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.

- Secured plant
- Secured network
- Secured system
- Secured component

Diagram:
- Central Computer
- Server
- Industrial PC/Panel PC
- HMI
- Field device
- PLC/micro PLC
- Linear actuator
- Motor control

Levels:
- Plant level
- Supervisory level
- Control level
# 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

<table>
<thead>
<tr>
<th>Year</th>
<th>Market size (in M pcs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2024</td>
<td>0</td>
</tr>
<tr>
<td>2025</td>
<td>50</td>
</tr>
<tr>
<td>2026</td>
<td>100</td>
</tr>
<tr>
<td>2027</td>
<td>150</td>
</tr>
<tr>
<td>2028</td>
<td>200</td>
</tr>
<tr>
<td>2029</td>
<td>250</td>
</tr>
<tr>
<td>2030</td>
<td>300</td>
</tr>
</tbody>
</table>

- Computers
- Datacenters & servers
- ICT / IoT Networking
- Emerging applications
- Printers
Quick facts about TPM with an I2C interface

- 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

<table>
<thead>
<tr>
<th>Asymmetric cryptosystems (RSA/ECC): Completely broken using Shor’s algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currently</td>
</tr>
<tr>
<td>Quantum world</td>
</tr>
<tr>
<td>ECC-256 and RSA-3072 have 128-bit security</td>
</tr>
<tr>
<td>Almost no security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Symmetric cryptography: Security levels halved by Grover’s algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currently</td>
</tr>
<tr>
<td>Quantum world</td>
</tr>
<tr>
<td>AES-128 has 128-bit security</td>
</tr>
<tr>
<td>64-bit security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quantum world (in 10 – 20 years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heavily affected: RSA, ECDSA, ECDH</td>
</tr>
<tr>
<td>Affected: AES-128, 3DES</td>
</tr>
<tr>
<td>Currently considered safe: AES-256, SHA256, SHA512, SHAKE256, SHA3-512, …</td>
</tr>
</tbody>
</table>

1 Preimage resistance
Considered timeline

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

- Average 15 years lifetime
- Components in field for 20 – 30 years
- Need of PQC
- Future Proof TPM

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
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

Previous generation TPM

- **Firmware update**
  - ECDSA

<table>
<thead>
<tr>
<th>Improvements</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCG certified Version 2</td>
</tr>
<tr>
<td>As per Revision 1.38</td>
</tr>
</tbody>
</table>

OPTIGA™ TPM SLB 9673

- **Firmware update**
  - ECDSA
  - XMSS

<table>
<thead>
<tr>
<th>Improvements</th>
</tr>
</thead>
<tbody>
<tr>
<td>New stronger crypto algorithms</td>
</tr>
<tr>
<td>Resiliency features</td>
</tr>
<tr>
<td>Quantum resistant</td>
</tr>
<tr>
<td>RSA 3k &amp; 4k SHA-384, ECC 384</td>
</tr>
<tr>
<td>To avoid any risk of FW corruption</td>
</tr>
</tbody>
</table>

| TCG certified Version 2 |
| As per Revision 1.59 |
## OPTIGA™ TPM SLB

### Interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>9673 FW 26.xx</th>
<th>9672 FW 15.xx</th>
<th>9672 FW 16.xx</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FC</strong></td>
<td></td>
<td>SPI</td>
<td>SPI</td>
</tr>
<tr>
<td></td>
<td>Network infrastructure and light industrial machines such as factory robots, Programmable Logic Controllers (PLC)</td>
<td>MSFT Windows environment/ ecosystem and connected devices with a &quot;PC platform&quot; architecture</td>
<td>Connected devices supporting enhanced security features (Chip Unique ID readout; AES encryption and decryption; Disabling EK key deletion)</td>
</tr>
<tr>
<td><strong>Temperature range</strong></td>
<td><strong>Standard:</strong> -20°C to +85°C</td>
<td><strong>Extended:</strong> -40°C to +85°C</td>
<td><strong>Extended:</strong> -40°C to +85°C</td>
</tr>
<tr>
<td><strong>Optimized for</strong></td>
<td><strong>Extended:</strong> -40°C to +85°C</td>
<td><strong>Extended (Industrial):</strong> -40°C to +105°C</td>
<td><strong>Extended (Industrial):</strong> -40°C to +105°C</td>
</tr>
<tr>
<td><strong>Interface speed</strong></td>
<td>Flexibility in terms of interface speed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100 kHz – I2C Standard Mode (lowest speed)</td>
<td></td>
<td>33 MHz</td>
<td>33 MHz</td>
</tr>
<tr>
<td>400 kHz – I2C Fast Mode</td>
<td></td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>1 MHz – I2C Fast Mode plus</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Availability

- July 2022 (with CC-certification)
- Available
- Available
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>Open for all to see</td>
<td>Software code easily readable by attackers</td>
<td>Hardware chip protects itself against code reading</td>
</tr>
<tr>
<td>Reading</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>Copying</td>
<td>Software code easily analyzed and understood using standard tools</td>
<td>Hardware protection for data processing, transport storage</td>
</tr>
<tr>
<td>Analyzing</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>
<tr>
<td>Root of Trust</td>
<td></td>
<td></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
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.**