

## Introduction

The ATECC608C-TFLXTLS is a pre-provisioned variant of the ATECC608C. The ATECC608C provides enhanced security measures over that of the ATECC608A and ATECC608B. These enhancements also apply to the ATECC608C-TFLXTLS. The TrustFLEX secure element is part of Microchip's family of generically provisioned security-focused devices. The device configuration was designed to make the secure element applicable to some of the most common use cases in the IoT market, while minimizing the learning and start-up curves associated with security devices.

The ATECC608C-TFLXTLS configuration is similar to that of the ATECC608C-TNGTLS. Some additional flexibility and capability has been provided with respect to data loaded into certificate and key slots and the locking options of those slots. These slot access policies will be set by the Trust Platform Design Suite tools prior to ordering the ATECC608C-TFLXTLS devices. A Single Wire Interface (SWI) option is also available for this device.

This data sheet provides the slot and key configuration information that is unique to the ATECC608C-TFLXTLS. This information clearly defines the access policies of each of the data zone slots. Limited command and I/O operating information has been provided since the devices are to be used with the Trust Platform Development Suite (TPDS) tools. An application section discussing Microchip's hardware and software tools that can aid in developing an application is also provided with additional links to the location of the tools.

## Features

- Specified Configuration Zone with limited selectable options.
- I/O Options
  - I<sup>2</sup>C Interface with One-Time Changeable I<sup>2</sup>C Address
  - Single Wire Interface (SWI)
- JIL High Rating – Validated to JIL Application of Attack Potential to Smartcards and Similar Devices, Version 3.1
- Internal High-Quality NIST SP 800-90A/B/C True Random Number Generator (TRNG) NIST CMVP ESV Certified
- One Permanent Primary P-256 Elliptic Curve Cryptography (ECC secp256r1) Private Key Fixed at Manufacturing Time
- One Internal Sign Private Key for Key Attestation
- Three Secondary P-256 ECC Private Keys that Can Be Regenerated by the User
- Signer Public Key from Signer Certificate
- Public Key Validation Support
- One Customizable Symmetric Secret Key Slot
- IO Protection Key Slot to Protect Interface Communication
- Secure Boot Enabled with Customizable Secure Boot Public Key at Time of Manufacture
- ECDH/KDF Key Slot Capable of Being Used with AES Keys and Commands
- X.509 Compressed Certificate Storage
- Customizable Certificate Storage Slots
- 1.8V to 5.5V IO Levels, 2.0V to 5.5V Supply Voltage

- Standard Industrial Temperature Range: -40°C to +85°C
- 30 nA nominal Sleep Current
- Available in 8-Pad UDFN and 8-Pin SOIC package options at a 2k MOQ

## Use Cases

- Secure IoT TLS 1.2 and 1.3 Connections including custom PKI
- Secure Boot/Secure Firmware Update
- Disposable/Accessory Authentication
- I/P and Data Protection

## Table of Contents

Introduction.....	1
Features.....	1
Use Cases.....	2
1. Pin Configuration and Pinouts.....	6
2. Security Information.....	7
2.1. Cryptographic Standards.....	7
2.1.1. SHA-256.....	7
2.1.2. HMAC/SHA-256.....	7
2.1.3. TLS V1.2 Pseudo Random Function (PRF).....	7
2.1.4. HMAC-based Extract-and-Expand KDF (HKDF).....	7
2.1.5. Elliptic Curve Digital Signature Algorithm (ECDSA).....	7
2.1.6. Elliptic Curve Diffie-Hellman (ECDH).....	7
2.1.7. Advanced Encryption Standard (AES).....	7
2.2. Certifications.....	7
2.2.1. NIST CAVP Algorithm Certifications.....	8
2.2.2. Vulnerability Analysis.....	8
2.2.3. RNG Certifications.....	8
3. EEPROM Memory and Data Zone Access Policies.....	9
3.1. ATECC608C-TFLXTLS Configuration Zone.....	9
3.1.1. Modifiable Configuration Zone Bytes.....	10
3.2. Data Zone and Access Policies.....	11
3.2.1. Data Zone Data Types.....	11
3.2.1.1. Private Keys.....	11
3.2.1.2. Public Keys.....	12
3.2.1.3. Certificate Storage.....	12
3.2.1.4. Secure Boot.....	13
3.2.1.5. Secret Key.....	13
3.2.1.6. AES Key Storage.....	13
3.2.1.7. I/O Protection Key.....	13
3.2.1.8. General Data Storage.....	14
3.2.2. Slot Configuration Terminology.....	14
3.2.3. ATECC608C-TFLXTLS Slot Configuration Summary.....	14
3.2.4. ATECC608C-TFLXTLS Detailed Slot Access Policies.....	15
3.3. ATECC608C-TFLXTLS EEPROM One Time Programmable (OTP) Zone.....	20
4. Static RAM (SRAM) Memory.....	22
5. General Command Information.....	23
5.1. I/O Transactions.....	23
5.2. Command Packets.....	23
5.3. Status/Error Codes.....	23
5.4. Address Encoding.....	24
5.4.1. Configuration Zone Addressing.....	24

5.4.2.	OTP Zone Addressing.....	25
5.4.3.	Data Zone Addressing.....	25
5.5.	Formatting of Keys, Signatures and Certificates.....	26
5.5.1.	ECC Key Formatting.....	26
5.5.1.1.	Public Key Formats.....	27
5.5.2.	Signature Format.....	28
5.5.3.	Certificate Storage.....	28
6.	Device Commands.....	30
6.1.	General Device Commands.....	31
6.1.1.	Counter Command.....	31
6.1.2.	Info Command.....	31
6.1.3.	Lock Command.....	31
6.1.4.	Nonce Command.....	32
6.1.5.	Random Command.....	32
6.1.6.	Read Command.....	32
6.1.7.	SelfTest Command.....	32
6.1.8.	SHA Command.....	32
6.1.9.	UpdateExtra Command.....	32
6.1.10.	Write Command.....	32
6.2.	Asymmetric Cryptography Commands.....	33
6.2.1.	ECDH Command.....	33
6.2.2.	GenKey Command.....	33
6.2.3.	SecureBoot Command.....	33
6.2.4.	Sign Command.....	33
6.2.5.	Verify Command.....	33
6.3.	Symmetric Cryptography Commands.....	34
6.3.1.	AES Command.....	34
6.3.2.	CheckMac Command.....	34
6.3.3.	GenDig Command.....	34
6.3.4.	KDF Command.....	35
6.3.5.	MAC Command.....	35
7.	Application Information.....	36
7.1.	Use Cases.....	36
7.2.	Development Tools.....	37
7.2.1.	Trust Platform Design Suite.....	37
7.2.2.	Hardware Tools.....	37
7.2.3.	CryptoAuthLib.....	38
7.3.	TrustFLEX vs. Trust&GO.....	38
8.	I <sup>2</sup> C Interface.....	40
8.1.	I/O Conditions.....	40
8.1.1.	Device is Asleep.....	40
8.1.2.	Device is Awake.....	41
8.2.	I <sup>2</sup> C Transmission to ATECC608C-TFLXTLS.....	42
8.2.1.	Word Address Values.....	43
8.2.2.	I <sup>2</sup> C Synchronization.....	43
8.3.	Sleep Sequence.....	44

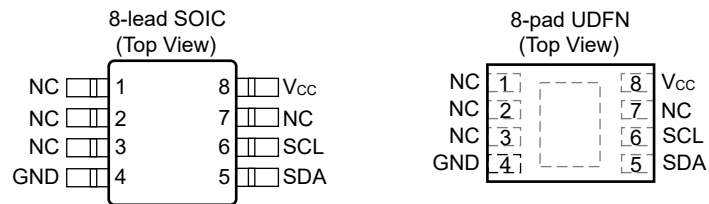
8.4.	Idle Sequence.....	44
8.5.	I <sup>2</sup> C Transmission from the ATECC608C-TFLXTLS.....	44
9.	Single-Wire Interface.....	45
9.1.	I/O Tokens.....	45
9.2.	I/O Flags.....	45
9.3.	Synchronization.....	46
9.3.1.	I/O Timeout.....	46
9.3.2.	Synchronization Procedures.....	47
9.4.	GPIO.....	47
9.5.	Wiring Configuration for Single-Wire Interface.....	47
10.	Electrical Characteristics.....	49
10.1.	Absolute Maximum Ratings.....	49
10.2.	Reliability.....	49
10.3.	AC Parameters: All I/O Interfaces.....	49
10.3.1.	AC Parameters: I <sup>2</sup> C Interface.....	50
10.3.2.	AC Parameters: Single-Wire Interface.....	51
10.4.	DC Parameters: All I/O Interfaces.....	52
10.4.1.	V <sub>IH</sub> and V <sub>IL</sub> Specifications.....	53
11.	Compatibility.....	54
12.	Package Drawings.....	55
12.1.	Package Marking Information.....	55
12.2.	8-Pad UDFN.....	56
12.3.	8-Lead SOIC.....	59
13.	Revision History.....	62
	Microchip Information.....	63
	The Microchip Website.....	63
	Product Change Notification Service.....	63
	Customer Support.....	63
	Product Identification System.....	64
	Microchip Devices Code Protection Feature.....	65
	Legal Notice.....	65
	Trademarks.....	65
	Quality Management System.....	66
	Worldwide Sales and Service.....	67

# 1. Pin Configuration and Pinouts

**Table 1-1.** Pin Configuration

Pin	Function I <sup>2</sup> C Devices	Function SWI Devices
NC	No Connect	No Connect
GND	Ground	Ground
SDA	I <sup>2</sup> C Serial Data	Single Wire I/O Signal
SCL	I <sup>2</sup> C Serial Clock Input	GPIO Signal
V <sub>CC</sub>	Power Supply	Power Supply

**Figure 1-1.** UDFN and SOIC Pinout



**Note:** The UDFN backside paddle is recommended to be connected to GND.

## 2. Security Information

### 2.1 Cryptographic Standards

The ATECC608C-TFLXTLS follows various industry standards for the computation of cryptographic results. These reference documents are described in the following sections.

#### 2.1.1 SHA-256

The ATECC608C-TFLXTLS computes the SHA-256 digest based upon the algorithm documented in the following site:

[nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf](http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf)

#### 2.1.2 HMAC/SHA-256

The ATECC608C-TFLXTLS can compute an HMAC digest based upon SHA-256 using a key stored in the EEPROM as documented below:

[http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1\\_final.pdf](http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf)

#### 2.1.3 TLS V1.2 Pseudo Random Function (PRF)

The ATECC608C-TFLXTLS KDF(PRF) command calculates the key derivation function (KDF) specified for TLSV1.2 (and earlier) at:

[tools.ietf.org/html/rfc5246](http://tools.ietf.org/html/rfc5246)

#### 2.1.4 HMAC-based Extract-and-Expand KDF (HKDF)

The ATECC608C-TFLXTLS KDF(HKDF) command calculates the HKDF key derivation function (KDF). This is the KDF that is used in the TLS1.3 specification. It is specified at:

[tools.ietf.org/html/rfc5869](http://tools.ietf.org/html/rfc5869)

#### 2.1.5 Elliptic Curve Digital Signature Algorithm (ECDSA)

The ATECC608C-TFLXTLS computes and verifies the Elliptic Curve signatures according to the algorithm documented in:

- ANSI X9.62-2005 [www.ansi.org/](http://www.ansi.org/)
- FIPS 186-5 specification [nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf](http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf)

#### 2.1.6 Elliptic Curve Diffie-Hellman (ECDH)

The ATECC608C-TFLXTLS executes the ECDH key agreement according to NIST Special Publication 800-56A recommendations:

[nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf)

#### 2.1.7 Advanced Encryption Standard (AES)

Symmetric encryption & decryption, if enabled, is implemented via the AES command using only AES-128 per:

[nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf](http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf)

### 2.2 Certifications

As part of the overall development effort of the ATECC608C-TFLXTLS, Microchip Technology worked in concert with certified industry laboratories to perform extensive certification and validation procedures. The following subsections provide more information on the certification and validation testing performed.

### 2.2.1 NIST CAVP Algorithm Certifications

The ATECC608C algorithms were certified through the NIST Cryptographic Algorithm Validation Program (CAVP) working in conjunction with a NIST certified laboratory. Microchip Technology was issued the following CAVP certificate numbers, attesting that the following algorithms are in compliance to NIST standards.

- [A4280](#): All algorithms other than AES-GCM
- [A4285](#): AES-GCM

**Table 2-1.** ATECC608C Certified CAVP algorithms

- |                            |                            |                            |
|----------------------------|----------------------------|----------------------------|
| • AES-ECB                  | • SHA2-256                 | • ECDSA KeyGen (FIPS186-5) |
| • AES-GCM                  | • Counter DRBG             | • ECDSA SigVer (FIPS186-5) |
| • ECDSA KeyVer (FIPS186-5) | • ECDSA SigGen (FIPS186-5) | • KDF TLS                  |
| • HMAC-SHA-256             | • KAS-ECC-SSC SP800-56Ar3  |                            |

### 2.2.2 Vulnerability Analysis

The ATECC608C-TFLXTLS device was evaluated by a third Party SOGIS certified laboratory on its overall vulnerability resistance to attack in accordance with the Joint Interpretation Laboratory (JIL) methodologies and standards. The device achieved the highest possible rating of JIL HIGH when measured against the JIL rating score defined in the JIL standard: [Application of Attack Potential to Smartcards and Similar Devices version 3.1](#).

### 2.2.3 RNG Certifications

The ATECC608C-TFLXTLS True Random Number Generator (TRNG) was developed in accordance with the NIST SP800-90A/B/C specifications. The DRBG and NRBG elements of the design were evaluated using a NIST certified laboratory to the procedures they have specified.

- **DRBG Certification:** The Deterministic Random Bit Generator (DRBG) was evaluated as part of the ATECC608C CAVP certification activity resulting in certificate number [A4280](#). NIST validated and attests that the DRBG, implemented as a Counter DRBG algorithm, complies with the SP800-90A specification.
- **NRBG Certification:** The ATECC608C-TFLXTLS NRBG Entropy Source module was certified through the NIST Cryptographic Module Validation (CMVP) Entropy Source Validation (ESV) program working in conjunction with a NIST certified laboratory. Microchip Technology was issued [Entropy Certificate #E46](#) by NIST. NIST validated and attests that the "ECC608 NRBG Entropy Source" module complies to the SP800-90B standard with a ring oscillator-based architecture for a physical non-deterministic random bit generator module that can be reused in product revisions of the ATECC608. This attestation is being extended to the ATECC608C revision of the product. The E46 certificate will be updated on the NIST validation site when the NIST extension review is complete.



### 3. EEPROM Memory and Data Zone Access Policies

The EEPROM memory contains a total of 1,400 bytes and is divided into the following zones:

**Table 3-1.** ATECC608C-TFLXTLS EEPROM Zones

Zone	Description	Nomenclature
Configuration	Zone of 128 bytes (1,024 bits) EEPROM that contains: <ul style="list-style-type: none"> <li>• Device configuration</li> <li>• Slot access policy information</li> <li>• Counter values</li> <li>• Device serial number</li> <li>• Lock information</li> </ul> The LockConfig byte has already been set. Nothing can be directly written to this zone. The zone can always be read.	Config[a:b] = A range of bytes within a field of the Configuration zone
Data	Zone of 1,208 bytes (9.7 Kb) split into 16 general purpose read-only or read/write memory slots. The access policy information defined by the Configuration zone bytes determines how each slot can be accessed. The Access Policy for each data slot in the ATECC608C-TFLXTLS device has already been set and the slot Access Policies defined by the Configuration zone are in full effect. Some slots can be read from or written to while others cannot, depending upon that slot's Access Policy.	Slot[YY] = The entire contents stored in Slot YY of the Data zone
One-Time-Programmable (OTP)	Zone of 64 bytes (512 bits) arranged into two blocks of 32 bytes each. For the ATECC608C-TFLXTLS, the zone is preloaded with a predefined value. This zone cannot be modified but can be read at any time. See Section 3.3. <a href="#">ATECC608C-TFLXTLS EEPROM One Time Programmable (OTP) Zone</a> for more information.	OTP[bb] = A byte within the OTP zone, while OTP[aa:bb] indicates a range of bytes

**Table 3-2.** Document Terms

Terms discussed within this document will have the following meanings:

Term	Meaning
Block	A single 256-bit (32-byte) area of a particular memory zone. The industry standard SHA-256 documentation also uses the term block to indicate a 512-bit section of the message input. Within this document, this convention is used only when describing hash input messages.
KeyID	KeyID is equivalent to the slot number for those slots designated to hold key values. Key 1 (sometimes referred to as key[1]) is stored in Slot[1] and so on. While all 16 slots can potentially hold keys, those slots that are configured to permit clear text reads are not normally used as private or secret keys by the crypto commands.
mode[b]	Indicates bit, b, of the parameter mode.
SRAM	Contains input and output buffers, as well as internal state storage locations. This memory is not directly accessible by the user.
Word	A single 4-byte word of data read from or written to a block. The word is the smallest unit of data access.
LSB/MSB	Least Significant Byte/Most Significant Byte.
LSb/MSb	Least Significant Bit/Most Significant Bit.

#### 3.1 ATECC608C-TFLXTLS Configuration Zone

The ATECC608C-TFLXTLS configuration is fixed and cannot be modified by the customer. When using the Microchip Trust Platform Design Suite, all configuration information is taken into account by the tools. Relevant information about how the device is configured is shown below or in the slot information.

## Device Configuration Information

- The serial number for each device is unique and stored in bytes [0:3, 8:12]. Bytes [0:1] are 0x01 0x23 and byte [8] is 0x01. All other bytes are unique.
- The default 7-bit I<sup>2</sup>C address is 0x36. The I<sup>2</sup>C address can be overwritten using the `UpdateExtra` command.



**Important:** The default I<sup>2</sup>C address of the ATECC608C-TFLXTLS differs from that of the standard ATECC608C device.

- The I/O levels are set to a fixed reference level; therefore, the host processor can operate at a lower voltage than the ATECC608C-TFLXTLS device.
- The Watchdog Timer (WDT) is set to a maximum time-out of 1.3s.
- The use of an I/O protection key is enabled with the key stored in Slot 6.
- For the ATECC608C-TFLXTLS, the following individual slots may be uniquely configured to be slot lockable or not: Slots 2-6, 8, 10-12, 13 and 15.
- SecureBoot is enabled for FullStore digest mode for the ATECC608C-TFLXTLS.
- Monotonic counters are available for use by the system and are not attached to any keys.
- The Health Test Failure bit is cleared after any time that a command fails as a result of a health test failure. If the failure symptom is transient, the command may pass when run a second time.

### 3.1.1 Modifiable Configuration Zone Bytes

No bytes within the Configuration Zone can be directly written because the Config Zone is already locked. Several bytes can still be modified through the use of other commands.

#### SlotLocked Bits

For the ATECC608C-TFLXTLS, the following individual slots may be uniquely configured to be slot lockable or not: Slots 2-6, 8, 10-12, 13 and 15. Through use of the Trust Platform Design Suite tools, each of these slots may be set to either be fixed or locked at time of manufacturing. Slots 10-12 must always be set the same way. If set to be lockable the SlotLock mode of the `Lock` command can be used to lock a given slot. Each slot where this feature is enabled can be individually locked just once. Once a slot has been locked, it can never be modified or unlocked but can still be used based on the Access Policies defined for that slot.

Bytes 88 and 89 store the SlotLocked bytes. Initially, all bits in these bytes are set to a value of one. For those slots that have been locked, the value of the respective bit will be set to a value of zero.

#### I<sup>2</sup>C Address Redefinition

This device configuration has been created such that the I<sup>2</sup>C address can be redefined one time. The `UpdateExtra` command can be used to rewrite byte 85 of the Configuration zone to a new I<sup>2</sup>C address. When this byte is set to a non-zero value, the device configuration uses byte 85 as its I<sup>2</sup>C address instead of the default address. Once this byte has been rewritten, the device must be powered-down or put into Sleep mode before this change takes effect.



**Important:** If there is no need to change the I<sup>2</sup>C address, this location must be written with the default I<sup>2</sup>C address.

### User Extra Byte

The UserExtra byte can be used for any desired purpose. This byte can be updated just once with the `UpdateExtra` command. The UserExtra byte is located at byte 84 of the Configuration zone.

### Counter[0,1]

While the counters are not used by this device, they are not disabled. If so desired, the monotonic counters may be used by the system. Note that the counters are initialized to zero and can count to the maximum value of 2,097,151. The counter value can be incremented or read through the use of the `Counter` command. How this counter is used is strictly up to the system and independent of anything else on the device. Counter values can be read or updated using the `Counter` command.

## 3.2 Data Zone and Access Policies

The following sections describe the detailed access policy information associated with each slot. The actual access policy information is stored within the Slot and Key configuration sections in the EEPROM Configuration zone. Each Data zone slot has two Slot Configuration bytes and two Key Configuration bytes associated with it. Together, these four bytes create the access policies for each slot. The actual type of data stored within the slot is determined by the access policies for that slot.

### 3.2.1 Data Zone Data Types

The following section provides more details on the various types of data capable of being stored in the ATECC608C-TFLXTLS data slots.

#### 3.2.1.1 Private Keys

ECC private keys are the fundamental building blocks of ECC Security. These keys are private and unique to each device and can never be read. ECC private keys are randomly generated by the secure element's TRNG and are securely held in slots configured as ECC private keys.

##### Primary Private Key

This is the primary authentication key. It is permanent and cannot be changed. Each device has its own unique private key.

This key is enabled for two primary elliptic curve functions:

- ECDSA Sign for authentication
- ECDH for key agreement. If encryption of the ECDH output is required, the IO protection key needs to be first set up. See Section [3.2.1.7. I/O Protection Key](#) for setup details.

This private key is the foundation for the generation of the corresponding public key and the X.509 Certificates.

##### Secondary Private Keys

There are additional private keys that can be used for future use cases, such as additional service authentication.

These keys are enabled for the following primary elliptic curve functions:

- ECDSA Sign for authentication.
- ECDH for key agreement. If encryption of the ECDH output is required, the IO protection key needs to be first set up. See Section [3.2.1.7. I/O Protection Key](#) for setup details.
- GenKey for overwriting the slot with a new internally-generated random private key.

While the primary private key and certificates are permanent, these other keys can be overwritten with a new internally-generated private key (`GenKey` command mode = 0x04) to enable key deletion, key rotation and remote provisioning. The keys are also slot-lockable (`KeyConfig.Lockable` bit is set to zero), meaning the `Lock` command can be used in `SlotLock` mode to render the current key permanent and prevent it from being changed by the `GenKey` command. When performing key

changes, [Key Attestation](#) is required to ensure to another system that the device's new public key being presented actually originated from the device in question.

### Key Attestation

The private key in slot 1 is configured as an internal sign-only key, which means it can only sign messages generated internally by the `GenKey` or `GenDig` commands and cannot be used to sign arbitrary external messages. This feature allows the internal sign key to be used to attest to what keys are in the device and their configuration/status to any system that knows (and trusts) the internal sign public key.

#### 3.2.1.2 Public Keys

Public keys are associated with ECC private keys. Every ECC private key will have its own unique public key. Public keys associated with private keys stored on the device can be retrieved by using the `GenKey` command. Public keys from an ECC private key stored off chip can be stored in the device in a slot configured for a public key.

### Permanent Parent Public Key

The parent public key is a primary system key generated from an ECC private key that is stored off chip. This key must be written to the slot labeled Parent Public Key, and, then, slot locked to make it permanent. This key cannot be changed. This key can be set up to be used as part of the validation process for a Validated Public key.

### Validated Updatable Public Key

A validated public key requires that a key be validated before use or invalidated before being updated. Validation and invalidation are done using the `Verify` command and the Parent Public Key in Validate/Invalidate mode. Here, a parent public key must be written and locked in the Parent Public Key slot. The public key to be validated must, then, be written to the Validated Public Key slot. This slot must not be locked if updating the key is desired. Finally, the private key counterpart to the parent public key (off chip) needs to be used to validate the public key to enable its use and prevent unauthorized changes.

#### 3.2.1.3 Certificate Storage

The ATECC608C-TFLXTLS storage is centered around securely holding keys. Since X.509 certificates tend to be larger than what will fit into a single ATECC608C-TFLXTLS device slot, a compressed format is used. This technique may be better called a partial certificate as it stores dynamic certificate information on the device and imposes some limitations. Dynamic information is certificate content that can be expected to change from device to device (e.g., public key, validity dates, etc.). Firmware is expected to have a certificate definition (`atcacert_def_t` from `CryptoAuthLib`) with a template of the full X.509 certificate containing static information (data that are the same for all certificates) and instructions on how to rebuild the full certificate from the dynamic information in the compressed certificate.

The following application note documents the compressed certificate format: [ATECC Compressed Certificate Definition](#).

The [CryptoAuthLib library](#) also contains the `atcacert` module for working with compressed certificates.

### Device Certificate

The device certificate consists of information associated with the actual end unit. For the ATECC608C-TFLXTLS, the device certificate is stored in Slot #10 in a compressed format.

### Signer Certificate

The signer certificate consists of the information associated with the signer certificate authority used to sign the device certificate. For the ATECC608C-TFLXTLS, the signer certificate is stored in Slot #12. The signer public key is also required to rebuild the full signer certificate.

### Signer Public Key

The signer public key is the public key needed to verify the signer and the information that is associated with the signer compressed certificate. For the ATECC608C-TFLXTLS, it is stored in Slot #11.

The following table shows all the slots associated with certificates in the ATECC608C-TFLXTLS:

Slot	Description
0	Primary private key. The public key can be generated at any time using the <code>GenKey</code> command in Mode = 0x00.
10	Device certificate. This is stored here in a compressed format.
11	Signer public key.
12	Signer certificate. This is stored in a compressed format.

For the ATECC608C-TFLXTLS production units, these slots can be configured as either permanent or slot lockable. To facilitate early development, slots 10-12 are set to slot lockable for the prototype units.

#### 3.2.1.4 Secure Boot

The `SecureBoot` command is enabled for the ATECC608C-TFLXTLS. This allows the system to cryptographically validate its firmware via a boot loader before performing a full boot. This functionality can also be used to validate new firmware images before they are loaded.

The secure boot feature requires establishing a P-256 firmware signing key before it can be used. The private key will be held by the firmware developers for signing the firmware image. The public key needs to be written to the secure boot public key slot and the slot needs to be locked to make it permanent.

For the ATECC608C-TFLXTLS, it is also possible to force the primary private key to require a valid secure boot prior to being authorized for use.

To implement the SecureBoot, several data slots are required.

#### Secure Boot Digest

The Secure Boot Digest is a 32-byte SHA-256 digest calculated over the firmware application code. This digest needs to be updated every time the firmware is updated. For the ATECC608C-TFLXTLS, the digest is stored in Slot #7.

#### Secure Boot Public Key

The Secure Boot public key is used to perform a verify function to validate the Secure Boot Digest and signature. The Secure Boot public key is stored in Slot #15.

#### 3.2.1.5 Secret Key

This slot can be used to store a secret 32-byte value or key. This key can be used with the ATECC608C-TFLXTLS's symmetric key commands (`GenDig`, `MAC`, `CheckMac`, `KDF`, `SHA/HMAC`, `AES`).

Writing this key requires an encrypted write with the IO protection key as the write key. Therefore, the [3.2.1.7. I/O Protection Key](#) must be set before the secret key can be written.

#### 3.2.1.6 AES Key Storage

Commands such as `ECDH` and `KDF` output symmetric keys. These commands can optionally save those keys to a slot for secure storage and use as AES keys. The AES key storage slot has been set as a destination slot for those keys. Multiple AES keys are capable of being stored in a slot.

#### 3.2.1.7 I/O Protection Key

The `Verify`, `ECDH`, `SecureBoot` and `KDF` commands can optionally use the I/O protection feature to encrypt some parameters and validate (via MAC) some responses. This is to help protect against man-in-the-middle attacks on the physical I<sup>2</sup>C bus. However, before this feature can be used, the MCU and ATECC608C-TFLXTLS need to generate and save a unique I/O protection key, essentially

pairing the MCU and ATECC608C-TFLXTLS devices to each other. The pairing process must happen on the first boot.

I/O protection key generation:

1. MCU uses a random command to generate a random 32-byte I/O protection key.
2. MCU saves the I/O protection key in its internal Flash.
3. MCU writes the I/O protection key to the I/O protection key slot.
4. MCU slot locks that slot to make the I/O protection key permanent.

As a pairing check, the MCU could use the `MAC` command to issue a challenge to the I/O protection key and verify that the I/O protection key stored in Flash matches the one in the ATECC608C-TFLXTLS.

### 3.2.1.8 General Data Storage

A number of slots have been set up to support general public data storage. These slots may be used to store any data that are allowed to be publicly accessible. These slots can always be read and written in the clear.

### 3.2.2 Slot Configuration Terminology

The following section provides a set of terms used to discuss configuration options. The terms are arranged alphabetically.

Term	Description
<b>AES Key</b>	Slot can be used as a key source for <code>AES</code> commands. The AES key is 128 bits in width for the ATECC608C-TFLXTLS.
<b>Always Write</b>	Slot can be written in the clear with the <code>Write</code> command.
<b>Clear Read</b>	Slot is considered public (non-secret) and its contents can be read in the clear with the <code>Read</code> command.
<b>ECDH</b>	Elliptic Curve Diffie Hellman. Private key can be used with the <code>ECDH</code> command.
<b>Encrypted Write</b>	Slot can only be written using an encrypted write based on the write key specified.
<b>Ext Sign</b>	Private key can be used to sign external (arbitrary) messages.
<b>Int Sign</b>	Private key can be used to sign internal messages generated by the <code>GenKey</code> or <code>GenDig</code> commands. Used to attest to the device's internal keys and configuration.
<b>Lockable</b>	Slot can be locked at some point in the future. Once locked, the slot contents cannot be changed (read/use only).
<b>No Read</b>	Slot is considered secret and its contents cannot be read with the <code>Read</code> command. Private keys and symmetric secrets must always be configured as No Read.
<b>No Write</b>	Slot cannot be changed with the <code>Write</code> command.
<b>Permanent</b>	Private key is permanent/unchangeable. It is internally generated during factory provisioning.
<b>Updatable</b>	Private key can be overwritten later with a new, random, internally-generated private key. Its initial value is internally generated during factory provisioning.
<b>Validated</b>	Public key can only be used with the <code>Verify</code> command once it has been validated by the parent public key.

### 3.2.3 ATECC608C-TFLXTLS Slot Configuration Summary

The ATECC608C-TFLXTLS has 16 slots that are configured for different use cases. Below is a summary of those slots with their configuration and proposed uses for the ATECC608C-TFLXTLS:

Slot	Use Case	Description	Primary Configuration
0	Primary private key	Primary authentication key.	Permanent, Ext Sign, ECDH
1	Internal sign private key	Private key that can only be used to attest to the internal keys and state of the device. It cannot be used to sign arbitrary messages.	Permanent, Int Sign
2	Secondary private key 1	Secondary private key for other uses.	Updatable, Ext Sign, ECDH, Lockable
3	Secondary private key 2	Secondary private key for other uses.	Updatable, Ext Sign, ECDH, Lockable



.....continued			
Slot	Use Case	Description	Primary Configuration
4	Secondary private key 3	Secondary private key for other uses.	Updatable, Ext Sign, ECDH, Lockable
5	Secret key	Storage for a secret key.	No Read, Encrypted write (6), Lockable, AES key
6	IO protection key	Key used to protect the I <sup>2</sup> C bus communication (IO) of certain commands. Requires setup before use.	No read, Always write, Lockable
7	Secure boot digest	Storage location for secure boot digest. This is an internal function, so no reads or writes are enabled.	No read, No write
8	General data	General purpose data storage (416 bytes).	Clear read, Always write, Lockable
9	AES key	Intermediate key storage for ECDH and KDF output.	No read, Always write, AES key
10	Device compressed certificate	Certificate primary public key in the CryptoAuthentication™ compressed format.	Clear read, No write or writable depending on access policies set.
11	Signer public key	Public key for the CA (signer) that signed the device cert.	Clear read, No write or writable depending on access policies set.
12	Signer compressed certificate	Certificate for the CA (signer) certificate for the device certificate in the CryptoAuthentication™ compressed format.	Clear read, No write or writable depending on access policies set.
13	Parent public key or general data	Parent public key for validating/invalidating the validated public key. It can also be used just as a public key or general data storage (72 bytes).	Clear read, Always write, Lockable
14	Validated public key	Validated public key cannot be used ( <i>Verify</i> command) or changed without authorization via the parent public key.	Clear read, Writable after being invalidated, Validated using key in Slot 13
15	Secure boot public key	Secure boot public key.	Clear read, Always write, Lockable

### 3.2.4 ATECC608C-TFLXTLS Detailed Slot Access Policies

Additional flexibility has been built into the Slot Access Policies of the ATECC608C-TFLXTLS device over that of the ATECC608C-TNGTLS. This flexibility occurs in two areas:

1. Whether slots are permanently locked or slot lockable.
2. Whether Secure Boot is connected to a key and the Persistent Latch.

#### Slot Locking Options

Slot locking options are called out for each individual slot and will be one of two types.

**Slot Lockable** A slot that has the slot lock option set allows for the end user to lock the slot at some point in the future after the initial manufacturing phase. This can be used to allow for a key to be set during a subsequent manufacturing step outside of Microchip or by the end user. The slot can be locked using the `Lock` command. Once the slot has been locked, no future modifications to the data in the slot is possible.

**Permanent Lock** A permanently locked slot is never able to be updated once it leaves the Microchip manufacturing facilities. The correct data or key must be provided to Microchip prior to the provisioning of these devices.

#### Secure Boot Option

The Secure Boot Access Policies provide an option to limit what commands are run prior to a successful secure boot or to provide unlimited command access. The Private Key in Slot 0 may be set to require a Secure Boot before this key will be authorized for use for most commands. To use this feature, a change to the SecureBoot Configuration Settings and to the Key Configuration values are required. These configuration changes will set the Persistent Latch upon a successful Secure Boot. The Slot Access Policy changes for Slot 0 tie usage of the key to the Persistent Latch being set.

#### Persistent Latch Operation

The Persistent Latch will retain state even during Idle and Sleep modes. This allows for a single Secure Boot operation to be run only once after initial power-up. If the device supply voltage

goes below the minimum allowed value, the Persistent Latch will be reset and a new Secure Boot operation will need to be performed.

### Prototype Units

Prototype units come with a specific default configuration that cannot be changed. The default configuration have all slots options set to Slot Lockable. This provides maximum flexibility when developing software to reprogram keys by an application. The final configuration does not need to be set this way. The Secure Boot option is not available with the prototype units. This option can only be selected for production units. Prototype units are also only available with an I<sup>2</sup>C interface.

### Detailed Slot Configurations

The following tables provide a more detailed description of the slot configuration and key configuration settings for each configured slot on the device. Relevant commands and command modes applicable to each configured slot are included. The table provides all allowed Key and Slot Configuration Values available for the ATECC608C-TFLXTLS device on a slot by slot basis. These options are available for both I<sup>2</sup>C and SWI options.

**Table 3-3.** Slot 0 Configuration Information

Slot	Configuration Value	Description of Enabled Features
0	<b>Option 1: Persistent Latch is not connected to Slot</b>	
	Key:	<b>Primary Private Key</b> <ul style="list-style-type: none"> <li>Contains P256 NIST ECC private key</li> <li>The corresponding public key can always be generated</li> <li>Random nonce is required</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Slot is secret</li> <li>Can sign external messages</li> <li>Can use with ECDH command</li> </ul>
	<b>Option 2: Slot is Connected to Persistent Latch</b>	
	Key:	<ul style="list-style-type: none"> <li>Same as Option 1</li> <li>Persistent Disable Option Enabled</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Same as Option 1</li> </ul>

**Table 3-4.** Slot 1 Configuration Information

Slot	Configuration Value	Description of Enabled Features
1	Key:	<b>Internal Sign Private Key</b> <ul style="list-style-type: none"> <li>Contains P256 NIST ECC private key</li> <li>The corresponding public key can always be generated</li> <li>Random nonce is required</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Slot is secret</li> <li>Can sign internal messages generated by GenDig or GenKey</li> <li>ECDH disabled</li> </ul>

**Table 3-5.** Slot and Key Configuration Slots 2-4

Slot	Configuration Value	Description of Enabled Features
2,3 or 4	<b>Option 1: Slot Lockable</b>	



.....continued

Slot	Configuration Value	Description of Enabled Features
	Key:	<b>Secondary Private Keys 1-3</b> <ul style="list-style-type: none"> <li>Contains P256 NIST ECC private key</li> <li>The corresponding public key can always be generated</li> <li>Random nonce is required</li> <li>This slot can be individually locked</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>GenKey can be used to generate a new ECC private key in this slot prior to locking</li> <li>Slot is secret</li> <li>Can sign external messages</li> <li>Can use with ECDH command</li> </ul>
<b>Option 2: Permanent Key</b>		
	Key:	<ul style="list-style-type: none"> <li>Same as Option 1 except slot is permanently locked</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Same as Option 1 except GenKey can not be used</li> </ul>

Table 3-6. Slot 5 Configuration Information

Slot	Configuration Value	Description of Enabled Features
5	<b>Option #1 Slot Lockable</b>	
	Key:	<b>Secret Key</b> <ul style="list-style-type: none"> <li>Slot can store up to 2 AES 128-bit (16 byte) symmetric keys</li> <li>This slot can be individually locked</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>New symmetric key can be written with an encrypted write only</li> <li>Key in slot 6 is the key used to encrypt the write</li> <li>The contents of the slot are secret</li> <li>Slot cannot be used for the CheckMac Copy command</li> </ul>
<b>Option #2 Permanent Key</b>		
	Key:	<ul style="list-style-type: none"> <li>Same as Option 1 except slot is permanently locked</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Same as Option 1 except an Encrypted Write can not be performed</li> </ul>

Table 3-7. Slot 6 Configuration Information

Slot	Configuration Value	Description of Enabled Features
6	<b>Option #1: Slot is Lockable</b>	
	Key:	<b>IO Protection Key</b> <ul style="list-style-type: none"> <li>Can contain a SHA256 symmetric key or other data. If the IO protection key is not used, this slot can be used for other data</li> <li>A random nonce is required when this key is used</li> <li>This slot can be individually locked</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Data can be written in the Clear</li> <li>The contents of this slot are secret and cannot be read</li> <li>Slot cannot be used for the CheckMac Copy command</li> </ul>
<b>Option 2: Permanent Lock</b>		
	Key:	<ul style="list-style-type: none"> <li>Same as Option 1 except slot is permanently locked</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Same as Option 1 except the slot cannot be written/</li> </ul>



In general, the I/O protection key stored in Slot 6 must be left to be Slot Lockable. In most cases the I/O Protection key is often unique to each device. If for some use case the I/O Protection key is the same for all devices then a Permanent Lock Option can be selected.

**Table 3-8.** Slot 7 Configuration Information

Slot	Configuration Value	Description of Enabled Features
7	Key:	<b>Secure Boot Digest</b> <ul style="list-style-type: none"> <li>This slot is designated to be used for other data.</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>This slot cannot be directly written or read</li> <li>This slot is secret and cannot be used by the <code>MAC</code> command</li> <li>This slot cannot be used for <code>CheckMac Copy</code> command</li> </ul>

**Table 3-9.** Slot 8 Configuration Information

Slot	Configuration Value	Description of Enabled Features
8	<b>Option 1: Slot Lockable</b>	
	Key:	<b>General Data</b> <ul style="list-style-type: none"> <li>This slot is designated for use with general data</li> <li>Slot is lockable</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Clear text writes and reads are permitted to this slot</li> <li>Slot cannot be used for the <code>CheckMac Copy</code> command</li> </ul>
	<b>Option 2: Permanent Lock</b>	
	Key:	<ul style="list-style-type: none"> <li>Same as Option 1 except slot is permanently locked</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Same as Option 1 except the slot cannot be written/</li> </ul>

**Table 3-10.** Slot 9 Configuration Information

Slot	Configuration Value	Description of Enabled Features
9	Key:	<b>AES Key</b> <ul style="list-style-type: none"> <li>Slot can store up to four AES 128-bit symmetric keys</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Clear text writes are allowed to this slot</li> <li>This slot is secret</li> <li>Slot cannot be used for the <code>CheckMac Copy</code> command</li> </ul>

**Table 3-11.** Slot 10 Configuration Information

Slot	Configuration Value	Description of Enabled Features
10	<b>Option 1: Permanently Locked</b>	

.....continued

Slot	Configuration Value	Description of Enabled Features
	Key:	<b>Device Compressed Certificate</b> <ul style="list-style-type: none"> <li>Slot defined to store other data</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Data cannot be overwritten</li> <li>Data can be read in the clear</li> </ul>
	<b>Option 2: Slot Lockable</b> <i>Note: This Configuration is Used for Prototype Units</i>	
	Key:	<ul style="list-style-type: none"> <li>All features as shown in Option 1</li> <li>Slot is lockable</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Same as Option 1 except the slot can be written</li> </ul>

**Table 3-12.** Slot 11 Configuration Information

Slot	Configuration Value	Description of Enabled Features
11	<b>Option 1: Permanently Locked</b>	
	Key:	<b>Signer Public Key</b> <ul style="list-style-type: none"> <li>Slot is defined for ECC key</li> <li>ECC key is a public key</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Data cannot be overwritten</li> <li>Data can be read in the clear</li> </ul>
	<b>Option 2: Slot Lockable</b> <i>Note: This Configuration is Used for Prototype Units</i>	
	Key:	<ul style="list-style-type: none"> <li>All features as shown in Option 1</li> <li>Slot is lockable</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Same as Option 1 except the slot can be written</li> </ul>

**Table 3-13.** Slot 12 Configuration Information

Slot	Configuration Value	Description of Enabled Features
12	<b>Option 1: Permanently Locked</b>	
	Key:	<b>Signer Compressed Certificate</b> <ul style="list-style-type: none"> <li>Slot defined to store other data</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Data cannot be overwritten</li> <li>Data can be read in the clear</li> </ul>
	<b>Option 2: Slot Lockable</b> <i>Note: This Configuration is Used for Prototype Units</i>	
	Key:	<ul style="list-style-type: none"> <li>All features as shown in Option 1</li> <li>Slot is lockable</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Same as Option 1 except the slot can be written</li> </ul>

**Table 3-14.** Slot 13 Configuration Information

Slot	Configuration Value	Description of Enabled Features
13	<b>Option 1: Slot Lockable</b>	

.....continued

Slot	Configuration Value	Description of Enabled Features
	Key:	<b>Parent Public Key or General Data</b> <ul style="list-style-type: none"> <li>Slot is defined for ECC key</li> <li>Slot is lockable</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Slot can be written in the clear (unless locked)</li> <li>Slot can always be read</li> </ul>
	<b>Option 2: Permanently Locked</b>	
	Key:	<ul style="list-style-type: none"> <li>Same as Option 1 except the slot is permanently locked</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Same as Option 1 except the slot cannot be written</li> </ul>



**Important:** If Slot 13 is configured as a Parent Public Key, in general it must be set to a Permanent Key and must not be updatable. For general data, either option can be selected.

**Table 3-15.** Slot 14 Configuration Information

Slot	Configuration Value	Description of Enabled Features
14	Key:	<b>Validated Public Key</b> <ul style="list-style-type: none"> <li>Slot is defined for ECC key</li> <li>Public key can be used by the <code>Verify</code> command if the key has been validated</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Write mode set to <code>PubInvalid</code></li> <li>Can write to slot if key is invalidated first</li> <li>Slot can always be read in the clear</li> </ul>

**Table 3-16.** Slot 15 Configuration Information

Slot	Configuration Value	Description of Enabled Features
15	<b>Option 1: Slot is Lockable</b>	
	Key:	<b>Secure Boot Public Key</b> <ul style="list-style-type: none"> <li>Slot is defined for ECC key</li> <li>Slot is lockable</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Always writable unless locked</li> <li>Slot can always be read</li> </ul>
	<b>Option 2: Permanently Locked</b>	
	Key:	<ul style="list-style-type: none"> <li>Same as Option 1 except the slot is permanently locked</li> </ul>
	Slot:	<ul style="list-style-type: none"> <li>Same as Option 1 except the slot cannot be written</li> </ul>

### 3.3 ATECC608C-TFLXTLS EEPROM One Time Programmable (OTP) Zone

The OTP zone of 64 bytes (512 bits) is part of the EEPROM array and is used for read-only storage. It is organized as two blocks of 32 bytes each. For the ATECC608C-TFLXTLS, the OTP zone is shipped pre-locked and contains the following information:

```
4B 51 70 32 5A 6B 44 38 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

The data byte values written into the OTP zone are always available for reading using either 4- or 32-byte reads but can never be modified.

**NOTICE**

**Notice:** The bytes in the OTP zone may change over time. These values should not be used in any cryptographic calculations.

## 4. Static RAM (SRAM) Memory

The device also includes an SRAM array that is used to store the input command or output result, nonces, intermediate computation values, ephemeral keys, the SHA context, etc. The contents of the SRAM can never be read directly; only used internally by the secure element. The entire contents of this memory are invalidated whenever the device goes into Sleep mode or the power is removed.

The SRAM Array consists of the following buffers:

### TempKey

TempKey is the primary storage register in the SRAM array that can be used to store various intermediate values generated by various commands. TempKey is 64 bytes long and is divided into an upper and lower half. The contents of this register can never be read from the device (although the device itself can read and use the contents internally).

### Message Digest Buffer

The Message Digest Buffer is a 64-byte register that is used to convey the input message digest to the `Verify` and `Sign` commands when the TempKey register is needed to retain different information. The `SHA` command can write a digest directly to this register to simplify external host programming.

### Alternate Key Buffer

The Alternate Key Buffer is a 32-byte register that can be used by the `KDF` command to store keys when the TempKey register is needed to retain different information. It can be written to a fixed input value by the `Nonce` command or to a secret value by the `KDF` command.

### SHA Context Buffer

The SHA context buffer allows for the generation of a digest to be interrupted to do other functions or to generate other digests. The `SHA` command uses a standard three-phase flow: Initialize, Update and Finalize. In many situations, the Update phase is run many times. Internal SRAM memory is used to store the intermediate state, aka SHA context, between these phases.

## 5. General Command Information

The following sections provide some general information on the basic I/O transactions, command structure, error codes, memory addressing and formatting of keys and signatures that are used in the ATECC608C-TFLXTLS.

### 5.1 I/O Transactions

The ATECC608C-TFLXTLS uses the I<sup>2</sup>C protocol to communicate with a host microcontroller. Security commands are sent to the device and responses are received from the device within a transaction that is constructed in the following way:

**Table 5-1.** I/O Transaction Format

Byte	Name	Meaning
0	Count	Number of bytes to be transferred to (or from) the device in the group, including the count byte, packet bytes and checksum bytes. Therefore, the count byte must always have a value of (N+1), where N is equal to the number of bytes in the packet plus the two checksum bytes. For a group with one count byte, 50 packet bytes and two checksum bytes, the count byte must be set to 53. The maximum size group (and value of count) is 155 bytes and the minimum size group is four bytes. Values outside this range will cause the device to return an I/O error.
1 to (N-2)	Packet	Command, parameters and data or response. See <a href="#">5.2. Command Packets</a> for general command packet information or <a href="#">6. Device Commands</a> for specific parameters for each command.
N-1, N	Checksum	CRC-16 verification of the count and packet bytes. The CRC polynomial is 0x8005. Prior to the start of the CRC calculation, the CRC register is initialized to zero. After the last bit of the count and packet is transmitted, the internal CRC register must have a value that matches the checksum bytes in the block. The first CRC byte transmitted (N-1) is the LSB of the CRC value, so the last byte of the group is the MSB of the CRC.

The ATECC608C-TFLXTLS is designed to have the count value in the input group consistent with the size requirements that are specified in the command parameters. If the count value is inconsistent with the command opcode and/or parameters within the packet, the ATECC608C-TFLXTLS responds in different ways depending upon the specific command. The response may either include an error indication or some input bytes may be silently ignored.

### 5.2 Command Packets

The command packet is broken down as shown in [Table 5-2](#):

**Table 5-2.** Command Packets

Byte	Name	Meaning
0	Opcode	The command code. See <a href="#">6. Device Commands</a> .
1	Param1	The first parameter; always present.
2-3	Param2	The second parameter; always present.
0-155	Data	Optional remaining input data.

After the ATECC608C-TFLXTLS receives all the bytes in a group, the device transitions to the Busy state and attempts to execute the command. Neither status nor results can be read from the device when it is busy. During this time, the I/O interface of the device ignores all transitions on the I<sup>2</sup>C SDA input signal.

### 5.3 Status/Error Codes

The device does not have a dedicated STATUS register, so the output FIFO is shared among status, error and command results. All outputs from the device are returned to the system as complete groups which are formatted identically to input groups:

- Count
- Packet
- Two byte CRC

After the device receives the first byte of an input command group, the system cannot read anything from the device until the system sends all the bytes to the device.

After the wake and execution of a command, there will be error, status or result bytes in the device's output register that can be retrieved by the system. For a four bytes length of that group, the codes returned are detailed in [Table 5-3](#). Some commands return more than four bytes when they execute successfully. The resulting packet description is listed in [6. Device Commands](#).

CRC errors are always returned before any other type of error. They indicate that an I/O error occurred and that the command may be resent to the device. No particular precedence is enforced among the remaining errors if more than one occurs.

**Table 5-3. Status/Error Codes in Four Byte Groups**

State Description	Error/Status	Description
Successful Command Execution	0x00	Command executed successfully.
CheckMac or Verify Mismatch	0x01	The CheckMac or Verify command was properly sent to the device, but the input response did not match the expected value.
Parse Error	0x03	Command was properly received but the length, command opcode or parameters are illegal regardless of the state (volatile and/or EEPROM configuration) of the ATECC608C-TFLXTLS. Changes in the value of the command bits must be made before it is re-attempted.
ECC Fault	0x05	A computation error occurred during ECC processing that caused the result to be invalid. Retrying the command may result in a successful execution.
Self Test Error	0x07	There was a Self Test error and the chip is in Failure mode waiting for the failure to be cleared.
Health Test Error	0x08	There was a random number generator Health Test error and the chip fails subsequent commands requiring a random number until it is cleared.
Execution Error	0x0F	Command was properly received but could not be executed by the device in its current state. Changes in the device state or the value of the command bits must be made before it is re-attempted.
After Wake, Prior to First Command	0x11	Indication that the ATECC608C-TFLXTLS has received a proper Wake token.
Watchdog About to Expire	0xEE	There is insufficient time to execute the given command before the WDT expires. The system must reset the WDT by entering the Idle or Sleep modes.
CRC or other Communications Error	0xFF	Command was not properly received by the ATECC608C-TFLXTLS and must be retransmitted by the I/O driver in the system. No attempt was made to parse or execute the command.

## 5.4 Address Encoding

The following subsections provide detailed information on how to address the various memory zones of the ATECC608C-TFLXTLS device.

### 5.4.1 Configuration Zone Addressing

The Configuration zone can be accessed either 4 or 32 bytes at a time. Individual bytes cannot be accessed. The Configuration zone address is a 2-byte (16-bit value). Only the lowest five bits of the



address word are used in addressing of the Configuration zone. For the ATECC608C-TFLXTLS device, these addresses can only be used with the read command.

**Table 5-4. Address Format**

Byte 1: Addr[15:8]		Byte 0: Addr[7:0]		
Unused		Unused	Block	Offset
Addr[15:8]		Addr[7:5]	Addr[4:3]	Addr[2:0]

**Table 5-5. Configuration Zone Addresses**

Block # (Addr[4:3])	Offset Value (Addr[2:0])							
	000	001	010	011	100	101	110	111
00	[0:3]	[4:7]	[8:11]	[12:15]	[16:19]	[20:23]	[24:27]	[28:31]
01	[32:35]	[36:39]	[40:43]	[44:47]	[48:51]	[52:55]	[56:59]	[60:63]
10	[64:67]	[68:71]	[72:75]	[76:79]	[80:83]	[84:87]	[88:91]	[92:95]
11	[96:99]	[100:103]	[104:107]	[108:111]	[112:115]	[116:119]	[120:123]	[124:127]

## 5.4.2 OTP Zone Addressing

The OTP zone can be accessed either 4 or 32 bytes at a time. The zone has a total of 64 bytes. Individual bytes cannot be accessed. The OTP zone address is a 2-byte (16-bit value). Only the lowest four bits are used in addressing.

For the ATECC608C-TFLXTLS device, these addresses can only be used with the read command.

**Table 5-6. Address Format**

Byte 1: Addr[15:8]		Byte 0: Addr[7:0]		
Unused		Unused	Block	Offset
Addr[15:8]		Addr[7:4]	Addr[3]	Addr[2:0]

**Table 5-7. OTP Zone Byte Addresses**

Block # (Addr[3])	Block Offset Value (Addr[2:0])							
	000	001	010	011	100	101	110	111
0	[0:3]	[4:7]	[8:11]	[12:15]	[16:19]	[20:23]	[24:27]	[28:31]
1	[32:35]	[36:39]	[40:43]	[44:47]	[48:51]	[52:55]	[56:59]	[60:63]

## 5.4.3 Data Zone Addressing

Read/Write access to the Data zone is much more complex than the Configuration and OTP zones. There are 16 slots and the size of the slots vary. Each slot's access policies individually control whether or not a slot has the ability to be read or written.

For the ATECC608C-TFLXTLS:

- Data Slots 8-9, 13 and 15 can be written as clear text.
- Data Slots 5-6 can be written with encrypted text.
- Data Slots 8 and 10-15 can be read as clear text.
- Any slots not specified cannot be read or written.

**Table 5-8. Address Format by Data Slot Size**

Data Zone	Byte 1: Addr[15:8]		Byte 0: Addr[7:0]		
	Unused	Block	Unused	Slot	Offset
Data Slots[7:0]	Addr[15:9]	Addr[8]	Addr[7]	Addr[6:3]	Addr[2:0]
Data Slot[8]	Addr[15:12]	Addr[11:8]	Addr[7]	Addr[6:3]	Addr[2:0]

.....continued

Data Zone	Byte 1: Addr[15:8]		Byte 0: Addr[7:0]		
	Unused	Block	Unused	Slot	Offset
Data Slots[15:9]	Addr[15:10]	Addr[9:8]	Addr[7]	Addr[6:3]	Addr[2:0]

### Data Slots[7:0]

To fully access one of these slots, require two 32-byte accesses or nine 4-byte accesses.

**Table 5-9.** Data Zone Addresses Slots 0-7

Slot# (Addr[6:3])	Block # (Addr[8])	Block Offset Value (Addr[2:0])							
		000	001	010	011	100	101	110	111
0x0 to 0x7	00	[0:3]	[4:7]	[8:11]	[12:15]	[16:19]	[20:23]	[24:27]	[28:31]
	01	[32:35]	Not Valid	Not Valid	Not Valid	Not Valid	Not Valid	Not Valid	Not Valid

### Data Slot[8]

To fully access this slot, require thirteen 32-byte accesses or 104 4-byte accesses or a combination of the two methods.

**Table 5-10.** Data Zone Addressing Slot 8

Slot# (Addr[6:3])	Block # (Addr[8])	Block Offset Value (Addr[2:0])							
		000	001	010	011	100	101	110	111
0x8	0x0	[0:3]	[4:7]	[8:11]	[12:15]	[16:19]	[20:23]	[24:27]	[28:31]
	0x1	[32:35]	[36:39]	[40:43]	[44:47]	[48:51]	[52:55]	[56:59]	[60:63]
	...	...	...	...	...	...	...	...	...
	0xC	[384:387]	[388:391]	[392:395]	[396:399]	[400:403]	[404:407]	[408:411]	[412:415]

### Data Slots[15:9]

To fully access these slots, require three 32-byte accesses or eighteen 4-byte accesses or a combination of the two methods.

**Table 5-11.** Data Zone Addressing Slots 9-15

Slot# (Addr[6:3])	Block # (Addr[8])	Block Offset Value (Addr[2:0])							
		000	001	010	011	100	101	110	111
0x9 to 0xF	00	[0:3]	[4:7]	[8:11]	[12:15]	[16:19]	[20:23]	[24:27]	[28:31]
	01	[32:35]	[36:39]	[40:43]	[44:47]	[48:51]	[52:55]	[56:59]	[60:63]
	10	[64:67]	[68:71]	Not Valid	Not Valid	Not Valid	Not Valid	Not Valid	Not Valid

## 5.5 Formatting of Keys, Signatures and Certificates

The following sections provide detailed formatting information for ECC keys, Signatures and Compressed certificates.

### 5.5.1 ECC Key Formatting

The format for public and private keys depends on the command and key length. In general, the Most Significant Bytes (MSB) appear first on the bus and at the lowest address in memory. In the remainder of this section below, the bytes on the left side of the page are the MSBs. Microchip recommends all pad bytes be set to zero for consistency.

- ECC private keys appear to the user only as the input parameter to the `PrivWrite` command. This parameter is always 36 bytes in length and the first four bytes (32 bits) are all pad bits. ECC public keys appear as the input or output parameters to several commands, and they can also be stored in EEPROM. They are composed of an X value first on the bus or in memory, followed by a Y value. They are formatted differently depending on the situation as noted below:

- **The public key is an output of the GenKey command or an input to the Verify command:**  
32 bytes of X, then 32 bytes of Y. (36 bytes) There are no pad bytes.
- **Write command:**  
Public keys can be written directly to the EEPROM using the Write command and are always 72 bytes long, formatted as follows: 4-pad bytes, 32 bytes of X, four pad bytes, then 32 bytes of Y.
- **GenKey command:**  
SHA Message: Public keys can be hashed and placed in TempKey by the GenKey command. The SHA message contains various bytes that are independent of the size of the key. These are followed by 25 bytes of pad, followed by 32 bytes of X, then by 32 bytes of Y.
- **Verify command:**  
SHA Message: When used to validate a stored public key, the Verify command expects an input signature created over a SHA-256 digest of a key stored in memory. Such an inner SHA calculation is always performed over 72 bytes formatted as they are stored in EEPROM as 4-pad bytes, 32 bytes of X, 4-pad bytes, then 32 bytes of Y.

When a public key is configured to be validated by the Verify command, the Most Significant four bits of the first byte in memory are used internally by the device to save the validation state. They are always set to the invalid state (0xA) by the Write command, and then may be set to the Valid state (0x5) by the Verify command.

The lowest levels of the I/O protocols are described below. Above the I/O protocol level, the exact same bytes are transferred to and from the device to implement the commands. Error codes are documented in the following sections.

### 5.5.1.1 Public Key Formats

The ATECC608C-TFLXTLS works with the P-256 elliptic curve public keys in two formats. The following example illustrates those two formats in detail.

For the following examples, we'll use a sample public key, with the X and Y integers expressed as fixed-width big-endian unsigned integers:

```
X: b2be345ad7899383a9aab4fb968b1c7835cb2cd42c7e97c26f85df8e201f3be8
Y: a82983f0a11d6ff31d66ce9932466f0f2cca21ef96bec9ce235b3d87b0f8fa9e
```

#### Command Public Key Format

Any command that returns a public key (GenKey) or accepts a public key as a parameter (Verify and ECDH) will format the public key as the X and Y big-endian unsigned integers concatenated together for a total of 64 bytes.

For example:

```
b2be345ad7899383a9aab4fb968b1c7835cb2cd42c7e97c26f85df8e201f3be8
a82983f0a11d6ff31d66ce9932466f0f2cca21ef96bec9ce235b3d87b0f8fa9e
```

#### Stored Public Key Format

When storing a public key in a slot for use with the Verify command, Verify or SecureBoot commands, the X and Y integers will be padded out to 36 bytes and concatenated together for a total of 72 bytes.

For example:

```
00000000b2be345ad7899383a9aab4fb968b1c7835cb2cd42c7e97c26f85df8e201f3be8
00000000a82983f0a11d6ff31d66ce9932466f0f2cca21ef96bec9ce235b3d87b0f8fa9e
```

**Note:** Only Slots 8-15 are large enough to hold a public key.

### Stored Validated Public Key Format

A validated or invalidated public key format is the same as a stored public key format with the exception of the four Most Significant bits of the LSB. If a key is validated, the Least Significant Nibble will be 0x5 and 0xA if invalidated. These values can be changed by the `Verify` command in Validate or Invalidate mode. When written, the key will be initially invalidated.

Validated Public Key Example:

```
50000000b2be345ad7899383a9aab4fb968b1c7835cb2cd42c7e97c26f85df8e201f3be8
00000000a82983f0a11d6ff31d66ce9932466f0f2cca21ef96bec9ce235b3d87b0f8fa9e
```

Invalidated Public Key Example:

```
A0000000b2be345ad7899383a9aab4fb968b1c7835cb2cd42c7e97c26f85df8e201f3be8
00000000a82983f0a11d6ff31d66ce9932466f0f2cca21ef96bec9ce235b3d87b0f8fa9e
```

**Note:** Only Slots 8-15 are large enough to hold a public key.

### 5.5.2 Signature Format

The ECDSA signature that is generated and output by the `Sign` command or input to the `Verify` or `SecureBoot` command is always 64 bytes in length. The signature is divided into R and S components. Both components are 32 bytes in length and R always appears before S on the bus. Each portion of the signature appears MSB first on the bus, meaning the MSB of the signature is in the lowest memory location.

#### Example R/S Signature

Any command that returns a signature (`Sign`) or accepts a signature as a parameter (`Verify` and `SecureBoot`) will format the signature as the R and S big-endian unsigned integers concatenated together for a total of 64 bytes.

For example:

```
R: 7337887F8C39DF79FD8BF88DDFBFB9DB15D7B1AD68196AE3FB0CE5BFA2842DF3
S: 72868A43A42831E950E1DA9F73B29F5C0ED8A96B2889E3CBBE8E61EA6C67F673
```

### 5.5.3 Certificate Storage

The amount of storage required for a full X.509 Certificate within the device can rapidly use up multiple EEPROM memory slots. Depending on the actual application, it may or may not be desirable to use these slots for certificate storage. Due to these memory limitations, Microchip has defined an encoding that allows for a full X.509 Certificate to be reconstructed from a minimal amount of information.

The host system would actually be responsible for reconstructing the full X.509 Certificate but how to do this will be determined by the data stored in the encoded certificate. Data that are common to all devices for a given system can readily be stored in the host system. Other data can readily be calculated or extracted from data that are already stored in the device. [Table 5-12](#) indicates the type of data that are stored in an X.509 Certificate and how it can be encoded to fit into a single 72-byte slot.

**Table 5-12.** Certificate Storage

X.509 Certificate		Encoded Certificate		
X.509 Element	Size (Bytes)	Encoded Certificate Element	Device Cert (Bits)	Signer Cert (Bits)
Serial Number	8-20	Serial number source	4	4
Issue Date	13	Compressed format	19	19
Expiry Date	13	# of years before expiration	5	5

.....continued

X.509 Certificate		Encoded Certificate		
X.509 Element	Size (Bytes)	Encoded Certificate Element	Device Cert (Bits)	Signer Cert (Bits)
Signer ID <sup>2</sup>	4	ID of the specific signer used to sign the certificate (device cert) or of the signer itself (signer cert)	16	16
AuthorityKeyIdentifier	20	SHA1 HASH of the authority public key	0	0
SubjectKeyIdentifier	20	SHA1 HASH of the subject public key	0	0
Signature R	32	Stored in device	256	256
Signature S	32	Stored in device	256	256
Public Key X <sup>1</sup>	32	Calculated from the private key or stored in the device <sup>1</sup>	0	256
Public Key Y <sup>1</sup>	32	Calculated from the private key or stored in the device <sup>1</sup>	0	256
n/a	0	Cert format	4	4
n/a	0	Template ID	4	4
n/a	0	Chain ID	4	4
n/a	0	Reserved/User Defined	8	8
Total	(206-218 bytes)	—	576 bits (72 bytes)	1088 bits (136 bytes)

**Notes:**

1. For the device certificate, the device public key can be regenerated from the private key. For the signer certificate, the public key is typically stored in a separate slot.
2. For the device certificate, the ID of the signer used to sign the certificate is stored. For the signer certificate, the actual ID of the signer is stored so that the device can identify it.

Slot 8 contains a total of 416 bytes. Depending on the size of the serial number stored in the cert, it may or may not be possible to store two complete certificates. Often within devices where a chain of trust has been created, the device certificate, the signer certificate and the signer public key must be stored within the device.

For more information, see the [Compressed Certificate Definition](#) Application Note.

## 6. Device Commands

The following section details all of the commands broken out by Command mode that are allowed in the ATECC608C-TFLXTLS. The commands have been broken into three categories:

### 1. General Device Commands

These commands fall into two categories:

- General device access commands that are used to send data to the device or retrieve data but typically do not perform any cryptographic functions.
- General cryptographic commands that can be used by the device or the system but typically do not operate on specific data slots.

### 2. Asymmetric Cryptography Commands

These commands perform asymmetric cryptographic operations, such as key generation, message signing and message verification that utilize an ECC public or private key. These commands are limited to use on ECC Data zone slots.

### 3. Symmetric Cryptography Commands

These commands perform a symmetric cryptographic function, such as generating a digest or MAC, key derivation or AES encryption and decryption.

### Input Parameters for all Commands

Multibyte input parameters are shown as big-endian (MSB first) values in the input parameters tables unless otherwise specified. Note that the ATECC608C-TFLXTLS device actually expects the data to be sent little-endian (LSB first).

**Table 6-1.** Commands, Descriptions and Command Categories

Command	Description	Command Category
AES	Execute the AES-ECB Encrypt or Decrypt functions. Calculate a Galois Field Multiply.	Symmetric Cryptography Command
CheckMac	Verify a MAC calculated on another CryptoAuthentication™ device.	Symmetric Cryptography Command
Counter	Read or increment one of the monotonic counters	General Device Commands
ECDH	Generate an ECDH pre-master secret using stored private key and input public key.	Asymmetric Cryptography Command
GenDig	Generate a data digest from a random or input seed and a stored value.	Symmetric Cryptography Command
GenKey	Generate an ECC public key. Optionally generate an ECC private key.	Asymmetric Cryptography Command
Info	Return device state information.	General Device Commands
KDF	Implement the PRF or HKDF key derivation functions	Symmetric Cryptography Command
Lock	Prevent further modifications to a zone or slot of the device.	General Device Commands
MAC	Calculate digest (response) from key and other internal data using SHA-256.	Symmetric Cryptography Command
Nonce	Generate a 32-byte random number and an internally stored Nonce.	General Device Commands
Random	Generate a random number.	General Device Commands
Read	Read 4 or 32 bytes from the device, with or without authentication and encryption.	General Device Commands
SecureBoot	Validate code signature or code digest on power-up	Asymmetric Cryptography Command
SelfTest	Test the various internal cryptographic computation elements	General Device Commands

.....continued		
Command	Description	Command Category
Sign	ECDSA signature calculation.	Asymmetric Cryptography Command
SHA	Compute a SHA-256 or HMAC digest for general purpose use by the system.	General Device Commands
UpdateExtra	Update bytes 84 or 85 within the Configuration zone after the Configuration zone is locked.	General Device Commands
Verify	ECDSA verify calculation.	Asymmetric Cryptography Command
Write	Write 4 or 32 bytes to the device, with or without authentication and encryption.	General Device Commands

## 6.1 General Device Commands

The following table provides a summary of the general device commands:

**Table 6-2.** General Device Commands

Command Name	Description
Counter	Increments and reads the monotonic counters
Info	Used to read revision and status information from the device
Lock	Used to lock the individual lockable slots in the device
Nonce	Used to generate or pass a number used once into the device
Random	Used to generate a 32-byte random number used by the system
Read	Used to read various zones of the device
SelfTest	Tests the various internal cryptographic computation elements
SHA	Computes a SHA-256 or HMAC digest for general purpose use by the system
UpdateExtra	Updates bytes 84 or 85 within the Configuration zone after the Configuration zone is locked
Write	Used to write 4 or 32 bytes to the device, with or without authentication and encryption

### 6.1.1 Counter Command

The `Counter` command reads the binary count value from one of the two monotonic counters located on the device within the Configuration zone. The maximum value that the counter may have is 2,097,151. Any attempt to count beyond this value will result in an error code. The counter is designed to never lose counts even if the power is interrupted during the counting operation. In some power loss conditions, the counter may increment by a value of more than one.

For the ATECC608C-TFLXTLS, the counters are not attached to any keys but may still be used by the system. Each count is set to its default value and can count to the maximum value.

### 6.1.2 Info Command

The `Info` command is used to read the status and state of the device. This information is useful in determining errors or to operate various commands.

### 6.1.3 Lock Command

For the ATECC608C-TFLXTLS, the Configuration zone has already been locked and the access policies of the Data zone have already been set. However, several of the data slots can still be updated through the use of other commands. If so desired, some of these slots can be permanently locked from future updates by using the Slot Locking mode of the `Lock` command.

#### 6.1.4 Nonce Command

The `Nonce` command generates a nonce (number used once) for use by a subsequent command by combining a random number (which can be generated internally or externally) with an input value from the system. The resulting nonce is stored internally in three possible buffers: TempKey, Message Digest Buffer and Alternate Key Buffer. Instead of generating a nonce, a value may be passed to the device if so desired.

#### 6.1.5 Random Command

The `Random` command generates a random number to be used by the system. Random numbers are generated via the internal NIST 800-90 A/B/C random number generator. The output of the command is always a 32-byte number placed on the bus. The number cannot be stored in any data slot or SRAM location.

#### 6.1.6 Read Command

The `Read` command can be used to access any of the EEPROM zones of the ATECC608C-TFLXTLS device. Data zone access is limited based on the access policies set for each of the slots. Encrypted reads are possible only on the Data zone slots if specific access policies are set.

#### 6.1.7 SelfTest Command

The `SelfTest` command performs a test of one or more of the cryptographic engines within the ATECC608C-TFLXTLS chip. Some or all of the algorithms will be tested depending on the Input mode parameter.

For the ATECC608C-TFLXTLS device, the `SelfTest` command has been disabled from running automatically after a Power-up or Wake event. However, the command may be executed by the system if so desired. There is no requirement to run this test.

If any self test fails, whether called automatically on power-up, wake or via this command, the chip will enter a Failure state, where chip operation is limited. The stored Failure state is always cleared upon a wake or power cycle.

#### 6.1.8 SHA Command

The `SHA` command computes a SHA-256 or HMAC/SHA digest for general purpose use by the host system. The SHA computation is performed in a special section of internal ATECC608C-TFLXTLS memory (Context Buffer) that is not read nor written by any other commands. Any arbitrary command can be interspersed between the various phases of the `SHA` command without problems. This SHA context is invalidated on power-up and wake. In most cases, if an error occurs during the execution of the `SHA` command, the context is retained without change.

#### 6.1.9 UpdateExtra Command

The `UpdateExtra` command is used to update the `UpdateExtra` and `UpdateExtraAdd` bytes, bytes 84 and 85 respectively, in the Configuration zone. These bytes can only be updated by this command. These bytes are one-time updatable bytes and can only be updated if the current value is 0x00. Trying to update this byte if the value is not 0x00 will result in an error.

For the ATECC608C-TFLXTLS device, the `UpdateExtraAdd` byte (byte 85) has been configured to be an alternate I<sup>2</sup>C address.

#### 6.1.10 Write Command

For the ATECC608C-TFLXTLS, the Configuration zone and OTP zone have been locked and no updates to these zones are possible. Limited write capability exists on the Data zone based on



access policies of each slot. Slots that can be written are described in the submodes of this command.

## 6.2 Asymmetric Cryptography Commands

The Asymmetric Cryptography command set is made up of those commands that are specifically used to generate or use ECC keys. Keys are typically stored in Data zone slots, but, for some commands, could also be in the SRAM array.

**Table 6-3.** Asymmetric Cryptography Commands

Command Name	Description
ECDH	Generates an ECDH pre-master secret using the stored private key and input public key
GenKey	Generates an ECC private key or optionally generates an ECC public key from the stored private key
SecureBoot	Validates code signature or code digest on power-up
Sign	Signs an internal or external message digest using an ECC private key with an ECDSA signature calculation
Verify	Verifies an internal or external message digest using an ECC public key with an ECDSA verify calculation

### 6.2.1 ECDH Command

The `ECDH` command is used to generate a shared secret between two devices. By passing an ECC public key from another device and combining it with the ECC private key stored in a slot or with an ephemeral key stored in TempKey and doing the reverse on the other device, both devices will generate the same shared pre-master secret. This can, then, be further combined with other common data in both sides to generate a shared session key between the devices. The `KDF` command is often used with TLS sessions to further diversify the shared secret.

### 6.2.2 GenKey Command

The `GenKey` command is used to generate ECC private keys, ECC public keys from private keys or generate a public key digest. This command is only applicable for those slots designated to be ECC private or public keys. Running this command on a non-ECC slot will result in an error.

### 6.2.3 SecureBoot Command

The `SecureBoot` command provides support for secure boot of an external MCU or MPU. The general approach is that the boot code within the system will use the ATECC608C-TFLXTLS to assist in validating the application code that is to be subsequently executed. The ATECC608C-TFLXTLS device has been configured to operate in the SecureBoot, Stored Digest mode. The digest will be stored in Slot 7 and the public key required to verify the SecureBoot is stored in Slot 15. The device can optionally be configured to use the persistent latch. Depending on the option selected SecureBoot may or may not be tied to power-up. Please see [3.2.4. Secure Boot Option](#)

In lieu of a return code, a MAC can optionally be generated from a nonce written to TempKey, the IO protection secret and various other data, dependent upon the mode of the command, to prevent tampering with the wire between the host and the ATECC608C-TFLXTLS.

### 6.2.4 Sign Command

The `Sign` command generates a signature using the ECDSA algorithm. The ECC private key in the slot specified by KeyID is used to generate the signature. Multiple modes of the device are available depending on what is being signed.

### 6.2.5 Verify Command

The `Verify` command takes an ECDSA [R,S] signature and verifies that it is correctly generated given an input message digest and public key. In all cases, the signature is an input to the command. The public key can be either stored on the device or provided as an input.

An optional MAC can be returned from the `Verify` command to defeat any man-in-the-middle attacks. If the verify calculation shows that the signature is correctly generated from the input digest, a MAC will be computed based on an input nonce stored in `TempKey` and the value of the I/O protection secret, which is stored in both the ATECC608C-TFLXTLS and the host MCU. MAC outputs can only be generated in External and Stored modes. The I/O protection function must be enabled for MAC computation.

In addition, the `Verify` command can be used to validate or invalidate a stored public key to enable its use or to allow it to be updated. This can only be done for public keys with the appropriate access policies set.

## 6.3 Symmetric Cryptography Commands

The Symmetric Cryptography command set is made of up of those commands associated with the generation or use of Symmetric Keys. Keys are typically stored in Data zone slots, but for some commands could also be in the SRAM memory locations.

**Table 6-4.** Symmetric Cryptography Commands

Command Name	Description
AES	Execute the AES-ECB Encrypt or Decrypt functions. Calculate a Galois Field Multiply.
CheckMac	Verify a MAC calculated on another CryptoAuthentication™ device.
GenDig	Generate a data digest from a random or input seed and a stored value.
KDF	Implement the PRF or HKDF key derivation functions
MAC	Calculate digest (response) from key and other internal data using SHA-256.

### 6.3.1 AES Command

The `AES` Command can be used to encrypt and/or decrypt a 16-byte block of data utilizing an AES key. Note that the key is stored in a 16 Byte (128 bit) location with a given slot or within the first 16 bytes of `TempKey`. Multiple keys may be stored in a given slot and accessed in successive 16-byte boundaries, starting with 0-15 up to the size of the slot, but not exceeding four keys in any slot. For the ATECC608C-TFLXTLS, an AES key may be stored in either Slot 5 or Slot 9. Slot 5 can accommodate up to two AES keys and Slot 9 can accommodate up to four AES keys.

In addition to AES encryption and decryption, the `AES` command may be used to generate a Galois Field Multiply (GFM) in support of other cryptographic operations.

### 6.3.2 CheckMac Command

The `CheckMac` command calculates a MAC response that would have been generated on a different CryptoAuthentication device<sup>1</sup> and then compares the result with the input value. The command returns a boolean result to indicate the success or failure of the comparison.

If a value in `TempKey` is used as an input to the `CheckMac`, then a `Nonce` and/or `GenDig` command must be run prior to the `CheckMac` command.

### 6.3.3 GenDig Command

The `GenDig` command uses a SHA-256 hash to combine a stored or input value with the contents of `TempKey`, which must be validated prior to the execution of this command. The stored value can come from one of the data slots, the Configuration zone, either of the OTP pages or the monotonic counters. The specific mode of the device determines which data are to be included in the `GenDig` calculation.

<sup>1</sup> Devices that generate a compatible MAC response include, ATECC608A/B/C, ATECC508A, ATSHA204A and SHA104. This includes Trust variants associated with the products.

In some cases, it is required to run the `GenDig` prior to the execution of some commands. The command can be run multiple times to include more data in the digest prior to executing a given command. The resulting digest is retained in `TempKey` and can be used in one of four ways:

1. It can be included as part of the message used by the `MAC`, `Sign` or `CheckMac` commands. Because the `MAC` response output incorporates both the data used in the `GenDig` calculation and the secret key from the `MAC` command, it serves to authenticate the data stored in the `Data` and/or `OTP` zones.
2. A subsequent `Read` or `Write` command can use the digest to provide authentication and/or confidentiality for the data, in which case, it is known as a data protection digest.
3. The command can be used for secure personalization by using a value from the transport key array. The resulting data protection digest would, then, be used by write.
4. The input value, typically a nonce from a remote device, is combined with the current `TempKey` value to create a shared nonce in which both devices can attest to the inclusion of the `RNG`.

### 6.3.4 KDF Command

For the ATECC608C-TFLXTLS, the `KDF` command implements several Key Derivation Functions including `PRF` for TLS 1.2, `HKDF` for TLS 1.3 and `AES`. Support for this function is available in `CryptoAuthLib`. See Section 7.2.3. [CryptoAuthLib](#) for more information.

For additional information on the `KDF` command contact Microchip Sales for more information.

### 6.3.5 MAC Command

The Message Authentication Code (`MAC`) command is used to generate a SHA-256 digest of a message, which consists of a key stored in the device, a challenge and other information on the device. The output of this command is the digest of this message.

The normal flow to use this command is as follows:

1. Run the `Nonce` command to load the input challenge and optionally combine it with a generated random number. The result of this operation is a nonce stored internally on the device.
2. Optionally, run the `GenDig` command one or more times to combine stored EEPROM locations in the device with the nonce. The result is stored internally in the device. This capability permits two or more keys to be used as part of the response generation.
3. Run this `MAC` command to combine the output of Step 1 (and Step 2, if desired) with an EEPROM key to generate an output response (i.e., digest).

Alternatively, data in any slot (which does not have to be secret) can be accumulated into the response through the same `GenDig` mechanism. This has the effect of authenticating the value stored in that location.

## 7. Application Information

The ATECC608C-TFLXTLS is a member of the Microchip's Trust&GO CryptoAuthentication™ family of products. The TrustFLEX products are easy to use, simple to implement and allow even low volume customers to implement security into their end system while leveraging Microchip's expertise and infrastructure in secure provisioning.

The ATECC608C-TFLXTLS device has been developed to take the guesswork out of adding security to an IoT- connected product. The product has been pre-configured to readily connect to the IoT Cloud through TLS connections and to provide support for multiple other security use cases including Secure Boot, Disposable and Accessory Authentication and User Data and I/P Protection.

In addition to the actual security device, Microchip has developed a series of tools that seamlessly integrate with our hardware devices to provide an easy path to develop your entire security solution. When the developers use Microchip's software security tools, they eliminate the complexity of setting up their own infrastructure and provide a rapid path to initial prototypes and production.

### 7.1 Use Cases

The ATECC608C-TFLXTLS has been defined to specifically address the IoT market. Through a single set of certificates, the device has been set to directly support the Google IoT Cloud™, Amazon Web Services (AWS®) and the Microsoft® Azure Cloud. Support for other IoT networks can be provided through use of custom certificates uploaded into Slot 8. A brief description of some of the use cases that this device addresses is provided below. These use cases can be implemented separately or in combination with each other. In order to prototype and implement these use cases, Microchip provides both hardware and software tools.

#### Secure TLS Connection

The ATECC608C-TFLXTLS allows the creation of secure TLS connections using a variety of protocols. The device is capable of establishing secure connections to the Google Cloud, to AWS and other cloud providers. Through the various modes of the Key Derivation Function (KDF), appropriate keys can be generated to support TLS1.2, TLS1.3 and earlier secure connection internet protocols.

#### Secure Boot

Protecting the boot image of a microcontroller or microprocessor is a concern for many vendors. By providing a mechanism to verify that the code being run is authentic and has not been modified, the overall integrity of the system is maintained. The ATECC608C-TFLXTLS has been configured to allow Secure Boot by storing the code digest of the system within a data slot of the device. Upon initial execution of the code, the system can regenerate the digest over the system firmware and compare it with the digest stored in the ATECC608C-TFLXTLS, verifying that the firmware has not been tampered with.

#### Disposable/Accessory Authentication

Ensuring the authenticity of system accessories and disposable add-ons is often highly desired by an OEM. Having this ability is crucial in preventing low-cost clones of products that can damage an OEM's reputation for quality, image in the marketplace and overall profit margins. The ATECC608C-TFLXTLS provides the ability to authenticate these types of products by providing a chain-of-trust from device to Root Certificate Authority.

#### I/P and Data Protection

Protecting Intellectual Property (IP) can be crucial to maintaining a company's competitive edge. IP protection describes the way of protecting the firmware or hardware developed by the customer from being copied. Firmware IP protection can be done with just a software-based approach, but the key information inside the firmware still remains quite vulnerable to attacks.

The ATECC608C-TFLXTLS device offers hardware-based secure key storage to ensure that a product with the firmware runs. The devices can perform both the Symmetric authentication

and Asymmetric authentication where the keys are securely stored in the secure element thereby reducing the hacker's ability to extract and modify the keys.

### General Data Storage

Sometimes there is a need to store a small amount of additional information for a given system. The ATECC608C-TFLXTLS can be used for this purpose by utilizing those data slots where data can be readily read and written. This eliminates the need to add an additional EEPROM memory device to just store data.

## 7.2 Development Tools

The ATECC608C-TFLXTLS is supported with multiple hardware and software tools and backend services that provide a path to rapidly develop applications. Initial development can start by using a family of easy-to-use Trust Platform Design Suite tools. These tools provide a graphical way to implement your use case and end with the C code necessary to implement your application.

If your application differs from what the predefined Trust Platform Design Suite tools can provide, then through use of the CryptoAuthLib or the Python® version of CryptoAuthLib and CryptoAuthTools, an application can be developed. CryptoAuthLib is also the backbone of the code that is output from the Trust Platform Design Suite tools.

Full verification of your application can be implemented via hardware tools along with samples of the ATECC608C-TFLXTLS device. The access policies of the device are already set, therefore, the focus revolves just around developing the system level code.

Once the application is complete, the ATECC608C-TFLXTLS devices can be ordered through Microchip Direct.

### 7.2.1 Trust Platform Design Suite

To simplify the implementation process, Microchip developed a web-based Trust Platform Design Suite of tools that will allow developers to go from concept to production via a guided flow. The tools allow you to develop and construct the transaction diagrams and code necessary to implement a particular application within the constraints of the configuration and defined access policies of the ATECC608C-TFLXTLS.

**Note:** More information on these tools can be found on Microchip's [Trust Platform](#) information page.

### 7.2.2 Hardware Tools

There are multiple hardware tools that can help in developing with the ATECC608C-TFLXTLS. Check the Microchip website for the availability of additional tools that are not mentioned here. Specific tools are also mentioned with the specific use case examples.

#### DM320118 - CryptoAuthentication Trust Platform

The [DM320118](#) is a compact development system consisting of an ATSAM21 microcontroller, 1- each of the ATECC608C-TNGTLS, ATECC608C-TFLXTLS and ATECC608C-TCSTM Trust devices, a USB Hub, a mikroBUS connector and an on-board debugger. The kit is intended for use with the Trust Platform Design Suite of tools used to implement various use cases for the ATECC608C-TFLXTLS devices. The kit can be used with either MPLABX or Atmel Studio Design environments to develop additional applications.

#### DT100104 - ATECC608C TRUST

The [DT100104](#) is a mikroBUS™ extension board that contains 1 - ATECC608C-TNGTLS, 3 - ATECC608C-TFLXTLS and 4 - ATECC608C-TCSM device. These boards can be used in lieu of loose sample devices. Each device on the board is individually selected through onboard DIP switches. The board can be directly connected to a DM320118 or any host board that supports a mikroBUS host interface.

### DM320109 - CryptoAuthentication Starter Kit

The [DM320109](#) consists of an ATSAM21-XPRO development board pre-programmed with firmware that can work with CryptoAuthentication Devices. The kit comes with the AT88CKSCKTSOIC-XPRO socket board but you will need to obtain the UDFN version of the board to work with the sample devices which are currently provided only in the UDFN package. Specific samples of the ATECC608C-TFLXTLS will need to be obtained separately.

### AT88CKSCKTUDFN(SOIC)-XPRO

The [AT88CKSCKTUDFN-XPRO](#) and [AT88CKSCKTSOIC-XPRO](#) are generic CryptoAuthentication socket kits that can be used with any Microcontroller development board with an XPRO interface. Specific samples of the ATECC608C-TFLXTLS must be acquired to be used with these kits.

## 7.2.3 CryptoAuthLib

CryptoAuthLib is a software library that supports Microchip's family of CryptoAuthentication devices. Microchip recommends working with this library when developing with the ATECC608C-TFLXTLS. The library implements the API calls necessary to execute the commands detailed in this data sheet.

The library was implemented to readily work with many of Microchip's microcontrollers but can easily be extended through a Hardware Abstraction Layer (HAL) to other microcontrollers, including those made by other vendors.

For more details on these tools, check the information on:

- [CryptoAuthLib – Web Link](#)
- [CryptoAuthLib – GitHub](#)

### API Calls

Each of the commands in the data sheet have one or more API calls that are associated with them. Typically, there is a base API call of the command where all input parameters can be specified. The parameter shown in the commands and subsections can be used with this command. There are also mode variants of each of the API calls. The table below shows examples of commands and base API calls. For the most accurate API information, refer to the GitHub information.

**Table 7-1.** Example Commands to CryptoAuthLib API Calls

Device Command	API Call	Comments
Info	atcab_info_base()	
Write	atcab_write()	
Read	atcab_read_zone()	
SHA	atcab_sha_base()	
Sign	atcab_sign_base()	
Random	atcab_random()	
Verify	atcab_verify()	

## 7.3 TrustFLEX vs. Trust&GO

Trust&GO products have been defined for customers with low volumes that can use a secure off-the-shelf solution. The product's simple onboarding procedure leverages Microchip's secure manufacturing solution and infrastructure. By using this flow, customers do not have to create their own secure manufacturing environment.

However, at times customers may want to have more control over their security environment while still enjoying the simplicity of the Trust&GO product use. The TrustFLEX product was created for these customers. TrustFLEX products are still capable of implementing the use cases of the Trust&GO product but provide additional flexibility for some of the security keys and certificates.

- Same locked configuration as that of the Trust&GO product.

- Same data slot definition as that of the Trust&GO.
- Ability to provision the customer's public key into the device for Secure Boot implementation.
- Ability to do Symmetric Key Authentication. Customers can securely provide their desired Symmetric Keys as part of the secure provisioning process.
- Ability to customize certificate elements and link the certificate chain to the customer's desired PKI.
- Option for either I<sup>2</sup>C or SWI interface devices.

For more information on TrustFLEX products and other provisioning options, see the Microchip [CryptoAuthentication](#) webpages.



## 8. I<sup>2</sup>C Interface

The I<sup>2</sup>C interface uses the SDA and SCL pins to indicate various I/O states to the ATECC608C-TFLXTLS. This interface is designed to be compatible at the protocol level with the Microchip AT24C16 Serial EEPROM operating at 1 MHz.

**Note:** There are many differences between the two devices (for example, the ATECC608C-TFLXTLS and AT24C16 have different default I<sup>2</sup>C addresses); therefore, designers must read the respective data sheets carefully.

The SDA pin is normally pulled high with an external pull-up resistor because the ATECC608C-TFLXTLS client includes only an open-drain driver on its output pin. The bus host may either be open-drain or totem pole. In the latter case, it must be tri-stated when the ATECC608C-TFLXTLS is driving results on the bus. The SCL pin is an input and must be driven both high and low at all times by an external device or resistor.



**Remember:** The I<sup>2</sup>C standard uses the terminology “Master” and “Slave”. The equivalent Microchip terminology used in this document is “Host” and “Client”, respectively.

### 8.1 I/O Conditions

The device responds to the following I/O conditions:

#### 8.1.1 Device is Asleep

When the device is asleep, it ignores all but the Wake condition.

- Wake – Upon the rising edge of SDA, after SDA is held low for a period  $\geq t_{WLO}$ , the device exits the Low-Power mode. After a delay of  $t_{WHI}$ , it will be ready to receive I<sup>2</sup>C commands.
- The device ignores any levels or transitions on the SCL pin when the device is idle or asleep and during  $t_{WLO}$ . At some point during  $t_{WHI}$ , the SCL pin is enabled and the conditions listed in [8.1.2. Device is Awake](#) are honored.

The Wake condition requires that either the system processor manually drive the SDA pin low for  $t_{WLO}$ , or a data byte of  $0 \times 00$  be transmitted at a clock rate sufficiently slow so that SDA is low for a minimum period of  $t_{WLO}$ . When the device is awake, the normal processor I<sup>2</sup>C hardware and/or software can be used for device communications. This includes the I/O sequences required to put the device back into Low-Power (i.e., Sleep) mode.



**Tip:** A simple way to generate a wake pulse is to send a byte of  $0 \times 00$  at 100 kHz. Subsequent commands can be run at a higher frequency.

In the I<sup>2</sup>C mode, the device will ignore a wake sequence that is sent when the device is already awake.

#### Multiple Devices on the Bus

When there are multiple devices on the bus and the I<sup>2</sup>C interface is run at speeds of less than  $\sim 300$  kHz<sup>2</sup>, the transmission of certain data patterns will cause the ATECC608C-TFLXTLS devices on the bus to wake up. The lower the frequency, the higher the probability that the device wakes up. Because subsequent device addresses transmitted along the bus only match the desired devices, the ATECC608C-TFLXTLS will not respond but will be awake. It is recommended that after

<sup>2</sup> The actual frequency for a given device will vary with process and environmental factors. This value is considered safe under all conditions.



communicating with another device at slow frequencies, a sleep or idle sequence be issued to place the ATECC608C-TFLXTLS back into a known state.



**Important:**  $t_{WLO}$  is the minimum time that the system must provide to ensure that the ATECC608C-TFLXTLS will wake under all manufacturing and environmental conditions. In actuality, the device may wake up with a lesser pulse width.

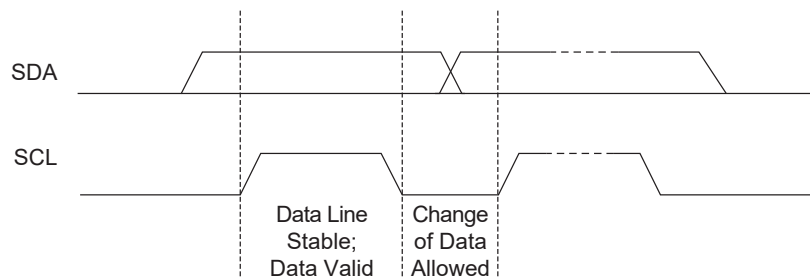
If multiple devices are on the I<sup>2</sup>C bus, it is recommended that the ATECC608C-TFLXTLS device be woken up after a power-up sequence and prior to communicating with any device on the bus. This is to ensure that the ATECC608C-TFLXTLS has properly initialized.

### 8.1.2 Device is Awake

When the device is awake, it honors the conditions listed below:

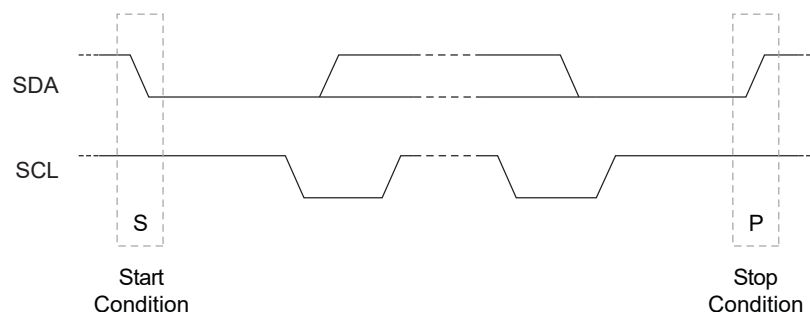
- **DATA Zero:** If SDA is low and stable while SCL goes from low to high to low, then a zero bit is being transferred on the bus. SDA can change while SCL is low.
- **DATA One:** If SDA is high and stable while SCL goes from low to high to low, then a one bit is being transferred on the bus. SDA can change while SCL is low.

Figure 8-1. Data Bit Transfer on I<sup>2</sup>C Interface



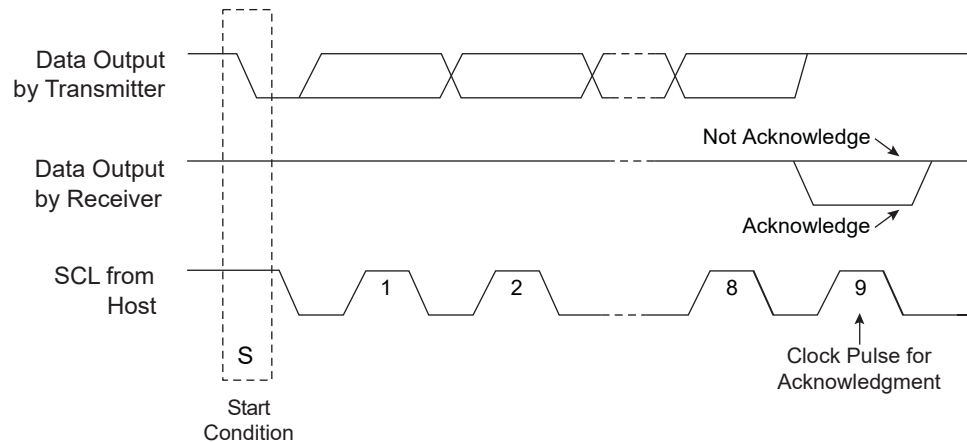
- **Start Condition:** A high-to-low transition of SDA with SCL high is a Start condition which must precede all commands.
- **Stop Condition:** A low-to-high transition of SDA with SCL high is a Stop condition. After this condition is received by the device, the current I/O transaction ends. On input, if the device has sufficient bytes to execute a command, the device transitions to the busy state and begins execution. The Stop condition must always be sent at the end of any packet sent to the device.

Figure 8-2. Start and Stop Conditions on I<sup>2</sup>C Interface



- **Acknowledge (ACK):** On the ninth clock cycle after every address or data byte is transferred, the receiver will pull the SDA pin low to acknowledge proper reception of the byte.
- **Not Acknowledge (NACK):** Alternatively, on the ninth clock cycle after every address or data byte is transferred, the receiver can leave the SDA pin high to indicate that there was a problem with the reception of the byte or that this byte completes the group transfer.

**Figure 8-3.** NACK and ACK Conditions on I<sup>2</sup>C Interface



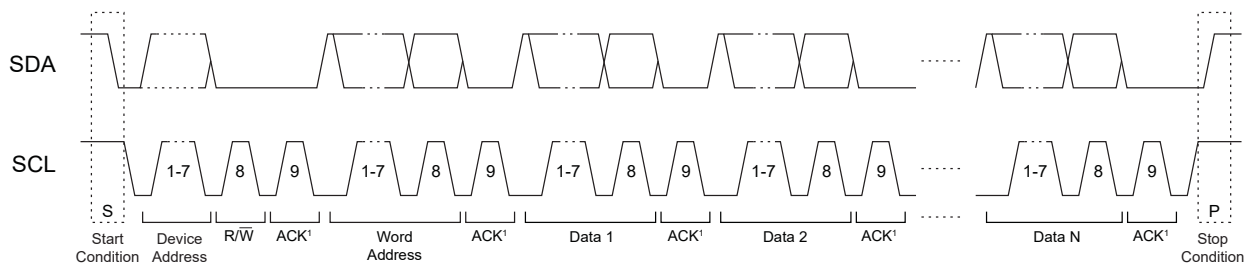
Multiple ATECC608C-TFLXTLS devices can easily share the same I<sup>2</sup>C interface signals if the I2C\_Address byte in the Configuration zone is programmed differently for each device on the bus. Because all seven of the bits of the device address are programmable, ATECC608C-TFLXTLS can also share the I<sup>2</sup>C interface with any I<sup>2</sup>C device, including any Serial EEPROM.

## 8.2 I<sup>2</sup>C Transmission to ATECC608C-TFLXTLS

The transmission of data from the system to the ATECC608C-TFLXTLS is summarized in the table below. The order of transmission is as follows:

- Start Condition
- Device Address Byte
- Word Address Byte
- Optional Data Bytes (1 through N)
- Stop Condition

**Figure 8-4.** Normal I<sup>2</sup>C Transmission to ATECC608C-TFLXTLS



SDA is driven low by the ATECC608C-TFLXTLS ACK periods.

The following tables label the bytes of the I/O transaction. The column labeled "I<sup>2</sup>C Name" provides the name of the byte as described in the AT24C16 data sheet.

**Table 8-1.** I<sup>2</sup>C Transmission to ATECC608C-TFLXTLS

Name	I <sup>2</sup> C Name	Description
Device Address	Device Address	This byte selects a particular device on the I <sup>2</sup> C interface. The ATECC608C-TFLXTLS is selected if bits 1 through 7 of this byte match bits 1 through 7 of the I2C_Address byte in the Configuration zone. Bit 0 of this byte is the standard I <sup>2</sup> C R/W bit and must be zero to indicate a write operation (the bytes following the device address travel from the host to the client).

.....continued

Name	I <sup>2</sup> C Name	Description
Word Address	Word Address	This byte must have a value of 0x03 for normal operation.
Command	Data1, N	The command group, consisting of the count, command packet and the 2-byte CRC. The CRC is calculated over the size and packet bytes.

Because the device treats the command input buffer as a FIFO, the input group can be sent to the device in one or many I<sup>2</sup>C command groups. The first byte sent to the device is the count, so after the device receives that number of bytes, it will ignore any subsequently received bytes until the execution is finished.

The system must send a Stop condition after the last command byte to ensure that ATECC608C-TFLXTLS will start the computation of the command. Failure to send a Stop condition may eventually result in a loss of synchronization; see [8.2.2. I2C Synchronization](#) for recovery procedures.

### 8.2.1 Word Address Values

During an I<sup>2</sup>C write packet, the ATECC608C-TFLXTLS interprets the second byte sent as the word address, which indicates the packet function as it is described in the table below:

**Table 8-2.** Word Address Values

Name	Value	Description
Reset	0x00	Resets the address counter. The next I <sup>2</sup> C read or write transaction will start with the beginning of the I/O buffer.
Sleep (Low-power)	0x01	The ATECC608C-TFLXTLS goes into the low-power Sleep mode and ignores all subsequent I/O transitions until the next Wake flag. The entire volatile state of the device is reset.
Idle	0x02	The ATECC608C-TFLXTLS goes into Idle mode and ignores all subsequent I/O transitions until the next Wake flag. The contents of TempKey, MessageDigestBuffer and Alternate Key registers are retained.
Command	0x03	Writes subsequent bytes to sequential addresses in the input command buffer that follow previous writes. This is the normal operation.
Reserved	0x04 – 0xFF	These addresses must not be sent to the device.

### 8.2.2 I<sup>2</sup>C Synchronization

It is possible for the system to lose synchronization with the I/O port on the ATECC608C-TFLXTLS, perhaps due to a system Reset, I/O noise or other conditions. Under this circumstance, the ATECC608C-TFLXTLS may not respond as expected, may be asleep or may be transmitting data during an interval when the system is expecting to send data. To resynchronize, the following procedure can be followed:

- To ensure an I/O channel Reset, the system must send the standard I<sup>2</sup>C software Reset sequence as follows:
  - A Start bit condition
  - Nine cycles of SCL, with SDA held high by the system pull-up resistor
  - Another Start bit condition
  - A Stop bit condition

It may, then, be possible to send a read sequence, and if synchronization completes properly, the ATECC608C-TFLXTLS will ACK the device address. The device may return data or may leave the bus floating (which the system will interpret as a data value of 0xFF) during the data periods.

If the device does ACK the device address, the system must reset the internal address counter to force the ATECC608C-TFLXTLS to ignore any partial input command that may have been sent. This can be accomplished by sending a write sequence to word address 0x00 (Reset), followed by a Stop condition.

- If the device does not respond to the device address with an ACK, then it may be asleep. In this case, the system must send a complete Wake token and wait  $t_{WHI}$  after the rising edge. The system may, then, send another read sequence, and if synchronization is complete, the device will ACK the device address.
- If the device still does not respond to the device address with an ACK, then it may be busy executing a command. The system must wait the longest  $t_{EXEC}$  (max.), then send the read sequence, which will be acknowledged by the device.

### 8.3 Sleep Sequence

Upon completion of the use of the ATECC608C-TFLXTLS by the system, it is recommended that the system issue a sleep sequence to put the device into Low-Power mode. This sequence consists of the proper device address followed by the value of 0x01 as the word address followed by a Stop condition. This transition to the Low-Power state causes a complete reset of the device's internal command engine and input/output buffer. It can be sent to the device at any time when it is awake and not busy.

### 8.4 Idle Sequence

If the total sequence of required commands exceeds  $t_{WATCHDOG}$ , then the device will automatically go to sleep and lose any information stored in the volatile registers. This action can be prevented by putting the device into Idle mode prior to completion of the watchdog interval. When the device receives the Wake token, it will then restart the Watchdog Timer and execution can be continued.

The idle sequence consists of the proper device address followed by the value of 0x02 as the word address followed by a Stop condition. It can be sent to the device at any time when it is awake and not busy.

### 8.5 I<sup>2</sup>C Transmission from the ATECC608C-TFLXTLS

When the ATECC608C-TFLXTLS is awake and not busy, the host can retrieve the current output buffer contents from the device using an I<sup>2</sup>C read. If valid command results are available, the size of the group returned is determined by the particular command that is run. Otherwise, the size of the group (and the first byte returned) will always be four: count, status/error and 2-byte CRC.

**Table 8-3.** I<sup>2</sup>C Transmission from the ATECC608C-TFLXTLS

Name	I <sup>2</sup> C Name	Direction	Description
Device Address	Device Address	To Client	This byte selects a particular device on the I <sup>2</sup> C interface and the ATECC608C-TFLXTLS will be selected if bits 1 through 7 of this byte match bits 1 through 7 of the I2C_Address byte in the Configuration zone. Bit 0 of this byte is the standard I <sup>2</sup> C R/W pin and must be one to indicate that the bytes following the device address travel from the client to the host (read).
Data	Data1, N	To Host	The output group, consisting of the count, status/error byte or the output packet followed by the 2-byte CRC.

The status, error or command outputs can be read repeatedly by the host. Each time a Read command is sent to the ATECC608C-TFLXTLS along the I<sup>2</sup>C interface, the device transmits the next sequential byte in the output buffer. See the following section for details on how the device handles the address counter.

If the ATECC608C-TFLXTLS is busy, idle or asleep, it will NACK the device address on a read sequence. If a partial command is sent to the device and a read sequence [Start + DeviceAddress (R/W == R) ] is sent to the device, the ATECC608C-TFLXTLS will NACK the device address to indicate that no data are available to be read.

## 9. Single-Wire Interface

In this mode, communications to and from the ATECC608C-TFLXTLS take place over SDA, a single asynchronously timed wire, and the SCL pin is not used as part of the communications channel. Instead, the SCL pin may be enabled to function as a GPIO pin.

The overall communications structure is a hierarchical format:

- Tokens** I/O Tokens implement a single data bit transmitted on the bus, or the wake-up event.
- Flags** Flags consist of eight tokens (bits) that convey the direction and meaning of the next group of bits (if any) that may be transmitted.
- Groups** Groups of data follow the command and transmit flags. They incorporate both a byte count and a checksum to ensure proper data transmission.
- Packets** Packets of bytes form the core of the group (minus the byte count and CRC). They are either the input or output parameters of a `CryptoAuthentication` command or status information from the ATECC608C-TFLXTLS.

See the Microchip website for the appropriate application notes for more details on how to use any microprocessor to easily generate the signaling necessary to send these elements to the device, including C source code libraries. Also see Section 9.5. [Wiring Configuration for Single-Wire Interface](#) for more information about how to connect the device in the Single-Wire Interface mode.

### 9.1 I/O Tokens

There are a number of I/O tokens, which may be transmitted over the Single-Wire Interface:

- **Input** (to the ATECC608C-TFLXTLS):
  - Wake — Wake the device up from either the sleep or idle modes, or reset the I/O interface.
  - Zero — Send a single bit from the system to the device with a value of zero.
  - One — Send a single bit from the system to the device with a value of one.
- **Output** (from the ATECC608C-TFLXTLS):
  - ZeroOut — Send a single bit from the device to the system with a value of zero.
  - OneOut — Send a single bit from the device to the system with a value of one.

The waveforms are the same in either direction, however, there are some differences in timing based upon the expectation that the host has a very accurate and consistent clock while the ATECC608C-TFLXTLS has part-to-part variability in its internal clock generator due to normal manufacturing and environmental fluctuations.

The bit timings are designed to permit a standard UART running at 230.4 kBaud to transmit and receive the tokens efficiently. Each byte transmitted or received by the UART corresponds to a single bit received or transmitted by the device.

The Wake token is special since it requires an extra long low pulse on the SDA pin, which cannot be confused with the shorter low pulses that occur during a data token (i.e., Zero, One, ZeroOut or OneOut). Devices that are either in the Idle or Sleep mode will ignore all data tokens until they receive a legal Wake token. If the processor is out of synchronization with the ATECC608C-TFLXTLS, it can send an additional Wake token to the device, which will reset the I/O channel hardware on the device.

**Note:** This may result in the loss of data stored in the command output buffer.

### 9.2 I/O Flags

The system is always host, so before any I/O transaction, the system must send an eight bit flag to the device to indicate the I/O operation that will be subsequently performed.

**Table 9-1.** IO Flags

Value	Name	Meaning
0x77	Command	After this flag, the system starts sending a command group to the device. The first bit of the group can follow immediately after the last bit of the flag.
0x88	Transmit	This command tells the device to wait for a bus turnaround time and then to start transmitting its response to the previously transmitted command group.
0xBB	Idle	Upon receipt of an idle flag, the device goes into the idle mode and remains there until the next Wake token is received.
0xCC	Sleep	Upon receipt of a sleep flag, the device enters the low-power sleep mode until the next Wake token is received.

**Note:** All other values are reserved and must not be used.

- **Transmit Flag**

The transmit flag is used to turn around the bus so that the ATECC608C-TFLXTLS can send data back to the system. The bytes that the device returns to the system depend on the current state of the device and may include status, error code, or command results.

When the device is busy executing a command, it ignores the SDA pin and any flags that are sent by the system. See the Command Summary for each command type's execution delays. The system must observe these delays after sending a command to the device.

- **Idle Flag**

The idle flag is used to transition the ATECC608C-TFLXTLS to the idle mode, which causes the input/output buffer to be flushed. It does not invalidate the contents of the TempKey, MessageDigest Buffer and Alt Key registers. This flag can be sent to the device at any time that it will accept a flag. When the device is in the idle mode, the watchdog timer is disabled.

- **Sleep Flag**

The sleep flag transitions the ATECC608C-TFLXTLS to the low-power sleep mode, which causes a complete reset of the device, including invalidation of the contents of the SRAM and all volatile registers. This flag can be sent to the device at any time that it will accept a flag.

## 9.3 Synchronization

Because the communications protocol is half-duplex, there is the possibility that the system and the ATECC608C-TFLXTLS will fall out of synchronization with each other. In order to speed recovery, the device implements a timeout that forces it to sleep under certain circumstances.

### 9.3.1 I/O Timeout

After a leading transition for any data token has been received, the ATECC608C-TFLXTLS will expect both the completion of the token and the start of the next (if this is not the last token of the group) to be properly received by the device within the  $t_{\text{TIMEOUT-SWI}}$  interval. Failure to send enough bits, or the transmission of an illegal token (e.g. a low pulse exceeding  $t_{\text{ZLO}}$ ), will cause the device to enter the Sleep mode after the  $t_{\text{TIMEOUT-SWI}}$  interval.

The same timeout applies during the transmission of the command group. After the transmission of a legal command flag, the I/O Timeout Circuitry is enabled until the last expected data bit is received.



**Important:** The Timeout Counter is reset after every legal token; therefore, the total time to transmit the command may exceed the  $t_{\text{TIMEOUT-SWI}}$  interval while the time between bits may not.

The I/O timeout circuitry is disabled when the device is busy executing a command.

### 9.3.2 Synchronization Procedures

If the device is not busy when the system sends a transmit flag, the device will respond within  $t_{\text{TURNAROUND}}$ . If  $t_{\text{EXEC}}$  time has not already passed, the device may be busy, and the system must poll or wait until the maximum  $t_{\text{EXEC}}$  time has elapsed. If the device still does not respond to a second transmit flag within  $t_{\text{TURNAROUND}}$ , it may be out of synchronization. At this point, the system may take the following steps to reestablish communication:

1. Wait  $t_{\text{TIMEOUT-SWI}}$ .
2. Send the transmit flag.
3. If the device responds within  $t_{\text{TURNAROUND}}$ , then the system may proceed with more commands.
4. Send a wake token.
5. Wait  $t_{\text{WHI}}$ .
6. Send the transmit flag.
7. The device will respond with a  $0 \times 11$  return status within  $t_{\text{TURNAROUND}}$ , after which the system may proceed with more commands.

### 9.4 GPIO

When working with the SWI mode device of the ATECC608C-TFLXTLS the SCL pin is configured as a general purpose output. The output signal will default to a LOW when the device is initially powered up. The output state can be changed by using the INFO command in GPIO Output mode.

The GPIO can be used as an enable or mode signal to other devices in the system or may be used to drive an LED.

The GPIO signal is not available when the device is an I<sup>2</sup>C mode device.

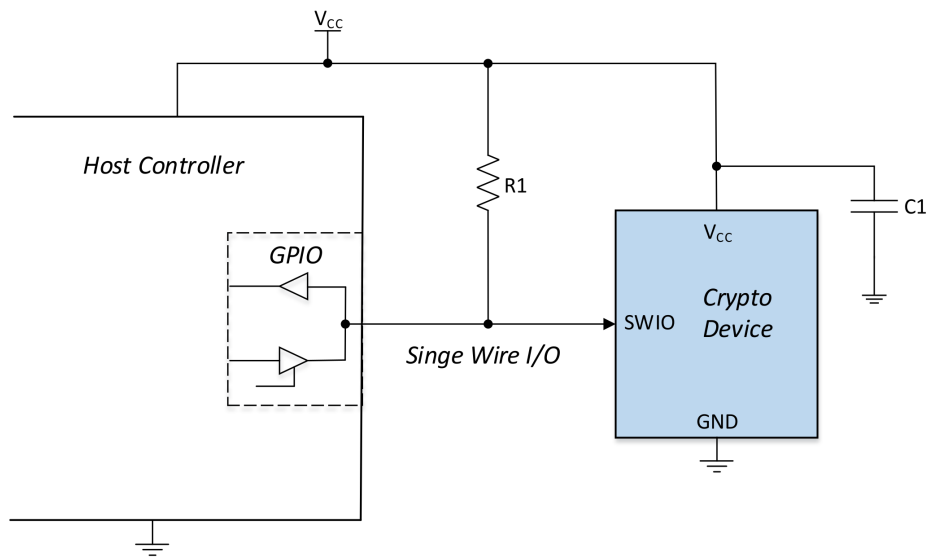
### 9.5 Wiring Configuration for Single-Wire Interface

Using the Single-Wire Interface allows the connection of ATECC608C-TFLXTLS to a host using only a single pin (SDA) to transfer data in both directions. This interface does not use the SCL pin which is configured as a GPIO output.

To prevent forward biasing the internal diode and drawing current across power planes in the system, the resistor pull-up on the SDA pin should either be connected to the same supply that is connected to the  $V_{\text{CC}}$  pin or to a lower voltage rail.

Since the ATECC608C-TFLXTLS is configured for a fixed I/O level the signal levels of the SDA signal may be different than the  $V_{\text{CC}}$  voltage level. This situation might occur if the ATECC608C-TFLXTLS device is physically distant from the bus master device and the supply voltage for the bus master is different than the supply voltage for ATECC608C-TFLXTLS.

Figure 9-1. 3-wire Configuration for Single-Wire Interface





## 10. Electrical Characteristics

### 10.1 Absolute Maximum Ratings

Operating Temperature	-40°C to +85°C
Storage Temperature	-65°C to +150°C
Maximum Operating Voltage	6.0V
DC Output Current	5.0 mA
Voltage on any pin -0.5V to (V <sub>CC</sub> + 0.5V)	-0.5V to (V <sub>CC</sub> + 0.5V)
ESD Ratings:	
Human Body Model(HBM) ESD	>4 kV
Charge Device Model(CDM) ESD	>1 kV

**Note:** Stresses beyond those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification are not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

### 10.2 Reliability

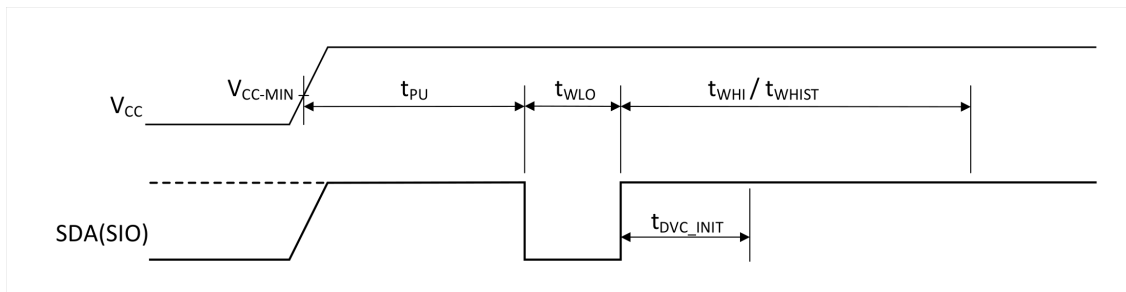
The ATECC608C-TFLXTLS is fabricated with Microchip’s high reliability CMOS EEPROM manufacturing technology.

**Table 10-1.** EEPROM Reliability

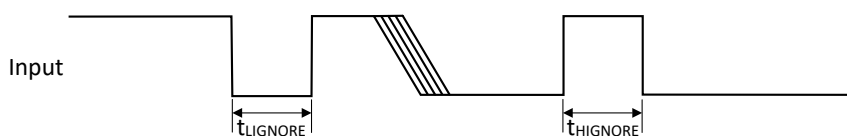
Parameter	Min.	Typ.	Max.	Units
Write Endurance at +85°C (Each Byte)	400,000	—	—	Write Cycles
Data Retention at +70°C	15	—	—	Years
Data Retention at +55°C	45	—	—	Years
Read Endurance	Unlimited			Read Cycles

### 10.3 AC Parameters: All I/O Interfaces

**Figure 10-1.** Wake Timing: All Interfaces



**Figure 10-2.** Input Noise Suppression: All Interfaces



**Table 10-2. AC Parameters: All I/O Interfaces**

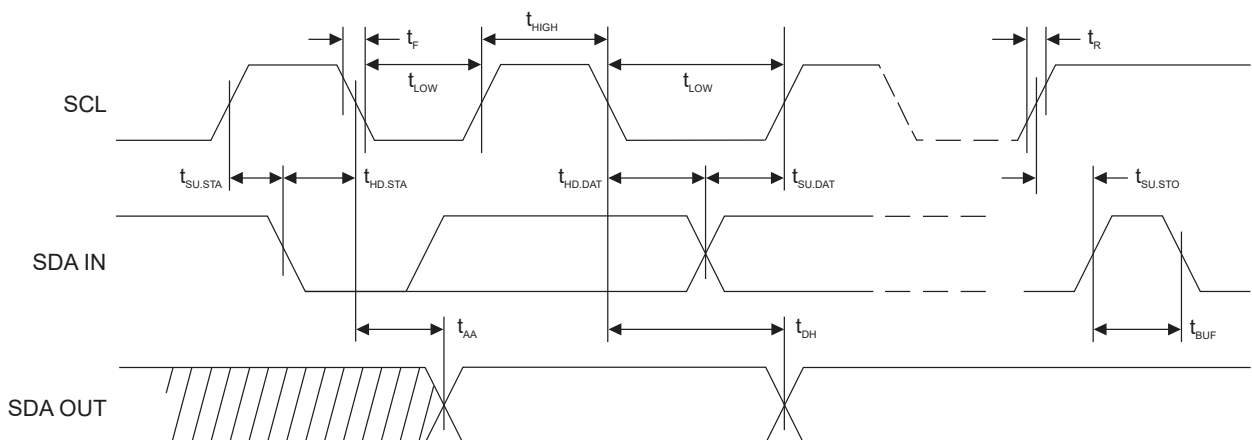
Parameter	Sym.	Direction	Min.	Typ.	Max.	Units	Conditions
Power-Up Delay	$t_{PU}$	To Crypto Device	100	—	—	$\mu s$	Minimum time between $V_{CC} > V_{CC\ min}$ prior to start of $t_{WLO}$ .
Wake Low Duration	$t_{WLO}$	To Crypto Device	60	—	—	$\mu s$	—
Initialization Time <sup>(1)</sup>	$t_{DVC\_INIT}$	Internal	—	—	400	$\mu s$	Maximum time from rising edge of wake pulse until device is initialized. <sup>(2)</sup>
Wake High Delay to Data Comm	$t_{WHI}$	To Crypto Device	1500	—	—	$\mu s$	SDA is recommended to be stable high for this entire duration unless polling is implemented. SelfTest is not enabled at power-up.
Wake High Delay when SelfTest is Enabled	$t_{WHIST}$	To Crypto Device	20	—	—	ms	SDA is recommended to be stable high for this entire duration unless polling is implemented.
High-Side Glitch Filter at Active <sup>(1)</sup>	$t_{HIGNORE\_A}$	To Crypto Device	45	—	—	ns	Pulses shorter than this in width will be ignored by the device, regardless of its state when active.
Low-Side Glitch Filter at Active <sup>(1)</sup>	$t_{LIGNORE\_A}$	To Crypto Device	45	—	—	ns	Pulses shorter than this in width will be ignored by the device, regardless of its state when active.
Low-Side Glitch Filter at Sleep <sup>(1)</sup>	$t_{LIGNORE\_S}$	To Crypto Device	15	—	—	$\mu s$	Pulses shorter than this in width will be ignored by the device when in Sleep mode.
Watchdog Time-out	$t_{WATCHDOG}$	To Crypto Device	0.7	1.3	1.7	s	Time from wake until device is forced into Sleep mode if Config.ChipMode[2] is 0.

**Notes:**

1. These parameters are characterized, but not production tested.
2. No communications, other than the wake pulse, on the I<sup>2</sup>C bus is recommended until after  $t_{DVC\_INIT}$  time has passed.

**10.3.1 AC Parameters: I<sup>2</sup>C Interface**

**Figure 10-3. I<sup>2</sup>C Synchronous Data Timing**



**Table 10-3. AC Characteristics of I<sup>2</sup>C Interface<sup>(2)</sup>**

Unless otherwise specified, applicable over recommended operating range from  $T_A = -40^\circ C$  to  $+85^\circ C$ ,  $V_{CC} = +2.0V$  to  $+5.5V$ ,  $C_L = 1$  TTL Gate and  $100$  pF.

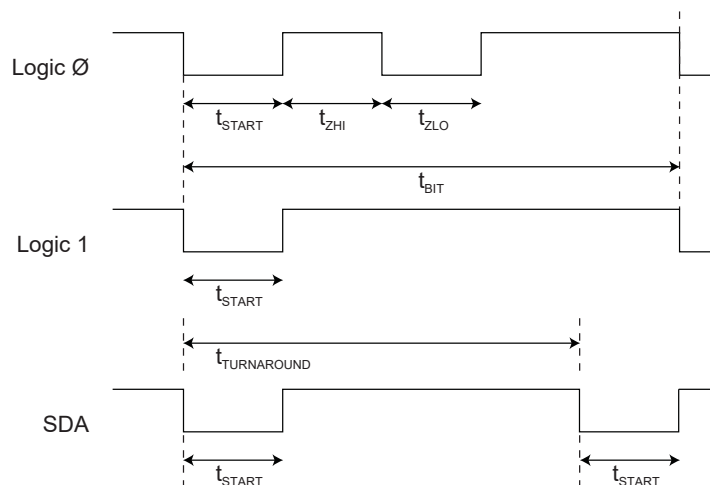
Parameter	Sym.	Min.	Max.	Units
SCL Clock Frequency	$f_{SCL}$	0	1	MHz
SCL High Time	$t_{HIGH}$	400	—	ns
SCL Low Time	$t_{LOW}$	400	—	ns
Start Setup Time	$t_{SU,STA}$	250	—	ns
Start Hold Time	$t_{HD,STA}$	250	—	ns
Stop Setup Time	$t_{SU,STO}$	250	—	ns
Data In Setup Time	$t_{SU,DAT}$	100	—	ns
Data In Hold Time	$t_{HD,DAT}$	0	—	ns
Input Rise Time <sup>1</sup>	$t_R$	—	300	ns
Input Fall Time <sup>1</sup>	$t_F$	—	100	ns
Clock Low to Data Out Valid	$t_{AA}$	50	550	ns
Data Out Hold Time	$t_{DH}$	50	—	ns
SMBus Time-Out Delay	$t_{TIMEOUT}$	25	35	ms
Time bus must be free before a new transmission can start <sup>1</sup>	$t_{BUF}$	500	—	ns

**Notes:**

- Values are based on characterization and are not tested.
- AC measurement conditions:
  - $R_L$  (connects between SDA and  $V_{CC}$ ): 1.2 k $\Omega$  (for  $V_{CC}$  = +2.0V to +5.0V)
  - Input pulse voltages: 0.3 $V_{CC}$  to 0.7 $V_{CC}$
  - Input rise and fall times:  $\leq$  50 ns
  - Input and output timing reference voltage: 0.5 $V_{CC}$

**10.3.2 AC Parameters: Single-Wire Interface**

Figure 10-4. AC Timing Diagram: Single-Wire Interface



**Table 10-4. AC Parameters: Single-Wire Interface**

Unless otherwise specified, applicable from  $T_A = -40^{\circ}\text{C}$  to  $+85^{\circ}\text{C}$ ,  $V_{CC} = +2.0\text{V}$  to  $+5.5\text{V}$ ,  $C_L = 100\text{ pF}$ .

Parameter	Symbol	Direction	Min.	Typ.	Max.	Unit	Conditions
Start Pulse Duration	$t_{START}$	To Crypto Device	4.10	4.34	4.56	$\mu\text{s}$	—
		From Crypto Device	4.60	6	8.60	$\mu\text{s}$	—

.....continued

Parameter	Symbol	Direction	Min.	Typ.	Max.	Unit	Conditions
Zero Transmission High Pulse	$t_{ZHI}$	To Crypto Device	4.10	4.34	4.56	$\mu\text{s}$	—
		From Crypto Device	4.60	6	8.60	$\mu\text{s}$	—
Zero Transmission Low Pulse	$t_{ZLO}$	To Crypto Device	4.10	4.34	4.56	$\mu\text{s}$	—
		From Crypto Device	4.60	6	8.60	$\mu\text{s}$	—
Bit Time <sup>(1)</sup>	$t_{BIT}$	To Crypto Device	37	39	—	$\mu\text{s}$	If the bit time exceeds $t_{TIMEOUT-SWI}$ , ATECC608C-TFLXTLS may enter Sleep mode.
		From Crypto Device	41	54	78	$\mu\text{s}$	—
Turn Around Delay	$t_{TURNAROUND}$	From Crypto Device	64	96	131	$\mu\text{s}$	ATECC608C-TFLXTLS will initiate the first low going transition after this time interval following the initial falling edge of the start pulse of the last bit of the transmit flag.
		To Crypto Device	93	—	—	$\mu\text{s}$	After ATECC608C-TFLXTLS transmits the last bit of a group, the system must wait this interval before sending the first bit of a flag. It is measured from the falling edge of the start pulse of the last bit transmitted by ATECC608C-TFLXTLS.
IO Timeout	$t_{TIMEOUT-SWI}$	To Crypto Device	45	65	85	ms	ATECC608C-TFLXTLS may transition to the Sleep mode if the bus is inactive longer than this duration.

**Note:**

- $t_{START}$ ,  $t_{ZLO}$ ,  $t_{ZHI}$  and  $t_{BIT}$  are designed to be compatible with a standard UART running at 230.4 kBaud for both transmit and receive. The UART must be set to seven data bits, no parity and one Stop bit.

## 10.4 DC Parameters: All I/O Interfaces

**Table 10-5.** DC Parameters on All I/O Interfaces

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Ambient Operating Temperature	$T_A$	-40	—	+85	$^{\circ}\text{C}$	Standard Industrial Temperature Range
Power Supply Voltage	$V_{CC}$	2.0	—	5.5	V	—
Active Power Supply Current	$I_{CC}$	—	2	3	mA	Waiting for I/O during I/O transfers or execution of non-ECC commands. Independent of Clock Divider value.
		—	—	14	mA	During ECC command execution. Clock divider = 0x0
Idle Power Supply Current	$I_{IDLE}$	—	800	—	$\mu\text{A}$	When device is in Idle mode, $V_{SDA}$ and $V_{SCL} < 0.4\text{V}$ or $> V_{CC} - 0.4$
Sleep Current	$I_{SLEEP}$	—	30	150	nA	When device is in Sleep mode, $V_{CC} \leq 3.6\text{V}$ , $V_{SDA}$ and $V_{SCL} < 0.4\text{V}$ or $> V_{CC} - 0.4$ , $T_A \leq +55^{\circ}\text{C}$
		—	—	2	$\mu\text{A}$	When device is in Sleep mode. Over full $V_{CC}$ range and $-40^{\circ}\text{C}$ to $85^{\circ}\text{C}$ temperature range.
Output Low Voltage	$V_{OL}$	—	—	0.4	V	When device is in Active mode, $V_{CC} = 2.5$ to $5.5\text{V}$

.....continued

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Output Low Current	$I_{OL}$	—	—	4	mA	When device is in Active mode, $V_{CC} = 2.5$ to $5.5V$ , $V_{OL} = 0.4V$
Theta JA	$\theta_{JA}$	—	166	—	$^{\circ}C/W$	SOIC (SS)
		—	173	—	$^{\circ}C/W$	UDFN (MA)

### 10.4.1 $V_{IH}$ and $V_{IL}$ Specifications

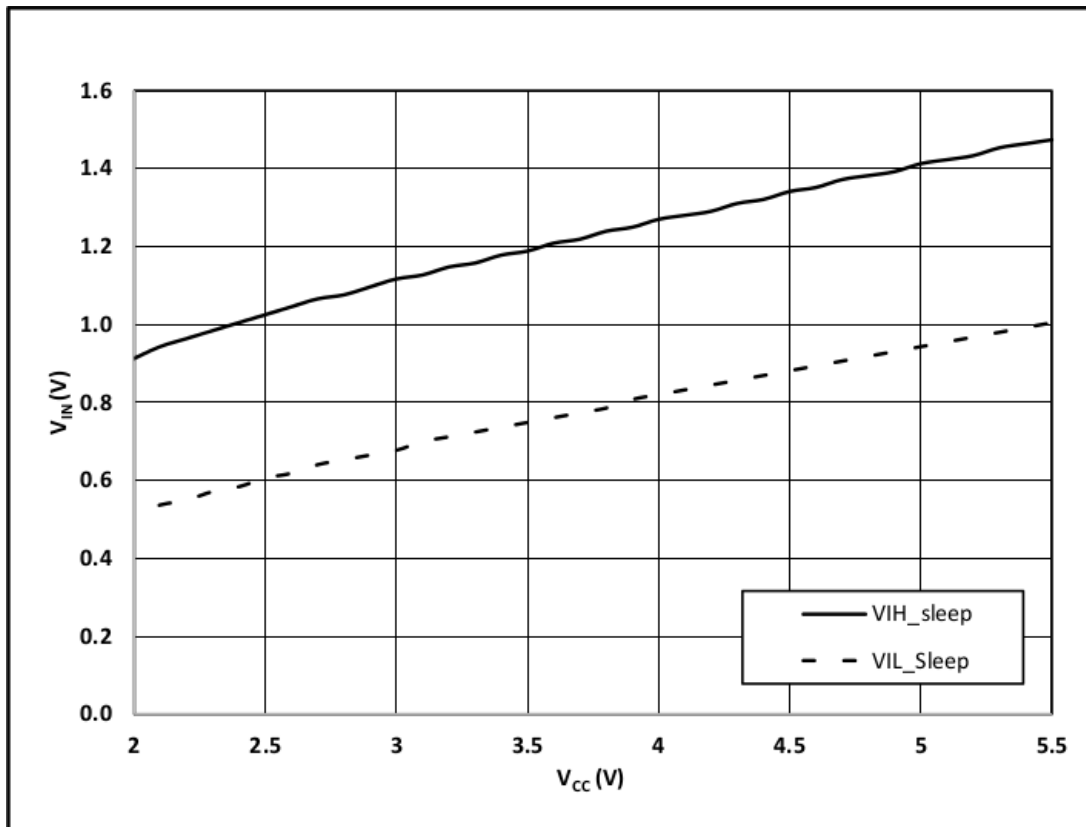
The input levels of the device will vary dependent on the mode and voltage of the device. The input voltage thresholds when in Sleep or Idle mode are dependent on the  $V_{CC}$  level as shown in Figure 10-5. When in Sleep or Idle mode the TTLenable bit has no effect.

The active input levels of the ATECC608C-TFLXTLS are fixed and do not vary with the  $V_{CC}$  level. The input levels transmitted to the device must comply with the table below.

**Table 10-6.**  $V_{IL}$ ,  $V_{IH}$  on All I/O Interfaces (TTLenable = 0)

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Input Low Voltage	$V_{IL}$	-0.5	—	0.5	V	When device is active and TTLenable bit in Configuration memory is zero; otherwise, see above.
Input High Voltage	$V_{IH}$	1.5	—	$V_{CC} + 0.5$	V	When device is active and TTLenable bit in Configuration memory is zero; otherwise, see above.

**Figure 10-5.**  $V_{IH}$  and  $V_{IL}$  in Sleep and Idle Mode



## 11. Compatibility

### **ATECC608B-TFLXTLS Compatibility**

The ATECC608C-TFLXTLS provides form, fit and function compatibility to the ATECC608B-TFLXTLS device. Device configuration zone and slot configuration values are identical, operating conditions are identical, all commands and command modes are still supported and the 8-Pad UDFN and 8-PIN SOIC packages and pinouts are identical. Improvements and enhancements included in the ATECC608B-TFLXTLS were also included in the ATECC608C-TFLXTLS.

If a design was implemented using the Microchip Trust Platform Design Suite, then migration from the ATECC608B-TFLXTLS is a relatively minor process.

For more information on migrating from the ATECC608B-TFLXTLS to the ATECC608C-TFLXTLS, reviewing the application note [AN5078](#) is recommended.

### **ATECC608A-TFLXTLS Compatibility**

The ATECC608C-TFLXTLS provides form, fit and function compatibility to the ATECC608A-TFLXTLS device. Device configuration zone and slot configuration values are identical, operating conditions are identical, all commands and command modes are still supported and the 8-Pad UDFN and 8-PIN SOIC packages and pinouts are identical. Improvements and enhancements included in the ATECC608B-TFLXTLS were also included in the ATECC608C-TFLXTLS.

If a design was implemented using the Microchip Trust Platform Design Suite, migration from the ATECC608A-TFLXTLS is a relatively minor process.

For more information on migrating from the ATECC608A-TFLXTLS to the ATECC608C-TFLXTLS, reviewing application notes [AN2237](#) and [AN5078](#) is recommended.

## 12. Package Drawings

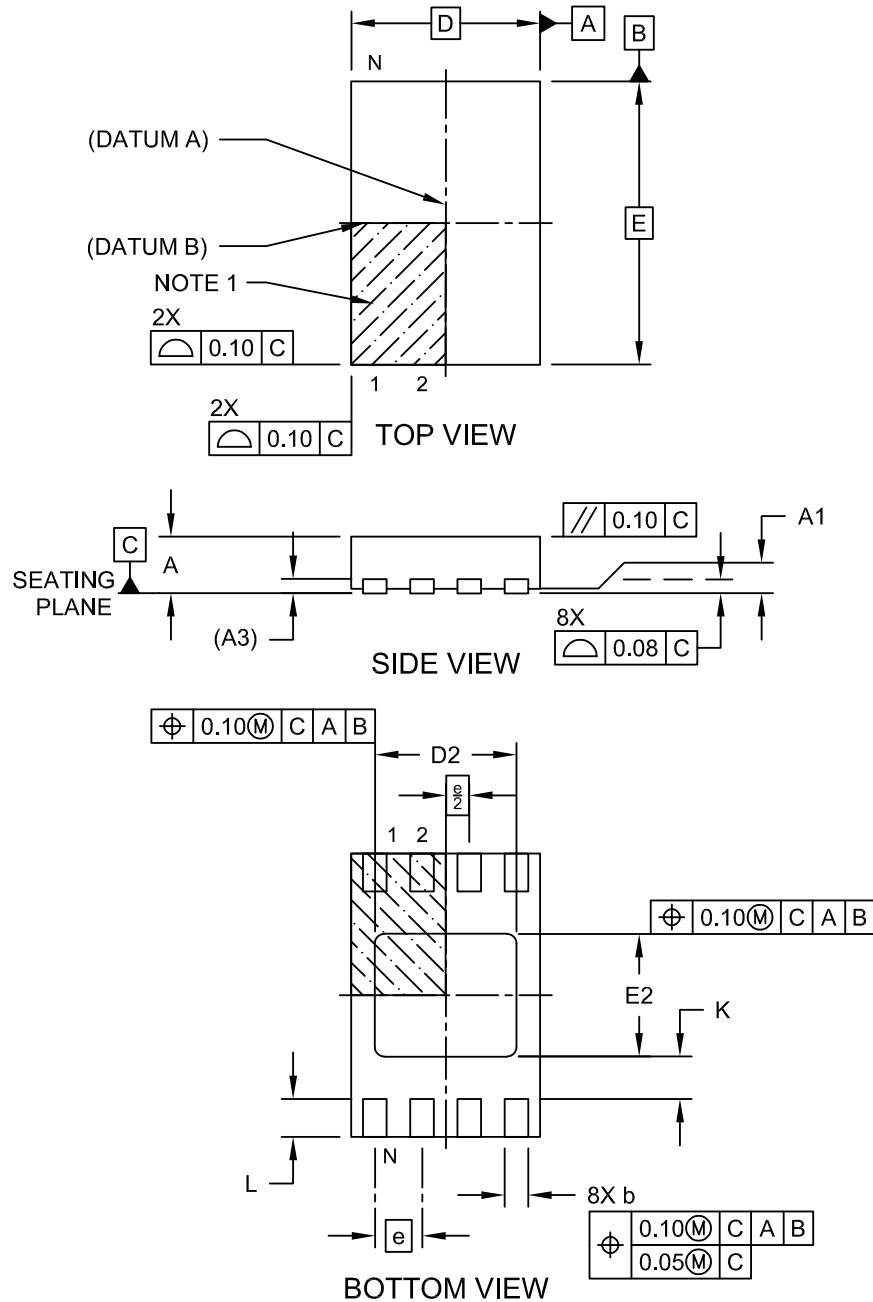
### 12.1 Package Marking Information

As part of Microchip's overall security features, the part marking for all crypto devices is intentionally vague. The marking on the top of the package does not provide any information as to the actual device type or the manufacturer of the device. The alphanumeric code on the package provides manufacturing information and will vary with assembly lot. It is recommended that the packaging mark not be used as part of any incoming inspection procedure.

## 12.2 8-Pad UDFN

### 8-Lead Ultra Thin Plastic Dual Flat, No Lead Package (Q4B) - 2x3 mm Body [UDFN] Atmel Legacy Global Package Code YNZ

**Note:** For the most current package drawings, please see the Microchip Packaging Specification located at <http://www.microchip.com/packaging>

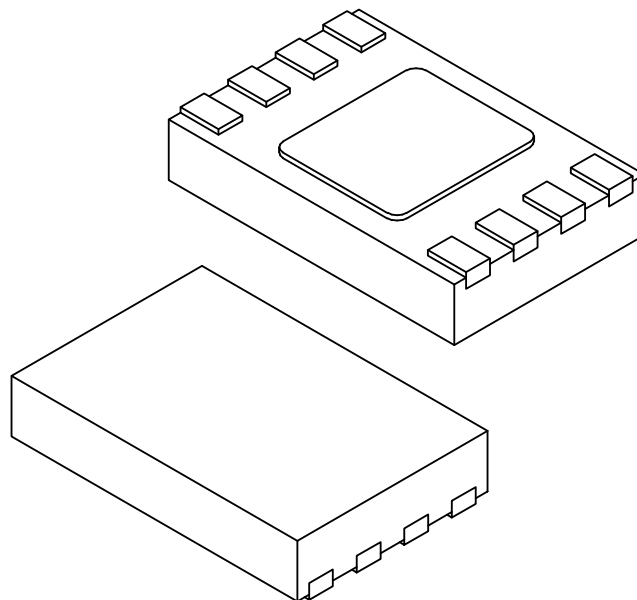


Microchip Technology Drawing C04-21355-Q4B Rev C Sheet 1 of 2



## 8-Lead Ultra Thin Plastic Dual Flat, No Lead Package (Q4B) - 2x3 mm Body [UDFN] Atmel Legacy Global Package Code YNZ

**Note:** For the most current package drawings, please see the Microchip Packaging Specification located at <http://www.microchip.com/packaging>



Dimension Limits	Units	MILLIMETERS		
		MIN	NOM	MAX
Number of Terminals	N	8		
Pitch	e	0.50 BSC		
Overall Height	A	0.50	0.55	0.60
Standoff	A1	0.00	0.02	0.05
Terminal Thickness	A3	0.152 REF		
Overall Length	D	2.00 BSC		
Exposed Pad Length	D2	1.40	1.50	1.60
Overall Width	E	3.00 BSC		
Exposed Pad Width	E2	1.20	1.30	1.40
Terminal Width	b	0.18	0.25	0.30
Terminal Length	L	0.25	0.35	0.45
Terminal-to-Exposed-Pad	K	0.20	-	-

**Notes:**

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M

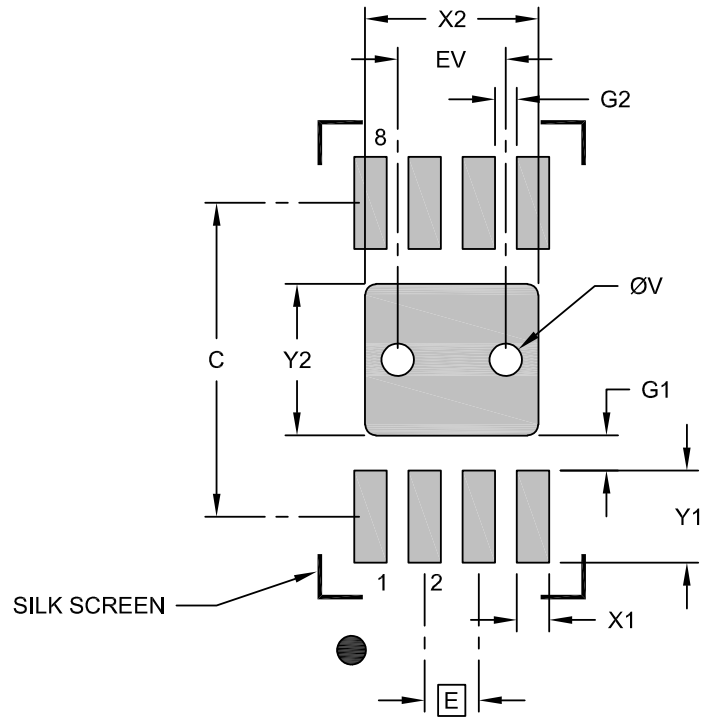
BSC: Basic Dimension. Theoretically exact value shown without tolerances.

REF: Reference Dimension, usually without tolerance, for information purposes only.

Microchip Technology Drawing C04-21355-Q4B Rev C Sheet 2 of 2

**8-Lead Ultra Thin Plastic Dual Flat, No Lead Package (Q4B) - 2x3 mm Body [UDFN]  
Atmel Legacy Global Package Code YNZ**

**Note:** For the most current package drawings, please see the Microchip Packaging Specification located at <http://www.microchip.com/packaging>



**RECOMMENDED LAND PATTERN**

Dimension Limits	Units	MILLIMETERS		
		MIN	NOM	MAX
Contact Pitch	E	0.50 BSC		
Optional Center Pad Width	X2			1.60
Optional Center Pad Length	Y2			1.40
Contact Pad Spacing	C	2.90		
Contact Pad Width (X8)	X1			0.30
Contact Pad Length (X8)	Y1			0.85
Contact Pad to Center Pad (X8)	G1	0.33		
Contact Pad to Contact Pad (X6)	G2	0.20		
Thermal Via Diameter	V		0.30	
Thermal Via Pitch	EV		1.00	

**Notes:**

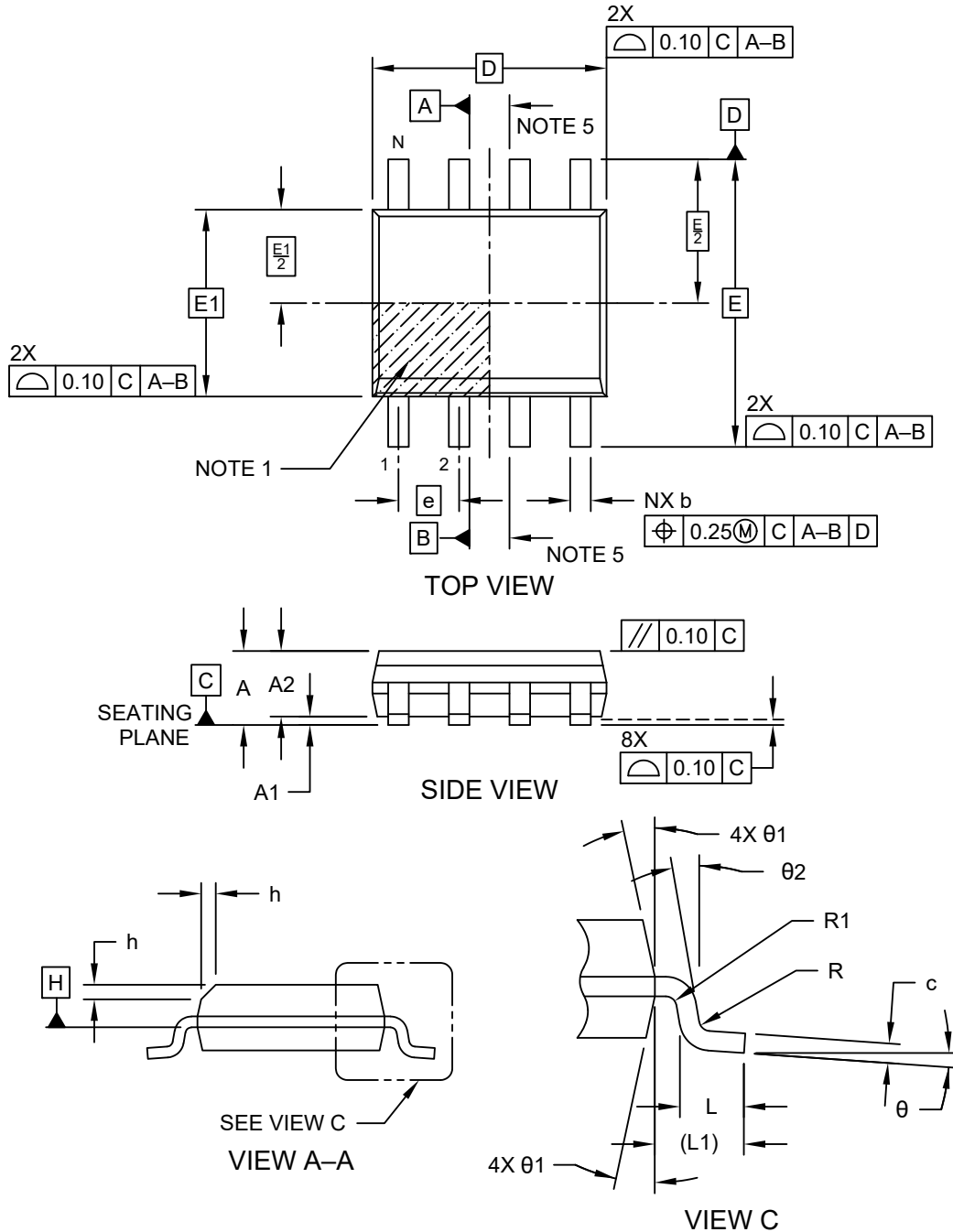
- Dimensioning and tolerancing per ASME Y14.5M  
BSC: Basic Dimension. Theoretically exact value shown without tolerances.
- For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

Microchip Technology Drawing C04-23355-Q4B Rev C

## 12.3 8-Lead SOIC

### 8-Lead Plastic Small Outline (C2X) - Narrow, 3.90 mm (.150 In.) Body [SOIC] Atmel Legacy Global Package Code SWB

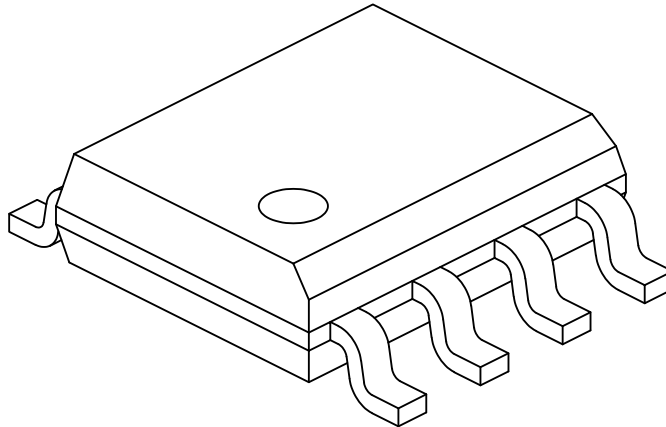
**Note:** For the most current package drawings, please see the Microchip Packaging Specification located at <http://www.microchip.com/packaging>



Microchip Technology Drawing No. C04-057-C2X Rev K Sheet 1 of 2

**8-Lead Plastic Small Outline (C2X) - Narrow, 3.90 mm (.150 In.) Body [SOIC]  
Atmel Legacy Global Package Code SWB**

**Note:** For the most current package drawings, please see the Microchip Packaging Specification located at <http://www.microchip.com/packaging>



Dimension Limits	Units	MILLIMETERS		
		MIN	NOM	MAX
Number of Pins	N	8		
Pitch	e	1.27 BSC		
Overall Height	A	–	–	1.75
Molded Package Thickness	A2	1.25	–	–
Standoff §	A1	0.10	–	0.25
Overall Width	E	6.00 BSC		
Molded Package Width	E1	3.90 BSC		
Overall Length	D	4.90 BSC		
Chamfer (Optional)	h	0.25	–	0.50
Foot Length	L	0.40	–	1.27
Footprint	L1	1.04 REF		
Lead Thickness	c	0.17	–	0.25
Lead Width	b	0.31	–	0.51
Lead Bend Radius	R	0.07	–	–
Lead Bend Radius	R1	0.07	–	–
Foot Angle	θ	0°	–	8°
Mold Draft Angle	θ1	5°	–	15°
Lead Angle	θ2	0°	–	–

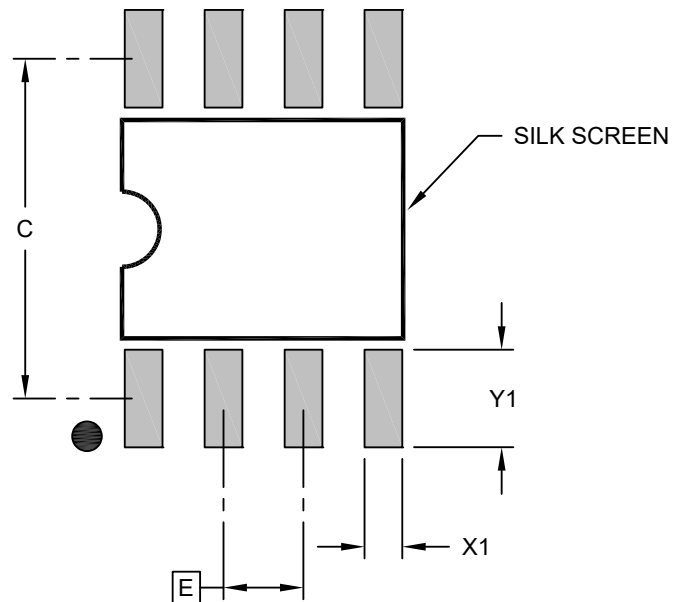
Notes:

- Pin 1 visual index feature may vary, but must be located within the hatched area.
- § Significant Characteristic
- Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.15mm per side.
- Dimensioning and tolerancing per ASME Y14.5M  
BSC: Basic Dimension. Theoretically exact value shown without tolerances.  
REF: Reference Dimension, usually without tolerance, for information purposes only.
- Datums A & B to be determined at Datum H.

Microchip Technology Drawing No. C04-057-C2X Rev K Sheet 2 of 2

### 8-Lead Plastic Small Outline (C2X) - Narrow, 3.90 mm (.150 In.) Body [SOIC]

**Note:** For the most current package drawings, please see the Microchip Packaging Specification located at <http://www.microchip.com/packaging>



RECOMMENDED LAND PATTERN

Dimension Limits	Units	MILLIMETERS		
		MIN	NOM	MAX
Contact Pitch	E	1.27 BSC		
Contact Pad Spacing	C		5.40	
Contact Pad Width (X8)	X1			0.60
Contact Pad Length (X8)	Y1			1.55

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M

BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-2057-C2X Rev K

## 13. Revision History

### Revision B (November 2023)

- [10.2. Reliability](#): Update to Data Retention values

### Revision A (August 2023)

- Original release of the document based on ATECC608B-TFLXTLS (DS40002249B)

## Microchip Information

### The Microchip Website

Microchip provides online support via our website at [www.microchip.com/](http://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](http://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](http://www.microchip.com/support)

## Product Identification System

To order or obtain information, e.g., on pricing or delivery, refer to the factory or the listed sales office.

PART NO - Trust Type Trust Option Package Type - Shipping Option  
 xxxxx - ttt vvv p - x

Device:	ATECC608C: Pre-configured Cryptographic Co-processor with secure hardware-based key storage	
Trust Type	TFLX	Type of Microchip Trust Product
Trust Option <sup>(1)</sup>	TLS	Configuration associated with Trust Product.
Package Options	U	8-Pad 2 x 3 x 0.6 mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat No Lead Package (UDFN)
	S	8-Lead (0.150" Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC)
Shipping Option <sup>(2)</sup>		<sup>(1)</sup> 2k Minimum Order Quantity (MOQ) is required.
	PROTO <sup>(3)</sup>	10 Unit Bulk - Prototype Units

### Examples:

- ATECC608C-TFLXTLSU: Trust Flex TLS, Provisioned, 8-UDFN, 2k MOQ, SWI or I<sup>2</sup>C Interface
- ATECC608C-TFLXTLSU-PROTO: Trust Flex TLS, Provisioned Prototype, 8-UDFN, 10 units bulk, SWI or I<sup>2</sup>C Interface
- ATECC608C-TFLXTLSS: Trust Flex TLS, Provisioned, 8-SOIC 2k MOQ, SWI or I<sup>2</sup>C Interface
- ATECC608C-TFLXTLSS-PROTO: Trust Flex TLS, Provisioned Prototype, 8-SOIC 10 units bulk, SWI or I<sup>2</sup>C

### Notes:

1. No special order code is required to order the SWI or I<sup>2</sup>C version of this device. This will be specified through use of the TPDS configuration tools.
2. Production orders will be delivered as Tape and Reel. Actual size of reel will vary based on customer order. 2k units is the minimum order quantity (MOQ) allowed.
3. Prototype units only come in 10-piece sample quantities but can be either I<sup>2</sup>C or SWI and can be provided in an SOIC or UDFN package option.



## 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](http://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, Klear, 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, 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, TimeCesium, TimeHub, TimePictra, TimeProvider, 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, EyeOpen, GridTime, IdealBridge, IGaT, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, IntelliMOS, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, MarginLink, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, mSiC, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, Power MOS IV, Power MOS 7, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, Trusted Time, TSHARC, Turing, 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: 978-1-6683-3367-9

## Quality Management System

For information regarding Microchip's Quality Management Systems, please visit [www.microchip.com/quality](http://www.microchip.com/quality).

# Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
<p><b>Corporate Office</b> 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: <a href="http://www.microchip.com/support">www.microchip.com/support</a> Web Address: <a href="http://www.microchip.com">www.microchip.com</a></p> <p><b>Atlanta</b> Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455</p> <p><b>Austin, TX</b> Tel: 512-257-3370</p> <p><b>Boston</b> Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088</p> <p><b>Chicago</b> Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075</p> <p><b>Dallas</b> Addison, TX Tel: 972-818-7423 Fax: 972-818-2924</p> <p><b>Detroit</b> Novi, MI Tel: 248-848-4000</p> <p><b>Houston, TX</b> Tel: 281-894-5983</p> <p><b>Indianapolis</b> Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380</p> <p><b>Los Angeles</b> Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800</p> <p><b>Raleigh, NC</b> Tel: 919-844-7510</p> <p><b>New York, NY</b> Tel: 631-435-6000</p> <p><b>San Jose, CA</b> Tel: 408-735-9110 Tel: 408-436-4270</p> <p><b>Canada - Toronto</b> Tel: 905-695-1980 Fax: 905-695-2078</p>	<p><b>Australia - Sydney</b> Tel: 61-2-9868-6733</p> <p><b>China - Beijing</b> Tel: 86-10-8569-7000</p> <p><b>China - Chengdu</b> Tel: 86-28-8665-5511</p> <p><b>China - Chongqing</b> Tel: 86-23-8980-9588</p> <p><b>China - Dongguan</b> Tel: 86-769-8702-9880</p> <p><b>China - Guangzhou</b> Tel: 86-20-8755-8029</p> <p><b>China - Hangzhou</b> Tel: 86-571-8792-8115</p> <p><b>China - Hong Kong SAR</b> Tel: 852-2943-5100</p> <p><b>China - Nanjing</b> Tel: 86-25-8473-2460</p> <p><b>China - Qingdao</b> Tel: 86-532-8502-7355</p> <p><b>China - Shanghai</b> Tel: 86-21-3326-8000</p> <p><b>China - Shenyang</b> Tel: 86-24-2334-2829</p> <p><b>China - Shenzhen</b> Tel: 86-755-8864-2200</p> <p><b>China - Suzhou</b> Tel: 86-186-6233-1526</p> <p><b>China - Wuhan</b> Tel: 86-27-5980-5300</p> <p><b>China - Xian</b> Tel: 86-29-8833-7252</p> <p><b>China - Xiamen</b> Tel: 86-592-2388138</p> <p><b>China - Zhuhai</b> Tel: 86-756-3210040</p>	<p><b>India - Bangalore</b> Tel: 91-80-3090-4444</p> <p><b>India - New Delhi</b> Tel: 91-11-4160-8631</p> <p><b>India - Pune</b> Tel: 91-20-4121-0141</p> <p><b>Japan - Osaka</b> Tel: 81-6-6152-7160</p> <p><b>Japan - Tokyo</b> Tel: 81-3-6880-3770</p> <p><b>Korea - Daegu</b> Tel: 82-53-744-4301</p> <p><b>Korea - Seoul</b> Tel: 82-2-554-7200</p> <p><b>Malaysia - Kuala Lumpur</b> Tel: 60-3-7651-7906</p> <p><b>Malaysia - Penang</b> Tel: 60-4-227-8870</p> <p><b>Philippines - Manila</b> Tel: 63-2-634-9065</p> <p><b>Singapore</b> Tel: 65-6334-8870</p> <p><b>Taiwan - Hsin Chu</b> Tel: 886-3-577-8366</p> <p><b>Taiwan - Kaohsiung</b> Tel: 886-7-213-7830</p> <p><b>Taiwan - Taipei</b> Tel: 886-2-2508-8600</p> <p><b>Thailand - Bangkok</b> Tel: 66-2-694-1351</p> <p><b>Vietnam - Ho Chi Minh</b> Tel: 84-28-5448-2100</p>	<p><b>Austria - Wels</b> Tel: 43-7242-2244-39 Fax: 43-7242-2244-393</p> <p><b>Denmark - Copenhagen</b> Tel: 45-4485-5910 Fax: 45-4485-2829</p> <p><b>Finland - Espoo</b> Tel: 358-9-4520-820</p> <p><b>France - Paris</b> Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79</p> <p><b>Germany - Garching</b> Tel: 49-8931-9700</p> <p><b>Germany - Haan</b> Tel: 49-2129-3766400</p> <p><b>Germany - Heilbronn</b> Tel: 49-7131-72400</p> <p><b>Germany - Karlsruhe</b> Tel: 49-721-625370</p> <p><b>Germany - Munich</b> Tel: 49-89-627-144-0 Fax: 49-89-627-144-44</p> <p><b>Germany - Rosenheim</b> Tel: 49-8031-354-560</p> <p><b>Israel - Ra'anana</b> Tel: 972-9-744-7705</p> <p><b>Italy - Milan</b> Tel: 39-0331-742611 Fax: 39-0331-466781</p> <p><b>Italy - Padova</b> Tel: 39-049-7625286</p> <p><b>Netherlands - Drunen</b> Tel: 31-416-690399 Fax: 31-416-690340</p> <p><b>Norway - Trondheim</b> Tel: 47-72884388</p> <p><b>Poland - Warsaw</b> Tel: 48-22-3325737</p> <p><b>Romania - Bucharest</b> Tel: 40-21-407-87-50</p> <p><b>Spain - Madrid</b> Tel: 34-91-708-08-90 Fax: 34-91-708-08-91</p> <p><b>Sweden - Gothenberg</b> Tel: 46-31-704-60-40</p> <p><b>Sweden - Stockholm</b> Tel: 46-8-5090-4654</p> <p><b>UK - Wokingham</b> Tel: 44-118-921-5800 Fax: 44-118-921-5820</p>