ESS – Embedded security solutions

January 2017

Chip Card & Security Application Portfolio

Smart Cards & eDocuments

- Payment
- National eID
- ePassport
- SIM
- eHealthcare
- eDriver's License
- Multi-Application
- Transport Ticketing
- Access control

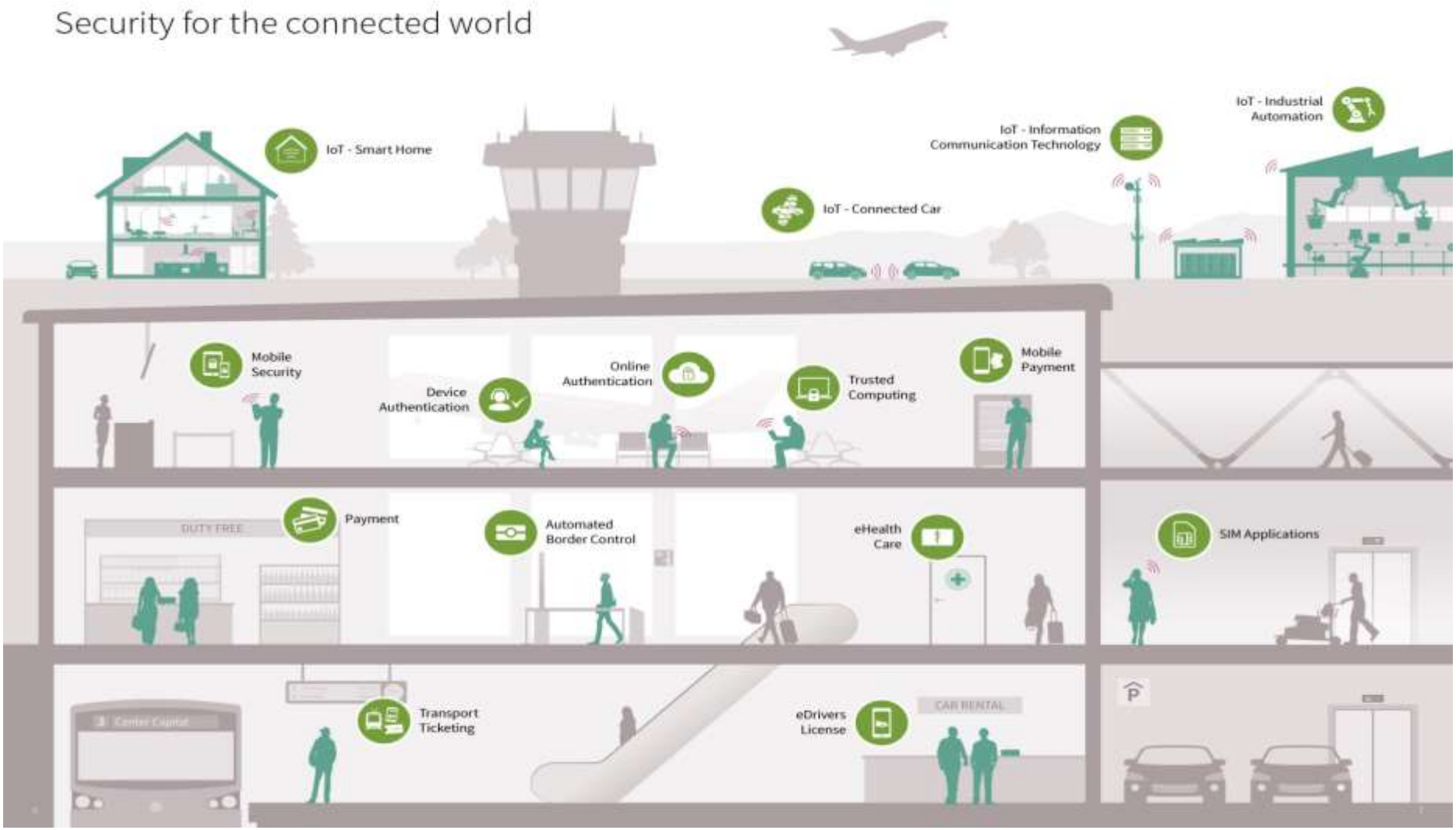
Embedded Security

IoT Security

- Connected Car
- Industry 4.0
- ICT*
- Smart Home
- Mobile Payment
- Mobile Ticketing
- NFC
- eSIM
- Mobile ID
- Authenti-cation
- Trusted Computing
- Mobile Security
- Entertain-ment

*) Note: ICT = Information & Communication Technology

Infineon security solutions are everywhere



Infineon is the market leader for embedded security and IoT

Infineon is the market leader in embedded security*
And is positioned as one of the leading vendors of IoT security**

*Source more than 31% in terms of unit shipments to IHS (Embedded Digital Security Report 2016)
**Source: Technavio | Global Internet of Things Security Market 2016-2020

Our market leadership is a result of knowledge, ecosystem support and solutions

Built on more than 30 years of security experience

Recognized market leader

Political engagement

Security leadership

Driving standardization

Innovating advanced security Technology

Enabling solutions with ISPN*

*ISPN = Infineon Security Partner Network

ESS application overview

Embedded Security Solutions (ESS)

Mobile Security

Mobile security

Mobile communication

Mobile payment

Industrial and Infrastructure Security

Industrial security

Automotive security

Infrastructure & Computing security

USB Tokens

Connected Device Security

Authentication

IoT & Consumer devices

Smart Home

Pay TV

ESS Marketing Communication

Recent updates

- Best Solution in manufacturing award at IoTSWC

Webinars

- Smart factory
- Connected car
- Smart home
- Smart network

Recent Press Releases

- Security for the Smart Home: Infineon teams up with Chinese appliance manufacturers for solutions (11/24/16)
- New FIDO certified Bluetooth solution for secure mobile internet usage (06/27/2016)
- Lenovo selects embedded security solutions from market leader Infineon (04/04/16)
- Infineon presents world's smallest plug-and-play NFC security module for smart wearables (03/21/16)
- Infineon and Partners Demonstrate IoT Security at RSA Conference 2016 (02/29/16)
- Mobile World Congress 2016: Infineon brings bank-level security to smart devices and mobile payment solutions (02/23/16)

Internet

- OPTIGA™ family
- IoT security
- Mobile Security
- SIM applications
- ISPN

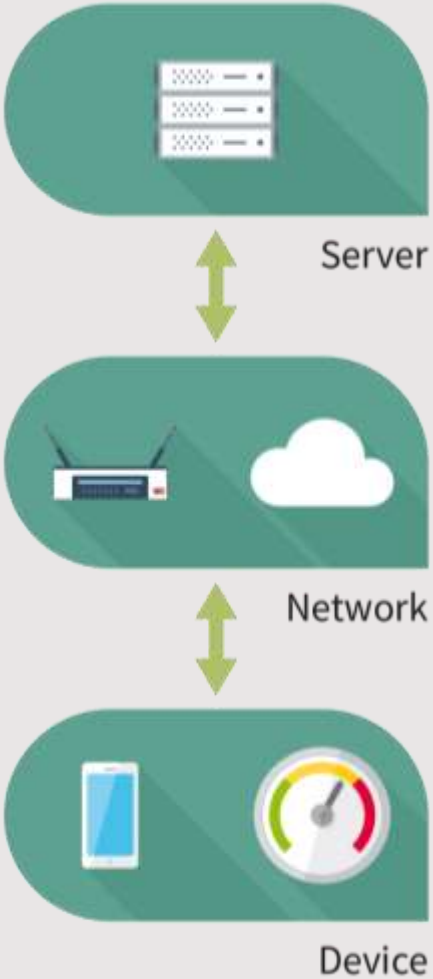
Videos

- Security for Smart Homes Demo
- Trusted Computing for IoT Security: Cisco and Infineon
- Securing communication in IoT – Raspberry Pi with OPTIGA™ TPM
- Embedded security for IoT
- Infineon's IoT Security Solution with Global Platform
- Security solutions for smart factories
- Partner security solutions (ISPN) playlist

OPTIGA™ family for embedded security

The IoT Architecture of networked components can be described as follows

IoT Architecture



Gather data
Analyze
Send commands

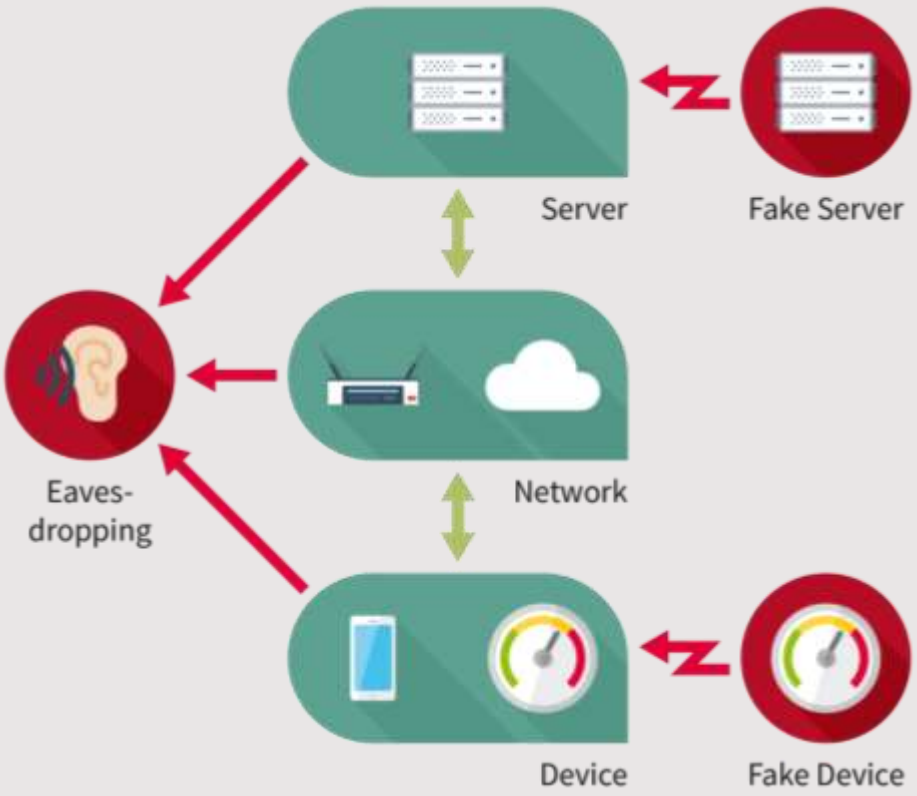
Reliably convey data and commands

Send and receive data and commands

Even though markets are diverse, they all share a set of security threats.

Security threats for IoT

An **Eavesdropper** listening in on data or commands can reveal confidential information about the operation of the infrastructure.



A **Fake Server** sending incorrect commands can be used to trigger **un-planned events**, to send some physical resource (water, oil, electricity, etc.) to an **unplanned destination**, and so forth.

A **Fake Device** injecting **fake measurements** can disrupt the control processes and cause them to **react inappropriately** or dangerously, or can be used to **mask physical attacks**.

Consequences of not integrating the right security in IoT are seen every day

BBC NEWS

Smart LED light bulbs leak wi-fi passwords

WIRED

Hackers Remotely Kill a Jeep on the Highway—With Me in It

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Context Security released details about how it was able to hack into the wi-fi network of one brand of network-enabled bulb, and control the lights remotely.

TECHNOLOGY 7:19am January 17, 2017

Smart-fridge goes viral after update leaves owner thirsty

By 9NEWS

"All I wanted was some water". (Twitter: @find_evil)

A photo of an uncooperative smart-fridge has gone viral online after a woman vented her frustration with the appliance on Twitter.

Intel Security's global director, Jackie Stokes, posted the picture of her fridge, which is connected to the internet, stuck in the middle of a program update.

Computer security

The My Friend Cayla doll has been shown in the past to be hackable

Call for privacy probes over Cayla doll and i-Que toys

Chris Baraniuk
Technology reporter

The makers of the i-Que and Cayla smart toys have been accused of subjecting children to "ongoing surveillance" and posing an "imminent and immediate threat" to their safety and security.

The accusations come via a formal complaint in the US by consumer groups.

They, along with several EU bodies, are calling for

The Economist

World politics | Business & finance | Economics | Science & technology | Culture

21 OCT 16

Hacked Cameras, DVRs Powered Today's Massive Internet Outage

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.

A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.

HOME | ABOUT | ICS JWG | INFORMATION PRODUCTS | TRAINING | FAQ

Alert (IR-ALERT-H-16-056-01)

Cyber-Attack Against Ukrainian Critical Infrastructure

Original release date: February 25, 2016

Security motivations and threats

IP / know-how protection

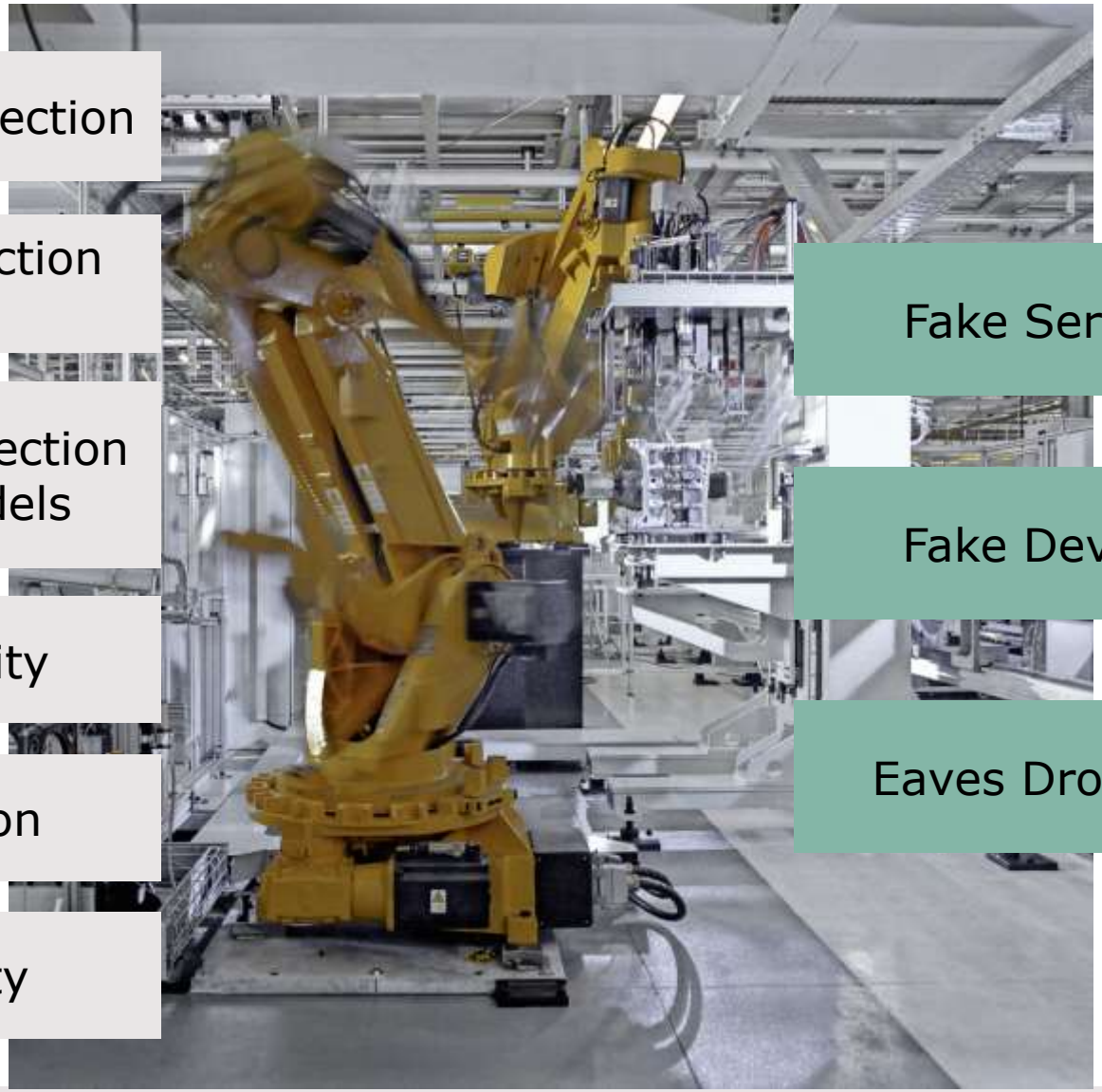
Increase of production uptime

Enablement & protection of business models

Quality/ reliability

Image protection

Liability / safety



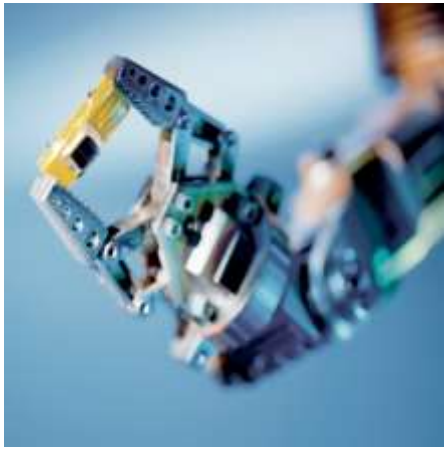
Fake Servers

Fake Devices

Eaves Dropping

OPTIGA™ family main application areas

Industrial Automation	Automotive	Information & communication	Smart Home




New services | new business models | new customer segments

Security must address the use cases in the right way

- Fit-for-purpose security products and solutions are required
- Security must be easy to integrate and to manage

Basic security use cases – OPTIGA™ family

Use case	Definition	Security Question
Authentication	Definite identification of people and systems	"Who am I talking to?"
Secured Communication	Secured data transfer	"Can software or data be secured during transfer?"
Confidentiality with Secured Storage	Securely store encryption keys, certificates, passwords, data (IP protection)	"Can my data or credentials be accessed by an attacker?"
System & Data integrity	The system and data has not been changed	"Is my system and data not manipulated & can a third party verify that information?"
Secured soft-ware and firm-ware update	Supporting (remote) software and firmware updates	"Can software or firmware be secured during transfer?"

Benefits of Hardware Security

		
NO SECURITY Open for all to see	**SOFTWARE ONLY** Secures against casual intrusion and basic software attacks	**HARDWARE SECURITY** Secures against hardware attacks and hardens against software attacks
Reading	Software code easily readable by hackers	Hardware chip protects itself against code reading
Copying	Software code easily copied and shared by hackers	Secure hardware cannot be easily copied. Must be fully reverse engineered and re-manufactured.
Analyzing	Software code easily analyzed and understood using standard tools	Secure hardware use proprietary designs and non-standard code that is not easily understood
Root of Trust	Software has no "Root of Trust", recovery of broken system practically impossible	Secure hardware provides "Root of Trust" anchor for system, providing detection, recoverability, secure updates

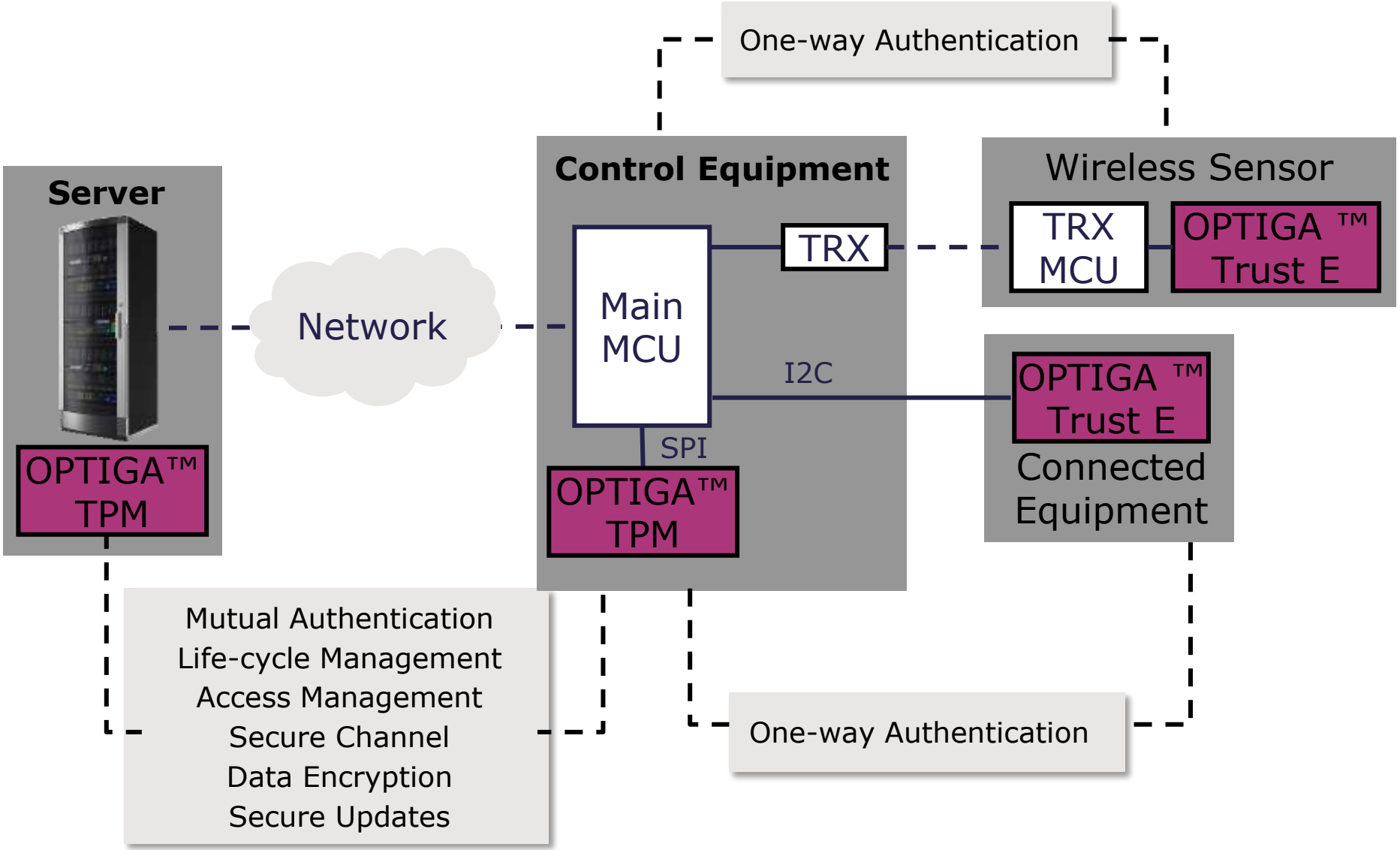
OPTIGA™
Security Products for Embedded Systems

OPTIGA™

Scalable and tailored to your needs: Infineon's OPTIGA™ product portfolio is the perfect match to secure embedded systems

OPTIGA™ Trust	Device authentication is the focus of the OPTIGA™ Trust family matching function and performance to value
OPTIGA™ TPM	Compliant to the Trusted Computing Group specifications, the OPTIGA™ TPM family is the Root-of-Trust for PC, mobile and embedded computing applications

Example use Case: Industrial Control Systems



OPTIGA™ Family

	OPTIGA™ Trust B	OPTIGA™ Trust E	OPTIGA™ Trust P	OPTIGA™ TPM
				
Security Level	Basic	CC EAL 6+ *	CC EAL 5+	CC EAL 4+
Functionality	Authentication	Authentication	Programmable	TCG standard
NVM (Data)	512Byte	3kByte	150kByte **	6kByte
Cryptography Private key stored in secure HW	ECC131	ECC256	ECC521 RSA2K	ECC256 RSA2K
Type of Host System	MCU without OS / proprietary OS / RTOS		Embedded Linux	Windows / Linux
Interface	SWI	I2C	UART	I2C, SPI, LPC
System integration	✓	✓	✓	Platform vendor

✓ Done by IFX ✓ Customer Implementation, support by IFX

* Based on certified HW

** Code & Data

Security and Complexity

OPTIGA™ Trust family Authentication

Customers require device authentication for different purposes

PROFIT
Toner & printer cartridges

LIABILITY
AC adapter

QUALITY
Projector

RELIABILITY
Docking station

SAFETY
Medical devices

IMAGE
Company Brand

Why OPTIGA™ Trust?
Asymmetric Elliptic Curve Cryptography

Symmetrical Algorithms can not afford SW implementations: They pose a high risk of "Break-once, Publish-everywhere"

Asymmetric: Two **different** keys for En- and Decryption

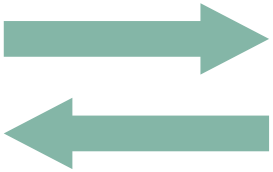
Non-Secure
SW environment
Public Key Only

SW-Encryption
Public Key

HW-Decryption
Secret Key

Private Key
is protected
in Hardware

microcontroler



OPTIGA™ Trust

The possible applications for OPTIGA™ Trust authentication products are endless

Electronic accessory authentication
(e.g. MP3 players)

ICT Infrastructure authentication
(e.g. routers)

Gaming authentication
(e.g. slot machines)

Industrial

Printer cartridge authentication

Medical equipment authentication

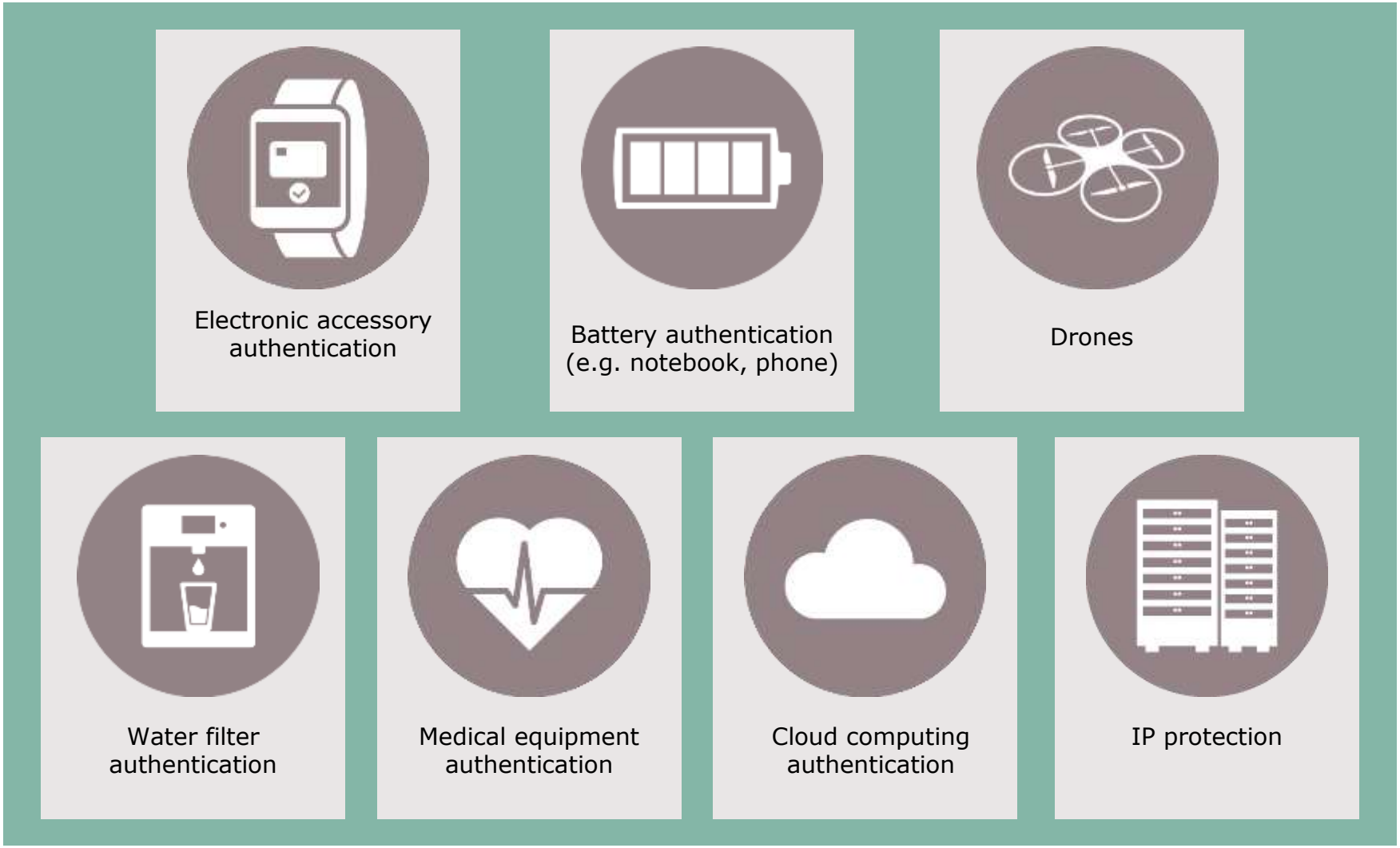
Cloud computing authentication

Software/ IP authentication

Internet of Things
- Connected Home
- M2M Communication

OPTIGA™ Trust B

Target Applications



Infineon OPTIGA™ Trust B Turnkey Authentication

Strong Asymmetric Cryptographic Engine

- Elliptic Curve Cryptography (131 bit key)
- Unique 96 bit identifier (UID)
- Public key certified by ODC-163 based digital certificate
- Optional kill feature

Protected Memory

- 512 bits lockable NVM
- Integrated Lifecycle Counter

Easy to Implement

- Full Turnkey Solution with Two Preloaded Key Pairs
- Host Code Provided
- Simple Single Wire Interface

Product Details

Programing	Turnkey	Interface	SWI
OS	N/A	Interface Speed	500kbps
Memory	512 b	Package	TSNP6
Cryptography	ECC131	Size	1.5 x 1.1 mm

More Info:

SLE 95250

www.infineon.com/optiga-trust

OPTIGA™ Trust E

OPTIGA™ Trust E applications

Industrial Automation	Smart Home	Medical	Other IoT
			
Automation components PLCs, edge/ node devices	**All objects** Any object inside a home	**Peripherals** High value accessories	**Edge Devices** License Management, etc

Others
Consumer electronics, Smart Lighting, Surveillance Cameras, 3D Printers, Telehealth Systems, robotics etc.

Infineon OPTIGA™ Trust E (SLS 32AIA)
Easy and cost effective security solution for high value goods

Premium Security
- High-end security controller
- ECC256, SHA256 implemented

Advanced Feature Set
- Highly secure data storage
- Cryptographic Functions for
  - Authentication
  - Certificate Exchange/ PKI support for customer domain
- -25 to +85°C and -40 to +85°C supported

Easy to Implement
- Full turnkey solution
- Host Code Provided
- Evaluation kit

Product Details

Set-up	Turnkey	Interface	I2C
Memory	Up to 3kB	Interface Speed	400kbps
Cryptography	ECC-256, SHA-256	Package	USON-10
Available	07/2015	Size	3 x 3 mm

More Info:

SLS 32AIA

www.infineon.com/optiga-trust

Contact your Infineon Sales Representative for more information

OPTIGA™ Trust E at a glance

Easy integration

- Easy and fast system integration turnkey solution (chip + OS + app + complete host side integration support)
- Industry standard I2C Interface
- Small outline of PG-USON-10 package (3x3mm)
- Industrial temperature range support: -40°C to +85°C

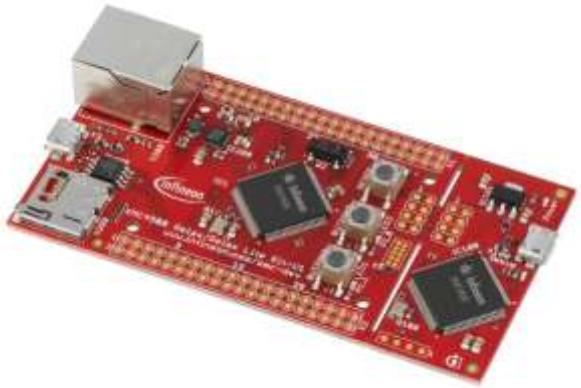
Cost effective

- All keys and certificates (x.509 supported) already programmed in security certified production site at Infineon
- Chip individual key pairs preloaded
- Advanced asymmetric cryptography (ECC 256) in advanced security controller → only 1 chip required

Enhanced security

- High-end security controller
- Advanced asymmetric cryptography (ECC 256) in a single-chip solution

Evaluation kit



For Demo

- Easy PC plug-in
- PC user interface
- Showcasing all OPTIGA™ Trust E use cases
- Based on Infineon XMC Relax Kit with OPTIGA™ Trust E extension board

Reference Design

- Available for customer projects
- Based on XMC4500

OPTIGA™ Trust P

OPTIGA™ Trust P Security Functions

Device Authentication
- One-way authentication
- Mutual authentication

Trust Anchor
- Secure Boot
- Memory Integrity

Secure Channel
- Key Generation
- DH/ECDH Key Exchange

Information Integrity
- Command Integrity
- Message Integrity
- Data Integrity

Audit Information
- Incident logs
- Protected storage

Lifecycle Management
- Supply chain tracking
- Lifecycle counter

Secure Updates
- Secure Channel
- Access Control

Infineon OPTIGA™ Trust P (SLJ 52ACA) Programmable Authentication and Device Security

Premium Security

- Common Criteria EAL5+
- ECC521 and RSA 2048 Supported

Flexible Programming Solution

- Java-based OS for On-Chip Programming
- Supports ECC, RSA, AES, TDES, SHA Cryptography
- Cryptographic Functions for
  - Authentication
  - Secure Updates
  - Access Management
  - Key Generation & Exchange
  - System Integrity
  - Lifecycle Management

Easy to Implement

- Reference Applets with Common Functions Provided
- Host Source Code Provided

Product Details

Programing	Programmable	Interface	ISO7816 UART
OS	JavaCard	Interface Speed	400kbps
Memory	150kB	Package	VQFN-32
Cryptography	ECC, RSA, AES, TDES, SHA	Size	5 x 5 mm

More Info:

www.infineon.com/optiga-trust

Contact your Infineon Sales Representative for more information

OPTIGA™ Trust P Demo Kit

Includes

- OPTIGA™ Trust P Board
- Host Controller Board
- Connection Cables
- Demo Utility Software (PC)
- Demo System User Guide
- OPTIGA™ Trust P Product Brief

Features

- Demonstrates Functionality of OPTIGA™ Trust P
- Expandable to Full Development Kit with Software Download
- SP001220816

OPTIGA™ TPM

OPTIGA™ TPM applications

Industrial Automation	Information & communication	Automotive	Smart Home
			
Automation components Industrial PCs, PLCs, Routers	**PC** Notebook, tablet, smartphone Workstation/ Desktop PC, Server	**In car** Telematic system, Infotainment system	**Focus Concentrators** Gateways, Management Devices, Smart Thermostats
Other industrial Single board computers (e.g for ATMs, gaming machines),	**Networking equipment** Routers, switches, Gateways, Wifi access points	**Others** Surveillance Cameras, 3D Printers, Telehealth Systems, Robotics, Smart Lighting	

Basic security use cases – OPTIGA™ TPM

Use case	Definition	Security Question
Authentication	Definite identification of people and systems	"Who am I talking to?"
Secured Communication	Secured data transfer	"Can software or data be secured during transfer?"
Confidentiality with Secured Storage	Securely store encryption keys, certificates, passwords, data (IP protection)	"Can my data or credentials be accessed by an attacker?"
System & Data integrity	The system and data has not been changed	"Is my system and data not manipulated & can a third party verify that information?"
Value chain support	Dedicated functionalities for manufacturers, platform owners, OS providers and more	"Can security be transported through the lifecycle, can each owner take ownership?"
Secured soft-ware and firm-ware update	Supporting (remote) software and firmware updates	"Can software or firmware be secured during transfer?"

The Trusted Platform Module (TPM) is

- a security controller for cryptographic operations
- physically separated from the main processor
- protecting security critical data (e.g. keys, passwords)
- capable to resist logical and physical attacks
- security evaluated by a third-party (Common Criteria standard)
- a passive device

TPM – Security Module

- Generic functions
- Secure hardware
- Crypto functions

A TPM- The “safe for your platform"

OPTIGA™ TPM Security Functions

Device Authentication
- One-way authentication
- Mutual authentication

System integrity
- Secure Boot
- Remote platform verification

Secure Channel
- Encrypted Communication
- Key Generation

Dedicated functions for
- Platform manufacturer
- System operators
- Vendor/User/Enterprises

User Management
- Password Protection
- User management and keys

Lifecycle Management
- Key Backup and refurbishment
- Personalization and identities
- Supply chain tracking

Secure Updates
- Remote maintenance
- In-field flexibility and reaction

Secure Clock and Time
- Reliable clock when offline
- Timer and Monotonic Counter

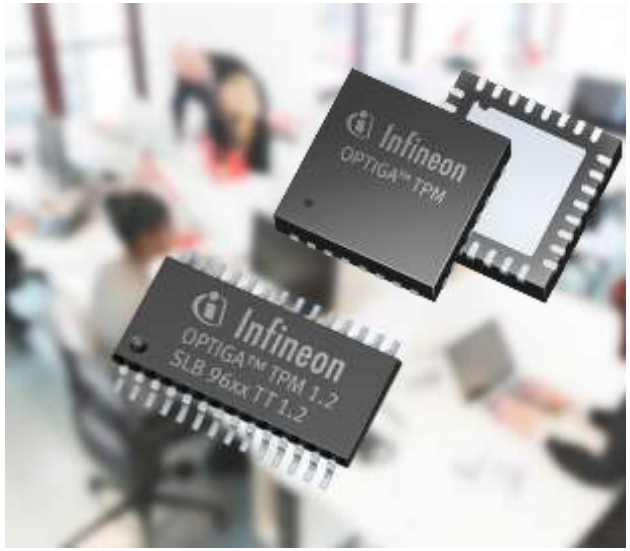
Overview Infineon OPTIGA™ TPM SLB 96xx TPM v1.2 and 2.0 for Highest Level of Certified Platform Protection

Trusted Platform Module: Secure your Software and Data

- Strong Authentication of Platform and Users
  - Unique embedded Endorsement Certificate
- Secure Storage and Management of Keys and Data
- Platform protection for embedded systems
  - Measured/Trusted Boot
- RNG, Tick-Counter, Dictionary Attack Lock-out
- Built-in algorithms including RSA, ECC, SHA-256

Certified & Standardized Security

- Official TPM product listed at Trusted Computing Group (TCG)
- Independently security evaluated and certified: According to the international standard Common Criteria



Infineon OPTIGA TPM products

Product	TPM	Interface	Domain
SLB 9645	TPM 1.2	I2C	Embedded systems, non-x86 architectures
SLB 9660	TPM 1.2	LPC	PC-based systems, x86 architectures
SLB 9665	TPM 2.0		
SLB 9670	TPM 1.2	SPI	PC-based systems, x86 architectures embedded systems, non-x86 architectures
SLB 9670	TPM 2.0	SPI	

Applications:

- Embedded Devices
  - Industrial, Medical, Networking, Transport, Gaming etc.
- PC and Mobile Computing
- Intel x86, ARM platforms and others

More Info:

www.infineon.com/tpm
www.trustedcomputinggroup.org

Benefits of an OPTIGA™ TPM

- TCG Certified & Listed on the TCG TPM Certified Products List
- Increased security based on certified security processes and products – Common criteria certified (security evaluation)
- Proven security based on established technology
- Reduced implementation costs due to implementation of TCG-standards
- Minimized system integration risk due to application of reviewed TCG-standards (proven technology)
- Improved security in manufacturing by secure personalization process

TPM – a security solution you can rely on

OPTIGA™ TPM
SLB 9645 (I2C) Support – Eval Board

- Plug-In Board (IRIDIUM) for the
  - RaspberryPi
  - BeagleBoard-xM
- Documentation
  - Linux setup and driver
  - Software Stack
  - TPM Initialization
  - OpenSSL/GnuTLS
- Demo for authentication and secure communication
- Order number: SP001265088

OPTIGA™ Family
Trust & TPM

OPTIGA™ Family

	OPTIGA™ Trust B	OPTIGA™ Trust E	OPTIGA™ Trust P	OPTIGA™ TPM
				
Security Level	Basic	CC EAL 6+ *	CC EAL 5+	CC EAL 4+
Functionality	Authentication	Authentication	Programmable	TCG standard
NVM (Data)	512Byte	3kByte	150kByte **	6kByte
Cryptography Private key stored in secure HW	ECC131	ECC256	ECC521 RSA2K	ECC256 RSA2K
Type of Host System	MCU without OS / proprietary OS / RTOS		Embedded Linux	Windows / Linux
Interface	SWI	I2C	UART	I2C, SPI, LPC
System integration	✓	✓	✓	Platform vendor

✓ Done by IFX ✓ Customer Implementation, support by IFX

* Based on certified HW

** Code & Data

Security and Complexity

Part of your life. Part of tomorrow.

infineon