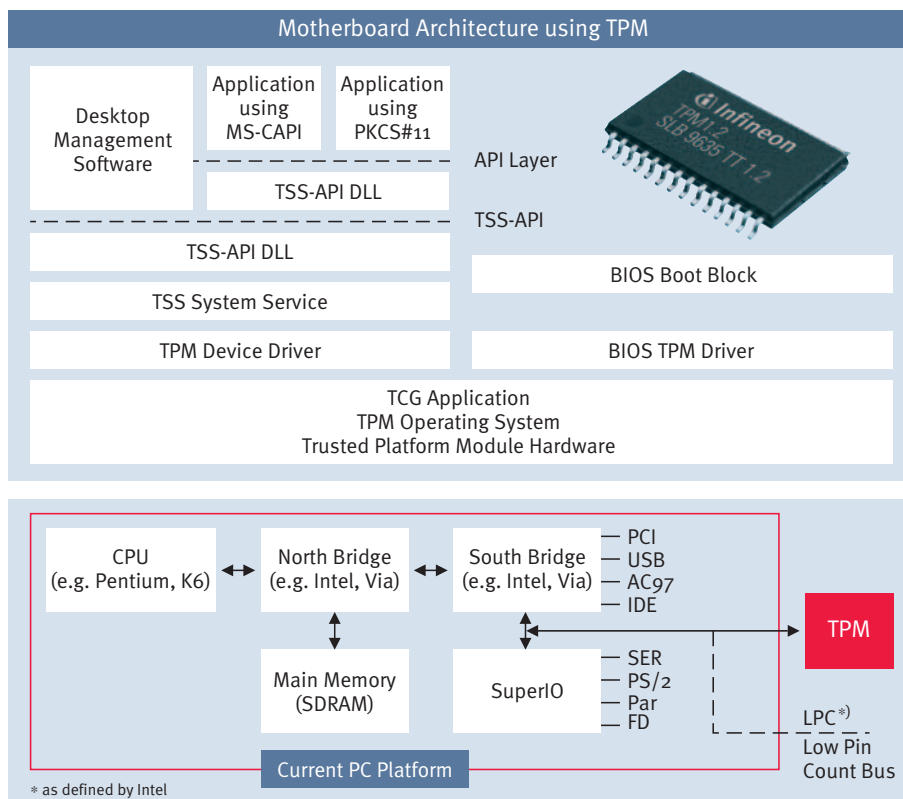


## Hardware Features of the TPM 1.2

- TCG 1.2 compliant trusted platform module (TPM)
- Security architecture based on Infineon SLE66CXxPE security controller family
- 16-bit microcontroller in 0.22 µm CMOS technology
- TCG 1.2 compliant embedded software
- EEPROM for TCG firmware enhancements and for user data and keys
- Advanced Crypto Engine (ACE) with RSA support up to 2048 bit key length
- Hardware accelerator for SHA-1 hash algorithm
- True Random Number Generator (TRNG)
- Tick counter with tamper detection
- Protection against Dictionary Attack
- Infineon's TPM 1.2 will be certified at Evaluation Assurance Level (EAL) 4 Medium at TÜVIT Labs in Germany
- General Purpose Input/Output
- Intel® Trusted Execution Technology Support
- AMD® Secure Virtual Machine Architecture Support
- Microsoft's recommended GPIO included
- Full personalization with Endorsement Key (EK) and EK certificate
- Power saving sleep mode
- 3.3 V power supply
- WHQL dual mode 1.1b + 1.2 TPM Windows Kernel Mode Driver
- Operating temperature range: 0°C to +70°C



Note:  
 Microsoft Outlook, Outlook Express, Explorer and Windows are registered trademarks of Microsoft Corporation.  
 Netscape Communicator is a registered trademark of Netscape Communications Corporation.  
 RSA SecureID is registered trademarks of RSA Security Inc.  
 Check Point, the Check Point logo, OPSEC, VPN-1 SecureClient, and VPN-1 SecuRemote are trademarks or registered trademarks of Check Point Software technologies Ltd. or its affiliates.  
 GemSafe for TPM is a registered trademark of Gemalto.

How to reach us:  
<http://www.infineon.com>

Published by  
 Infineon Technologies AG  
 81726 Munich, Germany

© Infineon Technologies AG 2006.  
 All Rights Reserved.

## Legal Disclaimer

The information given in this Product Brief shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffenheitsgarantie"). With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

## Information

For further information on technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies Office ([www.infineon.com](http://www.infineon.com)).

## Interfaces

- Low Pin Count (LPC) interface to allow easy system integration
- Operates from a single 33 MHz clock
- Support of power down signal to enter low-power standby mode
- Support of dynamic clock shutdown (CLKRUN)

## Package

- Small Low profile TSSOP-28 package
- Green package

## Security Features

- Over/Under voltage Detection
- Low frequency sensor
- High frequency filter
- Reset filter
- Memory Encryption (MED)
- Additional security features

## Software Features

- Embedded secure operating system
- Embedded TCG application
- Reference implementation for PC-BIOS integration
- TPM Professional Package (supporting Windows 2000, Windows XP Home, Windows® XP Professional, Windows XP Tablet, Windows 2000/2003 Server Windows Vista, Linux driver)
  - TSS software stack compliant to TCG specifications
  - TPM Cryptographic Service Provider (CSP)
  - Infineon's desktop management software for policy enforcement and security feature management

## Support of MS-CAPI and PKCS#11 Applications

- Microsoft Outlook® and Outlook Express®
- Microsoft Office 2000, Office XP and Office 2003
- Microsoft Internet Explorer®
- Netscape Communicator®
- Microsoft Encrypted File System
- RSA Secure ID®
- Check Point™ SecuRemote/SecureClient
- Check Point™ VPN-1®/FireWall-1 NG®
- Entrust™ Desktop Manager Solutions
- GemSafe for TPM /Smart Card



## Warnings

Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies Office.  
 Infineon Technologies Components may only be used in life-support devices or systems with the express written approval of Infineon Technologies, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system.  
 Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

Ordering No. B116-H7956-G7-X-7600  
 Printed in Germany  
 PS 11061. nb