866 951 9519 (English/German)
› Other countries .......... 00* 800 951 951 951 (English/German)
› Direct access ............. +49 89 234-0 (interconnection fee, German/English)

* Please note: Some countries may require you to dial a code other than “00” to access this international number, please visit www.infineon.com/service for your country!

Mobile Product Catalog
Mobile app for iOS and Android.

More information:
www.infineon.com/security
www.infineon.com/IoT-security
Contact us: security.chipcard.ics@infineon.com

Published by
Infineon Technologies AG
81726 Munich, Germany
© 2018 Infineon Technologies AG.
All rights reserved.

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.

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).

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.