TPM2.0

A **Trusted Platform Module** is a specialized chip on an endpoint device that stores RSA encryption keys specific to the host system for hardware authentication.

Features:

- lTPM SLB9665TT20FW561XUMA1
- compatible with 2x10p LPC
- operating voltage 3-3.3V
- meeting Intel **TXT**, **Microsoft Windows** and **Google Chromebook** certification criteria for successful platform qualification
- **True Random Number Generator** (TRNG)
- full personalization with Endorsement Key (EK) and EK certificate
- supports the **LPC interface** and interrupts are communicated with the serial interrupt (SERIRQ) protocol

Applications:

- disk encryption
- password protection
- platform integrity and other security issues