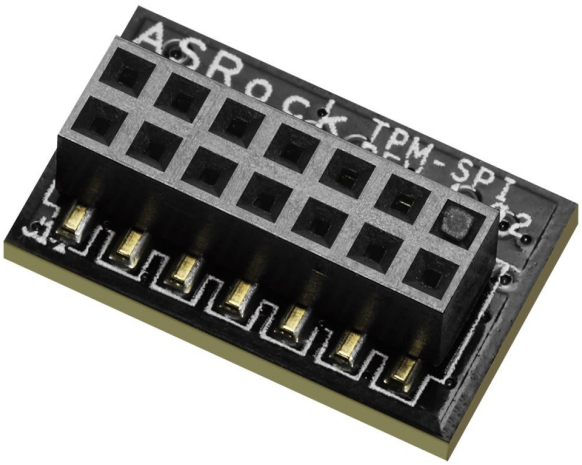
ASRock modul TPM-SPI

cena vč DPH:	**343 Kč**
cena bez DPH:	283 Kč
Kód zboží (ID):	4576435
PN:	TPM-SPI
Záruka:	24 měsíců



TPM-SPI

- V súlade s hlavnou špecifikáciou TPM, rodina "2.0", úroveň 00, revízia 01.16

Funkcie V súlade s hlavnou špecifikáciou TPM, rodina "2.0", úroveň 00, revízia 01.16 - Rozhranie SPI - Splnenie certifikačných kritérií Intel TXT, Microsoft Windows a Google Chromebook pre úspešnú kvalifikáciu platformy - Generátor náhodných čísel (RNG) podľa NIST SP800-90A - Úplná personalizácia s kľúčom Endorsement Key (EK) a certifikátom EK - Štandard (-20..+85 °C) a rozšírený teplotný rozsah (-40..+85 °C) - Balenie PG-VQFN-32-13 alebo PG-UQFN-32-1 - Piny kompatibilné s OPTIGA™ TPM SLB 9670 TPM1.2 verzia - Optimalizované pre zariadenia napájané z batérie: nízka spotreba energie v pohotovostnom režime (typ. 110µA) - 24 PCR (SHA-1 alebo SHA-256) - 7206 bajtov voľnej pamäte NV - Až 3 načítané relácie (TPM_PT_HR_LOADED_MIN) - Až 64 aktívnych relácií (TPM_PT_ACTIVE_SESSIONS_MAX) - Až 3 načítané prechodné objekty (TPM_PT_HR_TRANSIENT_MIN) - Až 7 načítaných trvalých objektov (TPM_PT_HR_PERSISTENT_MIN) - Až 8 čítačov NV - Až 1 kByte pre parametre príkazov a parametre odpovedí - 1280 bajtov vyrovnávacej pamäte I/O *Podporované na základných doskách platformy X570 a novších.

Systémové požiadavky - Windows 10, UEFI OS

Rozmery - 16.51 mm x 10.16mm

Rozmery pinov - 14-1pin.

TPM-SPI

V súlade s hlavnou špecifikáciou TPM, rodina "2.0", úroveň 00, revízia 01.16

Funkcie
V súlade s hlavnou špecifikáciou TPM, rodina "2.0", úroveň 00, revízia 01.16
- Rozhranie SPI
- Splnenie certifikačných kritérií Intel TXT, Microsoft Windows a Google Chromebook pre úspešnú kvalifikáciu platformy
- Generátor náhodných čísel (RNG) podľa NIST SP800-90A
- Úplná personalizácia s kľúčom Endorsement Key (EK) a certifikátom EK
- Štandard (-20..+85 °C) a rozšírený teplotný rozsah (-40..+85 °C)
- Balenie PG-VQFN-32-13 alebo PG-UQFN-32-1
- Piny kompatibilné s OPTIGA™ TPM SLB 9670 TPM1.2 verzia
- Optimalizované pre zariadenia napájané z batérie: nízka spotreba energie v pohotovostnom režime (typ. 110µA)
- 24 PCR (SHA-1 alebo SHA-256)
- 7206 bajtov voľnej pamäte NV
- Až 3 načítané relácie (TPM_PT_HR_LOADED_MIN)
- Až 64 aktívnych relácií (TPM_PT_ACTIVE_SESSIONS_MAX)
- Až 3 načítané prechodné objekty (TPM_PT_HR_TRANSIENT_MIN)
- Až 7 načítaných trvalých objektov (TPM_PT_HR_PERSISTENT_MIN)
- Až 8 čítačov NV
- Až 1 kByte pre parametre príkazov a parametre odpovedí
- 1280 bajtov vyrovnávacej pamäte I/O
*Podporované na základných doskách platformy X570 a novších.
Systémové požiadavky
- Windows 10, UEFI OS
Rozmery
- 16.51 mm x 10.16mm
Rozmery pinov
- 14-1pin.