

Intel Trusted Platform Module 2.0 TPM für Server System M50CYP1UR204 M50CYP1UR212 M50CYP2UR208 M50CYP2UR312

Artikelnummer 999607204

Gewicht 1kg

Länge 1mm

Breite 1mm

Höhe 1mm



Produktbeschreibung

Trusted-Platform-Modul (TPM 2.0) ist ein Mikrocontroller, der Schlüssel, Kennwörter und digitale Zertifikate speichert. Eine separate TPM 2.0 bietet die Funktionen der Intel Platform-Trust-Technik (Intel PTT) und unterstützt auch Intel vPro Technologie und Intel Trusted-Execution-Technik (Intel TXT).

Weitere Bilder

