

## Microchip Trusted Platform Module 1.2 Part Number Selection Guide Addendum

### 1.0 ORDERING INFORMATION

#### 1.1 AT97SC3205 SPI TPM

**TABLE 1-1: AT97SC3205 SPI TPM TSSOP/QFN ORDERING INFORMATION**

| Ordering Code       | Package                        | Description                                                                                            | Operation Range             |
|---------------------|--------------------------------|--------------------------------------------------------------------------------------------------------|-----------------------------|
| AT97SC3205-X3A12-10 | 28X1<br>(28-pin 4.4 mm TSSOP)  | Lead-free, RoHS v1.2 rev 116 Standard Mode SPI TPM with Real Mode EK, 2066B User NVM                   | 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 NVM  | Commercial (0°C to +70°C)   |
| AT97SC3205-U3A12-20 |                                |                                                                                                        | Industrial (-40°C to +85°C) |
| AT97SC3205-X3A15-10 |                                | Lead-free, RoHS v1.2 rev 116 FIPS/Flex Mode SPI TPM with Real Mode EK, 2066B User NVM                  | 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), 2066B User NVM | Commercial (0°C to +70°C)   |
| AT97SC3205-U3A15-20 |                                |                                                                                                        | Industrial (-40°C to +85°C) |
| AT97SC3205-G3M42-00 | 32M3<br>(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 I<sup>2</sup>C TPM

**TABLE 1-2: AT97SC3205T I<sup>2</sup>C TPM TSSOP/QFN ORDERING INFORMATION**

| Ordering Code        | Package                        | Description                                                                                                         | Operation Range             |
|----------------------|--------------------------------|---------------------------------------------------------------------------------------------------------------------|-----------------------------|
| AT97SC3205T-X3A1C-10 | 28X1<br>(28-pin 4.4 mm TSSOP)  | Lead-free, RoHS v1.2 rev 116 FIPS/Flex Mode I <sup>2</sup> C TPM with Real Mode EK, 2066B User NVM                  | Commercial (0°C to +70°C)   |
| AT97SC3205T-U3A1C-10 |                                |                                                                                                                     | Industrial (-40°C to +85°C) |
| AT97SC3205T-X3A1C-20 |                                | Lead-free, RoHS v1.2 rev 116 FIPS/Flex Mode I <sup>2</sup> C TPM with Signed EK (X.509 Certificate), 2066B User NVM | Commercial (0°C to +70°C)   |
| AT97SC3205T-U3A1C-20 |                                |                                                                                                                     | Industrial (-40°C to +85°C) |
| AT97SC3205T-G3M4C-00 | 32M3<br>(32-pin Very Thin QFN) | Lead-free, RoHS v1.2 rev 116 FIPS/Flex Mode I <sup>2</sup> C TPM with Compliance EK                                 | Commercial (0°C to +70°C)   |
| AT97SC3205T-H3M4C-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<br>(28-pin 4.4 mm TSSOP) | Lead-free, RoHS v1.2 rev 116 Standard Mode LPC TPM with Real Mode 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 Standard Mode LPC TPM with Signed EK (X.509 Certificate) | Commercial (0°C to +70°C)   |
| AT97SC3204-U2A1A-20 |                               |                                                                                       | Industrial (-40°C to +85°C) |
| AT97SC3204-X2MA-10  | 40ML1<br>(40-pin QFN)         | Lead-free, RoHS v1.2 rev 116 Standard Mode LPC TPM with Real Mode 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 Standard Mode LPC TPM with Signed EK (X.509 Certificate) | Commercial (0°C to +70°C)   |
| AT97SC3204-U2MA-20  |                               |                                                                                       | Industrial (-40°C to +85°C) |

## 2.0 TPM PACKAGE CONFIGURATION

### 2.1 TPM TSSOP Package EK Configuration

The 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. Microchip 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. Contact Microchip for more information regarding Microchip EK Certificates.

### 2.2 TPM QFN Package EK Configuration

The AT97SC3205 and AT97SC3205T TPM QFN package is shipped with a compliance endorsement key pair (EK). The TCG TPM main specification provides a fixed set of keys and other data that are otherwise random during normal TPM operation. The primary purpose of this data is to provide fixed inputs that 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.

**Compliance data must be cleared before Real/Normal mode operation.** 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.

Compliance data will only be 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.

## 3.0 FIPS/FLEXIBLE MODE

FIPS/Flexible devices are shipped by Microchip 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 Microchip Application Note, "Configuring FIPS/Flexible Devices" by contacting a Microchip Sales Representative.

|                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note:</b> TPM1.2 FIPS 140-2 certification was based on legacy FIPS requirements with deprecated algorithms prior to new NIST FIPS 140-2 requirements in 2015. |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## APPENDIX A: REVISION HISTORY

### **Revision A (3/2019)**

This document (DS50002854A) replaces Atmel document (8965A Atmel Trusted Platform Module Part Number Selection Guide).

## THE MICROCHIP WEBSITE

Microchip provides online support via our website at [www.microchip.com](http://www.microchip.com). This site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the website contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

## CUSTOMER SUPPORT

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

**Technical support is available through the website at:** <http://microchip.com/support>

## CUSTOMER CHANGE NOTIFICATION SERVICE

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip website at [www.microchip.com](http://www.microchip.com). Under "Support", click on "Customer Change Notification" and follow the registration instructions.

## NOTICE TO CUSTOMERS

**All documentation becomes dated, and this manual is no exception. Microchip tools and documentation are constantly evolving to meet customer needs, so some actual dialogs and/or tool descriptions may differ from those in this document. Please refer to our website ([www.microchip.com](http://www.microchip.com)) to obtain the latest documentation available.**

**Documents are identified with a "DS" number. This number is located on the bottom of each page, in front of the page number. The numbering convention for the DS number is "DSXXXXXA", where "XXXXX" is the document number and "A" is the revision level of the document.**

**For the most up-to-date information on development tools, see the MPLAB® IDE online help. Select the Help menu, and then Topics to open a list of available online help files.**

---

**Note the following details of the code protection feature on Microchip devices:**

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as “unbreakable.”

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

---

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

*Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.*

**QUALITY MANAGEMENT SYSTEM**  
**CERTIFIED BY DNV**  
**== ISO/TS 16949 ==**

### Trademarks

The Microchip name and logo, the Microchip logo, AnyRate, AVR, AVR logo, AVR Freaks, BitCloud, chipKIT, chipKIT logo, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Helder, JukeBlox, KeeLoq, Kleeer, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, SAM-BA, SpyNIC, SST, SST Logo, SuperFlash, tinyAVR, UNI/O, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

ClockWorks, The Embedded Control Solutions Company, EtherSynch, Hyper Speed Control, HyperLight Load, IntelliMOS, mTouch, Precision Edge, and Quiet-Wire are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, EtherGREEN, In-Circuit Serial Programming, ICSP, INICnet, Inter-Chip Connectivity, JitterBlocker, KleeerNet, KleeerNet logo, memBrain, Mindi, MiWi, motorBench, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICKit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, SAM-ICE, Serial Quad I/O, SMART-I.S., SQI, SuperSwitcher, SuperSwitcher II, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

Silicon Storage Technology is a registered trademark of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2019, Microchip Technology Incorporated, All Rights Reserved.

ISBN: 978-1-5224-4266-0

## Worldwide Sales and Service

### AMERICAS

**Corporate Office**  
2355 West Chandler Blvd.  
Chandler, AZ 85224-6199  
Tel: 480-792-7200  
Fax: 480-792-7277  
Technical Support:  
<http://www.microchip.com/support>  
Web Address:  
[www.microchip.com](http://www.microchip.com)

**Atlanta**  
Duluth, GA  
Tel: 678-957-9614  
Fax: 678-957-1455

**Austin, TX**  
Tel: 512-257-3370

**Boston**  
Westborough, MA  
Tel: 774-760-0087  
Fax: 774-760-0088

**Chicago**  
Itasca, IL  
Tel: 630-285-0071  
Fax: 630-285-0075

**Dallas**  
Addison, TX  
Tel: 972-818-7423  
Fax: 972-818-2924

**Detroit**  
Novi, MI  
Tel: 248-848-4000

**Houston, TX**  
Tel: 281-894-5983

**Indianapolis**  
Noblesville, IN  
Tel: 317-773-8323  
Fax: 317-773-5453  
Tel: 317-536-2380

**Los Angeles**  
Mission Viejo, CA  
Tel: 949-462-9523  
Fax: 949-462-9608  
Tel: 951-273-7800

**Raleigh, NC**  
Tel: 919-844-7510

**New York, NY**  
Tel: 631-435-6000

**San Jose, CA**  
Tel: 408-735-9110  
Tel: 408-436-4270

**Canada - Toronto**  
Tel: 905-695-1980  
Fax: 905-695-2078

### ASIA/PACIFIC

**Australia - Sydney**  
Tel: 61-2-9868-6733

**China - Beijing**  
Tel: 86-10-8569-7000

**China - Chengdu**  
Tel: 86-28-8665-5511

**China - Chongqing**  
Tel: 86-23-8980-9588

**China - Dongguan**  
Tel: 86-769-8702-9880

**China - Guangzhou**  
Tel: 86-20-8755-8029

**China - Hangzhou**  
Tel: 86-571-8792-8115

**China - Hong Kong SAR**  
Tel: 852-2943-5100

**China - Nanjing**  
Tel: 86-25-8473-2460

**China - Qingdao**  
Tel: 86-532-8502-7355

**China - Shanghai**  
Tel: 86-21-3326-8000

**China - Shenyang**  
Tel: 86-24-2334-2829

**China - Shenzhen**  
Tel: 86-755-8864-2200

**China - Suzhou**  
Tel: 86-186-6233-1526

**China - Wuhan**  
Tel: 86-27-5980-5300

**China - Xian**  
Tel: 86-29-8833-7252

**China - Xiamen**  
Tel: 86-592-2388138

**China - Zhuhai**  
Tel: 86-756-3210040

### ASIA/PACIFIC

**India - Bangalore**  
Tel: 91-80-3090-4444

**India - New Delhi**  
Tel: 91-11-4160-8631

**India - Pune**  
Tel: 91-20-4121-0141

**Japan - Osaka**  
Tel: 81-6-6152-7160

**Japan - Tokyo**  
Tel: 81-3-6880-3770

**Korea - Daegu**  
Tel: 82-53-744-4301

**Korea - Seoul**  
Tel: 82-2-554-7200

**Malaysia - Kuala Lumpur**  
Tel: 60-3-7651-7906

**Malaysia - Penang**  
Tel: 60-4-227-8870

**Philippines - Manila**  
Tel: 63-2-634-9065

**Singapore**  
Tel: 65-6334-8870

**Taiwan - Hsin Chu**  
Tel: 886-3-577-8366

**Taiwan - Kaohsiung**  
Tel: 886-7-213-7830

**Taiwan - Taipei**  
Tel: 886-2-2508-8600

**Thailand - Bangkok**  
Tel: 66-2-694-1351

**Vietnam - Ho Chi Minh**  
Tel: 84-28-5448-2100

### EUROPE

**Austria - Wels**  
Tel: 43-7242-2244-39  
Fax: 43-7242-2244-393

**Denmark - Copenhagen**  
Tel: 45-4450-2828  
Fax: 45-4485-2829

**Finland - Espoo**  
Tel: 358-9-4520-820

**France - Paris**  
Tel: 33-1-69-53-63-20  
Fax: 33-1-69-30-90-79

**Germany - Garching**  
Tel: 49-8931-9700

**Germany - Haan**  
Tel: 49-2129-3766400

**Germany - Heilbronn**  
Tel: 49-7131-67-3636

**Germany - Karlsruhe**  
Tel: 49-721-625370

**Germany - Munich**  
Tel: 49-89-627-144-0  
Fax: 49-89-627-144-44

**Germany - Rosenheim**  
Tel: 49-8031-354-560

**Israel - Ra'anana**  
Tel: 972-9-744-7705

**Italy - Milan**  
Tel: 39-0331-742611  
Fax: 39-0331-466781

**Italy - Padova**  
Tel: 39-049-7625286

**Netherlands - Drunen**  
Tel: 31-416-690399  
Fax: 31-416-690340

**Norway - Trondheim**  
Tel: 47-7288-4388

**Poland - Warsaw**  
Tel: 48-22-3325737

**Romania - Bucharest**  
Tel: 40-21-407-87-50

**Spain - Madrid**  
Tel: 34-91-708-08-90  
Fax: 34-91-708-08-91

**Sweden - Gothenberg**  
Tel: 46-31-704-60-40

**Sweden - Stockholm**  
Tel: 46-8-5090-4654

**UK - Wokingham**  
Tel: 44-118-921-5800  
Fax: 44-118-921-5820