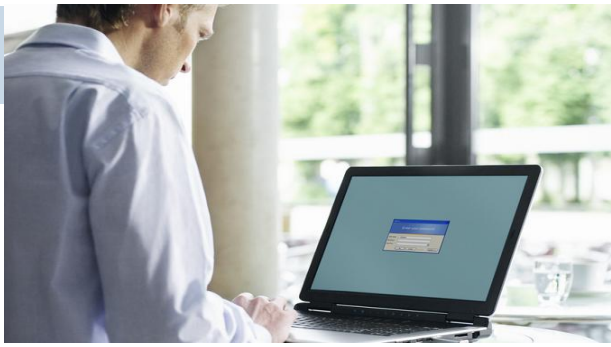
# Product Information

## Certified Trusted Platform Module

Common Criteria *EAL4+ Augmented* security certified TPM 1.2



**INFINEON TECHNOLOGIES's Trusted Platform Module (TPM) SLB9635 TT 1.2** is a fully standard compliant TPM which successfully passed the Trusted Computing Group (TCG) certification process. This process verifies the correct and secure implementation of the TCG standard specification based on the TCG Common Criteria protection profile.

### The TCG Certification Process for TPM

The members of the Trusted Computing Group (TCG) aligned with various market players and relevant organizations, defined and agreed on a certification program which includes:

- Compliance testing proving that the TPM is built and behaves according to the TCG standard
- Security evaluation by an independent, trusted, accredited and experienced third party lab which validates that the TPM has an appropriate resistance against logical and physical security attacks.

When both tests are completed successfully, the TPM product identification will be added to the public certification whitelist on the TCG website. This certification assures that the TPM meets or exceeds the technical and security specifications mandated by the TCG.

### Compliance Testing

The TCG has developed a robust Compliance Test Suite of more than 400 tests to validate product conformance to the TCG specifications.

Companies and organizations may request the Compliance Test Suite package from the TCG administration to verify the correct test execution.

The successful compliance test of a TPM also is an essential precondition for trusted applications to reliably run with the same behavior on all standard compliant TPMs.

Infineon offers a TCG version 1.2-compliant Trusted Platform Module which fulfills the requirements of the TCG certification program for TPM including:

- Successful Common Criteria certification at EAL4+ Augmented, according to the PC Client TPM 1.2 Protection Profile developed by the TCG.
- Functional testing (compliance) by using TCG-developed automated Compliance Test Suites, according to a test plan documented by the TCG.

In addition to TPM hardware, Infineon also develops Trusted Computing software that builds upon its strong TPM foundations, enabling standards-based TPM access from applications as well as delivering full manageability of TPMs within enterprise environments of all sizes.

Infineon maintains its leadership position in the industry for high security chips like TPMs or smartcards by proving the high quality of its TPMs which are independently certified using a well-defined, vendor-neutral open security evaluation standard like Common Criteria. This is a clear sign of Infineon's strong investment in and commitment to producing the best possible TPMs on the market.

Never stop thinking

## Security Evaluation

A TPM keeps and protects critical data and serves as a trusted anchor for security applications - which implies that also a security evaluation becomes a critical checkmark in the TCG's certification process.
The TCG has selected the Common Criteria rules (ISO 15408 standard) as the most appropriate and worldwide recognized scheme for evaluating the security level of a TPM.
Common Criteria (CC) methodology includes the definition of protection features as described in the product specific protection profile document (PP) according to the expected security threats and application requirements. As a precondition for CC security evaluation, the TCG has developed a neutral protection profile for the TPM and published it on their website. This protection profile delivers the evaluation metrics for TPMs, which will then be used by the officially accredited trusted test labs for security evaluation and certification.

## Common Criteria (CC) for security evaluation

CC provides a comprehensive, tiered structure for certifying that security products in general meet the specified security protection requirements. It has well-defined Evaluation Assurance Levels (EALs) that describe the scope of the evaluation process. Developed by government agencies the Common Criteria scheme is accepted worldwide and provides the necessary transparency to show in detail the degree of security protection which is incorporated in the evaluated product.
To obtain the certification, the product is submitted to an accredited, independent testing lab. Once the evaluation is completed, the resulting report is forwarded to the national certification body for review and certificate issuance.

The Infineon TPM 1.2 is certified to EAL4+ Augmented, which even exceeds the level required by the TCG's TPM Protection Profile. EAL4 alone specifies that the TPM itself is verified to have been methodically designed, tested and reviewed. Its entire lifecycle, starting with its design and development through to its post-production process for maintaining quality, has been carefully checked and these procedures will be maintained. The extension "Augmented" means that the protection level against attacks is not only oriented on the knowledge of experts, but it has additionally augmented protection mechanisms.
Additionally, Infineon's TPM has undergone systematic vulnerability analysis to show that it not only was designed to be as secure as possible, but it was specifically analyzed based on the latest threat and attack models. The Infineon TPM production process and facilities are also evaluated to ensure their overall integrity.

## Infineon's Certification History

This isn't the first time that Infineon has put one of its security chips through this type of certification. Infineon's first TPM (v1.1) was Common Criteria EAL3+ certified in 2004 while the new standard now requires EAL4+. Infineon has also put more than 100 of its products (e.g. high security smartcard processors used in payment or government applications) through such independent third-party certification - in most cases certifying them even up to CC EAL5+.

## A Certified TPM Is The Best Choice

Obtaining this certification is one way that Infineon's TPM clearly distinguishes itself from others. The Trusted Computing Group's Protection Profile for TPMs, the certification report for the Infineon TPM and the result of the compliance test are publicly available documents, which can be seen at the TCG certification program white list. This further allows customers and other stakeholders to reassure themselves in detail that Infineon's TPM specifically meets their requirements.

More information concerning TCGs certification program as well as the TCG white list can be found at the TCG-website under http://www.trustedcomputinggroup.org/certification.

For further questions and information please visit us at http://www.infineon.com/tpm or tpm-support@infineon.com.

**How to reach us:**
http://www.infineon.com/tpm

Published by
Infineon Technologies North America Corp.
640 N.McCarthy Blvd.
Milpitas, CA 95035



Ordering No. B189-H9422-X-X-7600