AN2237

Migrating from the ATECC608A to the ATECC608B

Introduction

Author: James Boomer – Microchip Technology Inc.

Over time, security capabilities and expectations evolve within the security world along with the capabilities of attacks that seek to compromise secure systems. Recognizing these changes, Microchip has developed a security-enhanced version of the ATECC608A, known as the ATECC608B. The security changes implemented in the device are largely behind the scenes and are not directly observable during normal operation. The ATECC608B has been designed to allow an easy migration from the ATECC608A, while improving the overall security.

For new designs, it is recommended that users start directly with the ATECC608B. For designs that are going through an upgrade or a revision, it is recommended that part of the upgrade include the ATECC608B. For other designs, users must do an overall security assessment and determine if they need to migrate to the ATECC608B.

The ATECC608B continues the line of security products developed as part of the Microchip CryptoAuthentication™ family of high-security cryptographic devices. These devices combine world-class hardware-based key storage with hardware cryptographic accelerators to implement various authentication and encryption protocols. All applications and use cases previously supported by the ATECC608A are also supported by the ATECC608B.

Applications Summary

- **Network/Internet of Things (IoT) Node Endpoint Security** – Manages node identity authentication and session key creation and management. Support is provided for the ephemeral session key generation flow for multiple protocols including TLS 1.2 and TLS 1.3.
- **Firmware Validation (Secure Boot)** – Supports the microcontroller (MCU) host by validating code digests and optionally enabling communication keys upon a successful secure boot. For an enhanced performance, various configurations are available.
- **Small Message Encryption** – Hardware Advanced Encryption Standard (AES) engine to encrypt and/or decrypt small messages or data such as Personally Identifiable Information (PII). The device supports the AES-ECB mode directly. Other AES modes are supported with help from the host. Additional Galois Field Multiply (GFM) calculation functions support the AES Galois Counter Mode (AES-GCM).
- **Secure Over-the-Air (OTA) Updates** – Supports local protected key generation for downloaded images. Both broadcasts of one image to many systems, each with the same decryption key, and point-to-point download of unique images per system are supported.
- **Accessory/Disposable Authentication** – Validates the authenticity of a system or component. This capability is often sought where disposable components are part of a system.

Table of Contents

1. Device Differences

The overall structure of the ATECC608B is identical to that of the ATECC608A. The ATECC608B does not introduce any new configuration bits and has the same number of data slots as that of the ATECC608A. All commands and command modes are still supported. The device supports both the I²C and SWI interface I/O protocols. The pinouts for the 8-pin SOIC and UDFN packages remain unchanged.

The following sections describe the differences between the ATECC608A and the ATECC608B devices.

Low-Frequency I²C Issue

The ATECC608A has an error in the I²C circuitry, where the device may respond incorrectly under the following conditions:

- Multiple I²C devices are on the same bus as the ATECC608A.
- The ATECC608A device was in Idle mode.
- The I²C operation frequency is ≤ 300 kHz.
- A data pattern from other devices on the I²C bus could be interpreted by the ATECC608A as a wake pulse.

Under the above conditions, the ATECC608A wakes up and may corrupt data being sent to other devices on the bus. Whether or not data are corrupted depends on the frequency of operation and the actual data being sent.

This issue has been corrected for the ATECC608B device by modifying the I²C circuitry to eliminate this issue. Note that the ATECC608B may still wake up at low frequency but it does not respond or cause data corruption.

Device Revision (DevRev) Differences

The package marking on Microchip security devices does not identify the device type. Therefore, the package marking cannot be used to identify the ATECC608B. The only way to identify the device is through use of the device revision. The hardware device revision of the device can be read by using the Revision mode (0x00) of the `Info` command. The output response of the `Info` command for each device is as follows:

Table 1-1. Revision Response

Device	Revision Response
ATECC608A	0x00 0x00 0x60 0x02
ATECC608B	0x00 0x00 0x60 0x03 (**Note**)

Note: The value of the fourth byte may change over time but it is 0x03 at the time of the initial product release.

Important: The value of the Revision mode response is not the same as the 4-byte RevNum (Bytes[4:7]) in the device configuration zone. Only the Revision mode response can be used for device identification.

Execution Time Differences

The implementation of security enhancements has resulted in changes to the execution times of a few commands. The variation depends on the actual Clock Divider mode as well as the specific mode of operation. The following table shows a list of commands and expected differences in execution times.

Notice: For a more detailed understanding of the execution times, refer to the complete data sheet.

Table 1-2. ATECC608A vs. ATECC608B Execution Time Differences

Command	Description of Changes
`Verify`	• The execution times of the `Verify` command will increase by no more than 10%. Actual variation may depend on the specific mode of the command. • The execution time increase will occur for all three Clock Divider modes.
`SecureBoot`	• The `SecureBoot` command includes a verify operation. The increase in execution time is due to the Verify portion of this command. • The execution times of the `SecureBoot` command will increase by no more than 10%. Actual variation may depend on the specific mode of the command. • The execution time increase will occur for all three Clock Divider modes.
`Read`	• The increase in read times is dependent on what is being read. • Reads of the configuration zone have increased by roughly 50% (0.8 ms to 1.2 ms) for a 32-byte read. • Reads of the data zone have approximately doubled. (0.9 ms to 1.8 ms) for a 32-byte read. • This does not apply to reading back a command response. This time will remain the same. • The execution time increase does not vary with the Clock Divider modes.
`Lock`	• The maximum lock time for either the configuration zone or the data zone increases by approximately 30%. • Since production units are shipped in a locked state, this does not impact normal device operation and is just observed by the user during the prototyping or development phase. • The execution time increase does not vary with the Clock Divider modes.

Enhanced Temperature Range

The ATECC608A is specified over the industrial temperature range of -40℃ to +85℃.

The ATECC608B is specified over the standard industrial range of -40℃ to +85℃ and an extended range of -40℃ to +100℃, for those users that need an upper ambient temperature value > +85℃. The enhanced temperature range devices have a unique ordering code that is found in the device's data sheet.

New Packages

The ATECC608B is now available in a 3-pin RBH contact package. This is in addition to the already existing 8-pin SOIC and UDFN packages. This package has been used previously for the ATSHA204A and the ATECC508A CryptoAuthentication devices. The RBH package is only available for devices in SWI interface mode.

The RBH package is a contact package that is typically mounted by gluing the package to an enclosure with the signal pads exposed. Contacts to the pads are usually made through pogo pins when the disposable unit is connected to the host system.

2. ATECC608B Migration

The ATECC608B has the same form, fit and function as the ATECC608A. The packages and pinouts are the same, the device structure is the same and so are the commands and command structure. This makes the ATECC608B a functional drop-in replacement of the ATECC608A. If the users implement their design utilizing the Microchip's software library (CryptoAuthLib), this further simplifies the migration process.

An additional factor that has to be considered is the timing differences between the ATECC608A and the ATECC608B for a specific design. This really depends on how the software was implemented. There are two cases that require consideration:

Fixed Timing Implementation

If the code is written assuming hardwired timing parameters, careful analysis must be undertaken to evaluate the impact of changing from the ATECC608A to the ATECC608B. Under this method, after a command is issued, the microcontroller will wait a fixed period of time before reading the response data back. If the delay required for the ATECC608B is significantly longer than the ATECC608A, this command may fail. Using an older version of CryptoAuthLib meant for the ATECC608A or a customer-generated library with the ATECC608B could cause some timing errors. Implementing the latest version of CryptoAuthLib correctly updates the timing information and, through just recompiling the code and reflashing the micro, the timing issues may be corrected. In general, the parameters used for fixed timing are broad enough that they will be conservative to actual worst-case timing values and may still not be an issue. As noted in **Section 1. Device Differences**, the timing changes of the ATECC608B and ATECC608A are relatively minor. Also, these are representative times for the specific command modes and there are other items (as noted in the data sheet) that could cause these values to step out further.

If timing is an issue, the following solutions can be considered:

1. Migrate the code to use the latest version of the CryptoAuthLib library.
2. Migrate the code to use polled timing. See **Section 2. Polled Timing Implementation** below.
3. If a custom library with fixed timing is used, update the library timing parameters needed for the ATECC608B.
4. Implement redundancy by trying to read back data a second time upon receiving a failure code that indicates the response was not yet ready.

Polled Timing Implementation

Polled timing is set as the default mode of operation when using the CryptoAuthLib library. If the code is written using polling, there will be no issues with migrating to the ATECC608B. In this scenario, the microcontroller would poll the ATECC608B to determine when data are available to be read. Minor timing differences would be absorbed by the polling command. These differences can be fully absorbed by the ATECC608B device because none of the execution times of the commands have stepped out significantly.

2.1 I^2C Low-Frequency ATECC608B Migration

Migrating an ATECC608A design that has to deal with the low-frequency I^2C issue requires no changes to either hardware or firmware. The changes implemented for a correct operation with the ATECC608A will not cause an issue with the fixed ATECC608B.

The user must consider if the operation of the system is better served by backing out the firmware changes implemented to correct the ATECC608A issues. Removing these changes would most likely result in reduced firmware size and improved system performance. Whether these are reasons valuable enough to modify the working code is up to the implementer.

3. Conclusion

Because the form, fit and function of the ATECC608B are nearly identical to those of the ATECC608A, the migration is typically a fairly minor task. The minor timing differences between the devices, in general, will not cause an issue and can be easily corrected if they do. The addition of the new RBH package and the enhanced temperature range also increase the market space for the ATECC608B secure element.

The changes implemented in the ATECC608B were primarily done to enhance device security and are largely transparent to the user. For new system designs and a refresh of the existing systems, it is strongly recommended to convert to the ATECC608B as a way to enhance overall system security.

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **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 (FAQs), technical support requests, online discussion groups, Microchip design partner 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

Product Change Notification Service

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

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

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.

Legal Notice

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.

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AnyRate, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, chipKIT, chipKIT logo, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PackeTime, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TempTrackr, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, FlashTec, Hyper Speed Control, HyperLight Load, IntelliMOS, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet-Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, Vite, WinPath, and ZL 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, BlueSky, 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, KleerNet, KleerNet logo, memBrain, Mindi, MiWi, 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.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, and Symmcom are registered trademarks 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.

ISBN: 978-1-5224-6331-3

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: www.microchip.com/support Web Address: 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	**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	**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	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4485-5910 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: 49-7131-72400 **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: 47-72884388 **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