

# smart security interface TPM

Logical Access Client and TSS stack for  
trusted platform modules

Windows, Linux, Mac

supports PIV / FIPS 201 cards

100% PKCS#11

PC logon, VPN, SSL security



## Turn your TPM chip into a Smart Card



The Trusted Platform Module (TPM) is a secure device integrated into the motherboard of enterprise class laptops and desktops, including computers from Dell, HP, Lenovo, and Acer. The TPM securely stores keys for pre-boot authentication, disk encryption and other security functions. Now, with charismathics smart security interface<sup>®</sup> TPM (CSSI-TPM), you can use the TPM chip you already have to function as a smart card for just about any application where a real smart card can be used, including VPN, remote access, computer logon, digital certificate signing and encryption.

## Components:

- TCG Software Stack (ver. 1.2 compliant)
- Microsoft CryptoAPI Cryptographic Service provider
- PKCS#11 Stack
- Token Configurator Application

## Benefits

- Makes the TPM available to applications that support smart cards and USB tokens
- Uses the Trusted Platform Chip already available on your enterprise class laptop or desktop
- Eliminates the need to deploy smart cards and readers to end users.
- Supports all major PIV card vendors including Infineon, Broadcom and Atmel.
- Wide application support: Remote logon, computer logon, digital signatures, email signing and encryption.

## How CSSI-TPM works

At the core of the charismathics CSSI-TPM solution is a version 1.2 compliant TCG Software Stack that supports TPMs from all the major vendors, including Infineon, Atmel ST Microsystems and Broadcom. Application support is provided through a Microsoft CryptoAPI compliant CSP – for support of applications that support CryptoAPI, such as Microsoft Outlook, as well as a PKCS#11 component, for applications such as Firefox. These same interfaces can be used by card management applications to load keys and certificates onto the cards, and manage the user PIN.

CSSI-TPM works seamlessly with CSSI for smart cards and USB tokens, including smart cards and tokens from all major vendors, and supporting all major card standards. A single management utility – the Token Configurator – allows the user and administrator to manage all devices and credentials on those devices, all from a single interface.

## Business Value

Companies that adopt digital certificates to secure critical business assets such as servers, computers and email need to manage and secure the certificate keys associated with these credentials. Smart cards and USB tokens are specifically designed for this purpose, but for many scenarios the time, cost and complexity of deploying smart card readers to users make this prohibitive expensive. The charismathics smart security interface TPM solution solves this problem by using the native Trusted Platform Module chip in the PC, eliminating the deployment complexities, and cost associated with readers, cards and tokens.

## TPM available computers

TPM enabled laptops and PCs are available in the business computer lines from all major vendors including:

**Dell:** Latitude

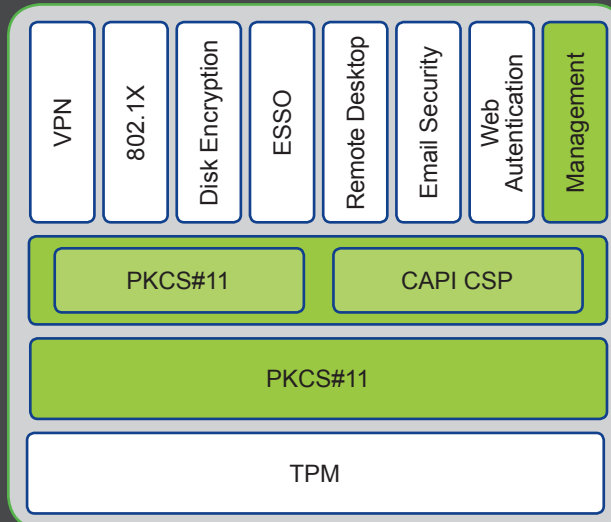
**HP:** Compaq, EliteBook and ProBook

**Lenovo:** ThinkPad

**Fujitsu:** LifeBook

**Acer:** Aspire and TravelMate

Not all versions of the above listed notebooks include a TPM. Check the manufacturer specifications.



## Platforms supported

- Atmel
- Broadcom
- Infineon
- Intel
- Sinosun
- STMicroelectronics
- Nuvoton (Winbond)
- Microsoft Windows XP (SP3)
- Vista (SP1)
- Windows 7
- Server 2003
- Server 2008

## Certified Applications

SSL Client Certificate Web Authentication	Microsoft Internet Explorer, Firefox
Digital Signatures	Microsoft Office, Adobe Acrobat
VPN/Remote Access	Microsoft, Cisco, Check Point, Nortel
Email signing and Encryption	Microsoft Outlook, Mozilla Thunderbird
Pre Boot Authentication/ Disk Encryption	Check Point, McAfee, PGP, Secude, Sophos
RDP	Windows Terminal Server, Citrix XenApp

**charismathics**

the middleware company

charismathics gmbh  
47 Sendlinger St  
Munich, Germany 80331  
www.charismathics.com  
sales@charismathics.com  
phone +49 (89) 3090-6700

**charismathics**

the middleware company

charismathics inc.  
2033 Gateway Place Suite 500  
San Jose, CA 95110, USA  
www.charismathics.com  
sales@charismathics.com  
phone +1 (408) 573 6440

charismathics