

SafeKeeper™ PC21100

Your Security Partner

The Problem

So much of our lives depend upon computers, it's alarming how vulnerable they are to security breaches and criminal mischief. Once PCs were totally isolated or, perhaps, only connected to a single network. Today's PCs are connected to the Internet and called upon to conduct e-commerce and tasks that were unheard of only a few years ago. The need for trust, security and privacy on the PC platform has become paramount for applications like e-business to truly flourish.

Trusted Computing focuses on building levels of trust into the computing platform, whether it's a PC, PDA or other device. Instead of the current strategy of continually adding and updating outside barriers to viruses and intrusions, Trusted Computing starts with a first level of trust integrated into both the hardware and pre-operating system environments. Once these environments are secured, following portions of the computing platform can be addressed to provide additional levels of trust.

The Consortium

In 1999, five companies – Compaq, HP, IBM, Intel and Microsoft – formed the Trusted Computing Platform Alliance as the first step in defining a standard for advancing and implementing the concepts of Trusted Computing. Today TCPA has over 160 members, including National Semiconductor who leads the way with innovative semiconductor solutions. All these companies are joined together in an open alliance to develop the necessary technology and cooperation to make Trusted Computing a reality.



SafeKeeper is a hardware element to enable trusted computing. It easily adds cryptographic and security functions to the PC.

The Concept

TCPA target is to provide an industry standard specification establishing an ubiquitous and standardized means to address trustworthiness of computing platforms.

A TCPA system uses SafeKeeper™, Trusted Platform Module (TPM), as a hardware block to verify that the PC is secure.

This enables the use of the high performance native computing power of the PC and its common software structure to securely perform any trusted operation which, in a normal environment, would have required much more complex and expensive add-ons.

In other words, by ensuring that it is trusted, TCPA technology provides base level security benefits to the PC at an appealing cost.

Advanced I/O

Overview

Advanced I/O products bring innovative solutions to functionality, reliability and security in single-chip, I/O peripheral devices - supporting your PC and IA leadership. To learn more about National Semiconductor's Advanced I/O products, visit:

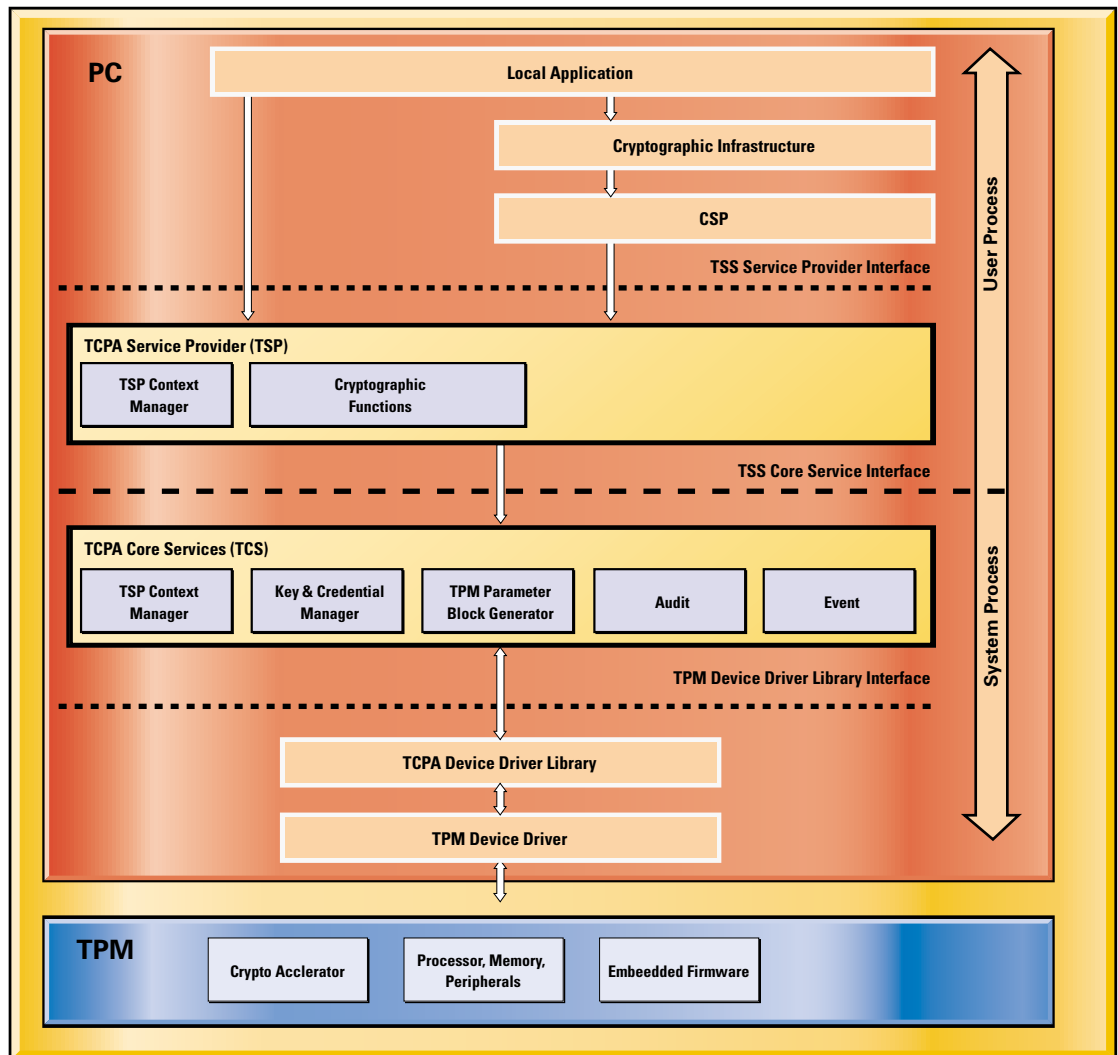
national.com/advancedio

The Hardware Solution

National Semiconductor provides the fundamental element of the Trusted Computing solution, a piece of security silicon named PC21100 or SafeKeeper. This device is not accessible by the host CPU except through formalized methods, secured by industry standard cryptographic techniques. The SafeKeeper chip acts as a “root of trust” – a dependable device that can report the security

status of the rest of the system. Since it is hardware-based, SafeKeeper is not vulnerable to attacks like conventional software-only solutions.

The SafeKeeper device that contains TPM functionality is fully TCGA 1.1 compliant and offers system designers all the advantages of Trusted Computing as defined by the TCGA.



Trust and Security

National Semiconductor's SafeKeeper provides a level of trustworthiness impossible to achieve before. The hardware device is much more resistant to attacks than possible with software solutions alone. The much-touted direction of leading software companies to increase the trust level of their offerings will be difficult without the support of a hardware element like SafeKeeper.

The SafeKeeper PC21100 is truly the basis for a thriving e-commerce infrastructure in the future. For even if the platform is broken or hacked, it is essential that all others who transact with that platform know its security has been compromised. In other words, the security may be damaged, but SafeKeeper maintains the trust as unbroken.

Trust National to Provide a Secure System Solution!

- Full stack implementation, from host standard crypto-libraries (CAPI, PKCS#11) down to the hardware device
- High performance, low power consumption
- Complete solution for easy system integration
- Backed by National's complete system experience, and superior device reliability
- Fast time-to-market

Overview

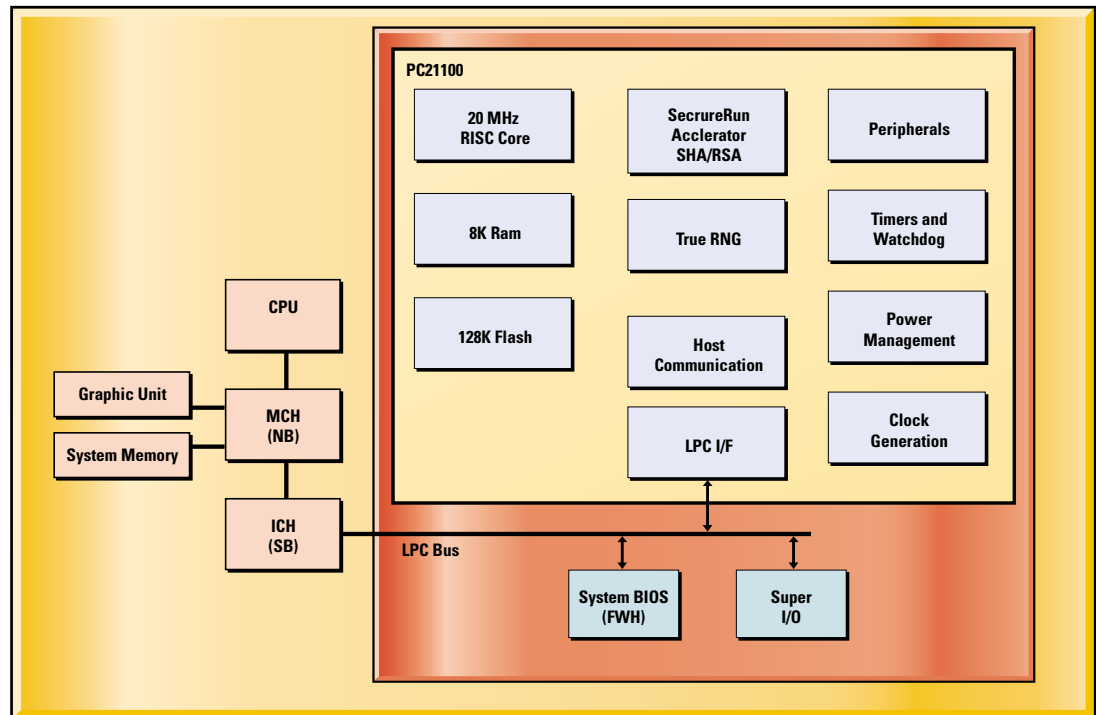
The SafeKeeper PC21100 is a member of National Semiconductor's TrustedI/O family and provides TCPA-compliant security functions. The PC21100 includes embedded RISC technology, flash memory-based secured

information storage, SecureRun, a performance accelerator that supports the 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 SafeKeeper PC21100 generates and stores RSA keys quickly and without any host intervention, maximizing the security of the platform. The interface architecture has been optimized to perform hashes without slowing system throughput. National's PC expertise comes to the forefront to provide the best possible solution.

SafeKeeper PC21100 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 embedded core technology
- Integrated 128 Kbyte secure flash memory and 8 Kb of RAM
- SHA-1 and RSA cryptographic accelerator
 - Storage for more than thirty 2048-bit RSA keys
- Secure GPIO port with wake-up events
- Low power consumption < 20 mA
 - Extremely low idle current < 10 μ A
- Hardware true-random number generator
- 28-pin PLCC and 36-pin LLP packages



The Benefits of SafeKeeper

National's SafeKeeper 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

- **Privacy:**

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 itself trustworthy

The Pay-Off

- Boost confidence in Internet-based commerce
- Increase the trustworthiness of every PC transaction
- Provide ubiquitous security solutions across a wide number of PC platforms
- Allow future extension to servers, mobile phones and Personal Digital Assistants (PDA)

National Semiconductor

2900 Semiconductor Drive
PO Box 58090
Santa Clara, CA 95052
1 408 721 5000

Visit our web site at:

www.national.com

For more information,

send email to:

new.feedback@nsc.com