OPTIGA™ TPM SLI 9670

Follow

The OPTIGA™ TPM SLI 9670 is a quality hardened Trusted Platform Module (TPM) for special use in automotive applications and based on a tamper resistant secured micro-controller using advanced hardware security technology.

As turn-key solution it is flashed with a securely coded firmware according to latest TCG family 2.0 specifications offering a rich feature set of security functions, like key management, authentication, signature functions (signing/verifying), encryption/decryption, secured logging and secured time.

The SLI 9670 is qualified according to the automotive AEC-Q100 standard making it an ideal solution for automotive applications in telematics, gateway, multimedia head units and other ECUs with strong security requirements. This TPM is also security certified according to Common Criteria EAL4+.

Datasheet SLI9670 2.0 Rev. 1.1 › EN
01_10 | 2019-02-21 | pdf | 542 KB

› MUST READs-compilation on Enhanced Cybersecurity for the IIoT – read now!

Summary of Features

- Standardized and market approved turn-key security solution (TCG standard TPM 2.0)
- High-end tamper resistant security controller with advanced cryptographic algorithms (RSA-2048, ECC-256, AES*-128, SHA-256) and enhanced security features (shielding, security sensors, TRNG and other security design measures) implemented in hardware
- Highly reliable NVM technology
- SPI interface
- Extended temperature range (-40°C to 105°C)
- Full system integration support
- Automotive qualification according to AEC-Q100
- Security certification according Common Criteria EAL4+
- VQFN-32 package

AES* symmetric cryptography: TPM_ALG_AES may be used for all specified use cases (as specified by TCG) except for bulk encryption via the commands TPM2_EncryptDecrypt or TPM2_EncryptDecrypt2 which are not implemented by this TPM.

Benefits

- High-end tamper resistant security solution based on market leading security expertise protecting most sensitive assets (keys, IP, data and business cases)
- Reduced security risk based on proven technology (standardized and market approved security solution preprogrammed with rich security functions (TCG standard TPM 2.0))
- High flexibility thanks to a wide range of integrated security functions (e.g. dedicated key management) offered ready-to-use
- Secured key store and management: secured personalization (key injection in secured environment) realizes cost savings in the logistical chain
- Updatability of TPM firmware offers long-term crypto agility and sustainability
- Easy and cost efficient system integration through available open source drivers (e.g. for LINUX) and fast time to market

Press

- › TCG: Trusted Computing Enters New Frontiers
- › A safe for sensitive data in the car: Volkswagen relies on TPM from Infineon
- › World's first TPM for cybersecurity in the connected car
- › Infineon Optiga TPM SLI-9670: Erstes TPM für das vernetzte Auto
- › Automotive Cybersecurity "A Race Without a Finish Line"
- › Infineon and XAIN to collaborate on bringing blockchain into the car
- › SOTA – Secure software updates over the air

Potential Applications

- Car sharing
- Remote car access
- Over the air updates
- Mobile phone integration in infotainment
- Fleet management

Realized in targeted ECUs:

- Telematics control units
- Connected gateways
- Multi media head units
- ECUs requiring strong security protection

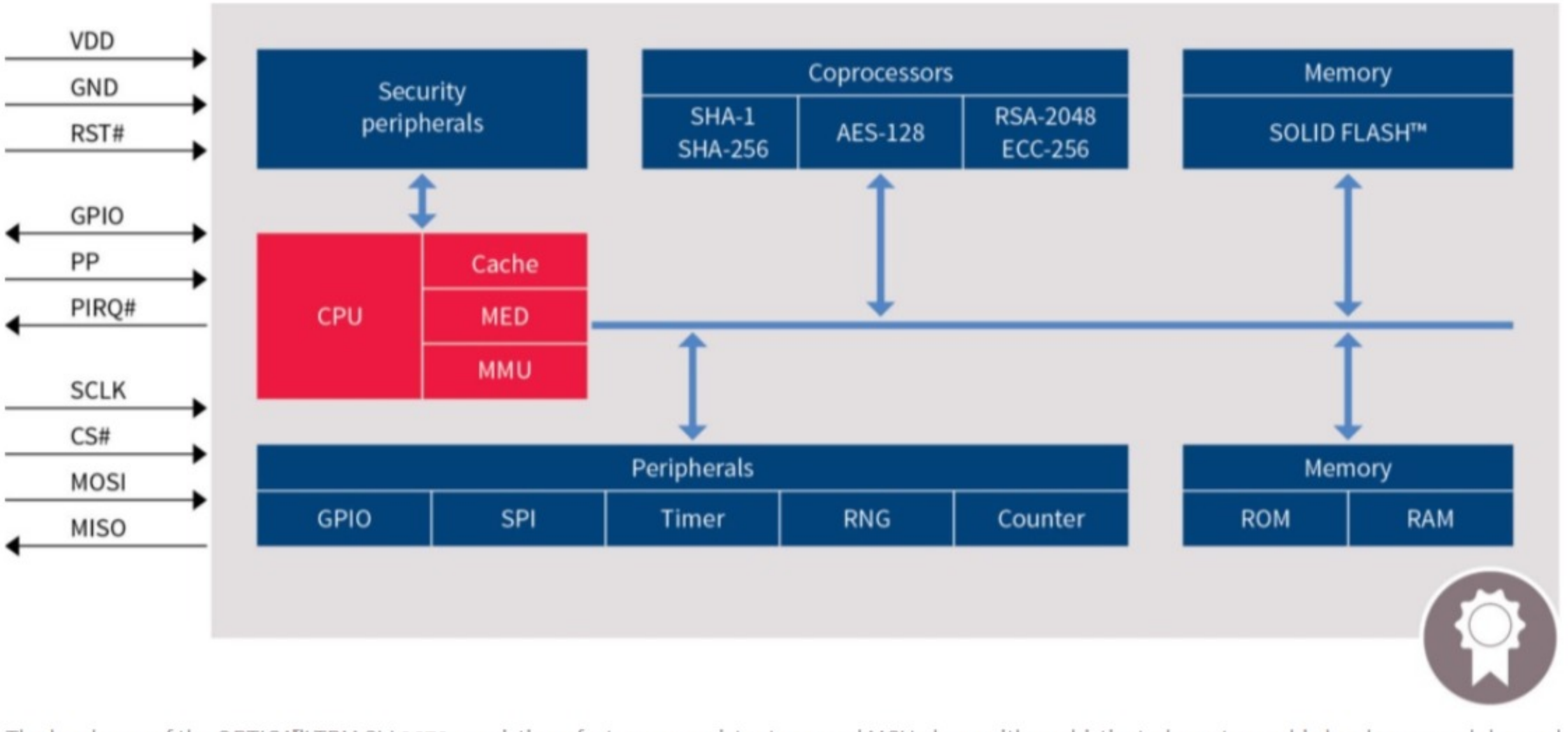
Automotive security use cases

- Secured key store and management
- Remote attestation
- Privacy protection
- Data store protection
- Mutual authentication
- Secured communication
- Diagnostic access
- Secured updates
- Platform integrity protection

Designers who used this product also designed with

- IPD90N06S4L-05 | 55V-60V N-Channel Automotive MOSFET
- SAK-TC397XP-256F300S BC | AURIX™ Family – TC39xXX
- SAK-TC397XX-256F300S BC | AURIX™ Family – TC39xXX
- TLE6389-2G V50 | OPTIREG™ Switchers (Automotive)
- TLF30681QVS01 | OPTIREG™ PMIC (Automotive)

Diagrams



The hardware of the OPTIGA™ TPM SLI 9670 consisting of a tamper-resistant secured MCU along with sophisticated cryptographic hardware modules and further peripherals, such as a random number generator. Advanced hardware security technology, which includes internal memory and bus encryption as well as shielding and sensors provides protection against physical and logical attacks.

Parametrics

Parametrics	SLI 9670
Additional Information	version 2.0 Rev. 01.38
Ambient Temperature min max	-40.0 °C 105.0 °C
Applications	automotive security
Asymmetric Cryptography	ECC ; ECC BN-256 ; ECC NIST P-256 ; ECC256 ; ECDH ; RSA1024 ; RSA2048
CPU	16-bit
Certifications	CC EAL4+ ; FIPS 140-2
Delivery Forms	VQFN-32
Interfaces	SPI
Package	VQFN-32
Product Description	FW13.11 ; security controller for automotive use cases
Symmetric Cryptography	HMAC ; SHA-1 ; SHA-256 ; AES* (AES* symmetric cryptography: TPM_ALG_AES may be used for all specified use cases (as specified by TCG) except for bulk encryption via the commands TPM2_EncryptDecrypt or TPM2_EncryptDecrypt2 which are not implemented by this TPM)
Use Cases	automotive TPM

Documents

+ Expand all

- + Data Sheets
- + Product Brief
- + Application Notes
- + Material Content Sheet (Info)
- + Application Brochure
- + Product Selection Guide
- + Certificates

Order

Sales Product Name	SLI 9670
OPN	SLI9670AQ20FW1311XUMA1
Product Status	active and preferred
Package name	PG-VQFN-32
Order online	
Completely lead free	yes
Halogen free	yes
RoHS compliant	yes
Packing Size	5000
Packing Type	TAPE & REEL
Moisture Level	3
Moisture Packing	DRY

Boards

Image	Board	Family	Description	Status
	OPTIGA TPM SLI9670 A-TPM	Security	Add OPTIGA™ TPM SLI 9670 to enhance security of AURIX™ 2nd generation MCU-based system for achieving high security standards. Infineon`s OPTIGA™ TPM SLI 9670 A-TPM board is featuring the automotive qualified OPTIGA™ TPM SLI 9670. It is an add-on board for the Infineon AURIX™ TC3xx host, supported by TPM Software Stack (TSS).	
	IRIDIUM SLI 9670 TPM2.0 (Buy online)	Security	Infineon TPM SLI 9670 Iridium add-on board for Raspberry Pi. For integration into the corresponding platform OS (Linux, Win10IoT, etc.). • SLI 9670	active and preferred

+ PCB Design Data

Tools & Software

Software and documentation - free download @ GitHub

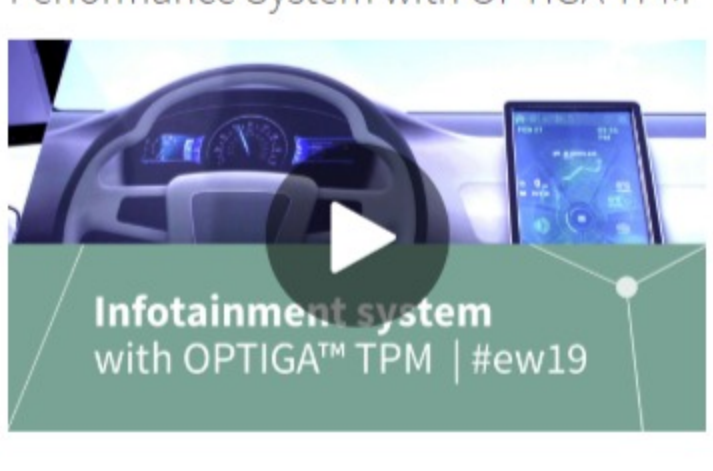
› Open-source Software Stack

› Embedded Linux TPM Toolbox 2

Intermediate CAs for the creation of certificates for the respective product and firmware version
› Intermediate certificates

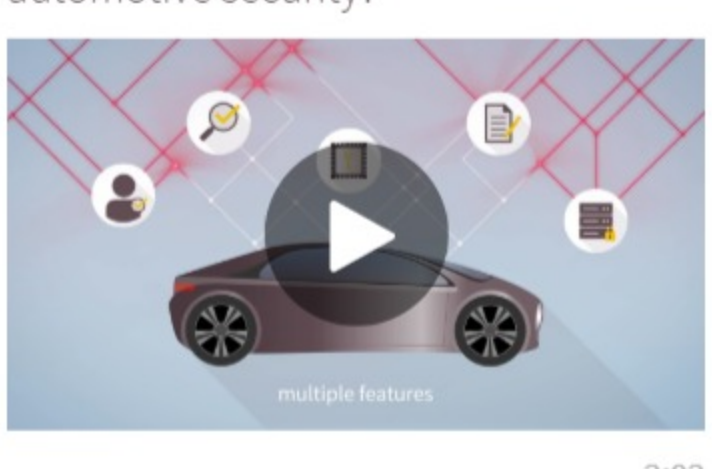
Videos

How to secure an Automotive High Performance System with OPTIGA TPM



Watch our demo-video and learn in the exemplary scenarios for Software-Update-Over-the-air (SOTA) and Remote Feature Activation how an automotive high performance ECU can be secured with the OPTIGA TPM SLI 9670

Why choose OPTIGA™ TPM for automotive security?



2:02

Infineon is the first supplier worldwide to offer an automotive-qualified TPM. Infineon's OPTIGA™ TPM offers a variety of features to protect automotive functions against malicious attacks. It brings easy to integrate, easy to use and easy to maintain security to your car.

Secured remote firmware updates and ECU integrity protection with OPTIGA™ TPM 2.0

2:15

OPTIGA™ TPM is a standardized, feature-rich security solution which protects the integrity and authenticity of devices and systems in automotive ECUs. It builds on proven technologies and supports the latest TPM 2.0 standard. This Fraunhofer SIT demo shows how OPTIGA™ TPM 2.0 can be used to protect user and OEM data from unauthorized access and to secure remote firmware updates.

Partners

5 out of **30** Partners

Name	Company Description	Region of Operations	Product Family	Partner Offering	Offering Details	Member Level
Entrust Datacard	Consumers, citizens and employees increasingly expect anywhere-anytime experiences — w ... › more	Americas, Asia-Pacific, Europe, Middle East, Africa, Greater China, Japan	Security & smart card solutions	Software, Services	The ioTrust™ software on TPM-equipped devices provides a secure wrap ... › more	Infineon Preferred Partner
Escrypt	ESCRYPT - Embedded Security is a leading system provider for embedded secu ... › more	Americas, Asia-Pacific, Europe, Middle East, Africa, Greater China, Japan	Microcontroller, Security & smart card solutions	Software, Services	Preferred Partner Solution provider for Embedded Security: - Consulting ... › more	Infineon Preferred Partner
Fraunhofer AISEC	The Fraunhofer Institute for Applied and Integrated Security AISEC under the responsibility of ... › more	Europe, Middle East, Africa	Security & smart card solutions	Software, Hardware, Services	Using cryptographic signatures to securely log data to SD cards without "se ... › more	Infineon Preferred Partner
Fraunhofer SIT	The Fraunhofer Institute for Secure Information Technology SIT is the leading expert fo ... › more	Europe, Middle East, Africa	Security & smart card solutions	Software, Hardware, Services	Protecting Remote Firmware Updates and system data protection i ... › more	Infineon Preferred Partner
GlobalSign	GlobalSign is the leading provider of trusted identity and security solutions. Its hig ... › more	Americas, Asia-Pacific, Europe, Middle East, Africa, Greater China, Japan	Security & smart card solutions	Services	Leveraging best in class hardware and software based security tec ... › more	Infineon Preferred Partner

› Show all 30 partners

Support

Search the FAQs! Enter your search terms...

Top 6 FAQs. Use the search bar above to show more!

Technical Support
In order to enable us to process your inquiry as efficiently as possible and ensure your case is duly reported, we kindly ask you to submit your request via the following support form:...
+ Read more

Partner Finder for software, hardware, dev tools, services, support
Infineon's partners offer products and services that complement our semiconductor device solutions to accelerate your development efforts and time to market. ...
+ Read more

Package information
The package information is available on our homepage at https://www.infineon.com/packages. Please note, that they are divided into the subcategories "Leaded and through-hol...
+ Read more

Notes on processing
Information regarding reflow profile, soldering temperature, soldering profile and further processing notes for most of the discrete products are mentioned in the Application Note....
+ Read more

Design-in support
We offer design-in support for your application.
You can find the Infineon Solution Finder at https://www.infineon.com/solutionFi...
+ Read more

Simulation Parameters/SPICE models
Please visit our Simulation Model Finder on the internet at https://www.infineon.com/simulation Please select "Simulation Models (SPICE, S-parameters, SABER)"...
+ Read more

Write to the Technical Assistance Center | Call us toll-free or request a call back | Live chat with our Support Center | Ask our community for support in the forum