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
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**

**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)

![Graph showing forecasted markets for discrete TPM]
What a TPM does

<table>
<thead>
<tr>
<th>Smart factory</th>
<th>IoT networking</th>
<th>PC &amp; laptops</th>
<th>Servers</th>
<th>Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart factory icon</td>
<td>IoT networking icon</td>
<td>PC &amp; laptops icon</td>
<td>Servers icon</td>
<td>Cloud icon</td>
</tr>
</tbody>
</table>

- 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
- 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, 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

- Components in field for 20 – 30 years
- Average 15 years lifetime
- 5 – 8 years
- 3 – 10 years

2035
Expected availability of quantum computers that could be used for cryptoanalysis

2022 2025 2030 2035 2040 2050
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
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

**OPTIGA™ TPM SLB 9672**

- **Firmware update**
  - ECDSA
  - XMSS

**Improvements**

- **Quantum resistant**
- **RSA 3k & 4k SHA-384, ECC 384**
- **To avoid any risk of FW corruption**

**TCG certified Version 2**
As per Revision 1.38

**Resiliency features**

**New stronger crypto algorithms**

**TCG certified Version 2**
As per Revision 1.59
One device – Two solutions

Firmware version

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

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

Enhanced Security for IoT networking (FW 16.1x)

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?

<table>
<thead>
<tr>
<th>No security</th>
<th>Software security only</th>
<th>Hardware security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reading</strong></td>
<td>Software code easily readable by attackers</td>
<td>Hardware chip protects itself against code reading</td>
</tr>
<tr>
<td><strong>Copying</strong></td>
<td>Software code easily copied and shared by attackers</td>
<td>Security hardware must be reverse engineered and re-manufactured</td>
</tr>
<tr>
<td><strong>Analyzing</strong></td>
<td>Software code easily analyzed and understood using standard tools</td>
<td>Hardware protection for data processing, transport storage</td>
</tr>
<tr>
<td><strong>Root of Trust</strong></td>
<td>Consequently, not so strong “Root of Trust” anchor for the system</td>
<td>Strong “Root of Trust” anchor for the system, providing detection, recoverability, secured updates</td>
</tr>
</tbody>
</table>
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
- 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 repository

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