



OPTIGA™ TPM SLB 9673

A future-proof new generation TPM with I2C interface

Infineon Technologies
September 2023



Infineon's award-winning TPM technology



Several awards testify to the innovative strengths and advanced cryptographic capabilities of

Our OPTIGA™ TPM SLB 9672/9673 solutions

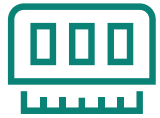
“Embedded Award 2023” from Embedded World
First place in the “Safety&Security” category

“Best in Show” award from Embedded Computing Design
Top spot in the “Security” category

Product of the Year” award from ELEKTRONIK
First prize in the “Software” category



Why security is essential



Security is a fundamental need of society with increasing importance



The connected world is further driving the demand for security

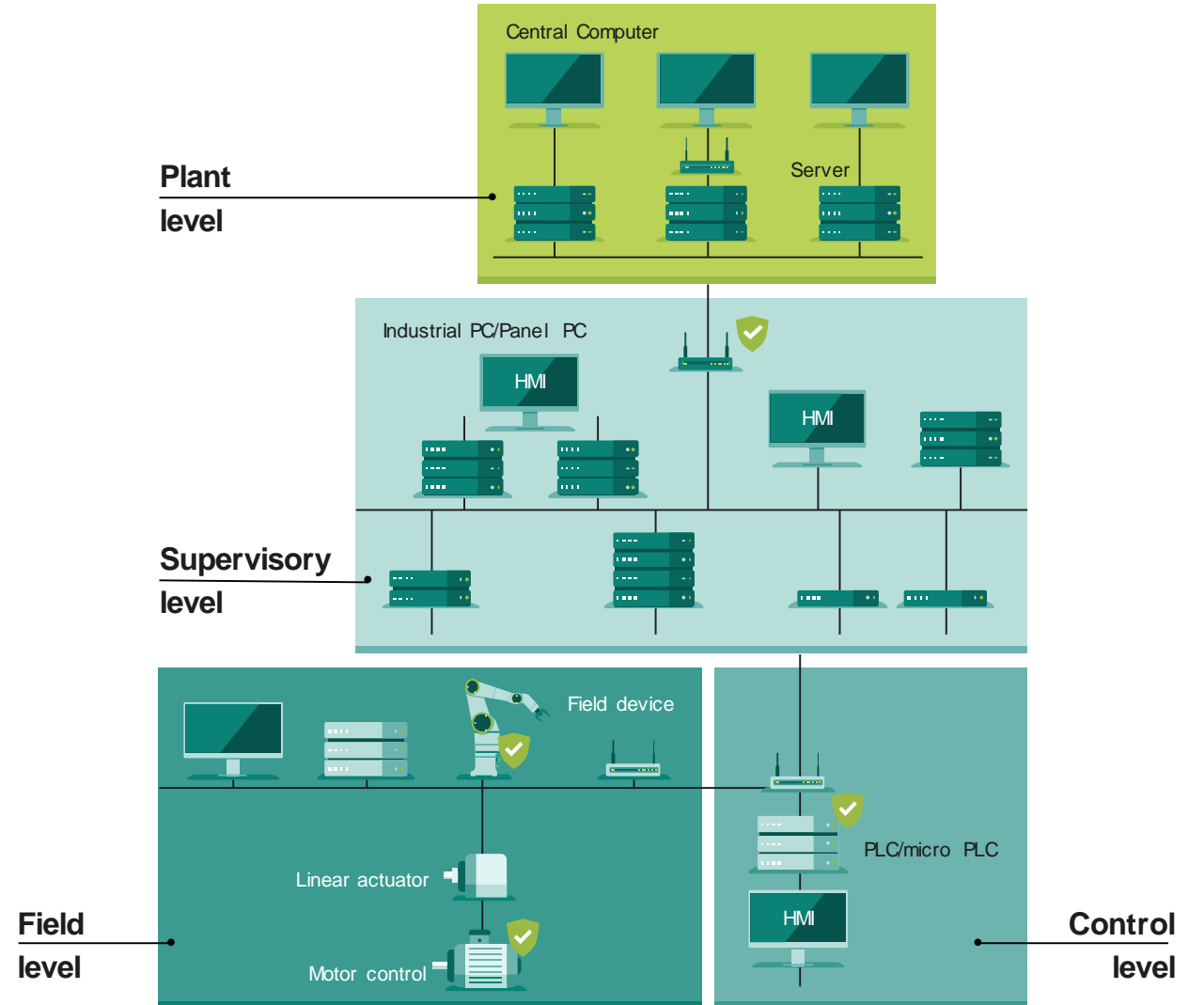
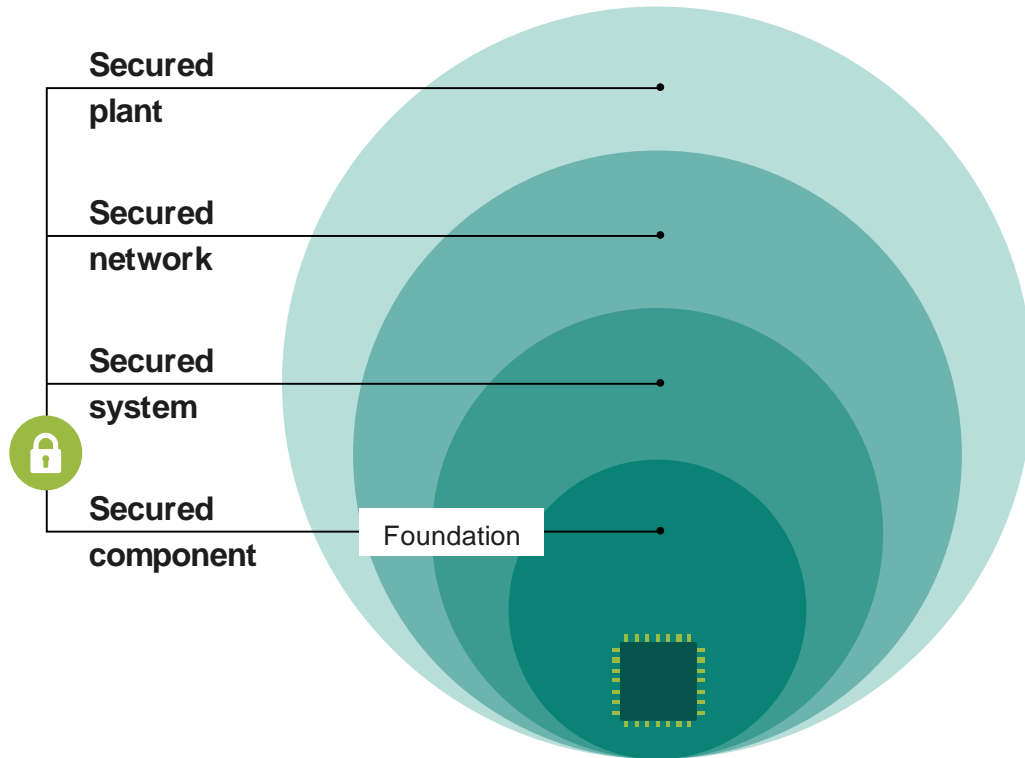


We believe in hardware-based security as the essential trust anchor

TPM as Root of Trust



Securing systems starts by securing components with hardware-based roots of trust



Discrete TPM, key Root-of-Trust for multiple applications

Key targets of discrete TPM

PC & laptops

- Professional PCs
- Industrial PCs

Servers

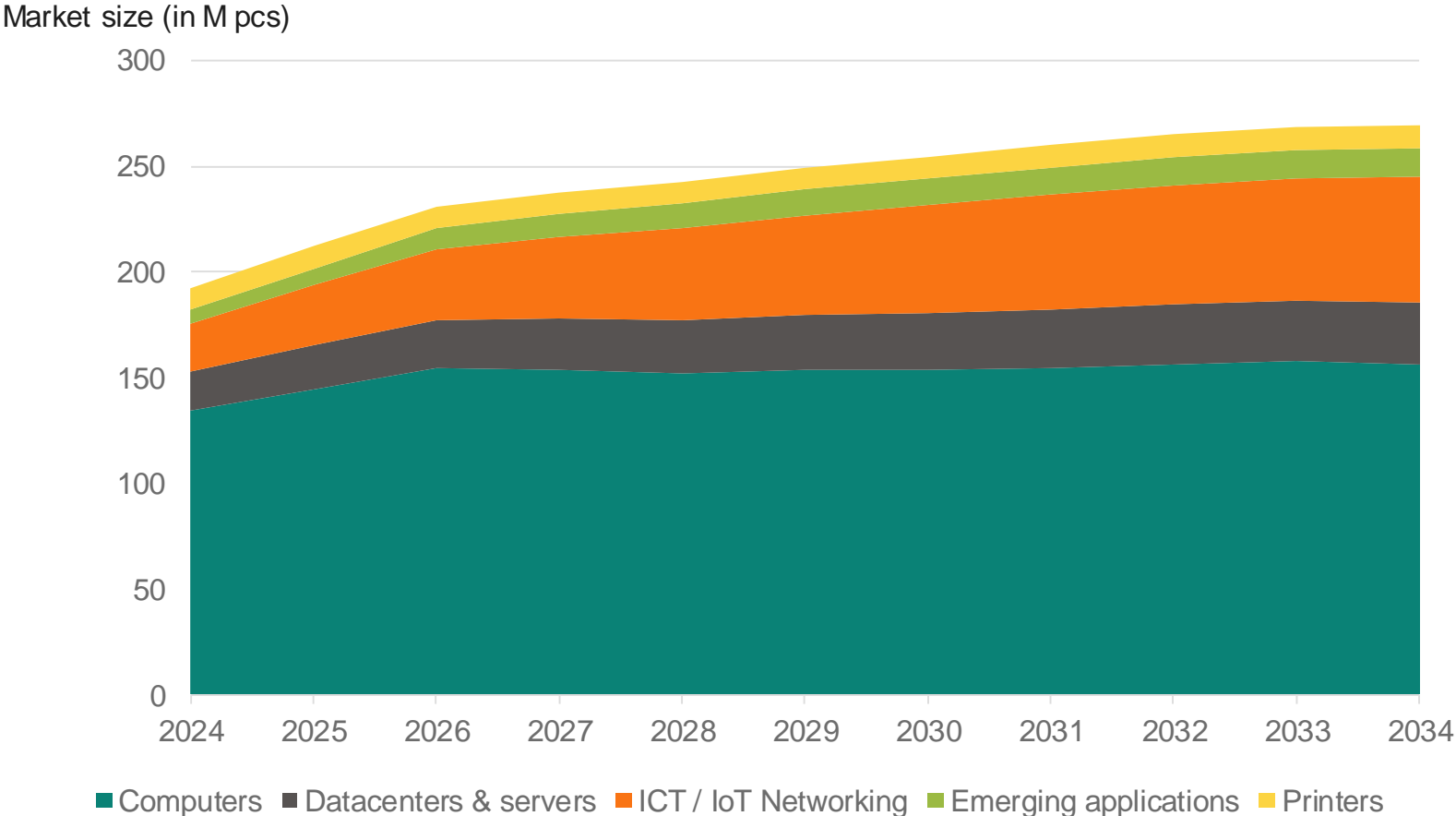
Servers

IoT networking

- Network Interface Cards
- Networking equipment
- Printers

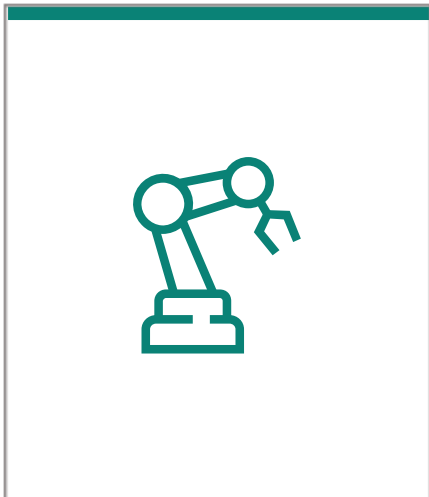
Forecasted markets for discrete TPM

A stable base market and significant growth in other segments



Quick facts about TPM with an I2C interface

Smart factory



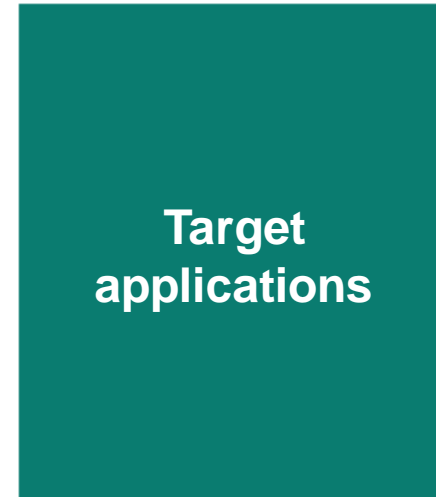
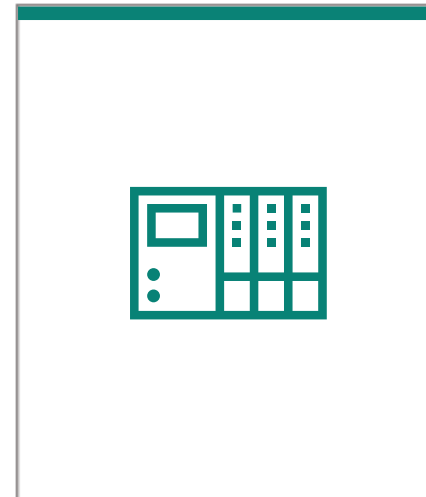
Smart building



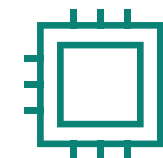
IoT networking



Programmable Logic Controller



- Fully standardized certified security solution **supporting future-proof PQC-protected FW Update mechanism**
- Allows **trusted and secured communications** with I2C up to 1MHz
- Supports the **latest TPM 2.0 specs** and corresponding security requirements
- Meets demanding requirements with operating temperature range **from -40 up to +105°C**
- Simple integration with **Linux-based OS** thanks to easy-to-understand materials and sample codes on GitHub
- Well suited for embedded system where **simplicity of design and lower system BOM cost** are important



Future challenges for TPM



The threat of quantum computers to cryptography

Within the next 10 to 20 years, quantum computer attacks on today's cryptography are expected to become reality.



Quantum computers, a threat to currently known security algorithms

**Asymmetric cryptosystems (RSA/ECC):
Completely broken using Shor's algorithm**

Currently

ECC-256 and RSA-3072 have **128-bit** security



Quantum world

Almost **no** security

**Symmetric cryptography:
Security levels halved by Grover's algorithm**

Currently

AES-128 has **128-bit** security



Quantum world

64-bit security

Quantum world
(in 10 – 20 years)

Heavily affected:
RSA, ECDSA, ECDH

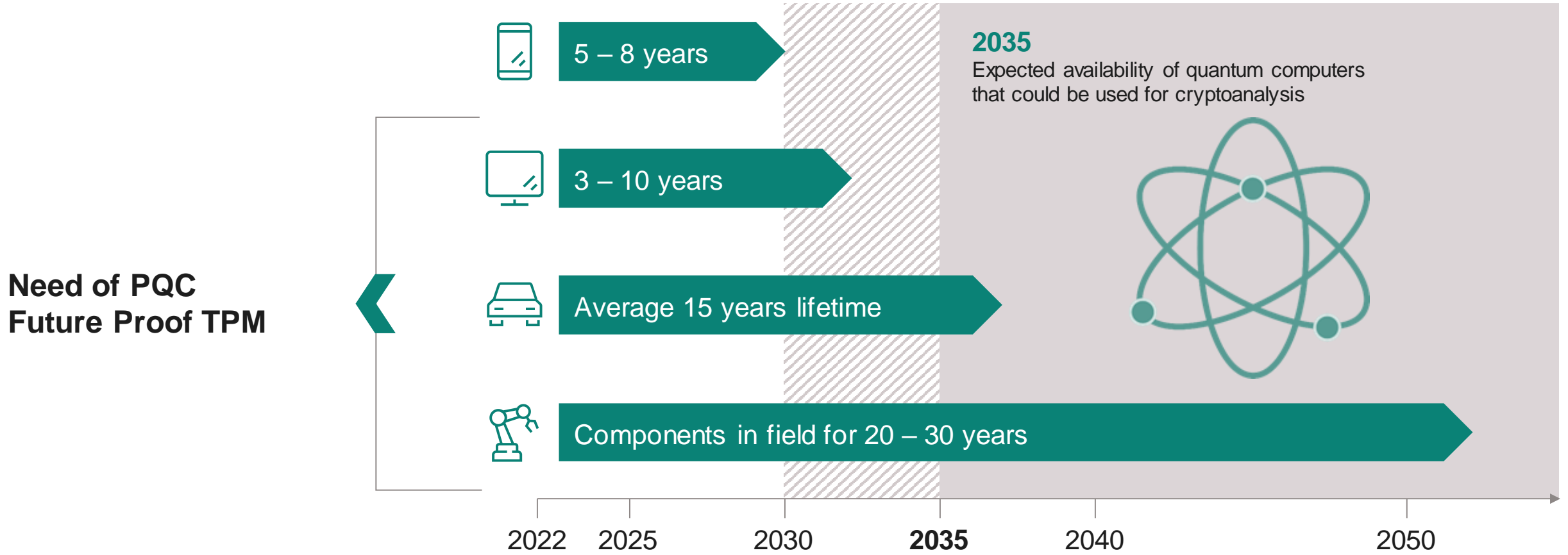
Affected:
AES-128, 3DES

Currently considered safe:
AES-256, SHA256¹, SHA512,
SHAKE256, SHA3-512, ...

¹ Preimage resistance

Considered timeline

Devices with over 10 years lifecycle must be prepared for the quantum computing age



The security of TPM applications can only be as high as the one of the firmware update mechanism



In the past

Embedded device

Firmware update mechanism

128-bit classical security

Embedded application
128-bit classical security



Today

Embedded device

Firmware update mechanism

128-bit PQC security

Embedded application
128-bit (or more) classical security



Use HBS standards available today



In the near future

Embedded device

Firmware update mechanism

128-bit PQC security

Embedded application
128-bit PQC security

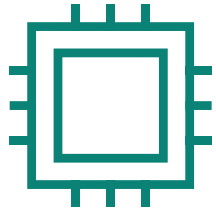


Upgrade to future PQC standards

OPTIGA™ TPM SLB 9673



Infineon has already taken the first steps into the world of quantum computing



Infineon's OPTIGA™ TPM family ...

offers the first TPMs on the market with a **PQC-protected** firmware update mechanism



Launched in **February 2022**



Launched in **September 2022**

The key benefits with Infineon's newest TPM family member



Future-proof

- PQC-protected firmware update mechanism
- Extended memory
- Stronger cryptographic algorithms



Robust security

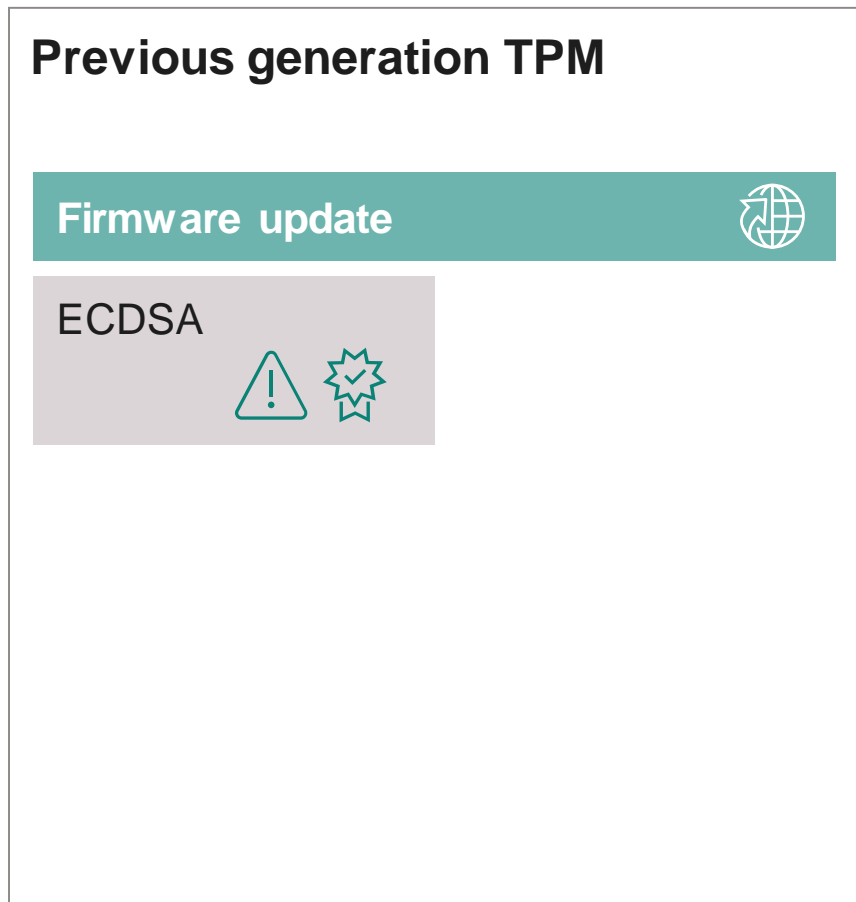
- Improved computational performances
- Resiliency features
- Fully compliant with the TCG requirements and certified accordingly



Easy integration

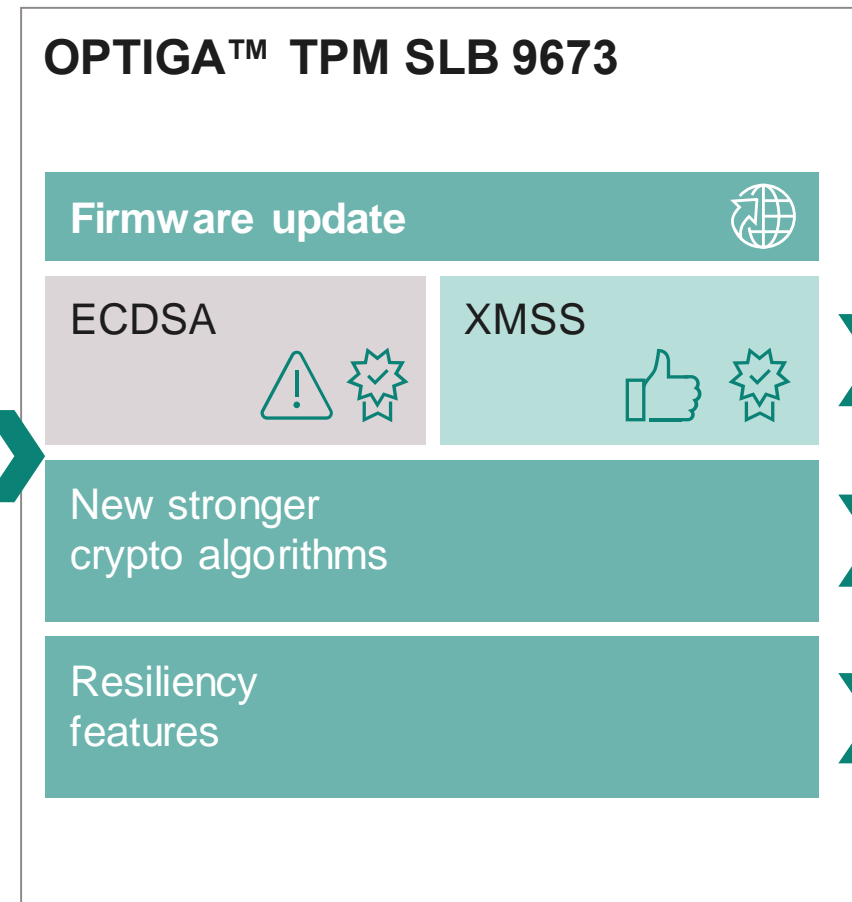
- Standardized Root of Trust
- Tools to support design activities
- Supports the latest version of Windows and Linux

OPTIGA™ TPM SLB 9673, a future-proof TPM



TCG certified Version 2
As per Revision 1.38

Improvements



TCG certified Version 2
As per Revision **1.59**

Quantum resistant

RSA 3k & 4k
SHA-384, ECC 384

To avoid any risk
of FW corruption

OPTIGA™ TPM SLB

OPTIGA™ TPM SLB

Interface

Optimized for

Temperature range

Interface speed

Availability

9673
FW 26.xx

I²C

Network infrastructure and light industrial machines such as factory robots, Programmable Logic Controllers (PLC)

Extended: -40°C to +85°C
Extended (Industrial): -40°C to **+105°C**

Flexibility in terms of interface speed
 – 100 kHz – I²C Standard Mode (lowest speed)
 – 400 kHz – I²C Fast Mode
 – 1MHz – I²C Fast Mode plus

July 2022
(with CC-certification)

9672
FW 15.xx

SPI

MSFT Windows environment/ ecosystem and connected devices with a “PC platform” architecture

Standard: -20°C to +85°C
Extended: -40°C to +85°C

33 MHz

Available

9672
FW 16.xx

SPI

Connected devices supporting enhanced security features (Chip Unique ID readout; AES encryption and decryption; Disabling EK key deletion)

Extended: -40°C to +85°C
Extended (Industrial): -40°C to +105°C

33 MHz

Available

The benefits of a hardware-based security



Why hardware-based security?



No security

Open for all to see



Software security only



Hardware security

Reading

Software code easily readable by attackers

Hardware chip protects itself against code reading

Copying

Software code easily copied and shared by attackers

Security hardware must be reverse engineered and re-manufactured

Analyzing

Software code easily analyzed and understood using standard tools

Hardware protection for data processing, transport storage

Root of Trust

Consequently, not so strong “Root of Trust” anchor for the system

Strong “Root of Trust” anchor for the system, providing detection, recoverability, secured updates

Relying on Infineon's hardware-based security protects secret keys against software vulnerabilities in OS and Apps



Why software security is often not enough?



Secret keys kept in the shared memory



Secret keys securely kept in the OPTIGA™ TPM

Security adds value by protecting your business, enabling growth and saving costs

Protecting

- Trust and reputation
- IP and process know-how
- Long-term revenue & profitability of investments



Enabling

- Growth
- New business models
- Security as a differentiation factor



Saving

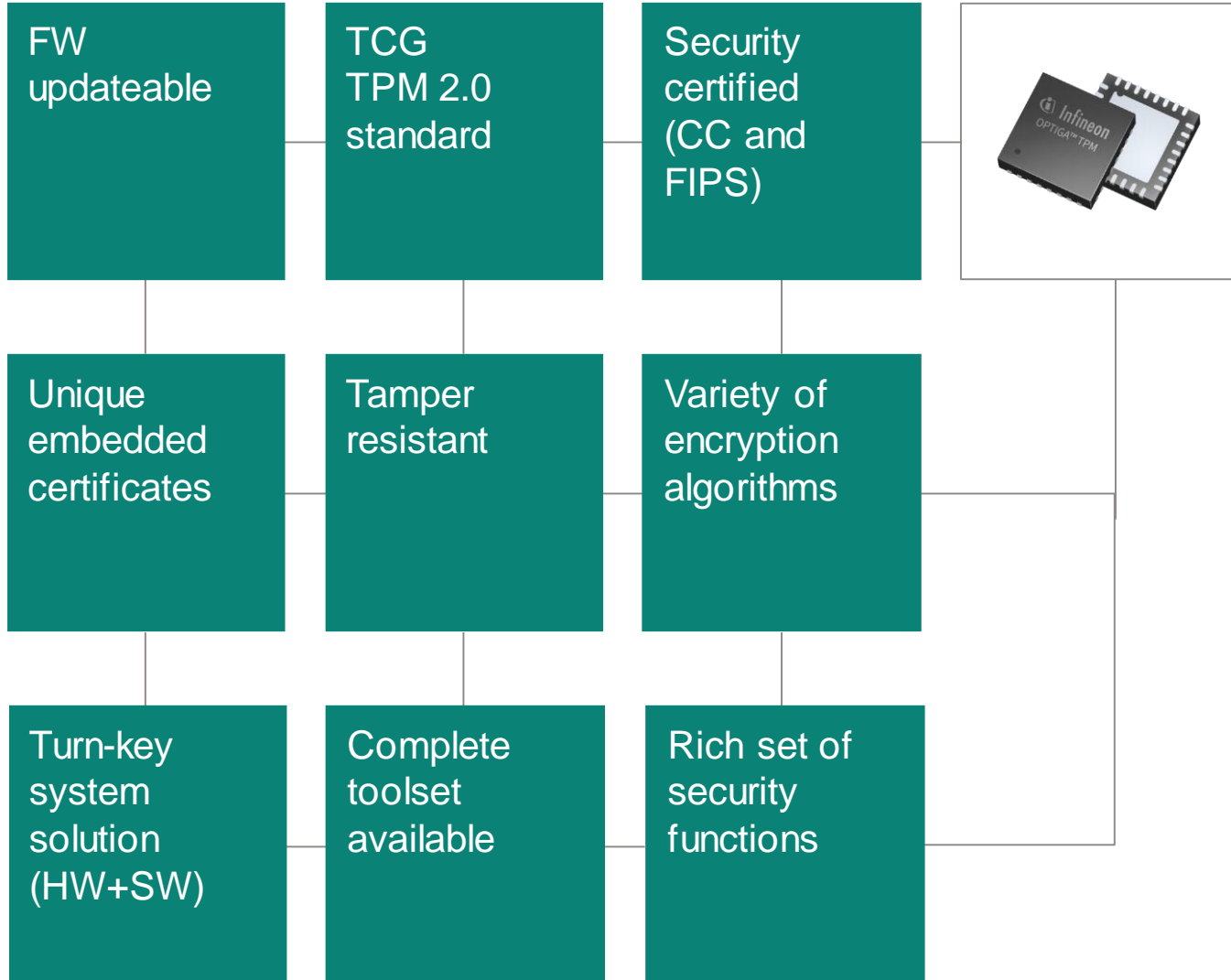
- Costs by preventing security-related system interruptions
- Cost based on new ways of solving a problem



**Why the
OPTIGA™ TPM
family**



Every second business laptop comes with an OPTIGA™ TPM



Our solution comes with service and support

We support you by ...



- Providing Design-In Application Notes for our Products
- Host side integration support
- Evaluation Kits



- Providing a secured Public Key Infrastructure
- Custom certificate loading in secured Production Environment



- Answering questions immediately
- Two Level Customer service



- Providing trainings for our security products
- Showing Demo Applications as a starting point for custom designs



Key take-aways

Security ...

... is essential and **HW-based security provides benefits beyond strong security** including time to market, logistics and scalability



New requirements ...

... coming in near the future because of **quantum computers** and the threat to existing cryptographic algorithms



OPTIGA™ TPM SLB 9673 ...

... with a **PQC-protected update mechanism** and an **I2C inter-face** suited for network infrastructure, light industrial machines such as factory robots, and Programmable Logic Controllers (PLC)



Find out more information and tools on the

[OPTIGA™ TPM SLB 9673 product page](#)

and our

[Github repository.](#)



