National Semiconductor

PRODUCT BRIEF
February 2002
Revision 1.0

PC21100 (SafeKeeper™) LPC-Based TCPA-Compliant Security Controller

General Description

The PC21100 is a single-chip Trusted Platform Module (TPM) solution for PC security based on the TCPA standard. It is fully TCPA-compliant and offers system designers all the advantages of Trusted Computing as defined by the TCPA.

The PC21100 is a member of the National Semiconductor® TrustedI/O family, which provides TCPA-compliant security functions. The PC21100 includes a CompactRISC embedded RISC core for hidden execution of security code, flash memory-based secured information storage, SecureRun, a performance accelerator that supports cryptographic algorithms (SHA-1 and RSA), and a true RNG. In addition, the PC21100 integrates a variety of system functions, enabling efficient implementation of a highly secure trustworthy system.

The PC21100 provides desktop and mobile PC platforms with:

System integrity checks:
Ensures that no unauthorized changes have been made to the hardware or software

Authentication:
Provides assurances that the source of the data is valid and as expected

Data integrity checks:
Provides assurances that received data is exactly as sent

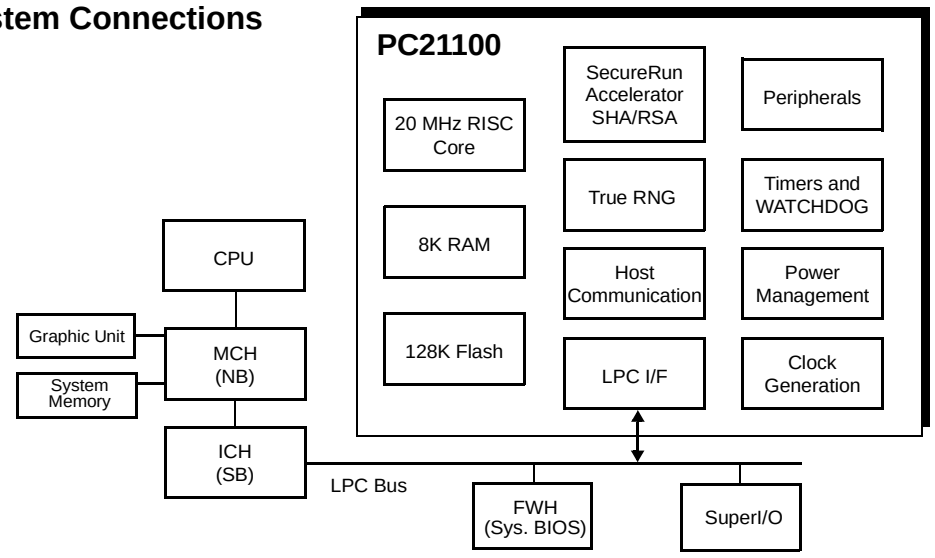
Secure storage:
Protects sensitive and confidential data, such as credit card numbers and passwords

Trustworthiness:
Allows the user to trust authorized third parties, while proving that the user's PC is trustworthy and maintaining privacy

Outstanding Features

- TCPA 1.1 compliant
- PC01 and ACPI 2.0 compliant
- LPC based Host interface (based on Intel's LPC Interface Specification Revision 1.0) with optimized communication modes and Mobile System Support
  - Fast BIOS hash mode
  - BIOS mode
  - OS mode with low communication overhead
- 16-bit RISC core, with 2 Mbyte address space, and 20 MHz execution cycle
- Integrated 128 Kbyte secure flash memory and 8 Kbyte of RAM
- Embedded TCPA 1.1 firmware
- Full Host Software Stack implementation
- Storage for more than thirty 2048-bit RSA keys
- SHA-1 and RSA cryptographic accelerator
- Platform attachment indicator
- Secure GPIO port
- Low power consumption
- Extremely low idle current
- Hardware True-Random Number Generator
- 28-pin PLCC and 36-pin LLP packages

PC21100 System Connections



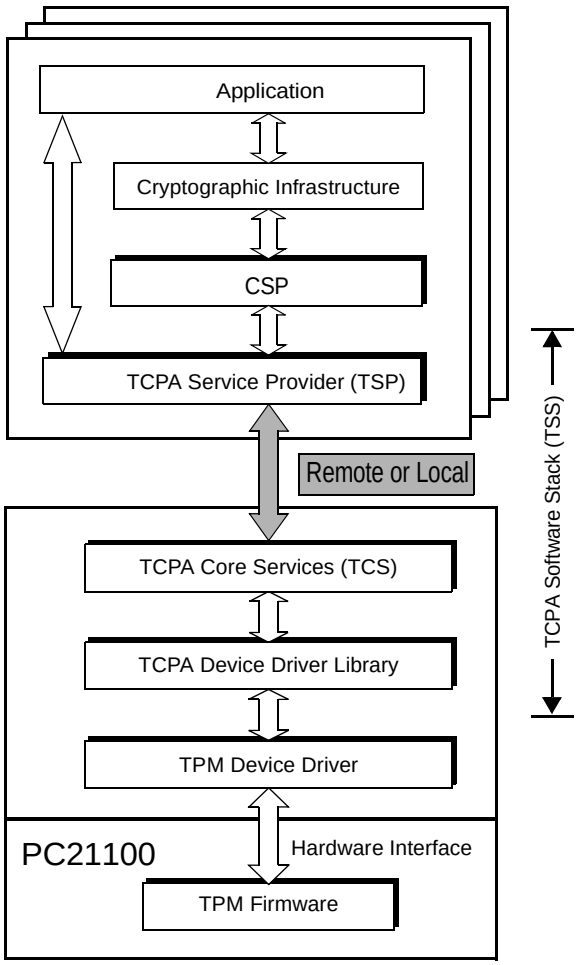
National Semiconductor is a registered trademark of National Semiconductor Corporation. SafeKeeper is a trademark of National Semiconductor Corporation.
All other brand or product names are trademarks or registered trademarks of their respective holders.

© 2002 National Semiconductor Corporation

Software Package

- TPM Firmware, TCPA V1.1 compliant
  - — Integrity Metrics (used for BIOS and OS authentication)
  - — Random Number Generation service
  - — Cryptographic Keys generation
  - — Secure digital sign/verify
  - — Secure storage
  - — Hidden execution using intenal memories (Flash and RAM)
- Full TCPA Software Stack implementation
  - — Device drivers (BIOS & OS)
  - — TDDL layer
  - — TSS (TCS and TSP)
- PKCS#11 and CAPI Crypto-Service Providers (CSP)

Software Block Diagram



LIFE SUPPORT POLICY

NATIONAL'S PRODUCTS ARE NOT AUTHORIZED FOR USE AS CRITICAL COMPONENTS IN LIFE SUPPORT DEVICES OR SYSTEMS WITHOUT THE EXPRESS WRITTEN APPROVAL OF THE PRESIDENT AND GENERAL CUNSEL OF NATIONAL SEMICONDUCTOR CORPORATION. As used herein:

1. Life support devices or systems are devices or systems which, (a) are intended for surgical implant into the body, or (b) support or sustain life, and whose failure to perform, when properly used in accordance with instructions for use provided in the labeling, can be reasonably expected to result in a significant injury to the user.
2. A critical component is any component of a life support device or system whose failure to perform can be reasonably expected to cause the failure of the life support device or system, or to affect its safety or effectiveness.

National Semiconductor Corporation Americas
Email: new.feedback@nsc.com

National Semiconductor Europe
Fax: +49 (0) 180-530 85 86
Email: europe.support@nsc.com
Deutsch Tel: +49 (0) 69 9508 6208
English Tel: +44 (0) 870 24 0 2171
Français Tel: +33 (0) 1 41 91 87 90

National Semiconductor Asia Pacific Customer Response Group
Tel: 65-2544466
Fax: 65-2504466
Email: ap.support@nsc.com

National Semiconductor Japan Ltd.
Tel: 81-3-5639-7560
Fax: 81-3-5639-7507
Email: nsj.crc@jksmtp.nsc.com

www.national.com

National does not assume any responsibility for use of any circuitry described, no circuit patent licenses are implied and National reserves the right at any time without notice to change said circuitry and specifications.