



PCN / EOL Notification

Product Change Notification Number: CC082402

Date*: July 14, 2008

Title: AT97SC3203 v1.2 TPM Version Change from 1.2.D.05 to 1.2.11.01

Product Identification:

Current Part Number	Replacement Part Number
AT97SC3203-X5A30	AT97SC3203-X9A10
AT97SC3203-X5M30	AT97SC3203-X9M10
AT97SC3203-X5A30-1	AT97SC3203-X9A10-1
AT97SC3203-X5M30-1	AT97SC3203-X9M10-1

Reason for Change:

- | | | |
|---|--|------------------------------------|
| <input checked="" type="checkbox"/> Design | <input type="checkbox"/> Processing | <input type="checkbox"/> Logistics |
| <input type="checkbox"/> Manufacturing Location | <input type="checkbox"/> Quality/Reliability | <input type="checkbox"/> Material |
| <input checked="" type="checkbox"/> Firmware | | |

Change Description:

As part of the 1.2.D.05 version, a checksum routine was added to the Clear operation as an aggressive response to out-of-specification clock conditions present during manufacturing initialization and testing at CMs. This undesirable clock condition was causing unintended writes in the TPM EEPROM. The checksum routine (CRC) internally verifies permanent EEPROM data and executable code in the TPM, and is automatically run when the Clear operation is executed. The CRC routine will return an error code if any change is detected in permanent data or TPM executable firmware. However, the CRC routine in 1.2.D.05 utilizes a Byte-read routine to read executable code and permanent data residing in the EEPROM. The Byte-read routine has a shorter read access time than the more frequently used Load from Program Memory (LPM) read operation. This shorter access time causes a subset of devices to be susceptible to misreading good data in the TPM EEPROM resulting in Clear CRC rejects (reported as a 001C Self Test failure). These Clear rejects represent an over-rejection rate of what would otherwise be functionally good TPMs because under all other conditions those locations would properly be read with the LPM mechanism.

Changes to version AT97SC3203-X5A30 containing firmware version 1.2.D.05 have been made to improve execution of TCG commands by the TPM and add protections against out of specification conditions known to exist in a manufacturing environment, with the goal to improve manufacturability during the TPM initialization process. A 2-cycle digital delay has been added to the Byte-read operation via a three layer metal change in revision AT97SC3203-X9A10 to address high speed read issues. Additionally, hardware changes have been made to include 2 fuses to block any unintended EEPROM write operations which may occur as a direct result of out-of-specification conditions existing during system manufacturing. These changes will improve the execution of TCG commands, provide greater protection against out of spec conditions and significantly decrease an over-rejection during the Clear operation of 1.2.D.05 revision devices. These modifications have been added to revision AT97SC3203-X9A10 (FW 1.2.11.01).

1. Mask changes include 1st Metal (ROM), 1st Via, 2nd Metal, 2nd Via, 3rd Metal.
2. Hardware changes implement the following functional changes
 - a. A 2-cycle digital delay has been added to the Byte-read operation
 - b. Function of 2 fuses altered to block EEPROM write operation
 - c. Additional EEPROM Write lock hardware control signal (WrtLck) added
 - d. Hardware changes to enable Read of fuses when chip is not asleep and not performing EEPROM Write operation
3. Firmware changes in ROM and EEPROM image:
 - a. Key heap “garbage collection” routines implemented to ensure residual data is not left in the Key Slots in the event of a power glitch received during key flush operations.
 - i. Key heap data is verified as valid whenever new key space is allocated. Any invalid information is deleted to free key heap space.
 - b. TPM flag and counter initialization actions (Writes to EEPROM) moved from TPM boot routine into TPM_Startup command firmware
 - c. EEPROM Write operations are now blocked by fuses when shipped from Atmel factory to protect against unintentional EEPROM writes triggered by out of spec Clock conditions present during system manufacturing (ICT test)
 - i. First TPM_Startup command unlocks fuse #1
 - ii. Next valid TCG command (any command) unlocks fuse #2
 - iii. Fuses remain unlocked for TPM lifetime
 - d. State flags (EEPROM Write permission) added to track command execution before unlocking EEPROM Write capability
 - i. Each stage verifies successful execution of all previous stages
 - ii. Final stage verifies proper state of all flags before unlocking EEPROM Write capability
 - iii. EEPROM Write execution performed as normal, then all flags reset to disable EEPROM Write capability before returning from subroutine
 - e. Execution of the EEPROM Write state machine modified to verify (Read and compare) that data was correctly written to the intended memory address. If the verification fails, the Write operation is repeated up to 10 times. If failure occurs on the 10th iteration, the TPM will return a failure code TPM_Fail.
 - i. EEPROM Write driver timeout counter added. If EE_Write routine does not return successfully within the time allowed, the subroutine will exit and return an error code TPM_Fail.
 - ii. Every call to an EEPROM Write subroutine will compare the new data to the existing data at the target address. If the existing data is identical to the new data, no Write operation will be executed. This will improve endurance performance.
 - f. Multiple bug fixes for NV_defineSpace, NV_WriteValueAuth, NV_ReadValueAuth

Identification Method to Distinguish Change:

The proposed new part numbers are: AT97SC3203-X9A10 & AT97SC3203-X9M10

New revision devices will be identified by package marking. Changes in **Red**:

Previous Device Marking

Atmel AT97SC3203 1.2.D.05 lotnumber datecode X PH

New Device Marking

Atmel AT97SC3203 1.2.11.01 lotnumber datecode X PH
--

Qualification Data:	<input type="checkbox"/> available	<input checked="" type="checkbox"/> will be available in July 18, 2008	<input type="checkbox"/> not applicable
Samples:	<input checked="" type="checkbox"/> available	<input type="checkbox"/> will be available in WW____	<input type="checkbox"/> not applicable

Quantifiable Impact on Quality & Reliability:

None

Forecasted Availability Date: July 7, 2008 (available now)**Last Time Buy Date:** December 31, 2008**Last Ship Date:** July 7, 2009

* All orders placed after the notification date are **non-cancellable** and **non-returnable (NCNR)**.

Atmel Contact: pcnadm@atmel.com

Atmel will deem this change accepted unless specific conditions of acceptance are provided in writing within 30 days from the date of this notice. All correspondence must be sent to the Atmel Contact e-mail address listed above.

Information provided herein is in connection with Atmel products and this information is provided "AS IS". Atmel assumes no responsibility for any errors that may appear in this document. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Atmel's Terms and Conditions of Sale for such products, Atmel assumes no liability whatsoever, and Atmel disclaims any express or implied warranty, including liability or warranties relating to fitness for a particular purpose, merchantability, or non-infringement of any patent, copyright or other intellectual property right. Atmel products are not intended for use in a product or system intended to support or sustain life which, if it fails, can be reasonably expected to result in significant personal injury. Atmel may make changes to specifications and product descriptions at any time, without notice.
