

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 ATECC608B, known as the ATECC608C. The security changes implemented in the device are largely behind the scenes and are not directly observable during normal operation. The ATECC608C was designed to allow an easy migration from the ATECC608B, while improving the overall security.

For new designs, it is recommended that users start directly with the ATECC608C. For designs that are going through an upgrade or a revision, it is recommended that part of the upgrade include the ATECC608C. For other designs, users must do an overall security assessment and determine if they need to migrate to the ATECC608C.

The ATECC608C 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 ATECC608B are also supported by the ATECC608C.

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

Introduction.....	1
1. Device Differences.....	3
2. ATECC608C Migration.....	5
3. Conclusion.....	6
Microchip Information.....	7
The Microchip Website.....	7
Product Change Notification Service.....	7
Customer Support.....	7
Microchip Devices Code Protection Feature.....	7
Legal Notice.....	7
Trademarks.....	8
Quality Management System.....	9
Worldwide Sales and Service.....	10

1. Device Differences

The overall structure of the ATECC608C is identical to that of the ATECC608B. The ATECC608C does not introduce any new configuration bits and has the same number of data slots as that of the ATECC608B. 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, 8-Pad UDFN and 3-Lead Contact package all remain unchanged. The V_{CC} voltage range, temperature ranges and power specifications are all identical to that of the ATECC608B.

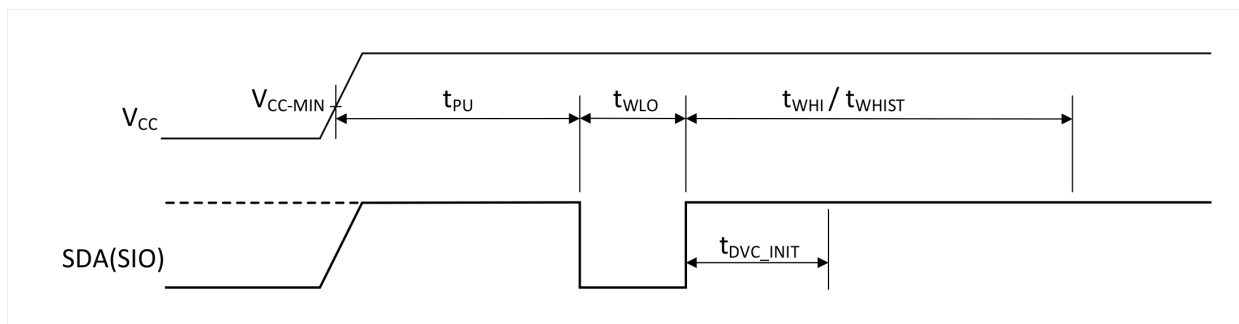
The following sections describe the differences between the ATECC608B and the ATECC608C devices.

Low-Temperature Lockup Issue

In a low number of devices, it was observed that, under low temperature conditions, the device would sometimes lock up when initially powering up. This lockup was due to the SCL pin changing state and switching to a GPIO output mode, as it is used in the Single Wire Interface (SWI) mode, and holding the SCL signal low. Typically, powering off the device and restarting the device would correct the issue.

This issue was corrected for the ATECC608C device by modifying the internal start-up circuitry and ensuring that the device will resolve to the correct state upon waking up the device. A new parameter was added to the data sheet called t_{DVC_INIT} that shows at what point the device is guaranteed to be in the correct state. It is recommended that no communication occur prior to this point to the ATECC608C or any other device on the I²C bus. The following diagram illustrates the timing.

Figure 1-1. Device Initialization Time



Important: Parameters, t_{PU} , t_{WLO} , t_{WHI} and t_{WHST} values were not changed from the ATECC608B. The t_{DVC_INIT} time is less than the t_{WHI}/t_{WHST} time, so the overall start-up time did not increase with this modification.

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 ATECC608C. The only way to identify the device is through the use of the device revision. The hardware 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
ATECC608B	0x00 0x00 0x60 0x03
ATECC608C	0x00 0x00 0x60 0x05 ^(1, 2)

**Tip:**

1. The value of the fourth byte may change over time but it is 0x05 at the time of the initial product release.
2. The value of the Revision mode response may not be the same as the 4-byte RevNum (Bytes[4:7]) in the device configuration zone. Only the Revision mode response of the `Info` command can be used for device identification.

Execution Time Differences

The implementation of security enhancements resulted in changes to the execution times of a few commands. The variation observed was very minimal and could have slightly improved or gotten worse. The only execution time change identified as a specification change in the data sheet is shown in the table below.

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

Table 1-2. ATECC608B vs. ATECC608C Execution Time Differences

Command	Description of Changes
Read	• The maximum execution times of the <code>Read</code> command when writing to data slots increased from 2.0 ms to 2.5 ms. • The timing of the <code>Read</code> command does not vary with the clock divider modes, so this increase occurs in all clock divider modes.

2. ATECC608C Migration

The ATECC608C has the same form, fit and function as the ATECC608B. The packages and pinouts are the same, the device structure is the same and so are the commands and command structure. This makes the ATECC608C a functional drop-in replacement of the ATECC608B. If the users implement their design utilizing the Microchip CryptoAuthLib (CAL), this further simplifies the migration process.

If a previous design implemented special measures to avoid or recover from the cold temp lockup issue, these may be removed as a way to simplify the firmware. Removing them, however, is not required and the device operation will not be harmed by leaving these measures in place.

An additional factor that has to be considered is the timing differences between the ATECC608B and the ATECC608C 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, an analysis must be undertaken to evaluate the impact of changing from the ATECC608B to the ATECC608C. 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 is greater than what is required by the ATECC608C, the command may fail. The timing implemented in the CAL library is broad enough to accommodate worst case conditions and are conservative to the worst case timing values. As noted in [1. Device Differences](#), the timing changes of the ATECC608C and ATECC608B are 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 the Polled Timing Implementation section below.
3. If a custom library with fixed timing is used, update the library timing parameters needed for the ATECC608C.
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 ATECC608C. In this scenario, the microcontroller would poll the ATECC608C 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 ATECC608C device because none of the execution times of the commands have stepped out significantly.

3. Conclusion

Because the form, fit and function of the ATECC608C are identical to those of the ATECC608B, the migration is a 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 changes implemented in the ATECC608C were primarily done to enhance device security and are largely transparent to the user. In addition, a low temperature lockup issue that rarely occurred was corrected. For new system designs and a refresh of the existing systems, it is recommended to convert to the ATECC608C as a way to enhance overall system security.

Microchip Information

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 products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable". Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications 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. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". 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 ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

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

AgileSwitch, APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet-Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, TrueTime, 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, Augmented Switching, BlueSky, BodyCom, Clockstudio, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, GridTime, IdealBridge, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, IntelliMOS, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, KoD, maxCrypto, maxView, 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, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQL, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, Trusted Time, TSHARC, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, 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.

© 2023, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.

ISBN: 978-1-6683-2830-9

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	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