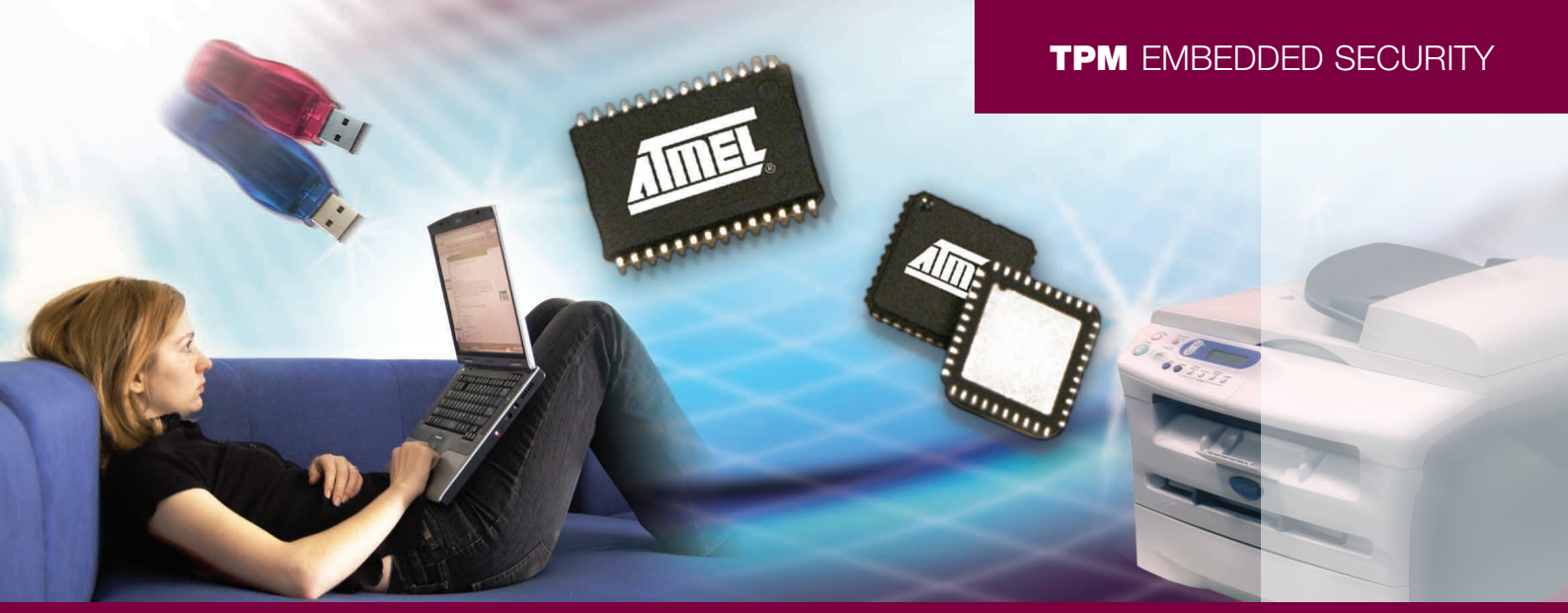


AT97SC3203
THE ATMEL TRUSTED PLATFORM MODULE

The Atmel® Trusted Platform Module (TPM) provides high levels of hardware security and interoperability in a single-chip, turnkey solution for next-generation PC and embedded computing environments.

Features:

- Complete Turnkey Design in a Single Chip (including integrated, protected nonvolatile storage for Cryptographic Keys, Secrets and Authorization information)
- Full Trusted Computing Group (TCG) V1.2 Specification Compatibility
- Hardware SHA-1 Accelerator; 50 µsec per 64-byte Block
- True Hardware Random Number Generator
- 33 MHz LPC Interface for Easy PC Integration
- 2-Wire SMBus™ Interface for Non-PC and Embedded Computing Systems
- BIOS Drivers (MAD and MPD) Available for Integration
- Proven Compatibility with Windows Vista™ Operating System
- Windows Drivers Available (WHQL certified) for Legacy Windows Operating Systems
- Linux® Drivers Available
- Common Criteria EAL 4+ Evaluation in Progress
- 3.3V Operation; Available in TSSOP and QFN Packages

Applications:

- PCs
- PDAs/Pocket PCs
- Servers
- Gaming
- Industrial Control
- Flash Drives
- Printers and Multifunction Office Equipment

The TCG Concept

The TPM, a secure microcontroller, provides functionality for performing strong authentication, key generation, secure storage and other mechanisms for verifying and reporting system integrity. Developed by industry leaders in the computing and security fields, the TCG framework enhances trust in computing systems by basing the foundation, or root of trust, on the TPM hardware security module, and extending that trust to include all system and network communication. Atmel was the first company to provide a TPM in volume production and remains a leader in hardware-based security products supporting the TCG initiative.

Optimized to support the TCG architecture, the Atmel TPM offers a standards-based approach to system security. The TCG standard defines a framework for usage of strong encryption and signature algorithms coupled with flexible authentication mechanisms. This framework supports a wide range of applications, including email, file encryption and network authentication.

The Atmel TPM

Hardware

The basis for the Atmel TPM is our nonvolatile memory technology, our AVR® microcontroller, and our expertise in silicon security technology. To these core blocks, we've added a well-proven 2048-bit asymmetric RSA® coprocessor and a true random number generator accessed through either an LPC or SMBus interface. Additional security measures, such as active shielding and a variety of tamper-detection and response circuits, are also featured. Atmel TPMs are available in 28-lead TSSOP and space-saving 28-lead QFN packages.

Firmware

Atmel TPM firmware is written to the high standards necessary to protect security systems that must reside in environments that are expected to be subject to attack. Atmel's experience in real-world security hardware and embedded firmware has driven innovative solutions that provide detection and protection when attacks are launched. A major difference between competing TPM solutions is the behavior of the chip when nonstandard conditions (rogue software, environmental, timing, or other attacks) are directed against the security module with the intent of gaining access to protected data, keys or operations. Atmel incorporates proven protections against many known attack conditions and robustly tests the TPM firmware to assure consistent responses under nonstandard conditions. These tests go far beyond compliance testing to assure proper implementation of the TCG specification.

Software Support

Atmel provides supporting software for TPMs incorporated into PC and embedded systems. BIOS drivers are available for inclusion into system BIOS code. Hardware drivers are also available for both Windows and Linux operating systems.

System software support is extended by middleware and application software written by Atmel partners. TPM Software Stack (TSS) and sophisticated application programs are available through licensing agreements.

Manufacturing TPM-enabled systems requires initialization and verification utility software, which is provided by Atmel to TPM customers to assure correct and consistent system configuration.

Embedded Systems

The SMBus protocol is available exclusively on Atmel TPMs and will support the entire TCG TPM command set over a 2-wire bus protocol. TPM development systems based on the Atmel STK500 and STK501 AVR Studio are available, together with code samples and supporting documentation, to enable easy integration and development of TPM applications in systems that do not contain the LPC bus interface.

Atmel TPMs

Atmel developed the world's first trusted platform module IC in 1996 and has since developed a variety of methods to prevent unauthorized access to the contents of secure ICs and smart card ICs, including metal shield layers above the active circuitry, encrypted internal busses, high-security test procedures, and defenses against timing and power supply attacks.

Atmel's v1.1b TPM has attained EAL3+ security certification on the Common Criteria worldwide security standard. As part of the certification process, Atmel TPMs undergo rigurous testing at a government certified laboratory, which is then audited and verified by a government agency, such as the National Institute of Standards and Technology (NIST).

TPMs marketed by Atmel conform to the 1.2 standard. In addition to TCG-compliance, Atmel TPMs incorporate additional features that enhance the security and capability of systems in which they are used.

Secure Password Checking

The use of a key in a TCG system may require the operator to enter a password or other authorization information as a final check before the operation is performed. If a system is stolen, the thief may try all the words in the dictionary or all the names in a list to find the right password. The Atmel TPM incorporates an owner-programmable method to detect such attacks.

Public Key Operations

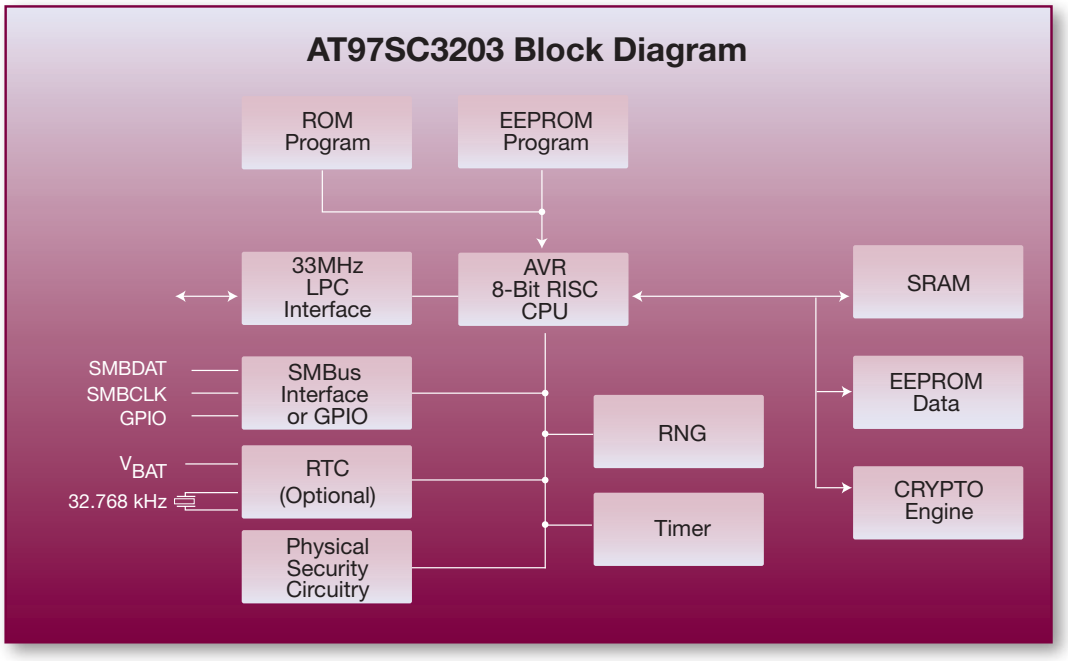
The TCG specification does not require the TPM to perform public key operations, assuming that the main system processor can do them faster and with the understanding that, being public, they do not require security. However, not all TPM applications are in personal computers. Some processors are embedded inside products (like phones and PDAs) that may not have the computing power to compute public key operations such as signature verification, which requires extra software. Since Atmel TPMs can compute public key operations internally, they simplify the addition of TPM-style security to embedded systems.

Theft Prevention

Legacy systems that wish to add TPM functionality are likely to do so using daughter cards that are inserted onto the motherboard. However, a thief could steal a user's identity by simply stealing the daughter card. Atmel TPMs solve this problem by providing various options that prevent use of the daughter card if it is disconnected from the system in which it was installed.

Timing Attack Defense

Some people try to exploit potential weaknesses in the TPM by using commonly available timing attack software downloaded from the Internet. Atmel TPMs have circuitry that can detect and foil such attacks by incorporating special circuitry and procedures to ensure that absolutely no useful information can be obtained.



Headquarters

Atmel Corporation
2325 Orchard Parkway
San Jose, CA 95131, ***USA***
Tel: 1(408) 441-0311
Fax: 1(408) 487-2600

International

Atmel Asia
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimshatsui
East Kowloon, ***Hong Kong***
Tel: (852) 2721-9778
Fax: (852) 2722-1369

Atmel Europe
Le Krebs 8, Rue Jean-Pierre
Timbaud BP 309
78054 Saint-Quentin-en-
Yvelines Cedex, ***France***
Tel: (33) 1-30-60-70-00
Fax: (33) 1-30-60-71-11

Atmel Japan
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033,
Japan
Tel: (81) 3-3523-3551
Fax: (81) 3-3523-7581
Product Contact

Literature Requests
www.atmel.com/literature

Web Site
www.atmel.com

REV.: 5128B-TPM-4/07/1K