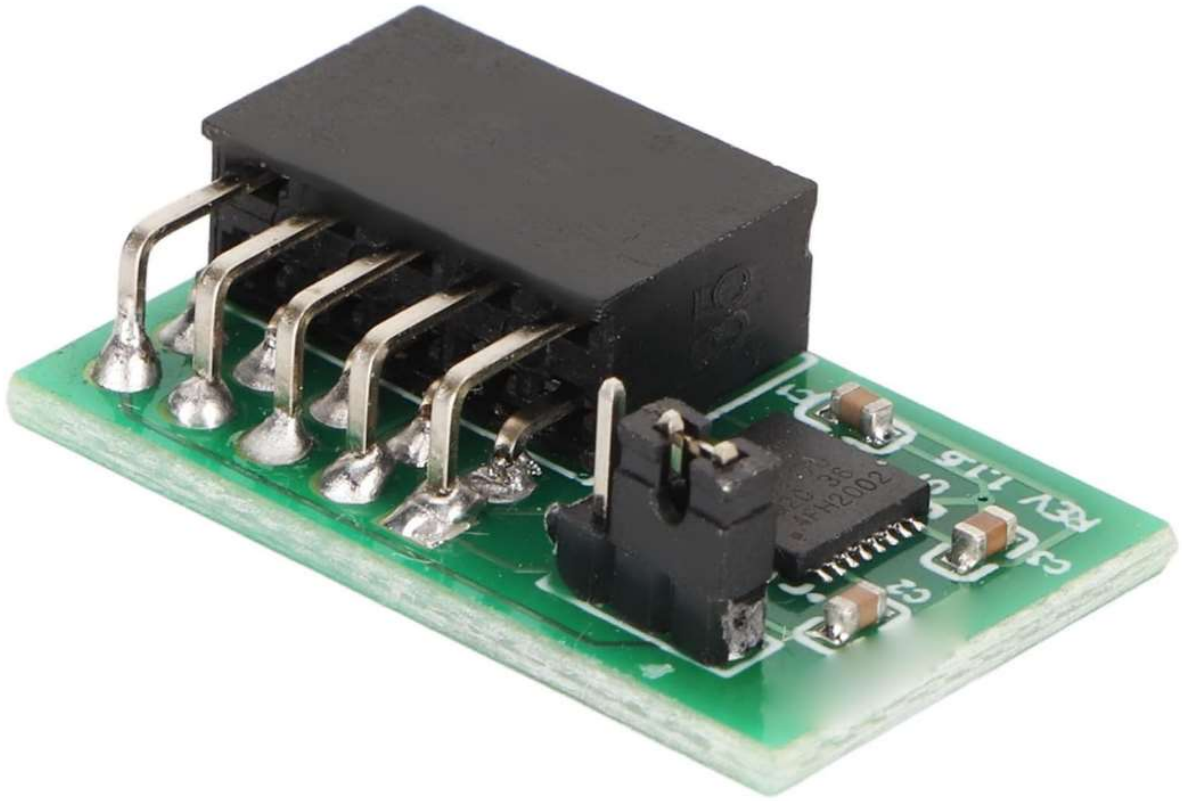
Puce de Module TPM 2.0, Module SPI 10 Broches, Chipset 9670 Vertical Stable, Haute Sécurité avec Processeur de Cryptage, pour SuperMicro AOM TPM 9670V S

Référence : Zunatew3d7e2s9tf



1. Conçu pour SuperMicro : ce module TPM 2.0 est spécialement conçu pour la plate-forme de confiance 10 broches SPI TMP2.0 pour SuperMicro AOM TPM 9670V S. Conforme au module de plate-forme de confiance (TPM) de TCG 2.0.
2. Compatibilité : ce module de sécurité TPM 2.0 est compatible avec les logiciels intégrés pour l'amélioration du micrologiciel TCG ainsi qu'avec les accélérateurs matériels pour les données utilisateur et les clés pour EEPROM SHA 1 et SHA 256, générateur de nombres aléatoires (RNG).
3. Norme prise en : ce module TPM SPI répond aux normes d'authentification TXT, Win et Chromebook pour empêcher les attaques par dictionnaire.
4. Performances stables : ce module de cryptage TPM 2.0 adopte matériau de carte de circuit imprimé de qualité supérieure qui garantit des performances stables et une efficacité élevée.
5. Mode veille pris en : pour la prise en de la technologie d'exécution de confiance , pour la pré-génération de clé RSA, pour la prise en intégrée du noyau Linux, prend en le mode veille d'économie d'énergie.

Spécification :

Type d'élément : Module TPM 2.0
Matériau : Circuit imprimé
Couleur : Vert
Chipset : Pour INFINEON 9670
Interface : SPI
Version Tpm : TPM 2.0
Définition des broches : 10 broches (10 1Pin)
Application : Conçu pour SuperMicro AOM TPM 9670V S
Alimentation : 3,3 V

Comment utiliser :
retirer et utiliser
>
Liste de colisage :
1 x module TPM 2.0

Remarque :
Veuillez consulter le manuel de la carte mère pour confirmer que votre carte mère prend en la technologie TPM2.0
Certaines cartes mères nécessitent l'insertion d' module TPM ou une mise à jour du dernier BIOS pour activer l'option TPM.
Supprimez les autres technologies de sécurité de votre ordinateur avant l'installation.