AN3539

Migrating from the ATECC508A to the ATECC608B

Introduction

Authors: James Boomer and Karthikeyan Logaswamy – Microchip Technology Inc.

The ATECC608B is a security enhanced version of the ATECC608A and a security enhanced and feature upgrade to the ATECC508A. All these devices are products in the Microchip CryptoAuthentication™ family of high-security cryptographic devices. The security changes implemented in the device are largely behind the scenes and are not directly observable during normal operation.

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, it is recommended that users 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 cryptographic functions and algorithms. All applications and use cases previously supported by the ATECC508A are also supported by the ATECC608B.

The ATECC608B device is compatible with the ATECC508A device and with some limited exceptions, allows for easy migration. If the ATECC608B is properly configured, the software written for the ATECC508A will work with the ATECC608B. For more information, see **Section 4. Migration from the ATECC508A to the ATECC608B**. This application note lists the features, commands and configuration differences between the ATECC608B and the ATECC508A. It provides high-level details about the differences. For detailed information on the commands and configurations, compare the ATECC608B and the ATECC508A data sheets.

References

- ATECC508A Product Page
- ATECC608B Product Page

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** – Contains a 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 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 downloads 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. Feature Differences

The overall architecture of the ATECC608B is very similar to that of the ATECC508A. The ATECC608B has some configuration mode changes but has the same number of data slots as the ATECC508A. The majority of commands are compatible but some new commands or modes have been introduced and a couple of commands of the ATECC508A are no longer supported.

Both devices support the I^2C and SWI interface I/O protocols. The pinouts and footprints for the 8-pin SOIC, 8-pad UDFN and 3-pin RBH contact packages remain unchanged, allowing a pin-to-pin compatibility between devices.

The following sections describe the various feature differences available for the ATECC608B compared to the ATECC508A.[1] This includes new features, updated features and features that have been removed from this device.

1.1 New Features

1.1.1 Secure Boot

The ATECC608B provides a mechanism to support secure boot operations in a connected MCU/MPU (microprocessor). This can help to identify situations in which fraudulent code has been installed on the host. On power-up, the boot code within the host MCU sends the code digest and/or signature to the ATECC608B. If the signature validates the digest using the public key stored in the ATECC608B or the digest is compared to the stored digest, a message is returned to the MCU host. It also enables a reduction in the execution time of the boot process with its different methods and thus provides the secure boot speed optimization. To mitigate the Man-in-the-Middle (MITM) attack, the ATECC608B returns the optional Message Authentication Code (MAC) value to the MCU host, where the MCU host verifies the returned MAC.

1.1.2 Key Derivation Function

The ATECC608B supports the key derivation function (KDF), which derives the KDF key from the premaster secret key. The final derived KDF key is mainly used in TLS transactions. The ATECC608B supports three key derivation functions: Pseudo Random Function (PRF), AES and HMAC-Based Extract-and-Expand KDF (HKDF). The PRF is used in TLS version 1.2 and the HKDF is used in TLS version 1.3.

1.1.3 AES

The ATECC608B supports a Hardware 128-bit AES engine to encrypt and/or decrypt small messages or data packets. It supports an Electronic Code Block (ECB) mode and a GFM calculation for AES-GCM.

1.1.4 Self-Test

The ATECC608B provides a mechanism to test the internal cryptographic algorithms. It supports the self validation testing of the Symmetric HASH Algorithm (SHA), AES, Random Number Generator (RNG), Elliptic Curve Diffie-Hellman (ECDH), Elliptic Curve Digital Signature Algorithm (ECDSA) verify and ECDSA sign functions. The self test can be run automatically on device power-up or wake-up or initiated by the `SelfTest` command from the host.

1.1.5 I/O Protection Key

The ATECC608B provides a method to protect the I/O transmissions between this device and the host MCU for `ECDH`, `KDF`, `Verify` and `Secure Boot` commands. The I/O protection key is a randomly-generated secret key stored in the slot and is shared between the host MCU and the device.

For example, the premaster key generated from ECDH or the generated KDF key are encrypted by the I/O protection key. The encrypted key is sent to the host and the host decrypts it with the I/O protection key. In the secure boot and the signature verification process, a MAC is sent to the host to provide additional security. This MAC is generated by including the I/O protection key.

[1] All differences described in this document are also applicable to the ATECC608A, with respect to the ATECC508A, except as noted.

1.1.6 Persistent Latch

The Persistent Latch is a single bit of volatile memory used to indicate to the device that an associated key has been enabled for use with cryptographic functions. It can retain its state as long as the V_{CC} remains above 2V. It is always set to low on power-up and can be manipulated using various operations. When the key in a slot is linked to the Persistent Latch, a Persistent Latch state activates/deactivates the key in the slot. There are four ways to control the Persistent Latch: volatile key usage, secure boot, authorization output and intrusion detection. When one of the above methods is run successfully, the Persistent Latch will be set, thus enabling the key in the designated slot.

Notice: The ATECC508A had a Persistent Latch, but it only supported the intrusion detection mode. Applications that utilize the intrusion detection latch can be implemented with the ATECC608B.

1.1.7 Volatile Key Usage Permission

The volatile key is used to control the state of the Persistent Latch. The volatile key must be the secret that is shared between the MCU and the device. The cryptographic operation is performed between the host and the device with the volatile key. If successful, the Persistent Latch can be set, thus enabling the keys in the slot that are attached to the Persistent Latch.

1.1.8 Programmable I^2C Address

The ATECC608B provides the flexibility to change the I^2C address after the configuration zone has been locked. It can only be changed once. This feature helps to update the device address dynamically after it has been provisioned in the factory. This allows for an additional configuration step in a user's manufacturing flow, where multiple devices may be deployed in a system, or it allows the address to be updated after the device is deployed in the field.

1.1.9 Counter Match

The counter match function provides a mechanism for altering the limit to which the first monotonic counter (Counter 0) can be incremented. The key usage can be connected to the counter to prevent its use when Counter 0 reaches the limit value of the counter match slot. The counter match value in the slot can be changed any number of times and, for each change, Counter 0 gets linked to the new limit.

1.1.10 Transport/UseLock

The general purpose usage of the device is prohibited until the device is cryptographically enabled. The cryptographic operation is performed with a shared secret, available from the host, and stored in the device slot. Once the operation is successful, the ATECC608B can be used normally.

1.1.11 Power Reduction

The ATECC608B provides an option for reducing power consumption. The power consumption is reduced at the cost of command execution times. The mode has been developed for applications where power is extremely critical and slower execution times can be tolerated. For more information, see **Section 3. Configuration Zone Updates**.

1.1.12 Additional Buffers for Improved Operation

The ATECC608B provides new SRAM buffers: Message Digest buffer, Alternate Key buffer and SHA Context buffer. The Message Digest buffer and Alternate Key buffer can be used when the TempKey register holds other information. Multiple buffers allow a reduction in transactions and in the transaction time between the device and the host, by allowing the execution of different commands directly from the buffers.

The ATECC608B supports multiple instances for the SHA calculation with SHA context. The SHA buffer helps the host to perform read and write operations on the SHA context, which enables the host to execute multiple instances of SHA calculations.

1.1.13 Enhanced Temperature Range

The ATECC508A is specified over the industrial temperature range of -40°C to +85°C.

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

1.2 Updated Features

Updated features include an enhancement of the TempKey buffer, an enhancement of the RNG, a correction to a low-frequency I^2C issue and an update to the device revision identification information.

1.2.1 TempKey Buffer

The TempKey buffer size has been increased by 32 bytes for a total of 64 bytes, thus providing more storage and easy operation for other commands like `AES`, `KDF`, etc. Some commands can write to either the upper or the lower 32 bytes of the TempKey buffer.

1.2.2 Random Number Generator

The ATECC608B includes an enhanced high-quality cryptographic RNG, implemented by using a combination of non-deterministic noise (entropy) source (NRBG) and seeding a deterministic algorithm (DRBG) implemented according to the National Institute of Standards and Technology (NIST) standards. The NRBG is used in the instantiation and each time an RNG number is required.

1.2.3 Low Frequency I^2C Idle Issue

The ATECC508A has an error in the I^2C circuitry, where the device may respond incorrectly under the following conditions:

- Multiple I^2C devices are on the same bus as the ATECC508A.
- The ATECC508A device is in Idle mode.
- The I^2C frequency of operation is ≤ 300 kHz.
- A data pattern from other devices on the I^2C bus could be interpreted by the ATECC508A as a wake pulse.

Under the above conditions, the ATECC508A 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 I^2C circuitry to eliminate this issue. Note that the ATECC608B may still wake up at low frequencies but it will not respond or cause data corruption.

1.2.4 Device Revision

The package marking on Microchip security devices does not identify the device type. Therefore, the package marking cannot be used to identify the ATECC608B device. The only way to identify the device is through use of the device revision. The hardware device revision 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:

Device	`Info` Command Revision Mode Response[2]
ATECC508A	0x00 0x00 0x50 0x00
ATECC608B	0x00 0x00 0x60 0x03[1]

Notes:

1. The value of the fourth byte may change over time, but it is 0x03 at the time of the initial product release.
2. 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.

1.3 Unsupported Features

The following sections detail the features that have been removed from the ATECC508A. While there is no ability to directly replace these features, some of them can be implemented in a slightly different way. Details are provided in the following sections for each feature removed from the device. For an alternate method to implement some of these features, see **Section 4.3 Migrating Applications with Unsupported Features**.

1.3.1 OTP Consumption Mode

The EEPROM One-Time-Programmable (OTP) Consumption mode has been eliminated from the ATECC608B. After the device configuration zone is locked, no change to the OTP zone is allowed. Only reading of the OTP zone data is allowed.

1.3.2 LastKeyUse

The LastKeyUse functionality for key 15 has been eliminated. Slot 15 of the ATECC608B has the same functionalities as other slots and can no longer support a limited use key through the LastKeyUse functionality.

1.3.3 Selector Byte

The functionality to select a device from multiple devices sharing the same medium, when operating in Single-Wire Interface (SWI) mode using the selector byte, has been removed.

2. Command Differences

The following section describes the various differences in the commands available for the ATECC608B, compared to the ATECC508A. This includes new commands, updated commands and commands that are no longer supported for this device.

2.1 New Commands

2.1.1 `SecureBoot` Command

The `SecureBoot` command verifies the user application code during booting. This command supports three modes:

Full Mode:	The signature and the digest are passed to the ATECC608B. The public key in the slot verifies the sent signature and digest. The response may be a Boolean or a MAC, depending on the `SecureBoot` command.
FullStore Mode:	In FullStore mode, the digest or the signature is stored in the slot. If the digest is stored in the slot, it is sent to the device for verification. If the signature is stored in the slot, the digest is transmitted to the device, which verifies it with the stored signature and the public key.
FullCopy Mode:	This mode is run when the secure boot code updates the user application. Both the digest and the signature are sent to the device, which verifies them with the stored public key. Once the command is executed successfully, either the digest or the signature is copied to the slot, depending on the secure boot settings in the configuration zone.

In a scenario where wire(s) protection is needed, the command has the option to inform the device that the encrypted digest is sent. In this case, the digest is encrypted using the I/O protection key and TempKey. The value returned from the device is either the validating MAC or the status code based on the selection of the digest encryption. When the encrypted digest is sent, the MAC is returned from the device. The host also calculates the MAC using the I/O protection key, the nonce and the digest, and verifies the returned MAC. If the mode is FullStore Signature, the signature is also included for calculating the MAC, and the host verifies the returned MAC. The command has the option to prohibit the secure boot function until the next power cycle.

2.1.2 `SelfTest` Command

The `SelfTest` command is used for testing cryptographic engines like AES, SHA, ECDH, ECDSA Verify, Sign and RNG. This command has different modes that help in testing the individual cryptographic engines separately or they can be combined. The status returned from the device gives the individual cryptographic engine test results.

2.1.3 `AES` Command

The `AES` command supports a 128-bit Advanced Encryption Standard - Electronic Code Book (AES- ECB) encryption, AES-ECB decryption and calculates the GFM of the input data. An operation for encryption and decryption is performed for 16 bytes at a time.

This command supports the selection of a 16-byte AES key, which can be taken from any of the below sources:

- TempKey – A feature used to select one of the 16 bytes as a key from TempKey
- Data Slot – A feature used to select one of the 16 bytes as a key from a data slot

The value returned from the device is the encrypted/decrypted data, GFM data or an error code.

2.1.4 `KDF` Command

The `KDF` command is used to generate the KDF key from the premaster secret key and the input data.

The command supports three modes for creating the KDF key:

- AES – This mode selects the source of the 16-byte key location.

- PRF – This mode selects the length of the source key, Authenticated Encryption with Associated Data (AEAD). It also selects the length of the target key to be generated.
- HKDF – This mode provides the flexibility to select the source location input data and the zero key. There is an IV Special Function in HKDF that compares the strings of the input data with the predefined string in the configuration zone and generates the KDF key once they match.

The command selects the source location of the source key and can select the target KDF key location. This additional feature provides more security without the KDF key being returned to the device. The source and the target key location can be the EEPROM slot, TempKey or Alternate Key Buffer. The command also provides the option to send the KDF key in plain text or encrypted text to the host. The host decrypts the encrypted KDF key using the I/O protection key and nonce.

Depending on the mode, the return value from the command is either the plain/encrypted KDF key or the return status code. If the encrypted KDF key is returned, a random nonce is also returned for decrypting the KDF key in the host.

2.2 Updated Commands

2.2.1 `ECDH` Command

The `ECDH` command has been updated to allow the selection of the source private key location and target the premaster secret key location. The two possible sources for the private key location are the TempKey and the EEPROM key slot. The target premaster key location can have any of the following locations: output buffer, EEPROM or TempKey.

When the Encrypted mode is selected by the `ECDH` command, the output premaster secret is encrypted using the I/O protection key.

2.2.2 `GenKey` Command

The `GenKey` command supports a new private key generation to TempKey and the resulting private key is used only by the `ECDH` command. When the private key is stored in TempKey, it frees the slot for other uses. The generated private key is used for the premaster secret key generation.

2.2.3 `Info` Command

The `Info` command is updated to set and reset the state of the Persistent Latch. This command helps to read the current state of the Persistent Latch.

2.2.4 `Nonce` Command

The `Nonce` command allows for the input data to be stored in any of the following buffers: TempKey buffer, Message Digest buffer or Alternate Key buffer. The `Nonce` command also allows up to 64 bytes to be passed into the TempKey or the Message Digest buffer when in PassThrough mode.

2.2.5 `SHA` Command

The `SHA` command supports write and read context switching. This allows for multiple SHA digests to be calculated concurrently. The SHA mode is updated to support variable length data compared to earlier, fixed 64-byte data. The output of the command is directed to any of the following locations: output buffer and TempKey, output buffer and Message Digest buffer or output buffer only.

2.2.6 `Sign` Command

In addition to signing the message in TempKey, the `Sign` command provides the message in the Message Digest buffer for signing the data, freeing the TempKey for other operations.

2.2.7 `Verify` Command

In addition to verifying the message in TempKey, the `Verify` command provides the message in the Message Digest buffer for verifying the data, freeing the TempKey for other operations. It has an additional mode to send the MAC from the device to the host, where the MAC is calculated from the I/O protection key.

2.3 Unsupported Commands

2.3.1 `Pause` Command

For the ATECC508A, the `Pause` command is useful when using multiple devices on the SWI interface. This allows the ATECC508A to select only the device that matches the selector byte and to use it for further communication, while all the other devices in the same shared medium enter the Idle mode. The selector byte functionality has been removed from the ATECC608B.

2.3.2 `HMAC` Command

While the `HMAC` command no longer exists for the ATECC608B, the HMAC calculation can still be performed. The ATECC608B provides the feature for calculating the HMAC value using the `SHA` command. For both ATECC608B and ATECC508A, the resulting HMAC value from using the `SHA` command always matches. However, the ATECC608B HMAC value calculated using the `SHA` command does not match the HMAC value calculated using the `HMAC` command in the ATECC508A.

3. Configuration Zone Updates

Table 3-1 lists the new fields added in the ATECC608B configuration zone. It also describes the differences between the two devices.

Table 3-1. Configuration Zone Updates

Byte	ATECC608B	ATECC508A
13	AES_Enable – This byte enables/disables the AES functionalities for both AES and KDF commands.	Reserved for future use.
18	CountMatch – This byte enables/disables the CountMatch function and selects the slot to be used as the counter match key.	OTP mode – Used to set Read-Only or Consumption mode to the OTP zone.
19	The Chip mode has been redefined. The new byte helps to reduce the power consumption of the device with three possible power modes. It also selects the source of the I^2C address, either from the I2C_Address or the UserExtraAdd byte.	Chip mode
68	UseLock – This new byte controls the transport lock functionality. It enables/disables the transport lock function and the slot to be used as the transport key.	LastKeyUse (16 bytes) – This field controls the KeyID 15 limited-use functionality.
69	VolatileKeyPermission – This new byte enables/disables the volatile key functionality and selects the volatile key slot for volatile key functionalities.	
70-71	SecureBoot – This new byte configures the secure boot functionalities: • Selection of one of the Secure Boot modes. • Whether to set the Persistent Latch on a successfully `Secure Boot` command execution. • The slot to be used for digest/signature. • The slot to be used for public key. • The RNG to be used for the `Secure Boot` command.	
72	kdfIvLoc – Index within the KDF (HKDF) input string, where the two bytes stored below (KdfIvStr) are located.	
73	KdfIvStr – 2-byte KDF IV string that must be found in the KDF message for the KDF (HKDF) Special IV mode.	
85	UserExtraAdd – If nonzero, it is the I^2C address this device will respond to on the bus.	Selector byte – It selects which device will remain in Active mode after the execution of the `Pause` command.
90	ChipOptions The new byte provides the following features: • Whether to run the self-test automatically on power-on or wake-up. • Enables/disables the I/O protection key. • Enables/disables the KDF AES function. • Sets the ECDH and KDF protection functionality. • The slot to be used for the I/O protection key.	Reserved for future use.
96-127	KeyConfig – In KeyType, two new types (AES, SHA) and the function to enable the key based on the state of the Persistent Latch were added.	KeyConfig

4. Migration from the ATECC508A to the ATECC608B

In most cases, the migration from the ATECC508A to the ATECC608B is straightforward and uncomplicated. When migrating, several factors need to be considered:

1. Package and Pinout – All packages that are supported for the ATECC508A continue to be supported for the ATECC608B. This includes the 8-pad UDFN, 8-pin SOIC and 3-pin RBH contact package. Pinouts for each of these package are consistent between the devices.
2. Voltage and Temperature Ranges – Both devices are specified over the same operating supply voltage, 2.0V to 5.5V, and industrial temperature range, 0℃ to 85℃. No issues exist over this range.
3. Configuration – A review of the configuration zone needs to be undertaken to determine if a design can be ported with minimal changes or if a change to the application code is required. A more detailed list of considerations is provided in **Section 4.1 Configuration Migration Considerations**.
4. Timing Differences – Significant timing differences exist between the ATECC508A and the ATECC608B. The difficulty of migrating to the new devices depends on the commands utilized and whether fixed timing or polled timing was implemented. For more information, see **Section 4.2 Timing Migration Considerations**.

4.1 Configuration Migration Considerations

To allow the ATECC608B to operate similarly to the ATECC508A, the configuration zone changes shown in Table 4-1 must be made. Note that this configuration does not take advantage of the new features or commands associated with the ATECC608B.

Table 4-1. ATECC508A to ATECC608B Migration

Byte	ATECC608B	ATECC508A
18	CountMatch – 0x00	OTP mode • 0xAA – Read-Only mode • 0x55 – Consumption mode (**Note**) • All other values are reserved
19	Chip mode – Bits 3-7 of the byte must be '0'.	Chip mode
68	UseLock – 0x00	LastKeyUse (**Note**) – generally initialized to 0xFF.
69	VolatileKey permission – 0x00	
70-71	SecureBoot – 0x0000	
72	kdfIvLoc – 0x00	
73	KdfIvStr – 0x00	
85	UserExtraAdd – 0x00	Selector byte (**Note**) – any value depending on the device configured for the `Pause` command.
90	ChipOptions – 0x00	Reserved for future use. 0x00

Important: If this mode is used on the ATECC508A, some application redefinition may be required for the implementation on the ATECC608B.

4.2 Timing Migration Considerations

The previous sections describe all the differences in features and commands for the ATECC608B compared to the ATECC508A. One additional factor that needs to be considered is if the timing differences between the ATECC508A and the ATECC608B matter for a specific design. The timing differences between the two devices are quite significant for many commands. For a detailed comparison of the differences, it is recommended that a comparison of the two data sheets be undertaken.

The difficulty in migrating from the ATECC508A to the ATECC608B 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 ATECC508A to the ATECC608B. Under this method, after a command has been issued, the microcontroller waits a fixed period of time before reading the response data back. If the delay required for the ATECC608B is significantly longer than that of the ATECC508A, this command may fail. Using an older version of CryptoAuthLib meant for the ATECC508A or a customer-generated library with the ATECC608B could cause some timing errors. Implementing the latest version of CryptoAuthLib updates the timing information correctly and, through just recompiling the code and reflashing the micro, correcting the timing issues.

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. For more information, see **Section 4.2 Polled Timing Implementation**.
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 is not yet ready.

Polled Timing Implementation

If the code was written using polling, there will be no issues with migrating to the ATECC608B. Under this scenario, the microcontroller polls the ATECC608B to determine when data are available to be read back. Most timing differences are absorbed by the polling command.

4.3 Migrating Applications with Unsupported Features

If any of the unsupported features of the ATECC508A are implemented in an application, some changes will be required to the application code in order to use the ATECC608B. The following sections describe possible alternate methods to implement these features.

OTP Consumption Mode

If the OTP Consumption mode was used in an ATECC508A design, it cannot be directly implemented by the ATECC608B. However, the capability can be implemented in an alternate method, through the use of the monotonic counters.

If the monotonic counters are not used, one of them can be configured to replicate the OTP Consumption mode. The number of bits set to '1' in the OTP zone must be converted into the equivalent count value for the monotonic counter. This value would be provisioned as the initial counter value. While any monotonic counter can be used for this purpose, monotonic counter 1 is recommended, as monotonic counter 0 could be connected to a key slot and used to limit key usage.

LastKeyUse

The LastKeyUse functionality was only implemented on slot 15 of the ATECC508A. An alternate method to implement this capability can be enabled on this slot through the use of the SlotConfig.LimitedUse bit and a monotonic counter.

To replicate the functionality to be as close as possible to that of the ATECC508A, the count value of the monotonic counter needs to be set to replicate the count implemented on the ATECC508A design, using the LastKeyUse field.

Important: If another slot contains a key that was previously using the limited key use functionality, implementing a limited use on slot 15 may not be feasible.

Selector Byte

The selector byte functionality was only available in the SWI mode of the ATECC508A. There is no capability within the ATECC608B to replicate or emulate this functionality.

4.4 I²C Low-Frequency ATECC608B Migration

Migrating an ATECC508A design that has to deal with the low-frequency I²C issue requires no changes to either hardware or firmware. The changes implemented for a correct operation with the ATECC508A 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 ATECC508A 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.

5. Conclusion

The form, fit and function of the ATECC608B are compatible with those of the ATECC508A. Device pinouts for all supported packages and voltage operating ranges are identical. The ATECC608B supports the standard industrial temperature range that the ATECC508A supports, but it also provides an extended temperature range of up to 100°C.

The functionality of the ATECC608B is largely a superset of the ATECC508A, with the exception of only a few commands. There are a few configuration zone bytes that must be changed in order to achieve compatible operation. While the timing differences are significant, they can be readily overcome in most scenarios. If polling was implemented, the timing differences will be relatively transparent.

The changes implemented for 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 use the ATECC608B as a way to enhance overall system security. The ATECC608B also provides its users with a chance to implement some enhanced functional security features to improve their overall system security and performance.

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: 978-1-5224-6330-6

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