Spotlight on embedded security
Keeping up with the Internet of Things

www.infineon.com/embedded-security
Rising concerns about embedded security

Embedded systems are becoming ubiquitous. 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.

With its OPTIGA™ family, Infineon offers easy-to-integrate, scalable and customizable turnkey solutions to meet your embedded 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.

Why do we need embedded 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
- Safeguard operations and business continuity from unintended interruptions
- Protect confidential data (e.g., process know-how, intellectual property (IP), customer data)
- Protect brand and enable business models

The answer

With its OPTIGA™ family, Infineon offers easy-to-integrate, scalable and customizable turnkey solutions to meet your embedded 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.

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**

**Smart home**
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.

**Connected Car**
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.

**Information & Communication Technology**
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.

**Smart factories**
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.
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 embedded security performance.

Secured software and firmware updates

Software and firmware in embedded systems often need regular updates. 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 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 secure code and data storage.

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 (cryptography 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.

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.

Stored data encryption and integrity protection

Embedded devices often store sensitive user data. The integrity and confidentiality of this data can be protected by encrypting or signing it. 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. The OPTIGA™ TPM also supports software and hardware integrity checks.

Boot process protection

Also known as secure, 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. We deliver a range of security ICs to enhance boot protection and take the complexity out of integrity metrics management. Our OPTIGA™ TPM products integrate a root of trust in the boot process compliant with Trusted Computing Group (TCG) standards.

Use cases in focus

The depth and range of our proven portfolio cover just about every conceivable typical use case scenario. The following outlines the most typical scenarios that can benefit from our tailored offering.
OPTIGA™ Trust family
Trust anchor for embedded systems

Basic authentication solution for your embedded application

Key features
- Advanced cryptographic algorithms as defined in NIST FIPS 140-2
- Two key sizes including tiny software for easy integration
- 3.3-V ID, size, and memory
- Low power per chip
- Leapmotion F414A (3 x 3 mm)
- Easy to implement in larger multi-chip designs

Key benefits
- Improved security with symmetric cryptography and chip-integrated HSM
- Easy integration thanks to fast key sizes

OPTIGA™ Trust (SLS 10ERE) is a robust cryptographic solution for embedded systems. It replaces and helps to maintain OEM authenticity. It replaces and helps to maintain OEM authenticity. It is designed to assist system and device manufacturers in proving the authenticity, integrity and safety of their original products. It is designed to assist system and device manufacturers in proving the authenticity, integrity and safety of their original products.

Key features
- 16-bit wide key size with advanced cryptographic algorithms implemented in hardware
- FIPS 140-2 validation
- DPA and side-channel attack protection
- Unique asymmetric key pair per chip
- 3.5 kbit user memory
- Turnkey solution including host-side software for easy integration
- ECC163 cryptographic algorithms implemented in hardware

Key benefits
- Reduced design and integration effort
- Protected access to data
- Protection of business model and company image
- Lower system costs due to single-chip solution
- Reduced design and integration effort
- Protected access to data
- Protection of business model and company image
- Lower system costs due to single-chip solution

OPTIGA™ Trust E
Easy, cost-effective security solution for high-value goods

Key features
- Compliant to USB Type-C standard
- Standard and extended temperature range -40° to +85°C
- I2C interface and PG-USON-10 package (3 x 3 mm)
- Turnkey solution with OS, applet and complete host-side integration support
- ECC256 cryptographic algorithms implemented in hardware

Key benefits
- Reduced risk based on proven technology
- Field failure in models through careful review
- Potentially leads to the wide adoption of security hardware
- Fast encryption with true random numbers
- Easy integration into all platforms and applications

OPTIGA™ Trust E (SLS 32AIA) is a high-end turnkey security controller with full system integration support. It is designed for easy integration and secured updates through key generation and access control. It bridges one-time pads, stored on-chip, with reference applets to simplify customization and support for easy and cost-effective deployment. It supports a broad range of use cases focused on the prevention of unauthorised transactions, business models and user experience. Easy usernames authentication mechanisms uniquely identify objects and protect them from unauthorized access.

Key features
- Easy and cost-effective security solution for high-value goods
- Compliant to USB Type-C standard
- Standard and extended temperature range -40° to +85°C
- I2C interface and PG-USON-10 package (3 x 3 mm)
- Turnkey solution with OS, applet and complete host-side integration support
- ECC256 cryptographic algorithms implemented in hardware

Key benefits
- Reduced risk based on proven technology
- Field failure in models through careful review
- Potentially leads to the wide adoption of security hardware
- Fast encryption with true random numbers
- Easy integration into all platforms and applications

OPTIGA™ Trust P
Programmable trust anchor for embedded systems

Key features
- Full heap control with advanced cryptographic algorithms implemented in hardware
- FIPS 140-2 validation
- Common Criteria EAL 5+ (high) certification
- Applet and API for system-level access
- Programmable digital and analog functions with reference applets to simplify customization and support for easy and cost-effective deployment
- SPI, I2C, UART and LPC interfaces
- 3.5 kbit user memory
- STM32F072K6 CPU (32-bit)
- TDF110231CFB microcontroller

Key benefits
- Increased flexibility and field solution
- Increased flexibility on programmable solutions and reference applets to simplify customization and support for easy and cost-effective deployment
- Security of systems relies on network and data integrity
- TCG and Common Criteria EAL4+
- SPI interface
- LPC interface
- TPM 1.2

OPTIGA™ TPM
Standardized, feature-rich security solution

Key features
- Based on EAL4+ certified TPM 1.2
- I2C interface
- LPC interface
- TPM 1.2

Key benefits
- Increased flexibility and field solution
- Increased flexibility on programmable solutions and reference applets to simplify customization and support for easy and cost-effective deployment
- Security of systems relies on network and data integrity
- TCG and Common Criteria EAL4+
- SPI interface
- LPC interface
- TPM 1.2

OPTIGA™ TPM is the trusted trusted microcontroller in standardized security solution that protects your business model, process know-how and IP. It uses your existing OPTIGA™ Trust products to protect your embedded systems against counterfeiting, countermeasures and IP theft. It offers on-chip support of the complete OPTIGA™ suite and secure execution based on the Trusted Computing Group (TCG) standard to suit all needs.

OPTIGA™ TPM (Trusted Platform Module) is a standardized security solution that protects your business model, process know-how and IP. It uses your existing OPTIGA™ Trust products to protect your embedded systems against counterfeiting, countermeasures and IP theft. It offers on-chip support of the complete OPTIGA™ suite and secure execution based on the Trusted Computing Group (TCG) standard to suit all needs.

Overview of OPTIGA™ TPM family

<table>
<thead>
<tr>
<th>Feature</th>
<th>OPTIGA™ TPM</th>
<th>OPTIGA™ Trust</th>
<th>OPTIGA™ Trust E</th>
<th>OPTIGA™ Trust P</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCG</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Common Criteria EAL4+</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Information Security</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Integrated, end-to-end</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
You get what you need
Our scalable OPTIGA™ family matches security performance to your precise embedded system needs.

You can adapt as your needs change
Tailored solutions based on open standards give you flexibility to grow and adapt.

You win new customers
Reliable, proven, certified products help you to build trust and enable new business and service models.

You can manage your security investment
We reduce integration effort and save valuable time-to-market through standardized designs.

You don’t need to worry about complexity
Extending across the entire security ecosystem, our experience and dedicated infrastructure will speed up and simplify your integration effort.

Trusted advisor at your side
Designers see us as a trusted advisor for their embedded security needs. When you partner with us, you can immediately put our extensive embedded security competence and dedicated security infrastructure to work for you – reducing your investment and integration effort, saving time and money and protecting your valuable assets and IP.

We complement one of the market’s broadest and most scalable portfolios with a rich partner ecosystem – the Infineon Security Partner Network (ISPN) – so you can tap into a vast global network of consulting and support expertise. Ultimately, not only will our security technologies help secure the future success of your current business case, they will also open up exciting new business and service models in security-critical applications.

www.infineon.com/ISPN
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/ccs
www.infineon.com/embedded-security
Contact us: security.chipcard.ics@infineon.com