

Atmel Trusted Platform Module Part Number Selection Guide

1. Ordering Information

1.1 AT97SC3205 SPI TPM

Table 1-1. AT97SC3205 SPI TPM TSSOP/QFN Ordering Information

| Atmel Ordering Code | Package | Description | Operation Range | |
|---------------------|--------------------------------|--|--|----------------------------|
| AT97SC3205-X3A12-10 | 28X1 (28-pin 4.4mm TSSOP) | Lead-free, RoHS v1.2 rev 116 Standard Mode SPI TPM with Real Mode EK, 2066B User NV | Commercial (0°C to 70°C) | |
| AT97SC3205-U3A12-10 | | | Industrial (-40°C to 85°C) | |
| AT97SC3205-X3A12-20 | | Lead-free, RoHS v1.2 rev 116 Standard Mode SPI TPM with Signed EK (X.509 Certificate), 2066B User NV | Commercial (0°C to 70°C) | |
| AT97SC3205-U3A12-20 | | | Industrial (-40°C to 85°C) | |
| AT97SC3205-X3A15-10 | | 32M3 (32-pin Very Thin QFN) | Lead-free, RoHS v1.2 rev 116 FIPS/Flex Mode SPI TPM with Real Mode EK, 2066 User NV | Commercial (0°C to 70°C) |
| AT97SC3205-U3A15-10 | | | | Industrial (-40°C to 85°C) |
| AT97SC3205-X3A15-20 | | | Lead-free, RoHS v1.2 rev 116 FIPS/Flex Mode SPI TPM with Signed EK (X.509 Certificate), 2066 User NV | Commercial (0°C to 70°C) |
| AT97SC3205-U3A15-20 | | | | Industrial (-40°C to 85°C) |
| AT97SC3205-G3M42-00 | 32M3 (32-pin Very Thin QFN) | Lead-free, RoHS v1.2 rev 116 Standard Mode SPI TPM with Compliance EK | Commercial (0°C to 70°C) | |
| AT97SC3205-H3M42-00 | | | Industrial (-40°C to 85°C) | |
| AT97SC3205-G3M45-00 | | Lead-free, RoHS v1.2 rev 116 FIPS/Flex Mode SPI TPM with Compliance EK | Commercial (0°C to 70°C) | |
| AT97SC3205-H3M45-00 | | | Industrial (-40°C to 85°C) | |

1.2 AT97SC3205T I²C TPM

Table 1-2. AT97SC3205T I²C TPM TSSOP/QFN Ordering Information

| Atmel Ordering Code | Package | Description | Operation Range | |
|----------------------|------------------------------|--|---|----------------------------|
| AT97SC3205T-X3A14-10 | 28X1 (28-pin 4.4mm TSSOP) | Lead-free, RoHS v1.2 rev 116 Standard Mode I ² C TPM with Real Mode EK, 2066 User NV | Commercial (0°C to 70°C) | |
| AT97SC3205T-U3A14-10 | | | Industrial (-40°C to 85°C) | |
| AT97SC3205T-X3A14-20 | | Lead-free, RoHS v1.2 rev 116 Standard Mode I ² C TPM with Signed EK (X.509 Certificate), 2066 User NV | Commercial (0°C to 70°C) | |
| AT97SC3205T-U3A14-20 | | | Industrial (-40°C to 85°C) | |
| AT97SC3205T-X3A16-10 | | 32M3 (32-pin Very Thin QFN) | Lead-free, RoHS v1.2 rev 116 FIPS/Flex Mode I ² C TPM with Real Mode EK, 2066 User NV | Commercial (0°C to 70°C) |
| AT97SC3205T-U3A16-10 | | | | Industrial (-40°C to 85°C) |
| AT97SC3205T-X3A16-20 | | | Lead-free, RoHS v1.2 rev 116 FIPS/Flex Mode I ² C TPM with Signed EK (X.509 Certificate), 2066 User NV | Commercial (0°C to 70°C) |
| AT97SC3205T-U3A16-20 | | | | Industrial (-40°C to 85°C) |
| AT97SC3205T-G3M44-00 | | | Lead-free, RoHS v1.2 rev 116 Standard Mode I ² C TPM with Compliance EK | Commercial (0°C to 70°C) |
| AT97SC3205T-H3M44-00 | | | | Industrial (-40°C to 85°C) |
| AT97SC3205T-G3M46-00 | | Lead-free, RoHS v1.2 rev 116 FIPS/Flex Mode I ² C TPM with Compliance EK | Commercial (0°C to 70°C) | |
| AT97SC3205T-H3M46-00 | | | Industrial (-40°C to 85°C) | |

1.3 AT97SC3204 LPC TPM

Table 1-3. AT97SC3204 LPC TPM TSSOP/QFN Ordering Information

| Ordering Code | Package | Description | Operation Range |
|---------------------|------------------------------|--|-------------------------------|
| AT97SC3204-X2A1A-10 | 28X1 (28-pin 4.4mm TSSOP) | Lead-free, RoHS v1.2 rev 116 LPC TPM with EK | Commercial (0°C to 70°C) |
| AT97SC3204-U2A1A-10 | | | Industrial (-40°C to 85°C) |
| AT97SC3204-X2A1A-20 | | Lead-free, RoHS v1.2 rev 116 LPC TPM with signed EK | Commercial (0°C to 70°C) |
| AT97SC3204-U2A1A-20 | | | Industrial (-40°C to 85°C) |
| <hr/> | | | |
| AT97SC3204-X2MA-10 | 40ML1 (40-pin QFN) | Lead-free, RoHS v1.2 rev 116 LPC TPM with EK | Commercial (0°C to 70°C) |
| AT97SC3204-U2MA-10 | | | Industrial (-40°C to 85°C) |
| AT97SC3204-X2MA-20 | | Lead-free, RoHS v1.2 rev 116 LPC TPM with signed EK | Commercial (0°C to 70°C) |
| AT97SC3204-U2MA-20 | | | Industrial (-40°C to 85°C) |

2. TPM TSSOP Configuration

2.1 TPM TSSOP Package EK Configuration

The Atmel® Trusted Platform Module (TPM) TSSOP package is shipped with pregenerated endorsement key pairs resident on the TPM. This configuration is considered the Real or Normal mode of the operation. Atmel can optionally support an X.509 EK Certificate (Signed-Real-Mode) stored in NV Storage as defined in the TCG Client Specific Implementation Specification for Conventional BIOS. Please contact Atmel for more information regarding Atmel EK Certificates.

3. TPM QFN Configuration

3.1 TPM QFN Package EK Configuration

The Atmel TPM QFN package is shipped with a compliance EK. The TCG TPM Main Specification provides a fixed set of keys and other data which are otherwise random during normal TPM operation. The primary purpose of this data is to provide fixed inputs which will generate predetermined outputs for use in verification of TPM firmware and for TPM interoperability testing. The data set also provides fixed values for known-answer tests of the TPM, which may be useful during manufacturing operations at OEM and ODM sites. All TPM commands will generate a fixed, predictable response while Compliance Data exists in the TPM.

3.2 Compliance Data

Compliance data must be cleared before Real/Normal mode operation. Compliance data is automatically deleted from the TPM when the command TPM_ForceClear is executed. It is expected the ForceClear command will be executed before legitimate TPM operation begins. The initial TPM commands used to generate the Endorsement Key (TPM_CreateEndorsementKeyPair), establish Ownership, and generate the Storage Root Key (TPM_TakeOwnership) will return fixed values before the Compliance data is cleared from the TPM.

4. FIPS/Flexible Mode

FIPS/Flexible devices are shipped by Atmel in the Flexible-mode allowing the customer to permanently set and lock the device into either Standard, Legacy FIPS-140-2 certified or WIN8 FIPS-140-2 certified mode during platform/device initialization. Please reference the Atmel Application Note, “Configuring FIPS/Flexible Devices” by contacting an Atmel Sales Representative:

<http://www.atmel.com/about/contact/distributors/default.aspx?contactType=Sales%20Representative>

5. Revision History

| Doc. Rev. | Date | Comments |
|-----------|---------|---------------------------|
| 8965A | 07/2015 | Initial document release. |



Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA T: (+1)(408) 441.0311 F: (+1)(408) 436.4200 | www.atmel.com

© 2015 Atmel Corporation. / Rev.: Atmel-8965A-TPM-Part-No-Selection-Guide-ApplicationNote_072015.

Atmel®, Atmel logo and combinations thereof, Enabling Unlimited Possibilities®, and others are registered trademarks or trademarks of Atmel Corporation in U.S. and other countries. Other terms and product names may be trademarks of others.

DISCLAIMER: The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. EXCEPT AS SET FORTH IN THE ATMEL TERMS AND CONDITIONS OF SALES LOCATED ON THE ATMEL WEBSITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS AND PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and products descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

SAFETY-CRITICAL, MILITARY, AND AUTOMOTIVE APPLICATIONS DISCLAIMER: Atmel products are not designed for and will not be used in connection with any applications where the failure of such products would reasonably be expected to result in significant personal injury or death ("Safety-Critical Applications") without an Atmel officer's specific written consent. Safety-Critical Applications include, without limitation, life support devices and systems, equipment or systems for the operation of nuclear facilities and weapons systems. Atmel products are not designed nor intended for use in military or aerospace applications or environments unless specifically designated by Atmel as military-grade. Atmel products are not designed nor intended for use in automotive applications unless specifically designated by Atmel as automotive-grade.