OPTIGA™ TPM SLB9672
A future-proof new generation TPM

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

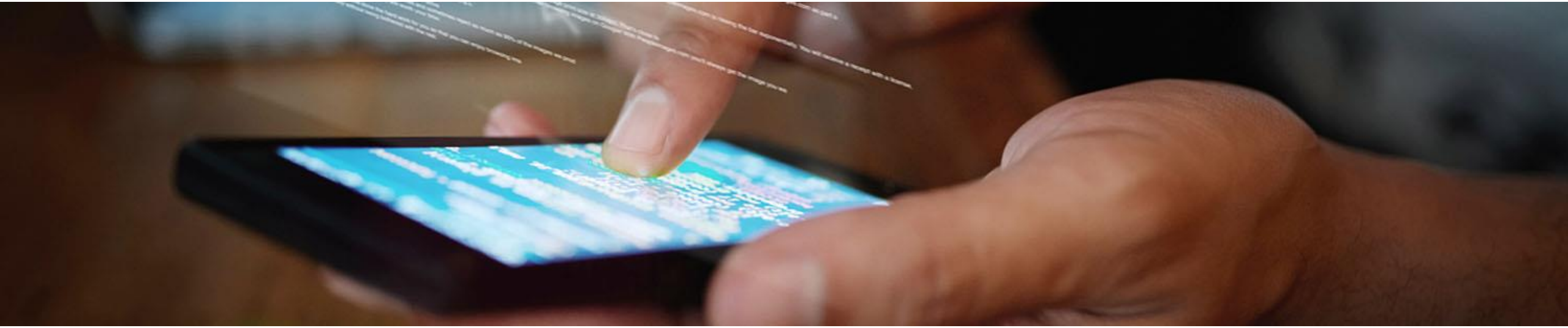
Product of the Year” award from ELEKTRONIK
First prize in the “Software” category

embeddedaward2023
winner: Safety & Security

Elektronik
Products of the Year
Software category: Winner
2023

BEST IN SHOW
Embedded
COMPUTING DESIGN
embeddedworld
WINNER

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

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

Key targets of discrete TPM

PC & laptops

- Professional PCs
- Industrial PCs

Servers

Servers

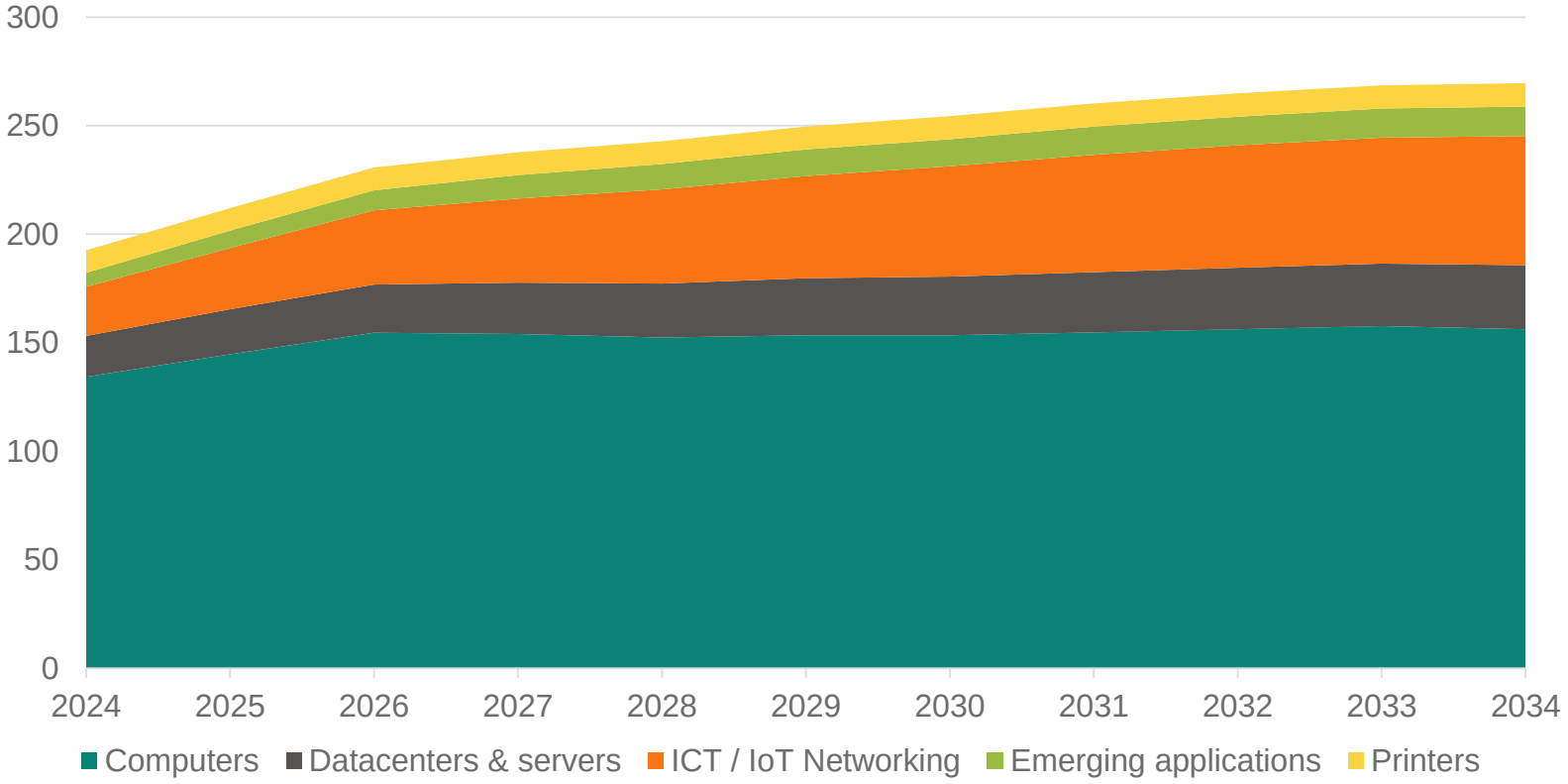
IoT networking

- Network Interface Cards
- Networking equipment
- Printers

Forecasted markets for discrete TPM

A stable base market and significant growth in other segments

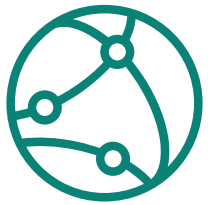
Market size (in M pcs)



What a TPM does

Smart factory

IoT networking

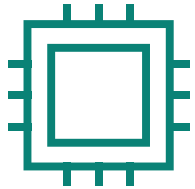


PC & laptops

Servers

Cloud

- Offers a standardized solution
- Allows trust and secured communications
- Allows protection of exchanged valuable data
- Supports the latest security requirements
- Is updatable



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		Quantum world
ECC-256 and RSA-3072 have **128-bit** security	›	Almost **no** security

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

Currently		Quantum world
AES-128 has **128-bit** security	›	**64-bit** security

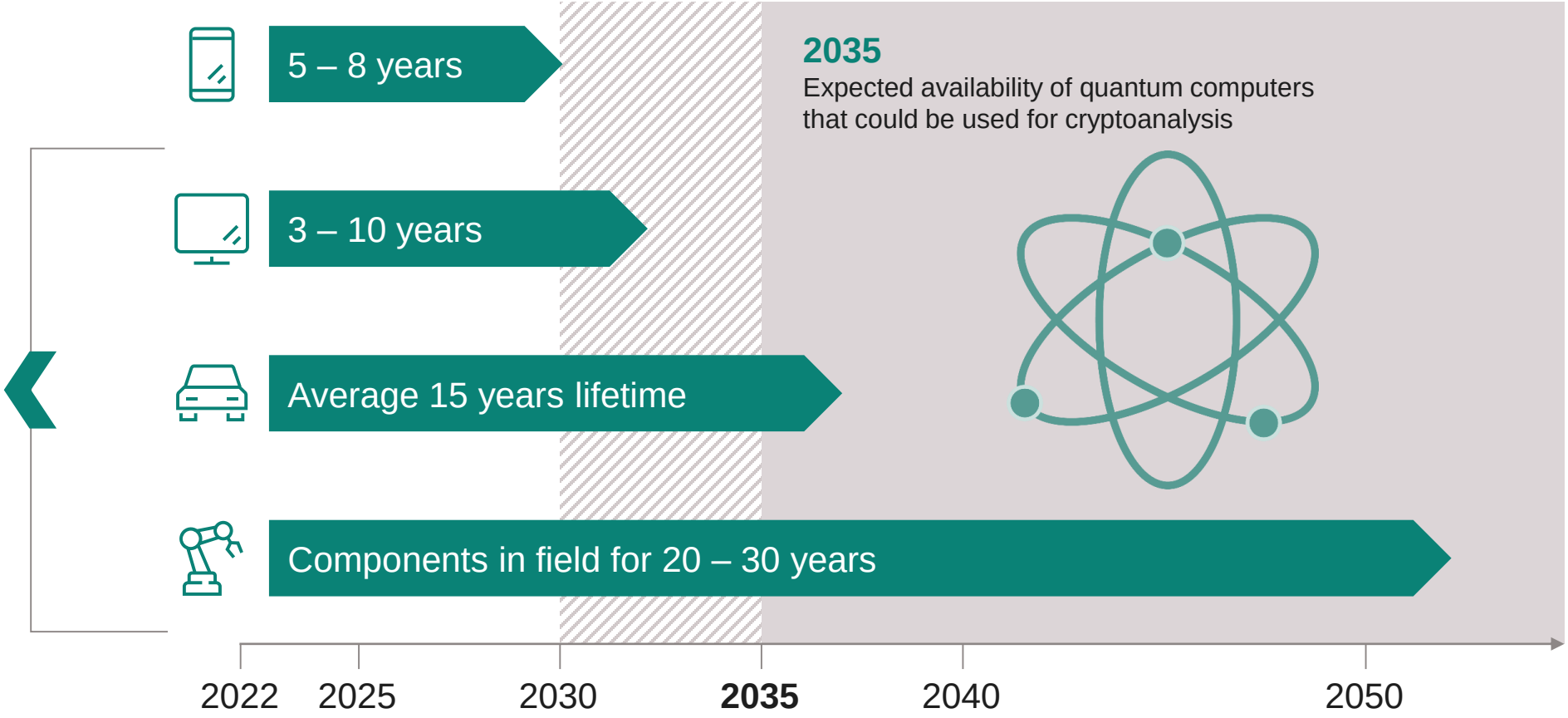
Quantum world (in 10 – 20 years)	**Heavily affected**	**Affected**	**Currently considered safe**
	RSA, ECDSA, ECDH	AES-128, 3DES	AES-256, SHA256[1], SHA512, SHAKE256, SHA3-512, …

[1] Preimage resistance

Considered timeline

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

Need of PQC
Future Proof TPM



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 9672

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

OPTIGA™ TPM SLB 9672

The first TPM on the market with a **PQC-protected** firmware update mechanism

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 9672, a future-proof TPM

Previous generation TPM

Firmware update

ECDSA

TCG certified Version 2
As per Revision 1.38

Improvements

OPTIGA™ TPM SLB 9672

Firmware update

ECDSA

XMSS

New stronger crypto algorithms

Resiliency features

Quantum resistant

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

To avoid any risk of FW corruption

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

One device – Two solutions

Firmware version

Standard Edition (FW 15.2x)
Optimized for PCs, servers

Enhanced Security for IoT networking (FW 16.1x)

Functionalities & applications

Primary choice for MSFT Windows environment/ecosystem
and connected devices
with a “PC platform” architecture.
- Two product variants:
- Standard temperature range -20° C to +85° C
- Extended temperature range -40° C to +85° C

Suitable for connected devices supporting enhanced security features
- Chip Unique ID readout
- AES encryption and decryption
- Disabling EK key deletion

Two product variants:
- Extended temperature range for -40° C to +85° C
- Extended temperature range for -40° C to +105° C

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

FW updateable

TCG TPM 2.0 standard

Security certified (CC and FIPS)

Unique embedded certificates

Tamper resistant

Variety of encryption algorithms

Turn-key system solution (HW+SW)

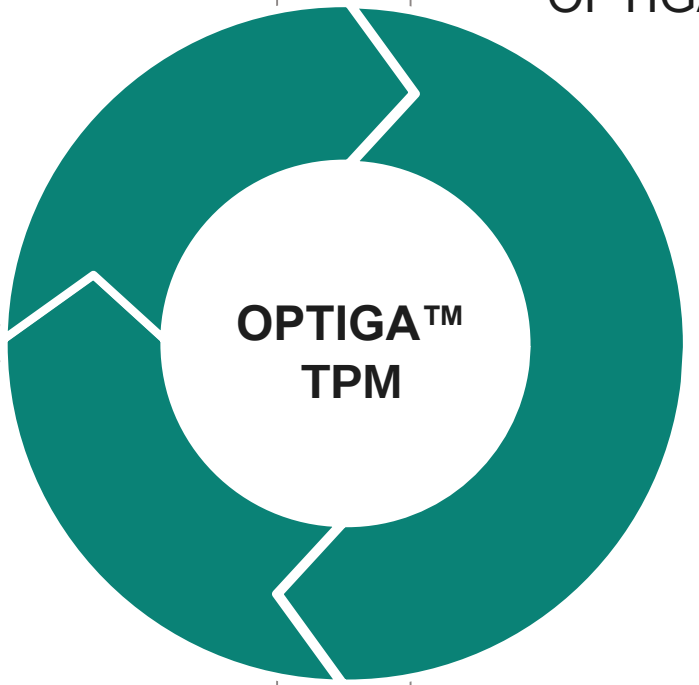
Complete toolset available

Rich set of security functions

OPTIGA™ TPM family offers rich functionality and flexibility

OPTIGA™ TPM SLM 9670
Industrial

OPTIGA™ TPM
SLI 9670
inCar



OPTIGA™ TPM SLB 9670
OPTIGA™ TPM SLB 9672
OPTIGA™ TPM SLB 9673
Consumer/IoT

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 9672 …

… is the right choice if you want to meet the challenges of today and tomorrow

Information and tools for OPTIGA™ TPM are easily available on Infineon's website

www.infineon.com/tpm

and our Github repositery

https://github.com/Infineon/OPTIGA-TPM

infineon