

## Main Features

- 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

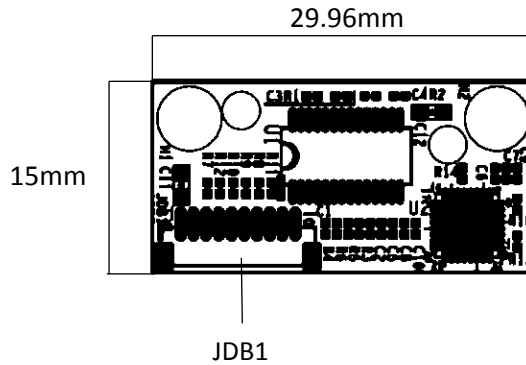
TPM (Trusted Platform Module) is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (your PC or laptop). These artifacts can include passwords, certificates, or encryption keys.

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                 | EBK-TPM2.0   |
| Board Layout                | 30 x 15 mm thickness: 1.6mm OSP  |
| Chipset                     | TPM2.0 : SLB9665TT2.0 FW5.62   |
| Input interface             | LPC interface  |
| Support                     | <b>TPM2.0 Supports :</b><br>RSA encryption and signature<br>ECC encryption and signature<br>ECC-DAA<br>ECDH<br>SHA-1, SHA-256<br>HMAC<br>AES and one-time-pad with XOR |
| Compatible Operating System | Windows  |
| Relative Humidity           | Operating 10%~90%, non-condensing<br>Non-operating 5%~95%, non-condensing  |

### Dimension

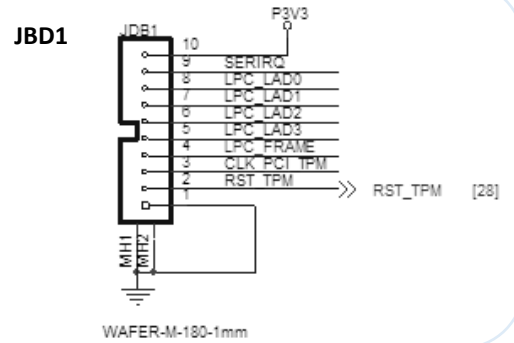


### Cable Optional:

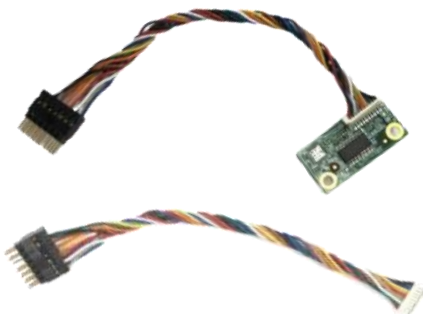
10 pin (pitch 1.0) to 10 pin (pitch 1.0)  
L= 65mm cable



#### Pin definition



10 pin (pitch 1.0) to 13 pin (pitch 2.0)  
L= 95mm cable



#### Pin definition

| Pin | Function   | Pin | Function |
|-----|------------|-----|----------|
| 1   | L_CLK      | 2   | L_AD1    |
| 3   | L_RST#     | 4   | L_AD0    |
| 5   | L_FRAME#   | 6   | 3V3      |
| 7   | L_AD3      | 8   | GND      |
| 9   | L_AD2      | 10  | Key      |
| 11  | INT_SERIRQ | 12  | GND      |
| 13  | 5VSB       | 14  | 5V       |