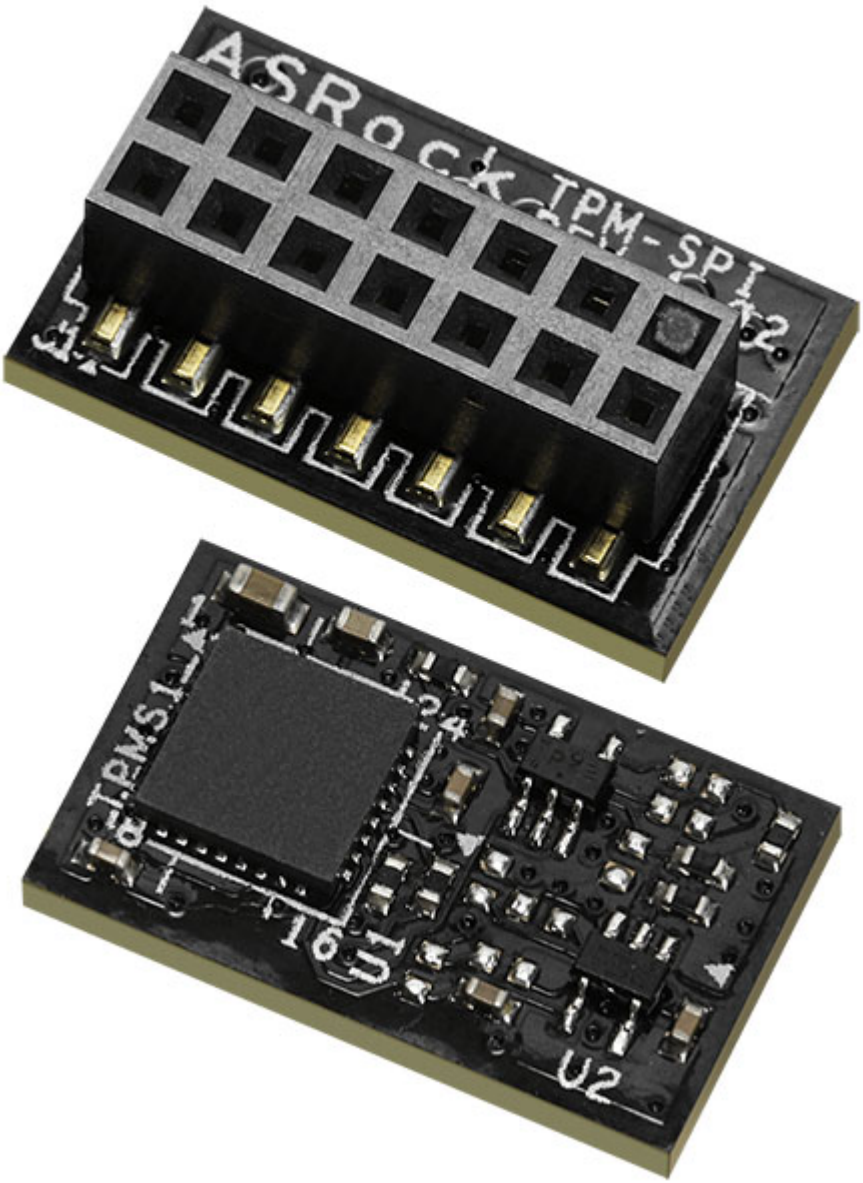

29.95 EUR
incl. 19% VAT, plus shipping

- TPM 2.0 !
- 13 pin connector !
- SPI Interface !
- 80-MCA080-1B01 !

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.

Compatible with all mainboards with TPM header.

- Compatible with Win 10, UEFI OS
- Dimmension: 16,51mm x 10,16mm
- 14-1pin

- Compliant to TPM Main Specification, Family "2.0", Level 00, Revision 01.16
- SPI interface
- TPM 2.0
- 13 pin connector
- Meeting 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) and Enhanced temperature range (-40..+85°C)
- PG-VQFN-32-13 or PG-UQFN-32-1 package
- Pin compatible to OPTIGA™ TPM SLB 9670 TPM1.2 version
- Optimized for battery operated devices: low standby power consumption (typ. 110µA)
- 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
- 1280 Byte I/O buffer