Giới thiệu + kiến trúc Asus MK TPM-M R2.0

Giới thiệu: (theo ASUSTek Computer Inc)

Asus MK TPM-M R2.0 là thiết bị giúp nâng cao Bảo mật cho Máy Tính

Thẻ TPM-M R2.0 lưu trữ một cách an toàn các khóa, chứng chỉ số, mật khẩu và dữ liệu. Nó giúp tăng cường bảo mật mạng, bảo vệ danh tính số, và đảm bảo tính toàn vẹn của nền tảng.

Thiết kế với giao diện 14-1 pin và LPC

Chip: Infineon SLB 9665, tuân thủ theo các quy định của TCG Family "2.0"

Được chứng nhận theo tiêu chuẩn Common Criteria EAL4+

Tuân thủ tiêu chuẩn CE và RoHS

Kích cỡ: 15mmx25mm

Hỗ trợ:

Windows® 7 64-bit, UEFI OS, with KB2920188 Windows hotfix installed  
Windows® 8.1 64-bit, UEFI OS  
Windows® 10, UEFI OS

