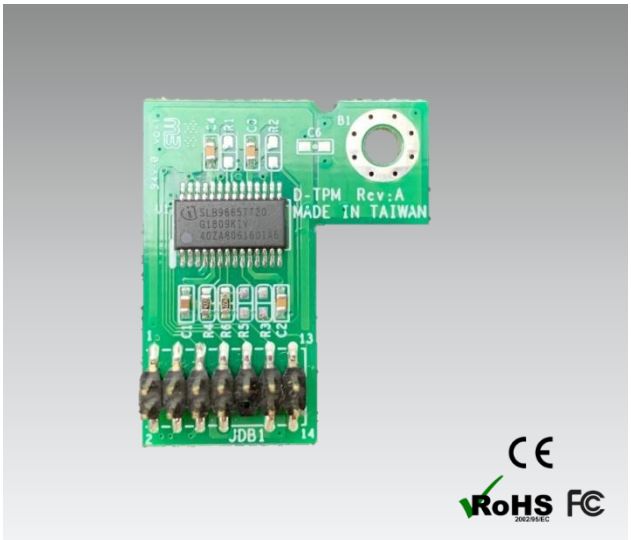
D-TPM

Trusted Platform Module



Main Features

- D-TPM 2.0 is a docking type TPM 2.0 module
- High-end security controller with advanced cryptographic algorithms implemented in hardware
- TCG and Common Criteria certified with EAL4+
- Flexible with LPC interface support and communicate with the serial interrupt(SERIRQ) protocol
- Extended temperature range (-40 to +85°C) for a variety of applications
- Industrial design, manufactured in Cadmus Taiwan

Product Overview

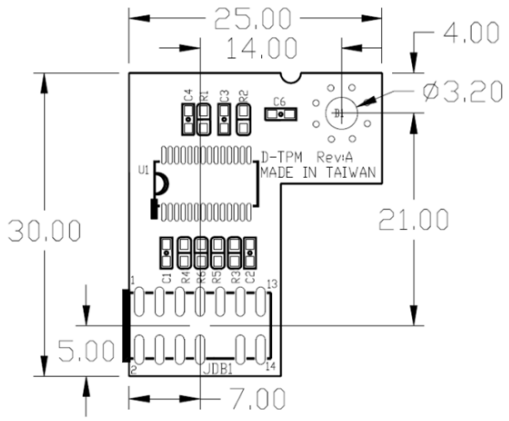
TPM (Trusted Platform Module) is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (your PC or laptop). These artifacts can include passwords, certificates, or encryption keys.

A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments.

Specifications

Module Name	D-TPM 2.0
Board Layout	30 x 15 mm thickness: 1.6mm OSP
Chipset	TPM2.0 : SLB9665TT2.0 FW5.62
Input interface	LPC interface
Support	**TPM2.0 Supports :** RSA encryption and signature ECC encryption and signature ECC-DAA ECDH SHA-1, SHA-256 HMAC AES and one-time-pad with XOR
Compatible Operating System	Windows Linux Kernel Version 3.10 and higher
Relative Humidity	Operating 10%~90%, non-condensing Non-operating 5%~95%, non-condensing

Dimension



Ordering Information

D-TPM2.0

- RoHS Compliance
- TPM SLB 9665 TT2.0

Pin definition