Product Brief
February 2006
Revision 1.0

PC8392T
SafeKeeper™ Notebook TrustedI/O with TPM 1.1b

General Description

The PC8392T, a member of the Winbond TrustedI/O family, is targeted for a wide range of notebook applications. PC8392T integration allows for a reduced system board size, reduced system current consumption, and saves on total system cost.

This device includes a SafeKeeper™ Trusted Platform Module (TPM), legacy SuperI/O functions, commonly used functions such as GPIO, and ACPI-compliant Power Management support.

The TPM provides a solution for PC security, based on the TCG standard. The complete security solution includes hardware, software, and firmware.

The Winbond PC8392T and PC87374T use the same TPM, enabling a single TCG-based security solution across notebook and desktop systems.

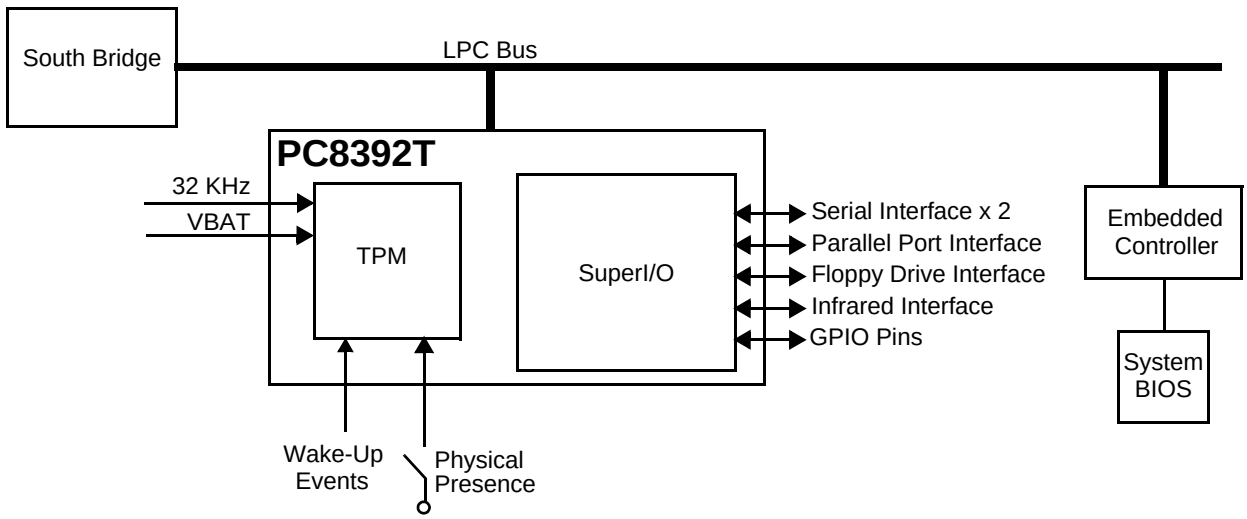
The PC8392T is pin and software compatible with the PC87392. This provides drop-in interchangeability using only a single motherboard and BIOS.

The PC8392T supports both I/O and memory mapping of module registers and enables building legacy-free systems.

Outstanding Features

- TCG 1.1b based Trusted Platform Module (TPM)
  - Non-volatile secure storage
  - Hardware and software protection schemes
  - Pin compatible to integrated TPM 1.2 device
- Legacy modules: IEEE 1284-compliant Parallel Port, Floppy Disk Controller (FDC), two Serial Ports and Fast InfraRed Port
- 28 GPIO pins (14 standard and 14 with IRQ support)
- Protection features, including GPIO lock and pin configuration lock
- I/O-mapped or memory-mapped registers
- Pin and software compatible with the PC87392
- 100-pin LQFP package

System Block Diagram



Features

SafeKeeper Trusted Platform Module (TPM)

- TCG 1.1b compliant
- LPC-based Host interface with optimized communication modes:
  - Fast BIOS hash mode
  - Notebook system support
  - Command/Data/Status standard (proven) interface
  - Device Driver for Windows 2000 and Windows XP
- 16-bit RISC embedded core technology
- Memory
  - On-chip, Non-Volatile memory for secure storage
  - On-chip data RAM
- SHA-1 and RSA cryptographic accelerator
- Hardware True-Random Number Generator
- Secure (Owner Authorized) General-Purpose I/O (GPIO)
  - Internal processor controlled
  - Three GPIO pins, one used for Physical Presence
  - I/O pins individually configured as input or output
  - Configurable internal pull-up resistors
- Performance-tuned low-power consumption
  - Power Management Controller (PMC) power modes, switched by software or hardware
- Hardware and software protection schemes

Bus Interface

- LPC System Interface
  - Based on Intel's *LPC Interface Specification Revision 1.1, August 2002*
  - I/O, Memory and 8-bit Firmware Memory read and write cycles, Firmware Memory writes may insert wait cycles
  - Up to four 8-bit DMA channels
  - $\overline{\text{LPCPD}}$ and $\overline{\text{CLKRUN}}$ support
  - Implements PCI mobile design guide recommendation (*PCI Mobile Design Guide 1.1, Dec. 18, 1998)*
- Configuration Control
  - Compliant with *PC2001 Specification Revision 1.0, 1999-2000*
  - PnP Configuration Register structure
  - Base Address strap ($\overline{\text{BADDR}}$) to setup the address of the Index-Data register pair (defaults to 2Eh/2Fh)
  - TPM Index-Data register pair Base Address set by the TPM or via SuperI/O Configuration registers
  - Flexible resource allocation for all logical devices
    - ❏ Relocatable base address
    - ❏ Fifteen IRQ routing options
    - ❏ Four optional 8-bit DMA channels
  - Supports register memory and I/O mapping

Power Management

- Supports *ACPI Specification Revision 3.0, September 2, 2004*

General-Purpose Modules

- 28 General-Purpose I/O (GPIO) pins
  - 8 GPIO pins powered by V_{SB}
  - 20 GPIO pins powered by V_{DD}
- Each pin individually configured as input or output (except two pins which are only outputs)
- Programmable features for each output pin:
  - Drive type (open-drain, push-pull or TRI-STATE®)
  - TRI-STATE on detection of falling V_{DD} for V_{SB}-powered pins driving V_{DD}-supplied devices
- Programmable option for internal pull-up resistor on each input pin
- Lock option for the configuration and data of each output pin
- 14 GPIO pins generate IRQ; each GPIO has separate:
  - Enable control of event status routing to IRQ
  - Polarity and edge/level selection
  - Input debouncing

Legacy Modules

- Floppy Disk Controller (FDC)
  - Software compatible with the PC8477 (the PC8477 contains a superset of the FDC functions in the μDP8473, NEC μPD765A/B and N82077 devices)
  - Error-free handling of data overrun and underrun
  - Programmable write protect
  - Supports FM and MFM modes
  - Supports Enhanced mode command for three-mode Floppy Disk Drive (FDD)
  - Perpendicular recording drive support for 2.88 Mbytes
  - Burst (16-byte data FIFO) and Non-Burst modes
  - Full support for IBM Tape Drive Register (TDR) implementation of AT and PS/2 drive types
  - High-performance digital separator
  - Supports up to four floppy disk drives
  - Supports fast tape drives (2 Mbps) and standard tape drives (1 Mbps, 500 Kbps and 250 Kbps)
- IEEE 1284-compliant Parallel Port
  - ECP, including Level 2 (14 mA sink and source output buffers)
  - Software or hardware control
  - Enhanced Parallel Port (EPP) compatible with EPP 1.7 and EPP 1.9
  - Supports EPP as mode 4 of the Extended Control Register (ECR)
  - Selection of internal pull-up or pull-down resistor for Paper End (PE) pin

Features (Continued)

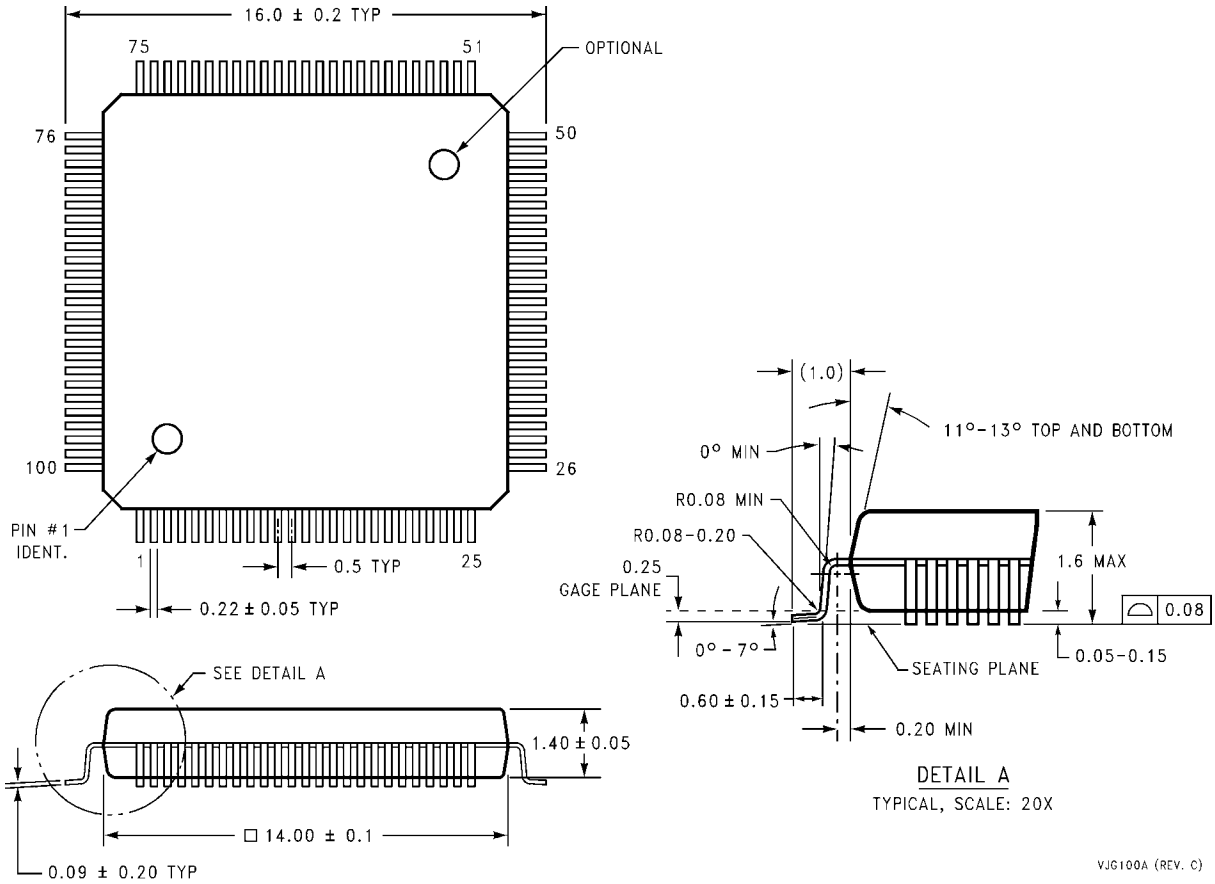
— Supports a demand DMA mode mechanism and a DMA fairness mechanism for improved bus utilizationProtection circuit that prevents damage to the parallel port when a printer connected to it is powered-up or is operated at high voltages (in both cases, even if the PC8392T is in power-down state)

- Serial Port 1 (SP1)
  - — Software compatible with the 16550A and the 16450
  - — Supports shadow register for write-only bit monitoring
  - — Data rates up to 1.5 Mbaud
- Serial Port 2 with Fast Infrared (SP2 with FIR)
  - — Software compatible with the 16550A and the 16450
  - — Supports shadow register for write-only bit monitoring
  - — Data rates up to 1.5 Mbaud
  - — FIR IrDA 1.1 compliant
  - — HP-SIR
  - — ASK-IR option of SHARP-IR
  - — DASK-IR option of SHARP-IR
  - — Consumer Remote Control supports RC-5, RC-6, NEC, RCA and RECS 80
  - — DMA support for one or two channels

Clocking, Supply, and Package Information

- Clocks
  - — LPC (PCI) clock input, 0 to 33 MHz
  - — 14.318 MHz or 48 MHz clock input
  - — On-chip Low-Frequency Clock Generator:
    - ❑ Generates 32.768 KHz internal clock
  - — On-chip SuperI/O Clock Generator:
    - ❑ Generates 48 MHz
    - ❑ Based on the 14.31818 MHz clock input
    - ❑ V_{DD} powered
  - — On-Chip TPM Clock Generator:
    - ❑ Calibration using 32.768 KHz clock reference.
    - ❑ Detection of reference clock corruption
- Protection
  - — All pins are 5V tolerant (except the LPC bus pins)
  - — All pins are back-drive protected (except the LPC bus pins)
  - — High ESD protection of all the device pins
  - — Pin multiplexing selection lock
  - — Configuration register lock
- Testability
  - — XOR-Tree structure
    - ❑ Includes all the device pins (except supply and NC pins)
    - ❑ Selected at V_{DD} power-up by strap input ($\overline{TEST}$)
  - — TRI-STATE® device pins, selected at V_{DD} power-up by strap input ($\overline{TRIS}$)
- Power Supply
  - — 3.3V supply operation
  - — Separate pin pairs for main (V_{DD}) and standby (V_{SB}) power supplies
  - — Separate pins for core voltage filtering (V_{CORF}, V_{CORF2})
  - — Optional battery (V_{BAT}), for forward compatibility
  - — Low standby power consumption
  - — Very low power consumption from backup battery (less than 1 μA)
- Package
  - — Regular 100-pin LQFP
  - — Lead-free 100-pin LQFP

Physical Dimensions (All dimensions are in millimeters)



Thin Quad Flatpack (LQFP), JEDEC

Important Notice

Winbond products are not designed, intended, authorized or warranted for use as components in systems or equipment intended for surgical implantation, atomic energy control instruments, airplane or spaceship instruments, transportation instruments, traffic signal instruments, combustion control instruments, or for other applications intended to support or sustain life. Furthermore, Winbond products are not intended for applications wherein failure of Winbond products could result or lead to a situation wherein personal injury, death or severe property or environmental damage could occur.

Winbond customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify Winbond for any damages resulting from such improper use or sales.

Headquarters
No. 4, Creation Rd. III,
Science-Based Industrial Park,
Hsinchu, Taiwan
TEL: 886-3-5770066
FAX: 886-3-5665577
http://www.winbond.com.tw/

Taipei Office
9F, No.480, Rueiguang Rd.,
Neihu District, Taipei, 114,
Taiwan, R.O.C.
TEL: 886-2-8177-7168
FAX: 886-2-8751-3579

Winbond Electronics Corporation America
2727 North First Street, San Jose,
CA 95134, U.S.A.
TEL: 1-408-9436666
FAX: 1-408-5441798

Winbond Electronics Corporation Japan
7F Daini-ueno BLDG, 3-7-18
Shinyokohama Kohoku-ku,
Yokohama, 222-0033
TEL: 81-45-4781881
FAX: 81-45-4781800

Winbond Electronics (Shanghai) Ltd.
27F, 2299 Yan An W. Rd. Shanghai,
200336 China
TEL: 86-21-62365999
FAX: 86-21-62365998

Winbond Electronics (H.K.) Ltd.
Unit 9-15, 22F, Millennium City,
No. 378 Kwun Tong Rd.,
Kowloon, Hong Kong
TEL: 852-27513100
FAX: 852-27552064

For Advanced PC Product Line information contact: APC.Support@winbond.com