



# The Motion Computing<sup>®</sup> Trusted Platform Module (TPM)

---

## Trusted Platform Module (TPM) Overview

---

Motion<sup>™</sup> L-Series Tablet PCs include a built-in Trusted Platform Module (TPM) that provides ultimate security for your organization. A TPM can be used to validate that a computer is indeed an authentic and known system to the organization, or it can be used to safely and securely store encryption keys. The TPM itself is a self-contained, secure micro-controller integrated into the Tablet PC's main printed circuit board. Unlike typical hard drive-only protection schemes, such as passwords or software encryption that can be easily removed or tampered with, the TPM adds a tamper-proof and secure foundation to build upon. By storing the keys that unlock the encrypted data in the TPM instead of on the hard drive, the encrypted data on the hard drive becomes more secure.

---

## TPM Use Cases

---

The TPM can be used to authenticate a Tablet PC or to protect cryptographic functions.

*Authentication:* An organization's security policy may require that critical financial data can only be viewed by executives on their assigned Tablet PCs. Using the unique TPM that is built-in to each platform, the Tablet PC can be authorized and approved to view this specific data. Using OmniPass Enterprise Edition<sup>1</sup> to create the binding, allows encrypted documents to be opened only on specified Tablet PCs.

*Encrypted Email:* The TPM can also be used to enhance the email signing and encryption features of Microsoft Outlook<sup>2</sup>. When an email is signed and encrypted, two keys are generated: a public key that is given to the recipient to unlock the email and a private key that is used by the sender to sign and encrypt the email. The TPM strengthens this process by creating the two keys and then storing the private key within itself. This makes the signature and encryption much less vulnerable to software attacks.

---

## Motion L-Series TPM Version

---

The Motion L-Series Tablet PCs have a built-in Trusted Computing Group 1.1b compliant TPM.

---

<sup>1</sup> OmniPass Enterprise Solution is a scalable software solution for managing user passwords and corporate authentication policies. It can support multi-device and multi-factor authentication, file and folder encryption with seamless file sharing, and server storage and backup of fingerprint data.

<sup>2</sup> A signed message enables users to validate the integrity of the email message and the identity of the sender. An encrypted message protects the body of the email message from unintended exposure, but it is not signed.

---

## **Using the TPM for Encryption**

---

The TPM can integrate with most secure applications that use Public Key Infrastructure (PKI) solutions through the Microsoft CryptoAPI or PKCS#11 interface. It uses 2048 bit RSA encryption to protect keys and secrets.

Some applications that can be strengthened by the TPM because of this PKI support include: Check Point VPN/FW, Entrust Enterprise PKI Solution, Internet Explorer, Adobe Acrobat, Verisign PKI, RADIUS EAP, Netscape, NS Messenger Sun ONE PKI and PGP.

---

## **Integrating the TPM with Motion OmniPass**

---

With the Motion OmniPass client software, you can use the TPM to authenticate users and platforms as well as enable strong encryption algorithms. Files can be encrypted with any algorithm you require. Motion OmniPass enables the basic and enhanced Microsoft encryption engines called Cryptographic Service Provider (CSP).

---

## **Managing the TPM**

---

The Infineon TPM software shipped with Motion L-Series Tablet PCs provides client-based maintenance functionality needed to backup and restore TPM keys.

---

## **Other TPM Functions**

---

The Infineon TPM software application also provides users with the capability to create a Personal Secure Drive (PSD). The software creates a virtual hard drive that is only visible and accessible by the user. Data contained in the PSD is automatically encrypted using the 192 bit Advanced Encryption System (AES) algorithm. Each user can configure a PSD up to 200MB.