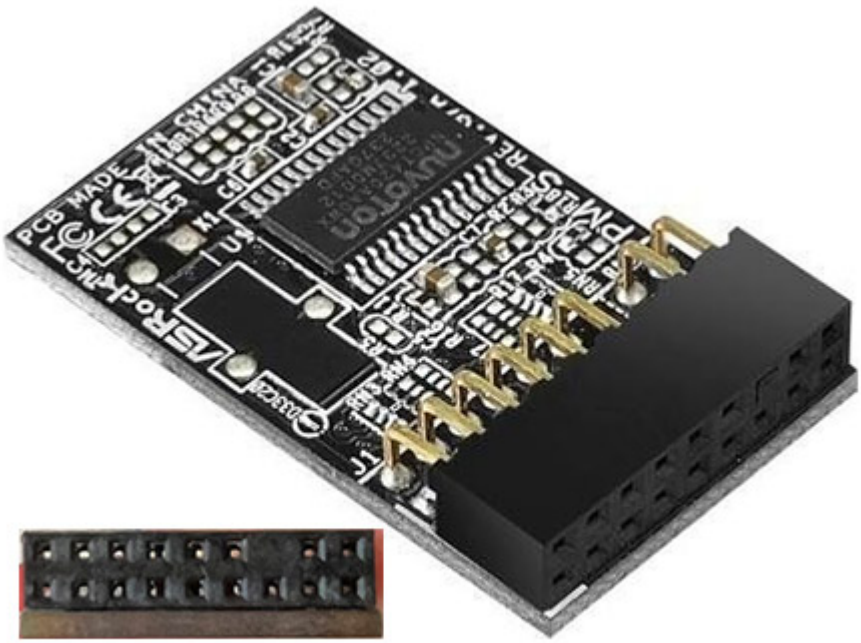

29.95 EUR
incl. 19% VAT, plus shipping

- TPM 2.0 !
- 17 pin connector !
- SPI Interface !
- 80-CXG5H1-1A12 !

The Trusted Platform Module (TPM) is a security device on the system board that will hold computer-generated keys for encryption. It is a hardware-based solution that helps to avoid attacks by hackers looking to capture passwords and encryption keys.

- Infineon TPM SLB 9665 TPM2.0
- Compliant to TPM Main Specification, Family "2.0", Level 00, Revision 01.16
- LPC interface
- Meets Intel TXT, Microsoft Windows and Google Chromebook certification criteria for successful platform qualification
- Random Number Generator (RNG) according to NIST SP800-90A
- Full personalization with Endorsement Key (EK) and EK certificate
- Standard (-20..+85°C)
- TSSOP-28
- Pin-compatible to SLB 9660
- Optimized for battery operated devices: low standby power consumption (typ. 150µA)
- 24 PCRs (SHA-1 or SHA-256)
- 7206 Byte free NV memory
- Up to 3 loaded sessions (TPM_PT_HR_LOADED_MIN)
- Up to 64 active sessions (TPM_PT_ACTIVE_SESSIONS_MAX)
- Up to 3 loaded transient Objects (TPM_PT_HR_TRANSIENT_MIN)
- Up to 7 loaded persistent Objects (TPM_PT_HR_PERSISTENT_MIN)
- Up to 8 NV counters
- Up to 1 kByte for command parameters and response parameters
- Up to 768 Byte for NV read or NV write
- 1280 Byte I/O buffer *Supported on selected motherboards. Please refer to motherboard selection for more details. Not supported with Intel® 8 and 9 series chipsets.