ECC608-TFLXWPC

ECC608-TFLXWPC CryptoAuthentication™ Data Sheet

Introduction

The ECC608-TFLXWPC is a pre-provisioned variant of the ATECC608 product family. The TrustFLEX secure element is part of the Microchip's family of generically-provisioned, security-focused devices. The device configuration was designed to meet the authentication requirements of the Wireless Power Consortium (WPC) Qi® 1.3 version of the standard.

The ECC608-TFLXWPC configuration is defined to meet the basic authentication needs of Qi transmitters that provide authentication. If so desired, dual WPC certificate slots can be implemented. In addition, extra support was implemented for users who want to provide proprietary extensions for implementing TLS authentication for WPC infrastructure products or to provide secure boot capabilities. While some data slots are required for specific use, others provide flexibility to be used for other applications. These slot access policies will be set by the Trust Platform Design Suite tools prior to ordering the ECC608-TFLXWPC devices.

This data sheet provides the slot and key configuration information that is unique to the ECC608-TFLXWPC. This information defines the access policies of each of the data zone slots. Only relevant command and I/O operating information is included. 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

- JIL High Rating – Validated to JIL Application of Attack Potential to Smartcards and Similar Devices, Version 3.1
- Specified Configuration Zone with Limited Selectable Options
- I^2C Interface with One-Time Changeable I^2C Address
- Support for WPC Slot 0 Manufacturing CA and Product Unit Certificates
  - WPC Manufacturing Certification Authority (CA) – Compressed certificate and public key
  - WPC product unit compressed certificate
  - WPC product unit P-256 Elliptic Curve Cryptography (ECC) private key
- Optional Support for WPC Slot 1 or WPC Slot 2 or 3 Proprietary Extensions
- Support for WPC Slot Digest to allow a Quick WPC Re-authentication of a Transmitter
- Support for TLS Authentication
  - Works with Google Cloud™, Amazon Web Services (AWS®), Microsoft® Azure Cloud Services or others
  - TLS signer – Compressed certificate and public key
  - TLS device compressed certificate
  - TLS device P-256 ECC private key
- I/O Protection Key Slot to Protect I^2C Communication
- Secure Boot Enabled with Customizable Secure Boot Public Key at Time of Manufacture
- Available in 8-Pad UDFN and 8-Pin SOIC Packages in 2k Unit Production Quantities

Applications

- WPC Qi 1.3 Authentication
- Secure IoT TLS 1.2 and 1.3 Connections
- Secure Boot/Secure Firmware Update

Table of Contents

Introduction.....1

Features.....1

Applications.....1

1. Pin Configuration and Pinout.....5

2. Wireless Power Consortium.....6
   2.1. Wireless Power Consortium Terminology.....6

3. EEPROM Memory and Data Zone Access Policies.....8
   3.1. ECC608-TFLXWPC Configuration Zone.....9
      3.1.1. Modifiable Configuration Zone Bytes.....9
   3.2. Data Zone and Access Policies.....10
      3.2.1. Data Zone Data Types.....10
         3.2.1.1. Private Keys.....10
         3.2.1.2. ECC Public Keys.....10
         3.2.1.3. Certificate Storage.....11
            3.2.1.3.1. TLS Certificate Storage.....11
            3.2.1.3.2. WPC Certificate Storage.....12
         3.2.1.4. WPC Slot Digests.....12
         3.2.1.5. Secure Boot.....13
         3.2.1.6. I/O Protection Key.....13
         3.2.1.7. General Data Storage.....13
      3.2.2. Slot Configuration Terminology.....13
      3.2.3. ECC608-TFLXWPC Slot Configuration Summary.....14
      3.2.4. ECC608-TFLXWPC Detailed Slot Access Policies.....15
   3.3. ECC608-TFLXWPC EEPROM One-Time-Programmable (OTP) Zone.....22

4. Device Commands.....23
   4.1. General Device Commands.....24
      4.1.1. `Counter` Command.....24
      4.1.2. `Info` Command.....24
      4.1.3. `Lock` Command.....24
      4.1.4. `Nonce` Command.....24
      4.1.5. `Random` Command.....25
      4.1.6. `Read` Command.....25
      4.1.7. `SelfTest` Command.....25
      4.1.8. `SHA` Command.....25
      4.1.9. `UpdateExtra` Command.....25
      4.1.10. `Write` Command.....25
   4.2. Asymmetric Cryptography Commands.....25
      4.2.1. `ECDH` Command.....26
      4.2.2. `GenKey` Command.....26
      4.2.3. `SecureBoot` Command.....26
      4.2.4. `Sign` Command.....26

4.2.5. Verify Command......26

4.3. Symmetric Cryptography Commands......27

4.3.1. GenDig Command......27

4.3.2. MAC Command......27

5. I^{2}C Interface......28

5.1. I/O Conditions......28

5.1.1. Device is Asleep......28

5.1.2. Device is Awake......29

5.2. I^{2}C Transmission to ECC608-TFLXWPC......30

5.2.1. Word Address Values......31

5.2.2. I^{2}C Synchronization......31

5.3. Sleep Sequence......32

5.4. Idle Sequence......32

5.5. SMBus Timeout......32

5.6. I^{2}C Transmission from the ECC608-TFLXWPC......32

6. Application Information......34

6.1. WPC Engagement......34

6.2. Use Cases......35

6.3. Development Tools......35

6.3.1. Trust Platform Design Suite......35

6.3.2. Hardware Tools......35

6.3.3. CryptoAuthLib......36

7. Electrical Characteristics......38

7.1. Absolute Maximum Ratings......38

7.2. Reliability......38

7.3. AC Parameters: All I/O Interfaces......38

7.3.1. AC Parameters: I^{2}C Interface......39

7.4. DC Parameters: All I/O Interfaces......40

7.4.1. V_{IH} and V_{IL} Specifications......41

8. Package Drawings......43

8.1. Package Marking Information......43

8.2. 8-pad UDFN......44

8.3. 8-lead SOIC......47

9. Revision History......50

The Microchip Website......51

Product Change Notification Service......51

Customer Support......51

Product Identification System......52

Microchip Devices Code Protection Feature......52

Legal Notice......52

Trademarks.. 53

Quality Management System... 53

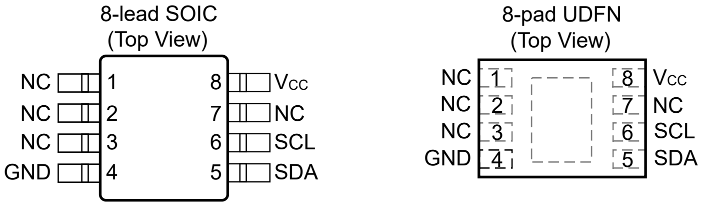
Worldwide Sales and Service...54

1. Pin Configuration and Pinout

Table 1-1. Pin Configuration

Pin	Function I^{2}C Devices
NC	No Connect
GND	Ground
SDA	I^{2}C Serial Data
SCL	I^{2}C Serial Clock Input
V_{CC}	Power Supply

Figure 1-1. UDFN and SOIC Pinout



Note: It is recommended that the UDFN backside paddle be connected to GND.

2. Wireless Power Consortium

The Wireless Power Consortium defines a complete ecosystem for the deployment of wireless charging for mobile devices. Starting with version 1.3 of the Qi specification, authentication was defined as a requirement for chargers that wish to charge at a power level higher than 5W. Version 1.3 of the specification allows charging of mobile devices up to 15W. All chargers are allowed to initially charge at the 5W level without authentication. Authentication must occur to allow charging at a level of higher than 5W.

To accommodate these changes, a chain of trust is defined as part of the Qi ecosystem. This chain of trust consists of three levels:

1. WPC root certificate – Consists of the root private key and root certificate.
2. WPC manufacturing certificate – Consists of a manufacturing certificate signed by the private key of the root certificate.
3. WPC product unit certificate – Consists of the product unit certificate signed by the private key of the WPC manufacturing certificate.

The WPC certificates follow the X.509 format. For WPC Slots 0 and 1, the certificate format is fixed. For WPC Slots 2 and 3, the format is not defined and allows for proprietary use of these certificate chain slots.

To participate in the WPC wireless charging ecosystem, one must be a member of the Wireless Power Consortium. Additional information on the standards and on the consortium can be found on the WPC website: www.wirelesspowerconsortium.com/.

2.1 Wireless Power Consortium Terminology

The following terminology used in this data sheet is included to aid in understanding items associated with the WPC Qi authentication standard. This section is intended to reflect the information in the WPC standard but, in all cases, the standard takes precedence over this section of the document.

Power Receiver The device that is charged by the power transmitter and provides communication to the power transmitter for the purpose of authentication or to control the power charging of the power receiver.

Power Transmitter The device that is used to communicate with and provide power to the power receiver. The secure storage subsystem resides within the power transmitter.

Qi The designator used by the WPC for the standards associated with wireless charging of mobile devices.

Revocation Sequential Identifier (RSID) The RSID is a unique identifier stored in the WPC device unit certificate that uniquely identifies a given transmitter and can be used to revoke high power or complete operational use of a power transmitter for noncompliance reasons.

Secure Storage Subsystem (SSS) The device used to store the security information used to authenticate a wireless power transmitter. This can be considered a secure element or secure crypto device.

WPC Manufacturer A company or entity licensed by the WPC to produce certified WPC power transmitters. All WPC manufacturers are required to sign a WPC manufacturer agreement.

WPC Manufacturing CA A company licensed by the WPC to produce secure storage subsystems for use in certified WPC power transmitters. Microchip is a licensed manufacturing CA.

Wireless Power Consortium (WPC) The standard body responsible for defining all aspects of wireless charging associated with the Qi standards and for licensing and certifying Qi-certified products. Membership in the WPC is required to produce Qi-compliant power transmitters or receivers. More information on the WPC can be found on the website: www.wirelesspowerconsortium.com/.

WPC Root Authority The WPC Root Authority is the head of the WPC certificate chain. All WPC manufacturing certificates will be signed by the WPC Root Authority.

WPC Slot The WPC authentication specification defines a slot as the element that holds a WPC certificate chain. There are four possible slots (Slots 0-3) defined by the WPC authentication specification, but only Slot 0 is required and must hold a WPC certificate chain. If used, Slot 1 is also reserved for use as a WPC certificate chain. The format of Slots 2 and 3 is undefined and they are reserved for optional proprietary extensions.

For the purpose of this document, the term “WPC Slot” will always be used when referring to a WPC certificate chain to distinguish it from the term “slot” used to indicate a data slot in the ECC608-TFLXWPC device.

WPC Slot Digest A 32-byte digest of the entire certificate chain stored in a WPC Slot.

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. ECC608-TFLXWPC EEPROM Zones

Zone	Description	Nomenclature
Configuration	Zone of 128 bytes (1,024 bits) EEPROM that contains: • Device configuration • Slot access policy information • Counter values • Device serial number • Lock information The LockConfig byte is already 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 ECC608-TFLXWPC device is 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 ECC608-TFLXWPC, the zone is preloaded with a predefined value. This zone cannot be modified but can be read at any time. See 3.3 ECC608-TFLXWPC EEPROM One-Time-Programmable (OTP) Zone 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 ECC608-TFLXWPC Configuration Zone

The ECC608-TFLXWPC configuration is largely 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^{2}C address is 0x38. The I^{2}C address can be overwritten using the `UpdateExtra` command.

Important: The default I^{2}C address of the ECC608-TFLXWPC is not the same as that of the generic nonconfigured ATECC608 device.

- The I/O levels are set to a fixed reference level; therefore, the host processor can operate at a lower voltage than the ECC608-TFLXWPC 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 ECC608-TFLXWPC, the following individual slots may be uniquely configured to be slot lockable or not: Slots 3-6 and 8-15.
- SecureBoot is enabled for FullStore digest mode for the ECC608-TFLXWPC.
- 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 Configuration zone is already locked. Several bytes can still be modified through the use of other commands.

SlotLocked Bits

For the ECC608-TFLXWPC, the following individual slots may be uniquely configured to be slot lockable or not: Slots 3-6 and 8-15. Through use of the Trust Platform Design Suite tools, each of these slots may be set to either be fixed or locked at the time of manufacturing. Slot group 10-12 and slot group 9, 13, 14 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 is 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 are locked, the value of the respective bit will be set to a value of zero.

I^{2}C Address Redefinition

This device is configured such that the I^{2}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^{2}C address. When this byte is set to a nonzero value, the device configuration uses byte 85 as its I^{2}C address instead of the default address. Once this byte is 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^{2}C address, this location must be written with the default I^{2}C address.

User Extra Byte
The UserExtra byte can be used for any desired purpose. This byte can only be updated 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 ECC608-TFLXWPC 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 HSM at provision time and are securely held in slots configured as ECC private keys.

TLS IoT Private Key
This is the primary authentication key used for IoT connectivity. This key is permanent and cannot be changed. Each device has its own unique private key.

This key is enabled for:

- ECDSA sign for authentication
- ECDH for key agreement. If encryption of the ECDH output is required, the I/O protection key needs to be set up first. See 3.2.1.6 I/O Protection Key for setup details.

This private key is the foundation for the generation of the corresponding public key and the IoT TLS X.509 certificates.

WPC Slot 0 and Slot 1 Private Key
These are the primary ECC keys used for WPC device authentication. Typically, only the key in the WPC Slot 0 will be used.

This key is enabled for:

- ECDSA sign for authentication

This private key is the foundation for the generation of the corresponding public key for the WPC X.509 product unit certificates for the WPC Slot 0 and WPC Slot 1, respectively.

3.2.1.2 ECC Public Keys

Public keys are always associated with ECC private keys. Every ECC private key will have its own unique public key. Public keys may be stored in the device or may be regenerated using the `GenKey` command if a given device slot is so configured. For the ECC608-TFLXWPC, seven possible public keys can be used or generated:

- Device Slots 0 and 1 contain an ECC private key for the WPC product unit certificates associated with the WPC Slot 0 and WPC Slot 1 certificate chains. The public key for each of these private keys can always be generated and used for a verify operation.
- Device Slot 2 contains an ECC private key for the TLS IoT authentication. The public key for this key can always be generated and used for a verify operation.
- Device Slot 9 contains an ECC public key for the WPC Slot 0 manufacturing X.509 certificate.
- Device Slot 8 contains an ECC public key for the WPC Slot 1 manufacturing X.509 certificate. The public key is stored in the first 72 bytes of the slot. If WPC Slot 1 is not used, this key may have an alternate use or not exist at all.
- Slot 11 contains an ECC public key as part of the X.509 IoT TLS signer certificate information.
- Slot 15 contains an ECC public key that can be used for secure boot operations.

3.2.1.3 Certificate Storage

The ECC608-TFLXWPC supports multiple certificate chains for different use case applications. There is the possibility to support up to three X.509 certificate chains. X.509 certificates tend to be larger than what will fit into a single ECC608-TFLXWPC device slot, therefore, 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 the certificate content that can be expected to change from device to device (e.g., public key, validity dates, etc.). Static data will be constant across all devices. Firmware is expected to have a certificate definition with a template for fully reconstructing each of the X.509 certificates for a specific use case. The full certificate is made up of a combination of dynamic and static data.

For the ECC608-TFLXWPC, there are two types of X.509 certificates to support the IoT TLS use case and the WPC authentication use case. Each of these use a different X.509 format, and, therefore, the ECC608-TFLXWPC will have a different compressed certificate format. If the WPC Slot 1 is not used and a propriety extension is used in WPC Slot 2 or WPC Slot 3, an additional type of certification chain may be required.

3.2.1.3.1 TLS Certificate Storage

The TLS X.509 certificate chain is the same as that used for Microchip Trust&GO and TrustFLEX TLS products. Specifically, the ATECC608B-TNGTLS and ATECC608B-TFLXTLS.

The following application note documents the compressed certificate format: ATECC Compressed Certificate Definition.

The CryptoAuthLib library also contains the atcacert module for working with TLS compressed certificates.

Device Certificate
The device certificate consists of information associated with the actual ECC608-TFLXWPC device.

Signer Certificate
The signer certificate consists of information associated with the signer certificate authority used to sign the device certificate. 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.

The following table shows all the slots associated with certificates in the ECC608-TFLXWPC:

Table 3-3. Slots for Certificates

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

...........continued

Slot	Description
12	Signer certificate. This is stored in a compressed format.

For the ECC608-TFLXWPC 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.

3.2.1.3.2 WPC Certificate Storage

The WPC X.509 certificate chain is documented in the WPC 1.3.0 authentication specification. The specification is only available to registered members of the WPC. The specific compressed format used by Microchip for the WPC X.509 certificates is a variant of what was previously used for the Microchip-defined TLS X.509 certificates.

The nomenclature used for the WPC certificates mirrors the nomenclatures used by the WPC authentication specification.

The CryptoAuthLib library also contains the atcawpccert module for working with WPC compressed certificates.

Product Unit Certificate
The product unit certificate consists of information associated with the Secure Storage Subsystem. The product unit certificate is the equivalent of the device certificate specified for the TLS authentication use case.

Manufacturer Certificate
The manufacturer certificate consists of the information associated with the manufacturer certificate authority and is used to sign the product unit certificate. The manufacturer certificate is the equivalent of the signer certificate specified for the TLS authentication use case.

Manufacturer Public Key
The manufacturer public key is the public key needed to verify the manufacturer and the information that is associated with the manufacturer compressed certificate. The manufacturer public key is the equivalent of the signer public key specified for the TLS authentication use case.

The following table shows all the slots associated with WPC certificates in the ECC608-TFLXWPC:

Table 3-4. Slots for Certificates

WPC Slot 0	WPC Slot 1	Description
0	1	Primary WPC private key. The public key can be generated at any time using the `GenKey` command in Mode = 0x00.
4	8	Extra data needed for the manufacturer or product unit certificate
5	8	RSID needed for the product unit certificate
13	8	Product unit certificate. This is stored in a WPC compressed format.
9	8	Signer public key.
14	8	Manufacturer certificate. This is stored in a WPC compressed format.

For the ECC608-TFLXWPC production units, these slots can be configured as either permanent or slot lockable. To facilitate early development, Slots 4, 5, 8, 9, 13 and 14 are set to slot lockable for the prototype units.

3.2.1.4 WPC Slot Digests

As an alternative to doing a full authentication using certificates, the WPC authentication specification allows for a rapid authentication to be done by simply comparing the digest associated with WPC Slot 0 or WPC Slot 1, if so defined. For this method to be used, a full authentication must be previously done and the digest of the WPC Slot must be calculated and stored.

The digest value is a 32-byte value calculated as a SHA-256 hash over the entire WPC Slot. The specification allows for a digest for each of the defined WPC certificate slot. The ECC608-TFLXWPC has storage for two digests. Device Slot 3 is used for WPC Slot 0. WPC Slot 1 digest is stored in Slot 8[288:319].

3.2.1.5 Secure Boot

The `SecureBoot` command is enabled for the ECC608-TFLXWPC. 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, then slot locked to make it permanent.

For the ECC608-TFLXWPC, it is also possible to enable the TLS primary private key and the WPC Slot 0 and WPC Slot 1 ECC keys to require a valid secure boot prior to being authorized for use. See 3.2.4 Secure Boot Option on how to enable this capability.

See 4.2.3 SecureBoot Command for full details.

To implement the secure boot, 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 ECC608-TFLXWPC, the digest is stored in Slot 7.

Secure Boot Public Key
The secure boot public key is used for a verify function to validate the secure boot digest and signature. The secure boot public key is stored in Slot 15.

3.2.1.6 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^{2}C bus. However, before this feature can be used, the MCU and ECC608-TFLXWPC need to generate and save a unique I/O protection key, essentially pairing the MCU and ECC608-TFLXWPC 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 ECC608-TFLXWPC.

3.2.1.7 General Data Storage

All slots are set up for a defined purpose but not all features are required. If the WPC Slot 1 information is not required, Slots 4 and 8 may be used for general purpose data storage. If the TLS authentication use case is not required, Slots 10-12 can be available for general purpose data storage. Data can be written during provisioning or can be left slot lockable and allowed to be written in the field.

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**

AES Key Slot can be used as a key source for `AES` commands. The AES key is 128 bits in width for the ECC608-TFLXWPC.

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

3.2.3 ECC608-TFLXWPC Slot Configuration Summary

The ECC608-TFLXWPC 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 ECC608-TFLXWPC:

Table 3-5. Slots Configuration

Slot	Use Case	Description	Primary Configuration
0	WPC Slot 0 authentication	WPC Slot 0 primary ECC authentication key	Permanent, Ext Sign, Not Readable, Optional Secure Boot Enable
1[1]	WPC Slot 1 authentication	WPC Slot 1 primary ECC authentication key	Permanent, Ext Sign, Not Readable, Optional Secure Boot Enable
2	TLS authentication	Primary TLS ECC authentication key	Permanent, Ext Sign, ECDH, Not Readable, Optional Secure Boot Enable
3	WPC Slot 0 authentication	WPC Slot 0 certificate chain digest	Permanent or Writable and Slot Lockable, Clear Text Read depending on access policies
4	WPC Slot 0 authentication	WPC Slot 0 extra information	Permanent or Writable and Slot Lockable, Clear Text Read depending on access policies
5	WPC Slot 0 authentication	WPC Slot 0 extra information	Permanent or Writable and Slot Lockable, Clear Text Read depending on access policies
6	I/O protection key	Key used to protect the I^2C bus communication (I/O) of certain commands. Requires setup before use.	Permanent or Writable and Slot Lockable, Never Read depending on access policies

...........continued

Slot	Use Case	Description	Primary Configuration
7	Secure Boot	Storage location for secure boot digest. This is an internal function, so no reads or writes are enabled.	No Read, No Write
8[2]	WPC Slot 1 authentication	Storage of WPC Slot 1 information public key, certificate and slot digest	Clear Text Read, Writable or Lockable depending on access policies
9	WPC Slot 0 authentication	WPC Slot 0 manufacturer public key	Permanent, Clear Read, No Write or Writable depending on access policies
10	TLS authentication	TLS device compressed certificate in CryptoAuthentication™ compressed format	Permanent, Clear Read, No Write or Writable depending on access policies
11	TLS authentication	TLS public key for the CA (signer) that signed the device certificate	Clear Read, No Write or Writable depending on access policies
12	TLS authentication	TLS 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
13	WPC Slot 0 authentication	WPC Slot 0 compressed device certificate	Permanent, Clear Read, No Write or Writable depending on access policies
14	WPC Slot 0 authentication	WPC Slot 0 compressed manufacturer certificate	Permanent, Clear Read, No Write or Writable depending on access policies
15	Secure Boot	Secure boot public key	Permanent or Writable and Lockable with Clear Text Read

Notes:

1. This slot is always reserved for an ECC private key. If WPC Slot 1 is not required, it may alternately contain a private key for use with WPC Slot 2 or some other purpose.
2. If WPC Slot 1 is not used in the application, this slot may be used for the WPC Slot 2 or 3 information. It is recommended that this slot be locked if it is used for public key or certificate information. If no other WPC slots are required, this slot may be used to store general purpose data.

3.2.4 ECC608-TFLXWPC Detailed Slot Access Policies

The ECC608-TFLXWPC default configuration for WPC uses only the information associated with WPC Slot 0. All information in the device slots associated with WPC Slot 0 is mandatory as part of the authentication procedure or certificate chain, with the exception of the WPC Slot 0 digest stored in Slot 3.

Attention: Check with Microchip prior to using features beyond the default WPC Slot 0 configuration as not all features are initially implemented in the provisioning systems.

The ECC608-TFLXWPC provides flexibility in two areas.

1. Whether slots are permanently locked or slot lockable.
2. Whether secure boot is connected to keys 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 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 is locked, no future modifications to the data in the slot is possible.

Permanent Lock A permanently locked slot can never 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 ECC private keys in Slot 0, 1 and 2 may be set to require a secure boot before these keys are authorized for use for most commands. To use this feature, a change to the secure boot configuration settings and to the key configuration values is required. These configuration changes will set the persistent latch upon a successful secure boot. The slot access policy changes for Slot 0 tie use of the key to the persistent latch being set.

Persistent Latch Operation

The persistent latch will retain its 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 has all the 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 only available with an I^{2}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 ECC608-TFLXWPC device on a slot by slot basis.

Table 3-6. Slot 0 Configuration Information

Slot	Configuration Value	Description of Enabled Features
0	**Option 1: Not Connected to Persistent Latch**	
	Key:	**WPC Slot 0 ECC Private Key** • Contains P-256 NIST ECC private key • The corresponding public key can always be generated • Random nonce is required
	Slot:	• Slot is secret • Can sign external messages
	Option 2: Connected to Persistent Latch	
	Key:	Same as above plus: • Secure boot must be run before this key can be used
	Slot:	Same as above

Table 3-7. Slot 1 Configuration Information

Slot	Configuration Value	Description of Enabled Features
1	**Option 1: Not Connected to Persistent Latch**	
	Key:	**WPC Slot 1 ECC Private Key** • Contains P-256 NIST ECC private key • The corresponding public key can always be generated • Random nonce is required
	Slot:	• Slot is secret • Can sign external messages
	Option 2: Connected to Persistent Latch	
	Key:	Same as above plus: • Secure boot must be run before this key can be used
	Slot:	Same as above

Table 3-8. Slot 2 Configuration Information

Slot	Configuration Value	Description of Enabled Features
2	**Option 1: Not Connected to Persistent Latch**	
	Key:	**TLS Session Private Key** • Contains P-256 NIST ECC private key • The corresponding public key can always be generated • Random nonce is required
	Slot:	• Slot is secret • Can sign external messages • Can use with `ECDH` command
	Option 2: Connected to Persistent Latch	
	Key:	• Same as Option 1 • Persistent Disable Option Enabled
	Slot:	• Same as Option 1

Table 3-9. Slot 3 Configuration Information

Slot	Configuration Value	Description of Enabled Features
3	**Option 1: Permanently Locked**	

...........continued

Slot	Configuration Value	Description of Enabled Features
	Key:	**WPC Slot 0 Digest** • Contains 32-byte digest of WPC Slot 0 certificate chain • This slot is permanently locked
	Slot:	• Can always be read in the clear • Permanent
	Option 2: Slot Lockable and Writable	
	Key:	• Slot is lockable
	Slot:	• Slot can be written in the clear • Slot can always be read

Table 3-10. Slot 4 Configuration Information

Slot	Configuration Value	Description of Enabled Features
4	**Option 1: Permanent Data**	
	Key:	**WPC Slot Other Data** • Used to store WPC Slot 0 other data • Slot is permanent
	Slot:	• Can always be read in the clear • Permanent
	Option 2: Slot Lockable and Writable	
	Key:	• Used to store WPC Slot 0 other data • Slot is writable
	Slot:	• Can always be read in the clear • Slot can be locked

Table 3-11. Slot 5 Configuration Information

Slot	Configuration Value	Description of Enabled Features
5	**Option 1: Permanent Data**	
	Key:	**WPC Slot 0 Other Data (Cont)** • Used to store WPC Slot 0 other data • Slot is permanent
	Slot:	• Can always be read in the clear • Permanent
	Option 2: Slot Lockable and Writable	
	Key:	• Used to store WPC Slot 0 other data • Slot is writable
	Slot:	• Can always be read in the clear • Slot can be locked

Table 3-12. Slot 6 Configuration Information

Slot	Configuration Value	Description of Enabled Features
6	**Option 1: Slot is Lockable**	
	Key:	**I/O Protection Key** • Can contain a SHA-256 symmetric key or other data. If the I/O protection key is not used, this slot can be used for other data. • A random nonce is required when this key is used • This slot can be individually locked
	Slot:	• Data can be written in the clear • The contents of this slot are secret and cannot be read • Slot cannot be used for the `CheckMac Copy` command
	Option 2: Permanent Lock	
	Key:	• Same as Option 1 except the slot is permanently locked
	Slot:	• Same as Option 1 except the slot cannot be written

Important: 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, a Permanent Lock option can be selected.

Table 3-13. Slot 7 Configuration Information

Slot	Configuration Value	Description of Enabled Features
7	Key:	**Secure Boot Digest** • This slot is designated to be used for other data
	Slot:	• This slot cannot be directly written or read • This slot is secret and cannot be used by the `MAC` command • This slot cannot be used for `CheckMac Copy` command

Table 3-14. Slot 8 Configuration Information

Slot	Configuration Value	Description of Enabled Features
8	**Option 1: Slot Lockable**	
	Key:	**WPC Slot 1 Data** • This slot is designated for WPC Slot 1 data • Slot is lockable
	Slot:	• Clear text writes and reads are permitted to this slot • Slot cannot be used for the `CheckMac Copy` command
	Option 2: Permanent Lock	
	Key:	• Same as Option 1 except the slot is permanently locked
	Slot:	• Same as Option 1 except the slot cannot be written

Table 3-15. Slot 9 Configuration Information

Slot	Configuration Value	Description of Enabled Features
9	**Option 1: Permanently Locked**	
	Key:	**WPC Slot 0 Public Key** • Slot is defined for ECC key • ECC key is a public key
	Slot:	• Data cannot be overwritten • Data can be read in the clear
	Option 2: Slot Lockable *Note: This Configuration is Used for Prototype Units*	
	Key:	• All features as shown in Option 1 • Slot is lockable
	Slot:	• Same as Option 1 except the slot can be written

Table 3-16. Slot 10 Configuration Information

Slot	Configuration Value	Description of Enabled Features
10	**Option 1: Permanently Locked**	
	Key:	**Device Compressed Certificate** • Slot defined to store other data
	Slot:	• Data cannot be overwritten • Data can be read in the clear
	Option 2: Slot Lockable *Note: This Configuration is Used for Prototype Units*	
	Key:	• All features as shown in Option 1 • Slot is lockable
	Slot:	• Same as Option 1 except the slot can be written

Table 3-17. Slot 11 Configuration Information

Slot	Configuration Value	Description of Enabled Features
11	**Option 1: Permanently Locked**	
	Key:	**Signer Public Key** • Slot is defined for ECC key • ECC key is a public key
	Slot:	• Data cannot be overwritten • Data can be read in the clear
	Option 2: Slot Lockable *Note: This Configuration is Used for Prototype Units*	
	Key:	• All features as shown in Option 1 • Slot is lockable
	Slot:	• Same as Option 1 except the slot can be written

Table 3-18. Slot 12 Configuration Information

Slot	Configuration Value	Description of Enabled Features
12	**Option 1: Permanently Locked**	
	Key:	**Signer Compressed Certificate** • Slot defined to store other data
	Slot:	• Data cannot be overwritten • Data can be read in the clear
	Option 2: Slot Lockable *Note: This Configuration is Used for Prototype Units*	
	Key:	• All features as shown in Option 1 • Slot is lockable
	Slot:	• Same as Option 1 except the slot can be written

Table 3-19. Slot 13 Configuration Information

Slot	Configuration Value	Description of Enabled Features
13	**Option 1: Permanently Locked**	
	Key:	**WPC Slot 0 Device Compressed Certificate** • Slot defined to store other data
	Slot:	• Data cannot be overwritten • Data can be read in the clear
	Option 2: Slot Lockable *Note: This Configuration is Used for Prototype Units*	
	Key:	• All features as shown in Option 1 • Slot is lockable
	Slot:	• Same as Option 1 except the slot can be written

Table 3-20. Slot 14 Configuration Information

Slot	Configuration Value	Description of Enabled Features
14	**Option 1: Permanently Locked**	
	Key:	**WPC Slot 0 MFG Compressed Certificate** • Slot defined to store other data
	Slot:	• Data cannot be overwritten • Data can be read in the clear
	Option 2: Slot Lockable *Note: This Configuration is Used for Prototype Units*	
	Key:	• All features as shown in Option 1 • Slot is lockable
	Slot:	• Same as Option 1 except the slot can be written

Table 3-21. Slot 15 Configuration Information

Slot	Configuration Value	Description of Enabled Features
15	**Option 1: Slot is Lockable**	
	Key:	**Secure Boot Public Key** • Slot is defined for ECC key • Slot is lockable
	Slot:	• Always writable unless locked • Slot can always be read
	Option 2: Permanently Locked	
	Key:	• Same as Option 1 except the slot is permanently locked
	Slot:	• Same as Option 1 except the slot cannot be written

3.3 ECC608-TFLXWPC 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 ECC608-TFLXWPC, the OTP zone is shipped pre-locked and contains the following information:

I^{2}C device version

```
60 1B 1E 85 3B 13 C7 75 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 00 00 00 00
```

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

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

4. Device Commands

The following section details all the commands broken out by the Command mode that are allowed in the ECC608-TFLXWPC. There are 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
The multibyte input parameters display as big-endian (MSB first) values in the input parameters tables, unless otherwise specified. Note that the ECC608-TFLXWPC device actually expects the data to be sent little-endian (LSB first).

Table 4-1. Command Opcodes, Short Descriptions and Command Categories

Command	Description	Command Category
`Counter`	Reads or increments one of the monotonic counters	General Device Commands
`ECDH`	Generates an ECDH pre-master secret using stored private key and input public key	Asymmetric Cryptography Command
`GenKey`	Generates an ECC public key. Optionally generates an ECC private key	Asymmetric Cryptography Command
`Info`	Returns device state information	General Device Commands
`Lock`	Prevents further modifications to a zone or slot of the device	General Device Commands
`Nonce`	Generates a 32-byte random number and an internally stored Nonce	General Device Commands
`Random`	Generates a random number	General Device Commands
`Read`	Reads 4 or 32 bytes from the device, with or without authentication and encryption	General Device Commands
`SecureBoot`	Validates code signature or code digest on power-up	Asymmetric Cryptography Command
`SelfTest`	Tests the various internal cryptographic computation elements	General Device Commands
`Sign`	ECDSA signature calculation	Asymmetric Cryptography Command
`SHA`	Computes a SHA-256 or HMAC digest for general purpose use by the system	General Device Commands
`UpdateExtra`	Updates bytes 84 or 85 within the Configuration zone after the Configuration zone is locked	General Device Commands

...........continued

Command	Description	Command Category
Verify	ECDSA verify calculation	Asymmetric Cryptography Command
Write	Writes 4 or 32 bytes to the device, with or without authentication and encryption	General Device Commands

4.1 General Device Commands

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

Table 4-2. 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

4.1.1 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 ECC608-TFLXWPC, 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.

4.1.2 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.

4.1.3 Lock Command

For the ECC608-TFLXWPC, the Configuration zone is already locked and the access policies of the Data zone are 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.

4.1.4 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.

4.1.5 `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.

4.1.6 `Read` Command

The `Read` command can be used to access any of the EEPROM zones of the ECC608-TFLXWPC 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.

4.1.7 `SelfTest` Command

The `SelfTest` command performs a test of one or more of the cryptographic engines within the ECC608-TFLXWPC chip. Some or all of the algorithms will be tested depending on the Input mode parameter.

For the ECC608-TFLXWPC 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.

4.1.8 `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 ECC608-TFLXWPC 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.

4.1.9 `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 ECC608-TFLXWPC device, the UpdateExtraAdd byte (byte 85) is configured to be an alternate I^2C address.

4.1.10 `Write` Command

For the ECC608-TFLXWPC, the Configuration zone and OTP zone are 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.

4.2 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 4-3. 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

4.2.1 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.

4.2.2 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.

4.2.3 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 ECC608-TFLXWPC to assist in validating the application code that is to be subsequently executed. The ECC608-TFLXWPC device is 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, the SecureBoot may or may not be tied to power-up. 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 ECC608-TFLXWPC.

4.2.4 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.

4.2.5 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.

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 ECC608-TFLXWPC 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.

4.3 Symmetric Cryptography Commands

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

Table 4-4. Symmetric Cryptography Commands

Command Name	Description
`GenDig`	Generates a data digest from a random or input seed and a stored value
`MAC`	Calculates the digest (response) from the key and other internal data using SHA-256

4.3.1 `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.

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.

4.3.2 `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.

5. I^{2}C Interface

The I^{2}C interface uses the SDA and SCL pins to indicate various I/O states to the ECC608-TFLXWPC. 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 ECC608-TFLXWPC and AT24C16 have different default I^{2}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 ECC608-TFLXWPC 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 ECC608-TFLXWPC 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^{2}C standard uses the terminology “Master” and “Slave”. The equivalent Microchip terminology used in this document is “Host” and “Client”, respectively.

5.1 I/O Conditions

The device responds to the following I/O conditions:

5.1.1 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 ≥ t_{WLO}, the device exits the Low-Power mode. After a delay of t_{WHI}, it will be ready to receive I^{2}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 5.1.2 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 0x00 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^{2}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 0x00 at 100 kHz. Subsequent commands can be run at a higher frequency.

In the I^{2}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^{2}C interface is run at speeds of less than ~300 kHz[1], the transmission of certain data patterns will cause the ECC608-TFLXWPC 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 ECC608-TFLXWPC will not respond but will be awake. It is recommended that after communicating with another device at slow frequencies, a sleep or idle sequence be issued to place the ECC608-TFLXWPC back into a known state.

[1] The actual frequency for a given device will vary with process and environmental factors. This value is considered safe under all conditions.

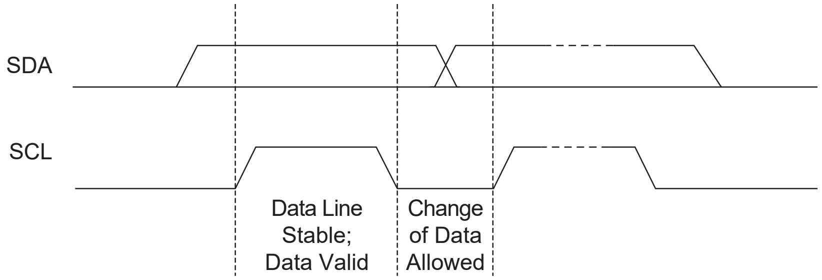
Important: t_{WLO} is the minimum time that the system must provide to ensure that the ECC608-TFLXWPC will wake under all manufacturing and environmental conditions. In actuality, the device may wake up with a lesser pulse width.

5.1.2 Device is Awake

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

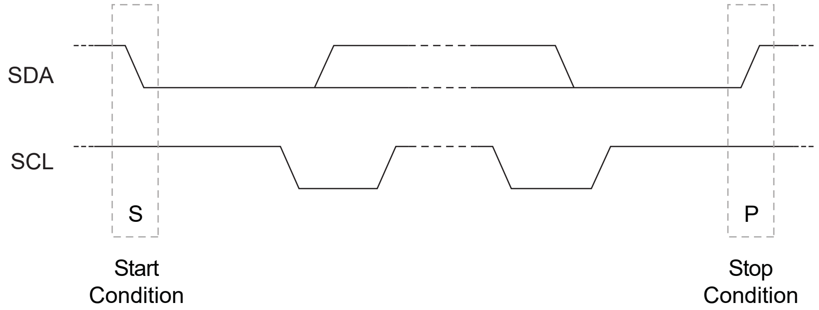
- **DATA Zero**: If SDA is low and stable while SCL goes from low to high to low, then a zero bit is being transferred on the bus. SDA can change while SCL is low.
- **DATA One**: If SDA is high and stable while SCL goes from low to high to low, then a one bit is being transferred on the bus. SDA can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

Figure 5-1. Data Bit Transfer on I^{2}C Interface



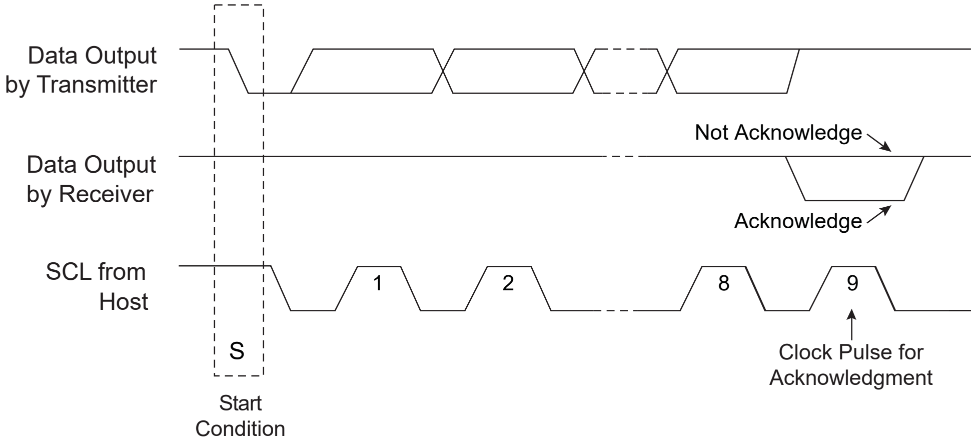
- **Start Condition**: A high-to-low transition of SDA with SCL high is a Start condition which must precede all commands.
- **Stop Condition**: A low-to-high transition of SDA with SCL high is a Stop condition. After this condition is received by the device, the current I/O transaction ends. On input, 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 5-2. Start and Stop Conditions on I^{2}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 5-3. NACK and ACK Conditions on I^{2}C Interface



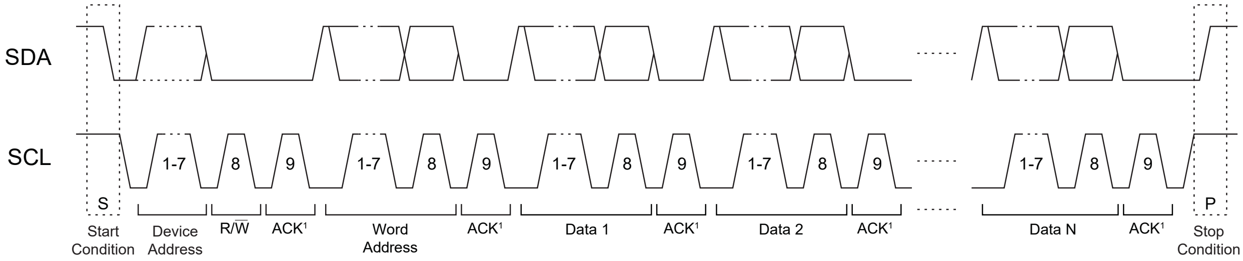
Multiple ECC608-TFLXWPC devices can easily share the same I^{2}C interface signals if the I2C_Address byte in the Configuration zone is programmed differently for each device on the bus. Because all seven of the bits of the device address are programmable, ECC608-TFLXWPC can also share the I^{2}C interface with any I^{2}C device, including any Serial EEPROM.

5.2 I^{2}C Transmission to ECC608-TFLXWPC

The transmission of data from the system to the ECC608-TFLXWPC 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 5-4. Normal I^{2}C Transmission to ECC608-TFLXWPC



SDA is driven low by the ECC608-TFLXWPC ACK periods.

The following tables label the bytes of the I/O transaction. The column labeled “I^{2}C Name” provides the name of the byte as described in the AT24C16 data sheet.

Table 5-1. I^{2}C Transmission to ECC608-TFLXWPC

Name	I^{2}C Name	Description
Device Address	Device Address	This byte selects a particular device on the I^{2}C interface. The ECC608-TFLXWPC 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^{2}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).
Word Address	Word Address	This byte must have a value of 0x03 for normal operation.

...........continued

Name	I^2C Name	Description
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^2C 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 ECC608-TFLXWPC will start the computation of the command. Failure to send a Stop condition may eventually result in a loss of synchronization; see 5.2.2 I2C Synchronization for recovery procedures.

Related Links

5.2.1 Word Address Values

5.2.1 Word Address Values

During an I^2C write packet, the ECC608-TFLXWPC interprets the second byte sent as the word address, which indicates the packet function as it is described in the table below:

Table 5-2. Word Address Values

Name	Value	Description
Reset	0x00	Resets the address counter. The next I^2C read or write transaction will start with the beginning of the I/O buffer.
Sleep (Low-power)	0x01	The ECC608-TFLXWPC 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 ECC608-TFLXWPC 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.

5.2.2 I^2C Synchronization

It is possible for the system to lose synchronization with the I/O port on the ECC608-TFLXWPC, perhaps due to a system Reset, I/O noise or other conditions. Under this circumstance, the ECC608-TFLXWPC 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:

1. To ensure an I/O channel Reset, the system must send the standard I^2C 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 ECC608-TFLXWPC 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 ECC608-TFLXWPC 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.

2. 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.
3. 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.

5.3 Sleep Sequence

Upon completion of the use of the ECC608-TFLXWPC 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.

5.4 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.

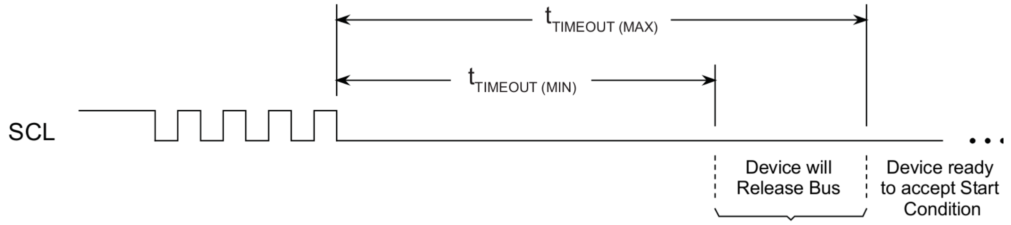
The idle sequence consists of the proper device address followed by the value of 0x02 as the word address followed by a Stop condition. It can be sent to the device at any time when it is awake and not busy.

5.5 SMBus Timeout

The ECC608-TFLXWPC supports the SMBus Timeout feature in which the ECC608-TFLXWPC will reset its serial interface and release the SMBus (i.e., stop driving the bus and let SDA float high) if the SCL pin is held low for more than the minimum $t_{TIMEOUT}$ specification.

When t $_{TIMEOUT}$ is reached, the device will go into sleep mode. The ECC608-TFLXWPC will be ready to accept a new wake sequence followed by a Start condition once the $t_{TIMEOUT}$ maximum has elapsed.

Figure 5-5. SMBus Timeout



5.6 I^{2}C Transmission from the ECC608-TFLXWPC

When the ECC608-TFLXWPC is awake and not busy, the host can retrieve the current output buffer contents from the device using an I^{2}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 5-3. I^2C Transmission from the ECC608-TFLXWPC

Name	I^2C Name	Direction	Description
Device Address	Device Address	To Client	This byte selects a particular device on the I^2C interface and the ECC608-TFLXWPC 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^2C 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 ECC608-TFLXWPC along the I^2C 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 ECC608-TFLXWPC 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 ECC608-TFLXWPC will NACK the device address to indicate that no data are available to be read.

Related Links

7.3.1 AC Parameters: I2C Interface

6. Application Information

The ECC608-TFLXWPC is a member of the Microchip's Trust CryptoAuthentication™ family of products. The TrustFLEX products are easy to use, simple to implement and allow even low volume users to implement security into their end system while leveraging Microchip's expertise and infrastructure in secure provisioning.

The ECC608-TFLXWPC device was developed to take the guesswork out of adding security to Qi-compliant wireless charging transmitters. The product is pre-configured to readily store one or two WPC certificate slot chains. If the WPC Slot 1 certificate chain is not utilized, it is available for a proprietary certificate chain to be stored and associated with WPC Slot 2.

Additionally, the ECC608-TFLXWPC device supports connections to the IoT Cloud in the same seamless manner as that of the ATECC608B-TFLXTLS and ATECC608B-TNGTLS products. This allows connections for wireless charging deployed in industry infrastructure applications such as restaurants, hotels, etc. If so required, the secure boot features enabled in the device can also be used to do a firmware check of the micro in the wireless charging transmitter prior to connecting to the cloud.

In addition to the actual security device, Microchip developed a series of tools that seamlessly integrate with their hardware devices to provide an easy path to developing an entire security solution. When 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.

6.1 WPC Engagement

All companies selling Qi-certified products must be members of the Wireless Power Consortium. All products intended to be sold as Qi certified must go through the Qi validation, test and certification procedures. Products are not allowed to claim Qi compliance or Qi certification if they do not go through the proper validation and test procedures. Manufacturers of Qi-certified products must be in good standing with Wireless Power Consortium.

For Qi 1.3 products that require authentication, additional measures are also required. An entity that wishes to manufacture products with authentication must be licensed as a Qi-certified manufacturer. Products that need to be authenticated must have a Secure Storage Subsystem (SSS) that securely stores the ECC P-256 private key. A corporation that provides the SSS must be a WPC Qi Licensed Manufacturing Certificate Authority. Microchip has several products that meet the requirements of an SSS and the ECC608-TFLXWPC is one such product. Microchip is a Qi Certified Manufacturing CA.

Note that it is the responsibility of the manufacturer to select an SSS from a Qi-certified provider and the responsibility of the manufacturer CA to verify that a manufacturer is in good standing with the WPC.

Secure Production Provisioning Flow
The following is a typical provisioning flow for WPC production units:

1. The customer begins development work using the ECC608-TFLXWPC.
2. The customer opens a Microchip Sales Force support ticket for provisioned SSS.
3. The customer provides the PTMC and Qi ID to Microchip through the support ticket system.
4. Microchip validates the PTMC and Qi ID with the WPC to validate ownership.
5. Once validated, Microchip generates the appropriate certificates and sets up a certificate signing request to sign the manufacturing certificate with the WPC Root CA. (Note: Check with the WPC when this can happen.)
6. Once the signing ceremony is completed, Microchip will generate a limited number of validation units for the customer to evaluate. Evaluation consists of verifying that the units are programmed correctly and meet all requirements of the customer.
7. The customer provides notification to Microchip that the validation units are accepted.
8. The customer proceeds with completion of WPC certification testing.
9. Upon successful completion, the customer can request full production units and quantities.

6.2 Use Cases

The ECC608-TFLXWPC is defined to specifically address the authentication needs of the WPC Qi charging market. Microchip is an authorized Manufacturing CA for the WPC. In addition to security IC’s, Microchip also offers complete power receiver and power transmitter solutions with and without authentication for the wireless charging market.

Secure TLS Connection
The ECC608-TFLXWPC allows the creation of secure TLS connections using a variety of protocols. This application is beyond the specifications of the WPC authentication requirements but it is seen as an important piece in allowing Qi transmitters to proliferate in the Qi infrastructure market.

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 was not modified, the overall integrity of the system is maintained. The ECC608-TFLXWPC is 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 ECC608-TFLXWPC, verifying that the firmware was not tampered with. In addition, the authentication of TLS or WPC transmitters can be prevented until the secure boot occurs, based on the device configurations.

General Data Storage
Sometimes there is a need to store a small amount of additional information for a given system. The ECC608-TFLXWPC can be used for this purpose by using those data slots where data can be readily read and written. This eliminates the need to add an additional EEPROM memory device to store data.

6.3 Development Tools

The ECC608-TFLXWPC 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 ECC608-TFLXWPC 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 ECC608-TFLXWPC devices can be ordered through Microchip Direct.

6.3.1 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 ECC608-TFLXWPC.

Note: More information on these tools can be found on Microchip’s Trust Platform information page.

6.3.2 Hardware Tools

There are multiple hardware tools that can help in developing with the ECC608-TFLXWPC. 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 ATSAMD21 microcontroller, 1-each of the ATECC608B-TNGTLS, ATECC608B-TFLXTLS and ATECC608B-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 associated with the various Trust devices. The kit can be used with either MPLAB® X or Microchip Studio Design environments to develop additional applications. Through use of mikroBUS add-on boards, the kit can be used with ECC608-TFLXWPC.

DM320109 – CryptoAuthentication Starter Kit
The DM320109 consists of an ATSAMD21-XPRO development board pre-programmed with firmware that can work with CryptoAuthentication devices. The kit comes with the AT88CKSCKTSOIC-XPRO socket board but the UDFN version of the board will need to be obtained to work with the sample devices that are currently provided only in the UDFN package. Specific samples of the ECC608-TFLXWPC 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 ECC608-TFLXWPC must be acquired to be used with these kits.

Microchip Wireless Power Solutions
Complete wireless power transmitters and receivers are also available based on dsPIC® Digital Signal Controllers. The Microchip solutions encompass both Qi 1.3 solutions that require authentication and Qi 1.2 solutions as well as other proprietary solutions. More information on all Microchip Wireless Power Solutions can be found at www.microchip.com/en-us/solutions/power-management-and-conversion/intelligent-power/wireless-power.

6.3.3 CryptoAuthLib

CryptoAuthLib is a software library that supports Microchip's family of CryptoAuthentication devices. Microchip recommends working with this library when developing with the ECC608-TFLXWPC. 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 6-1. 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()	

...........continued

Device Command	API Call	Comments
Verify	atcab_verify()	

7. Electrical Characteristics

7.1 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_{CC} + 0.5V)	-0.5V to (V_{CC} + 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.

7.2 Reliability

The ECC608-TFLXWPC is fabricated with Microchip’s high reliability CMOS EEPROM manufacturing technology.

Table 7-1. EEPROM Reliability

Parameter	Min.	Typ.	Max.	Units
Write Endurance at +85°C (Each Byte)	400,000	—	—	Write Cycles
Data Retention at +55°C	10	—	—	Years
Data Retention at +35°C	30	50	—	Years
Read Endurance	Unlimited			Read Cycles

7.3 AC Parameters: All I/O Interfaces

Figure 7-1. AC Timing Diagram: All Interfaces

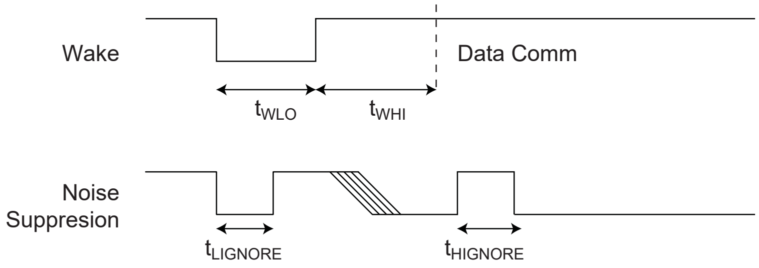


Table 7-2. AC Parameters: All I/O Interfaces

Parameter	Sym.	Direction	Min.	Typ.	Max.	Units	Conditions
Power-Up Delay[2]	t_{PU}	To Crypto Device	100	—	—	μs	Minimum time between V_{CC} > V_{CC} min prior to start of t_{WLO}.
Wake Low Duration	t_{WLO}	To Crypto Device	60	—	—	μs	—
Wake High Delay to Data Comm	t_{WHI}	To Crypto Device	1500	—	—	μs	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	$t_{HIGNORE\_A}$	To Crypto Device	45[1]	—	—	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	$t_{LIGNORE\_A}$	To Crypto Device	45[1]	—	—	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	$t_{LIGNORE\_S}$	To Crypto Device	15[1]	—	—	μs	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. The power-up delay will be significantly longer if power-on self test is enabled in the Configuration zone.

7.3.1 AC Parameters: I²C Interface

Figure 7-2. I²C Synchronous Data Timing

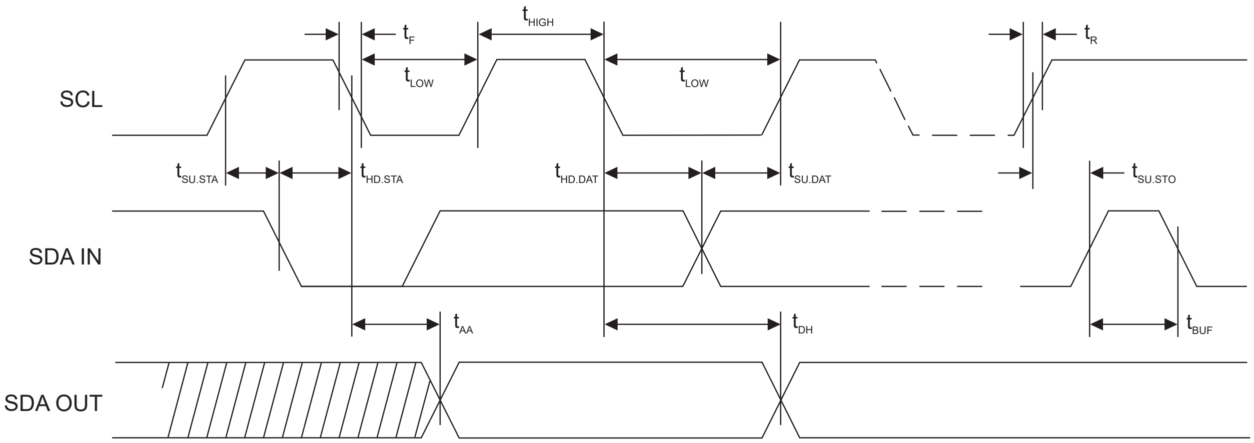


Table 7-3. AC Characteristics of I²C Interface(2)

Unless otherwise specified, applicable over recommended operating range from T_A = -40°C to +85°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[1]	t_R	—	300	ns
Input Fall Time[1]	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[1]	t_{BUF}	500	—	ns

Notes:

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

7.4 DC Parameters: All I/O Interfaces

Table 7-4. DC Parameters on All I/O Interfaces

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Ambient Operating Temperature	T_A	-40	—	+85	°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	—	µA	When device is in Idle mode, V_{SDA} and V_{SCL} < 0.4V or > V_{CC} – 0.4
Sleep Current	I_{SLEEP}	—	30	150	nA	When device is in Sleep mode, V_{CC} ≤ 3.6V, V_{SDA} and V_{SCL} < 0.4V or > V_{CC} – 0.4, T_A ≤ +55°C
		—	—	2	µA	When device is in Sleep mode. Over full V_{CC} and temperature range.

...........continued

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Output Low Voltage	V_{OL}	—	—	0.4	V	When device is in Active mode, V_{CC} = 2.5 to 5.5V
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	Θ_{JA}	—	166	—	°C/W	SOIC (SSH)
		—	173	—	°C/W	UDFN (MAH)

7.4.1 V_{IH} and V_{IL} Specifications

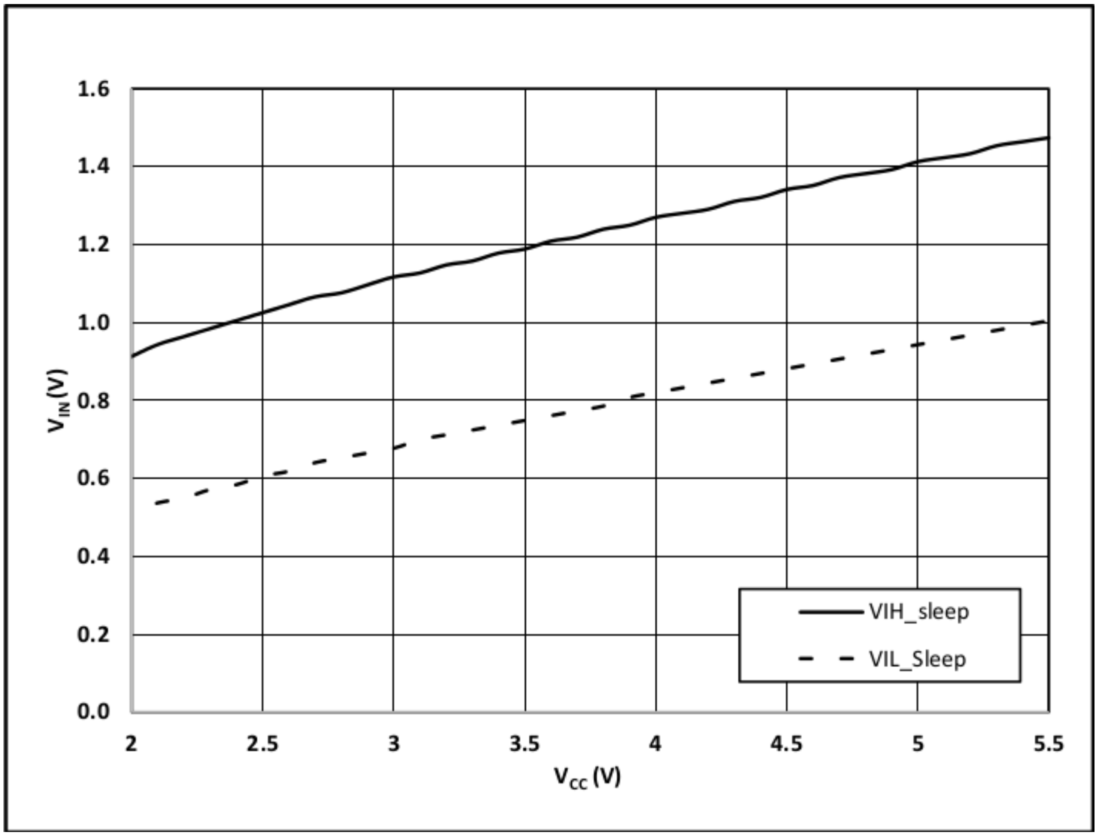
The input levels of the device will vary dependent on the mode and voltage of the device. The input voltage thresholds when in Sleep or Idle mode are dependent on the V_{CC} level as shown in Figure 7-3. When in Sleep or Idle mode the TTLenable bit has no effect.

The active input levels of the ECC608-TFLXWPC 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 7-5. 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 7-3. V_{IH} and V_{IL} in Sleep and Idle Mode



8. Package Drawings

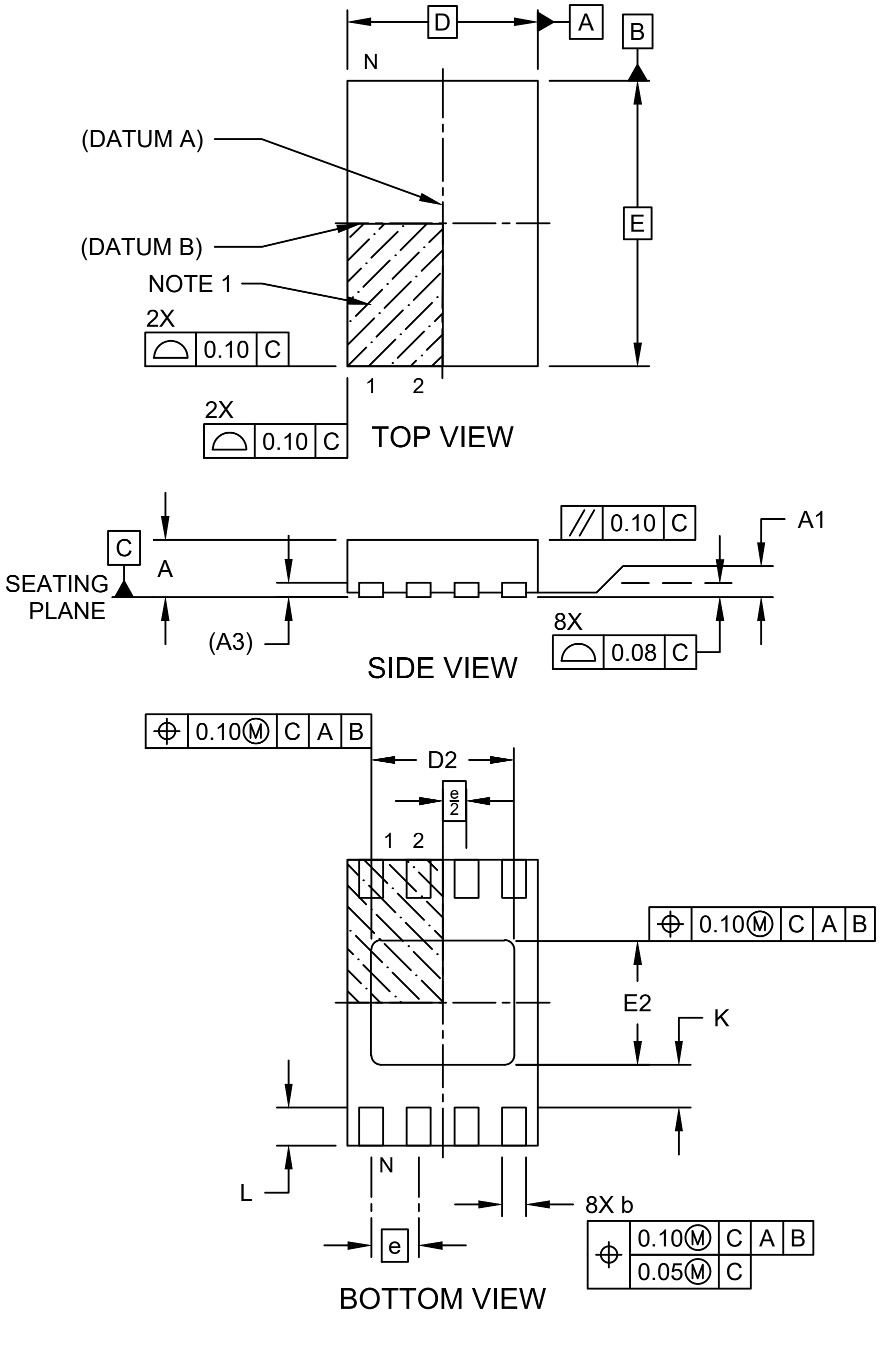
8.1 Package Marking Information

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.

8.2 8-pad UDFN

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

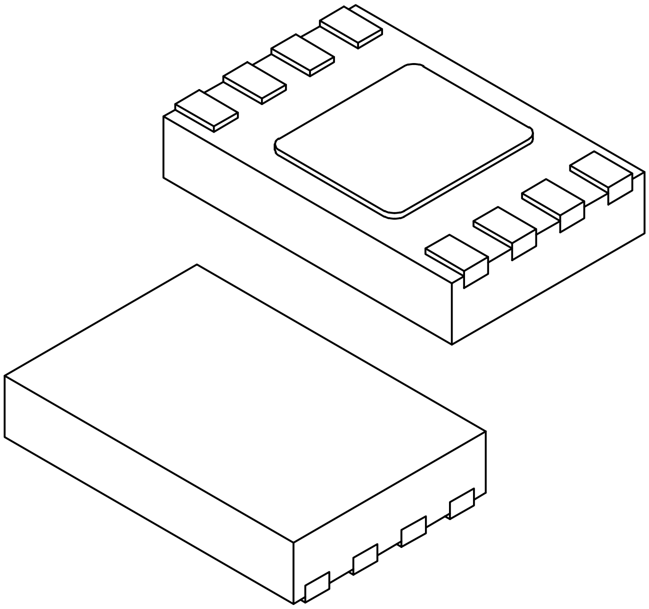
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing C04-21355-Q4B Rev B 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



	Units	MILLIMETERS		
	Dimension Limits	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	0.35	0.40	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

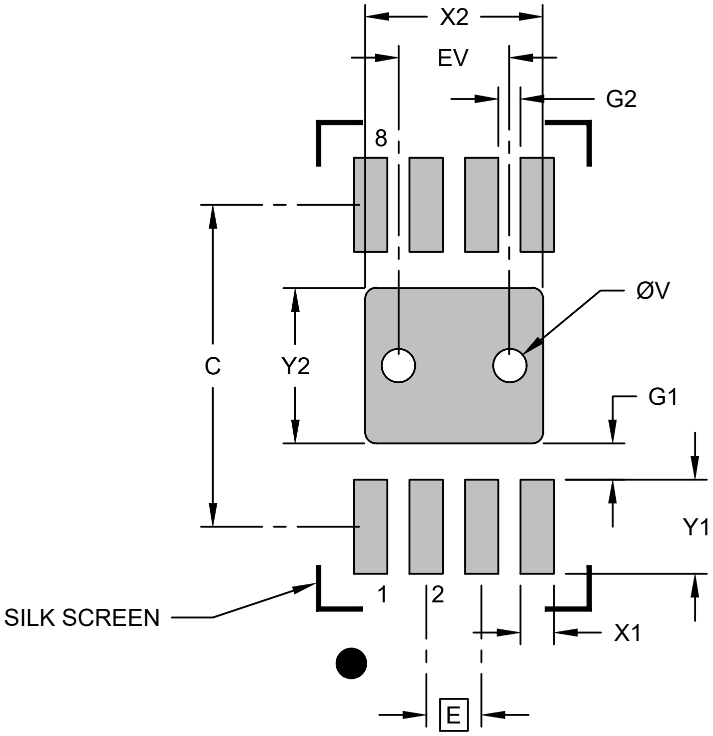
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

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

Microchip Technology Drawing C04-21355-Q4B Rev B 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

	Units	MILLIMETERS		
	Dimension Limits	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:

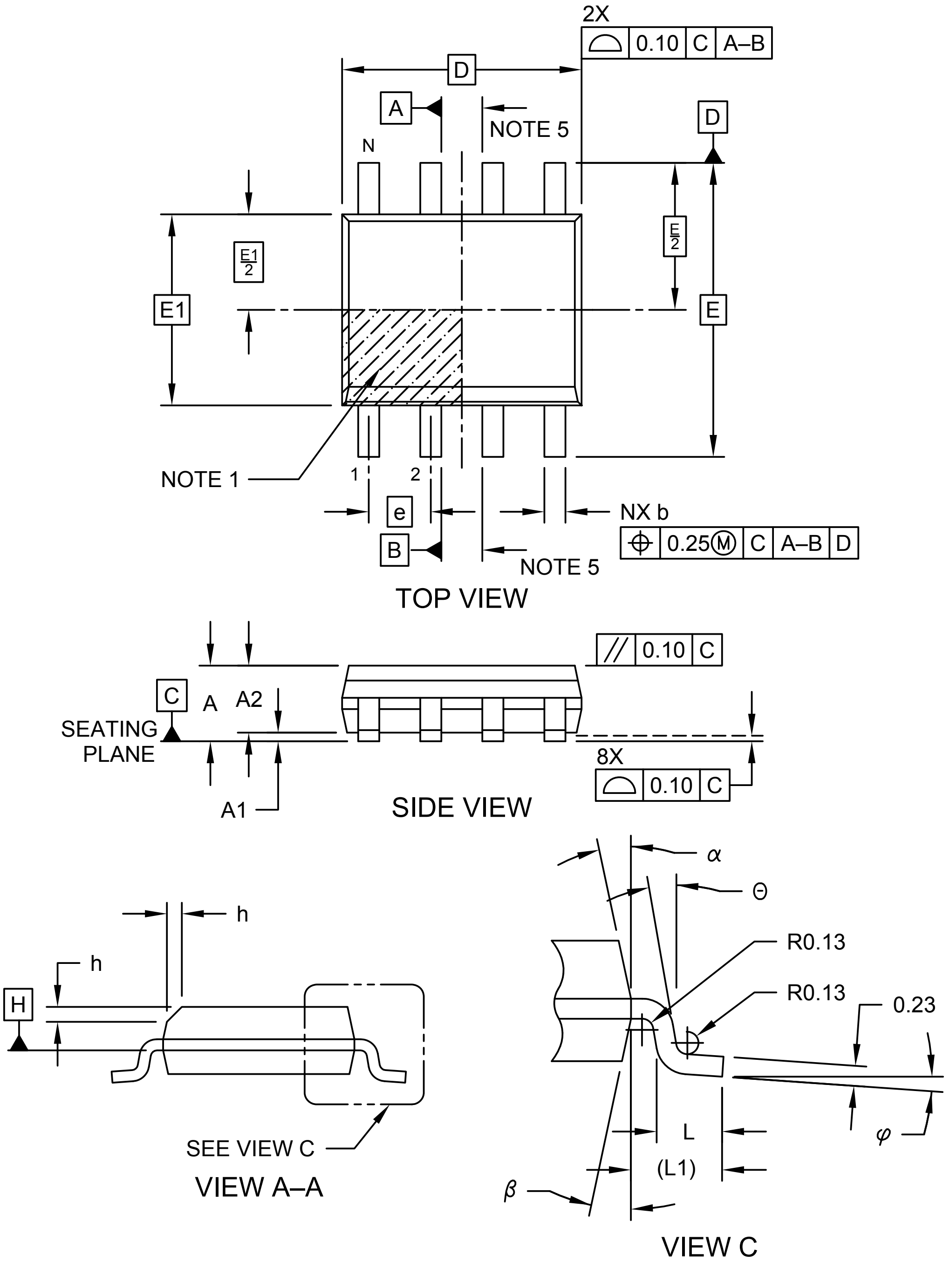
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
2. For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

Microchip Technology Drawing C04-23355-Q4B Rev B

8.3 8-lead SOIC

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

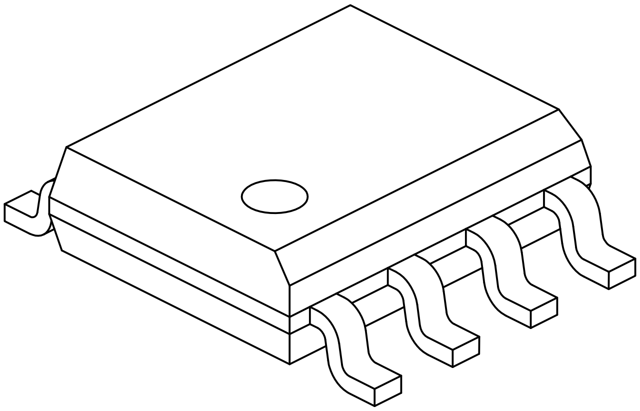
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing No. C04-057-SWB Rev E Sheet 1 of 2

8-Lead Plastic Small Outline - 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



	Units	MILLIMETERS		
	Dimension Limits	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		
Foot Angle	φ	0°	-	8°
Lead Thickness	c	0.17	-	0.25
Lead Width	b	0.31	-	0.51
Mold Draft Angle Top	α	5°	-	15°
Mold Draft Angle Bottom	β	5°	-	15°

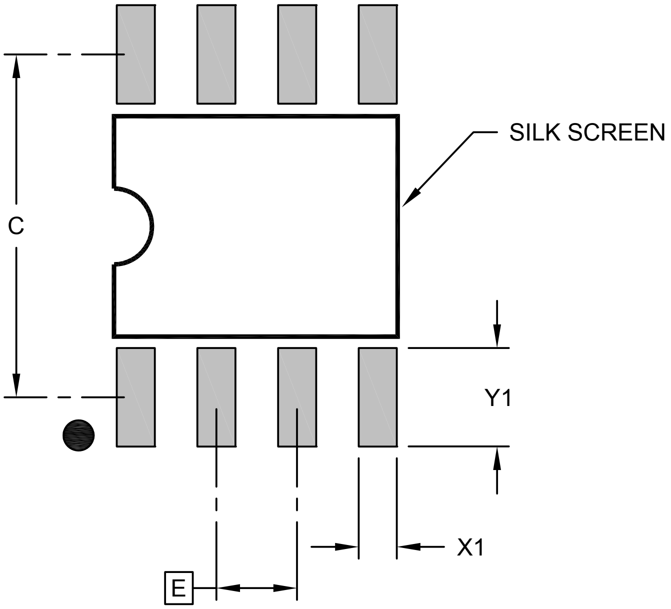
Notes:

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. § Significant Characteristic
3. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.15mm per side.
4. 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.
5. Datums A & B to be determined at Datum H.

Microchip Technology Drawing No. C04-057-SWB Rev E Sheet 2 of 2

8-Lead Plastic Small Outline - 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



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		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-SWB Rev E

9. Revision History

Revision A (September 2021)
Original release of the document

The Microchip Website

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

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

Product Change Notification Service

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

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

Customer Support

Users of Microchip products can receive assistance through several channels:

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

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

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

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.	X	-X
Device	Package Type	Tape and Reel

Device:	ECC608-TFLXWPC: Pre-configured Cryptographic Coprocessor with secure hardware-based key storage	
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)
Tape and Reel Options		2k Reel
	PROTO	10 Units Bulk – Prototype Units

Examples:

- ECC608-TFLXWPCU: TrustFLEX TLS, Provisioned, 8-UDFN, 2K Reel MOQ, I^{2}C Interface
- ECC608-TFLXWPCU-PROTO: TrustFLEX TLS, Provisioned Prototype, 8-UDFN, 10 Units Bulk, SWI or I^{2}C Interface
- ECC608-TFLXWPCS: TrustFLEX TLS, Provisioned, 8-SOIC 2K Reel MOQ, I^{2}C Interface
- ECC608-TFLXWPCS-PROTO: TrustFLEX TLS, Provisioned Prototype, 8-SOIC 10 Units Bulk, I^{2}C Interface

Note:

1. Tape and Reel identifier only appears in the catalog part number description. This identifier is used for ordering purposes and is not printed on the device package. Check with your Microchip Sales Office for package availability with the Tape and Reel 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.

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

AgileSwitch, APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, IntelliMOS, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet- Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, TrueTime, WinPath, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, Augmented Switching, BlueSky, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, GridTime, IdealBridge, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, NVM Express, NVMe, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, TSHARC, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

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

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, Symmcom, and Trusted Time are registered trademarks of Microchip Technology Inc. in other countries.

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

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

ISBN: 978-1-5224-8662-6

Quality Management System

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

Worldwide Sales and Service

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
www.microchip.com/support
Web Address:
www.microchip.com

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

Austin, TX
Tel: 512-257-3370

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

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

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

Detroit
Novi, MI
Tel: 248-848-4000

Houston, TX
Tel: 281-894-5983

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

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

Raleigh, NC
Tel: 919-844-7510

New York, NY
Tel: 631-435-6000

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

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

ASIA/PACIFIC

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

China - Xiamen
Tel: 86-592-2388138

China - Zhuhai
Tel: 86-756-3210040

ASIA/PACIFIC

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

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

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

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

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

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

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

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

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

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

Singapore
Tel: 65-6334-8870

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

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

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

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

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

EUROPE

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

Denmark - Copenhagen
Tel: 45-4485-5910
Fax: 45-4485-2829

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

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

Germany - Garching
Tel: 49-8931-9700

Germany - Haan
Tel: 49-2129-3766400

Germany - Heilbronn
Tel: 49-7131-72400

Germany - Karlsruhe
Tel: 49-721-625370

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

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

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

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

Italy - Padova
Tel: 39-049-7625286

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

Norway - Trondheim
Tel: 47-72884388

Poland - Warsaw
Tel: 48-22-3325737

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

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

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

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

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