

Trusted Platform Module (TPM) v2.0

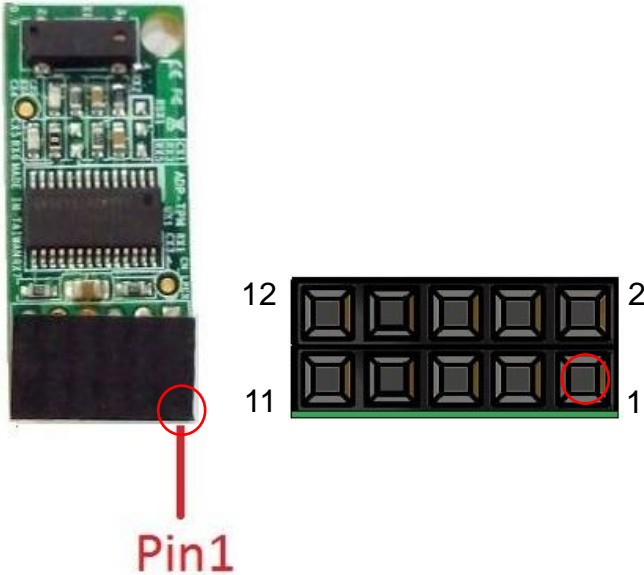
LPC Interface

ADP-TPM2E2

Complete solution implementing version 2.0 of the Trusted Computing Group specifications



IC Model	Infineon SLB9665 TT2.0
Interface	12-Pin Low Pin Count
Key Features	<ul style="list-style-type: none">➤ TCG 2.0 compliant trusted platform module (TPM)➤ Meets Intel TXT, Microsoft Windows and Google Chromebook certification criteria for successful platform.➤ LPC interface➤ Hardware accelerator for SHA-1 and SHA-256 hash algorithm.➤ Standard (-20 to +85°C)➤ 3.3 V power supply
OS Support	For integration into the corresponding platform OS (Windows, Linux, Win 10 IoT, etc.).
Dimension	30 x 13mm
Ordering Code	
ADP-TPM2E2	12-Pin TPM 2.0 module, Firmware V5.63



Pin Assignment

Pin	Description	Pin	Description
1	LPC_CLK	2	RESET-
3	-LFRAME	4	LAD3
5	LAD2	6	LAD1
7	LAD0	8	+3.3V
9	SERIRQ	10	Ground
11	+3.3VSB	12	N/C