SHA104-TFLXAUTH CryptoAuthentication™ Data Sheet

SHA104-TFLXAUTH

Introduction

The SHA104-TFLXAUTH is a member of the Microchip Technology Inc. Trust Platform product family. The device is a preprovisioned SHA104 targeted for symmetric authentication applications and is ideally suited for consumable and disposable applications. The device can be used in systems where either the host can assist in the authentication by way of a challenge-response pair or, for more security, can be used with a host side security device to perform a CheckMAC operation. The SHA104-TFLXAUTH can be paired with the SHA105-TFLXAUTH or other Microchip CryptoAuthentication host side devices.

Features

- Cryptographic Authentication Device with Secure Hardware-Based Key Storage:
  - Protected storage for symmetric key
- Hardware Support for MAC Generation
- Internal High-Quality NIST SP 800-90A/B/C Random Number Generator (RNG)
- Extensive Security Measures Against Attacks
- Strong Physical Protection Mechanisms Against Invasive Attacks
- Field-Programmable EEPROM
  - Single symmetric secret key
  - 384-byte user memory
  - 40-year data retention at +55℃
- Monotonic Counter with Max Count Value of 10,000
  - Counter can be attached to key for limited use
- Unique 72-Bit Serial Number
- Interface Options:
  - 125 kbps Pulse Width Modulated (PWM) Single-Wire Serial Interface
  - 400 KHz fast-mode I^2C interface
- Voltage Supply Range: 1.65V to 5.5V
- 130 nA Nominal Sleep Current
- Human Body Model (HBM) ESD: I^2C Devices >4 kV; SWI Devices >7 kV
- Packaging Options:
  - 8-pad UDFN (3 mm x 3 mm), 8-lead SOIC
  - 3-lead contact (2.5 mm x 6.5 mm)

Use Cases

- Disposables and accessory authentication
- Ecosystem control

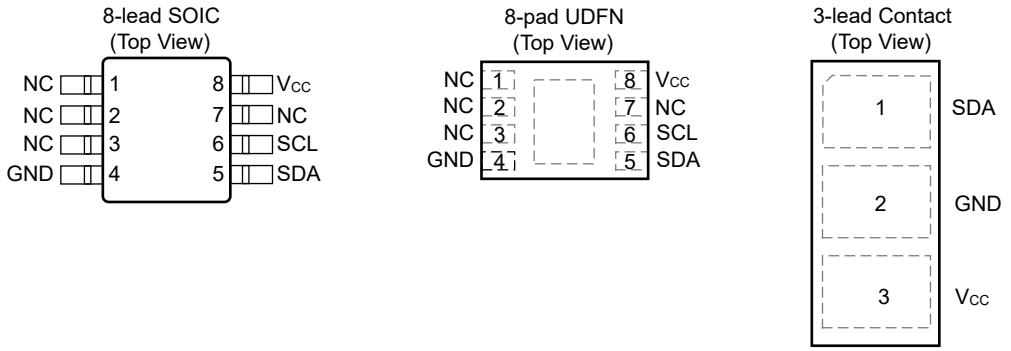
- Anti-cloning

Pin Configuration and Pinouts

Table 1. Pin Configuration

Package = 8-PAD SOIC or 8-Lead UDFN				Package = 3-Lead Contact		
Pin #	Function	I²C	SWI-PWM	Pin #	Function	SWI-PWM
1-3,7	No Connect	NC	NC	1	Serial I/O	SI/O
4	Ground	GND	GND	2	Ground	GND
5	Seria I/O	SDA	SI/O	3	Supply	VCC
6	Serial Clock	SCL	NC	—	—	—
8	Supply	VCC	VCC	—	—	—

Figure 1. Pinouts(1)



Note:

1. Connecting the exposed backside paddle of the UDFN package to GND is recommended.

Table of Contents

1. Overview

1.1 Use Cases

SHA104-TFLXAUTH is a member of the Microchip CryptoAuthentication family of high-security cryptographic devices that combine world class hardware-based key storage with hardware cryptographic accelerators to implement authentication.

SHA104-TFLXAUTH has a command set that allows for its usage in multiple symmetric key applications. The primary uses include the following:

- **Accessory/Disposable Authentication**
  Allows for authentication of accessory and/or disposable system components. For disposable components, the use may be restricted through the use of a monotonic counter.
  - **Challenge/Response authentication** – Requires a SHA104 on the accessory/disposable side only. SHA104 will be provisioned with a symmetric key, host firmware will embed one or several challenge/response pair(s).
  - **Shared Key authentication** – Requires integrating a SHA104 on the accessory/disposable and an SHA105 on the host side – both Secure Element will be provisioned with the same symmetric key.
  - **Diversified Key authentication** – Requires integrating a SHA104 on the accessory/disposable and a SHA105 on the host side. SHA104 will be provisioned with a unique symmetric key derived from a root symmetric key and the SHA104 unique serial number. SHA105 will be provisioned with the root symmetric key.
- **Ecosystem Control and Anti-Counterfeiting**
  Validates that a system or component is authentic and came from the OEM shown on the nameplate.

In typical applications, the SHA104-TFLXAUTH will be used on the accessory/disposable side of an application and the SHA105 will be used on the host side of that application. SHA104-TFLXAUTH can be ordered as either an I^2C or SWI I/O option. If an SWI device is implemented in a given application, it can optionally be used in parasitic power mode.

Tip: If it is desirable to not have a PCB or to have a minimal number of signals connected to the accessory/disposable side, then the SHA106 should be considered for the application. This device has an integrated capacitor that allows for a true 2-wire implementation.

1.2 Device Features

SHA104-TFLXAUTH includes an EEPROM array that can be used for storage of one secret key, miscellaneous read/write data, consumption logging and security configurations. Write access to the various data zone slots and configuration subzones of memory can be restricted.

The SHA104 comes in one of two possible serial interfaces. The I^2C version of the device supports a standard I^2C interface at speeds of up to 400 KHz. The interface is compatible with standard-mode and fast-mode I^2C interface specifications. The device also supports a Microchip proprietary PWM Single-Wire Interface (SWI), which can reduce the number of GPIOs required on the system processor and/or reduce the number of pins on connectors. When in SWI mode, the SHA104 can be operated in parasitic power mode, reducing the pin count to just 2 pins.

Each SHA104-TFLXAUTH unit ships with a unique 72-bit serial number. Also, SHA104-TFLXAUTH features a wide array of defense mechanisms specifically designed to prevent physical attacks on the device itself or logical attacks on the data transmitted between the device and the system.

Hardware restrictions on the ways in which a key is used or generated provide further defense against certain styles of attack.

An enhanced mode of self-test can be enabled by setting the SelfTest bit in the Configuration Zone. In this mode, the tests are required to run prior to the execution of the commands that require cryptographic algorithms.

The SHA104-TFLXAUTH device has a monotonic counter that can be used by the host system for a purpose of its choosing. The maximum value of the counter is limited to a maximum of 10,000 uses. A lower value can be programmed into the device during provisioning if so desired. If so desired, the counter can be attached to the symmetric key in Slot 3 to limit the use of this key. The monotonic counter will be automatically updated when the MAC command is run if the key in Slot 3 is configured for limited use.

2. EEPROM Memory

The EEPROM memory is divided into data zone with slots and a configuration zone made up of several subzones. Each data slots or configuration subzones can be locked independently.

Terms discussed within this document will have the following meanings:

Table 2-1. Document Terms

Term	Meaning
Block	A single 256-bit (32-byte) area of a slot in the Data zone. Data slots will have between 1 and 10 blocks. The industry 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.
Configuration Subzone	A portion of the Configuration zone that stores device identification or configuration information. Each subzone can be individually locked.
Data Zone Slot	A separate portion of the Data zone that stores customer-specific data. Each slot can be individually locked.
KeyID	KeyID is equivalent to the slot number for those slots designated to hold key values.
mode[b]	Indicates bit b of the parameter mode.
SRAM	Contains input and output buffers.
LSB/MSB	Least Significant Byte/Most Significant Byte.
LSb/MSb	Least Significant bit/Most Significant bit.

Related Links

2.1. EEPROM Data Zone

2.1 EEPROM Data Zone

The data zone has a total of 3 usable slots where write access restrictions are individually programmable. The following table lists the typical uses for each slot, along with any special characteristics of data for that slot.

Table 2-2. Data Zone

Slot	Blocks	Bytes	Bits	Typical Use	Notes
1	10	320	2560	User Data	Slot can be locked when written or can be left open to be updated.
2	2	64	512	User Data	Slot can be locked when written or can be left open to be updated.
3	1	32	256	Secret Key or Diversified Key	Can be written in the clear or via an encrypted Write. Slot must be locked before deployed in the field. No Read access.

The secret key stored in the SHA104-TFLXAUTH may either be the secret key used for authentication in the system or may be a diversified key. The key diversification must be consistent with the ability of the host device to generate the diversified key from the parent secret key.

2.2 EEPROM Configuration Zone

The SHA104-TFLXAUTH configuration is largely fixed and cannot be modified by the customer. Relevant information about how the device is configured is shown below, as well as the parameters that may be modified with the TPDS tools.

Device Configuration Information

- The serial number for each device is unique and stored in bytes [0:8] of configuration subzone #1. Default values of bytes [0:1] are 0x01 0x23 and byte[8] is 0xEE. All other bytes are unique.
- The default 7-bit I^2C address is 0x41. The I^2C address can be overwritten by writing CSZ3.

- The I/O levels are set to be V_{CC} referenced by default. This allows for the full operating voltage range to be available.
- Maximum command speed is enabled by setting the clock speed of the device to divide by 1.
- Monotonic counters are available for use by the system. By default, the counter is not attached to any keys.
- The SelfTest mode is set to standard operation, which does not require the self tests to be run prior to executing a command.
- A Health Test Failure will be cleared after any time that a command fails as a result of a health test failure. If the failure symptom is transient, the command is expected to pass when run a second time.
- By default, Slot[3] can be written in the clear.

Modifiable Configuration Information

Through use of the TPDS tools, the following parameters may be modified provided the zones were not already locked.

- I^2C address
- I/O levels can be modified to have a fixed reference. This allows for the I^2C Bus to run at a lower voltage level than the SHA104-TFLXAUTH supply. Supply is limited to a minimum of 2.0V in this mode.
- Data Slot[3] can be required to only allow encrypted writes.
- The initial Counter value can be limited to something less than 10,000.
- Health Tests can be set to require manual clearing through use of a power-up or sleep-wake cycle.
- Monotonic Counters can be attached to the symmetric key to limit the total number of uses of the device.
- Serial Number byte[8] can be modified from the default values to uniquely identify a given customer or application. The specific value used will be assigned by Microchip.

Important: For proper operation, the SN[0:1] and SN[8] bytes must be identical between the host side security devices and the client side devices as they are automatically included in some cryptographic operations. SN[2:7] bytes will always be unique between all devices.

3. Security Information

3.1 Cryptographic Standards

SHA104-TFLXAUTH follows various industry standards for the computation of cryptographic results. These reference documents are described in the following sections. See the Microchip website for further documentation on NIST CAVP certification of these cryptographic functions.

3.1.1 SHA-256

The SHA104-TFLXAUTH computes the SHA-256 digest based on the algorithm documented here:

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

3.2 Key Uses and Restrictions

3.2.1 Symmetric Keys

The parent symmetric secret key is stored in Slot 3 of the data zone and is 32 bytes (256 bits) in length. This key is based on SHA-256 cryptography and provides 128 bits of key strength. For the host (SHA105) device, the parent symmetric key must always be programmed into the device. For the client device, either the parent or a diversified key may be programmed into Slot 3.

3.2.2 Monotonic Counter

SHA104-TFLXAUTH supports one nonvolatile monotonic counter that can count to a value of 10,000.

The counters can be used in one of two methods :

- **Cryptographic Counters**:
  In this mode, the value of the counter can be read or incremented. It is the responsibility of the host to determine how this counter is used.
- **Limited Key Use**:
  The monotonic counter can be attached to the Symmetric Key stored in Slot 3 to restrict the number of times this key can be used.

Related Links

6.1. Counter Command

3.3 Security Features

3.3.1 Physical Security

The SHA104-TFLXAUTH incorporates a number of physical security features designed to protect the EEPROM contents from unauthorized exposure.

3.3.2 Random Number Generator (RNG)

The SHA104-TFLXAUTH device includes a high-quality cryptographic RNG implemented according to the NIST standards SP800-90A/B/C.

4. I/O Interfaces

The I^2C interface uses the SDA and SCL pins to transfer commands/data/status to and from the SHA104-TFLXAUTH device. The SWI transfers data using a single pin. Data flow is controlled by the host controller for both interfaces. Power is provided to the device through the SI/O signal when used in a parasitic power application.

Interface Terminology

Host:	The host MCU generates the command and controls the data flow on the bus to one or more client devices.
Client:	The SHA104-TFLXAUTH device always operates as a client device on the bus and cannot take control of the bus.
Device Address:	7-bit address used to address a client device. This is part of the first byte sent to a client device for each write or read transaction.
Open-Drain:	The SHA104-TFLXAUTH device has an open-drain output buffer where the bus is actively pulled low by the output buffer when data are read from the device but are passively pulled high by an external pull-up resistor.

Remember: The I^2C standard uses the terminology “Master” and “Slave”. The equivalent Microchip terminology used in this document is “Host” and “Client”, respectively. This terminology was also adopted for the SWI.

4.1 General I/O Information

The SHA104-TFLXAUTH operates as a client device and utilizes a single-wire digital serial interface or I^2C to communicate with a host controller. The host device controls all read and write operations to the client device(s) on the serial bus. The protocols are selected by specifying the part number that is ordered:

- **Single-Wire Interface:** Uses a single GPIO connection on the system microprocessor that is connected to the SDA pin on the device. The interface is compatible with Microchip AT21CS01 and AT21CS11 in High-Speed mode. It permits the lowest number of pins connected to any removable or replaceable entity. The bit rate is variable with a maximum achievable bit rate of 125 kbps. SWI can be operated in Parasitic Power or Direct Power mode. Multiple client devices are permitted when the client device is powered directly. Only one single-wire client on the interface is supported in Parasitic Power mode.
- **Single-Wire Interface – Parasitic Power Mode:**In parasitic power mode the device is charged through the SWIO Signal. It is recommended that the host micro have a totem pole CMOS output driver. Whenever this output is High, the SHA104-TFLXAUTH will charge the C1 capacitor if the voltage of V_{CC_DVC} is less than V_{SIO}. Internal circuitry will prevent this charge from being bled off when the SWIO signal is driven low. This signal must be driven High during the write phase or calculation phase of any command. The host microcontroller is providing the needed power for the device to operate. The internal circuity will allow for the V_{CC_DVC} to be charged to the V_{SIO} level. In a normal application, this will be the same as the V_{PUP} voltage. V_{PUP} is the supply voltage on the high side of the R_{PUP} pull-up resistor. When data is being read from the SHA104-TFLXAUTH device, the host micro I/O will be placed into an input mode. The SHA104-TFLXAUTH device will pull the signal low and the R_{PUP} resistor will pull the signal high as required.

Figure 4-1. Application Diagram for Using the Parasitic Powered SWI

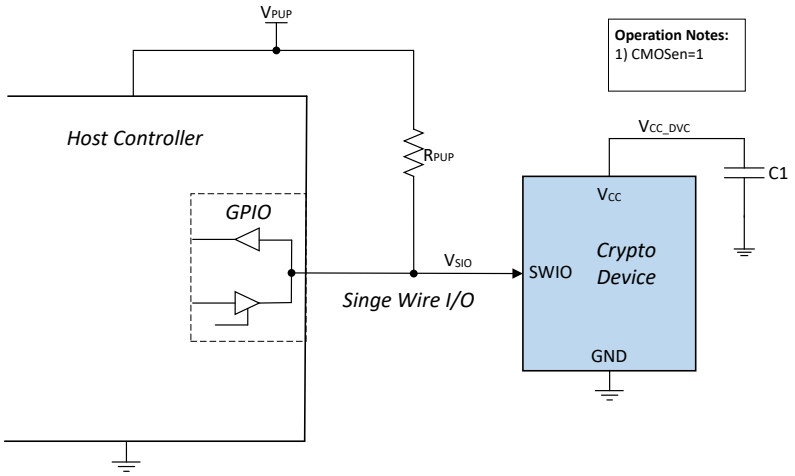
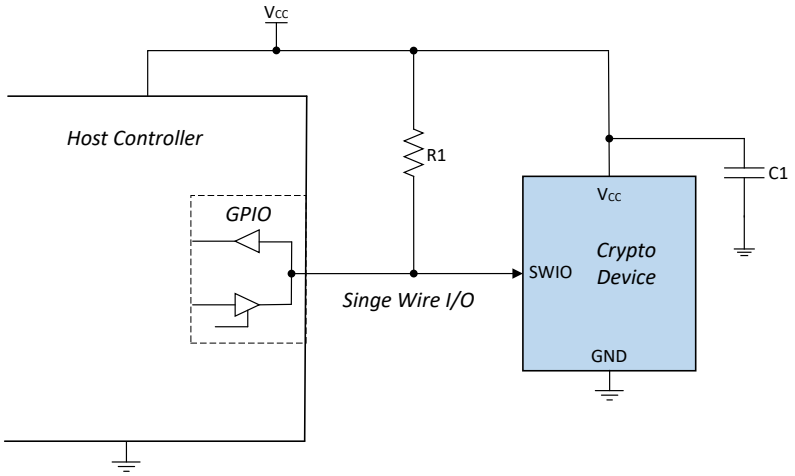


Figure 4-2. Application Diagram for Using the V_{CC} Powered SWI



- **I^2C Interface:**
  This mode is compatible with the I^2C standard and with the Microchip AT24C16 Serial EEPROM interface. Two pins, Serial Data (SDA) and Serial Clock (SCL), are required. The I^2C interface supports a bit rate of up to 400 kbps.

Figure 4-3. Application Diagram for Using the I²C Interface with CMOSen=1

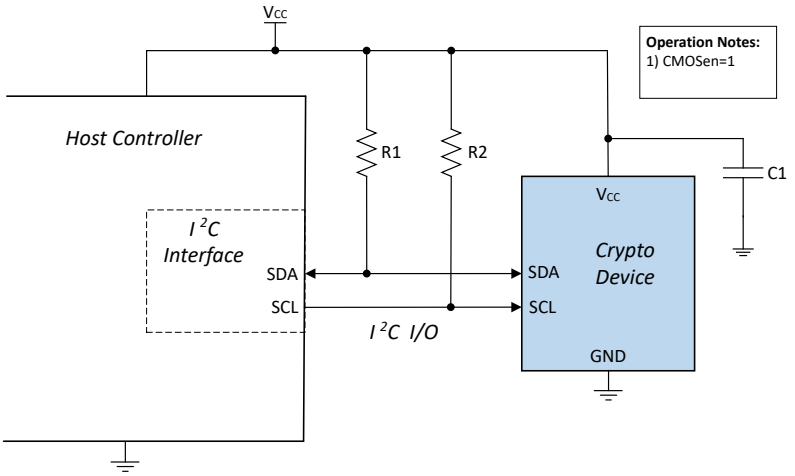
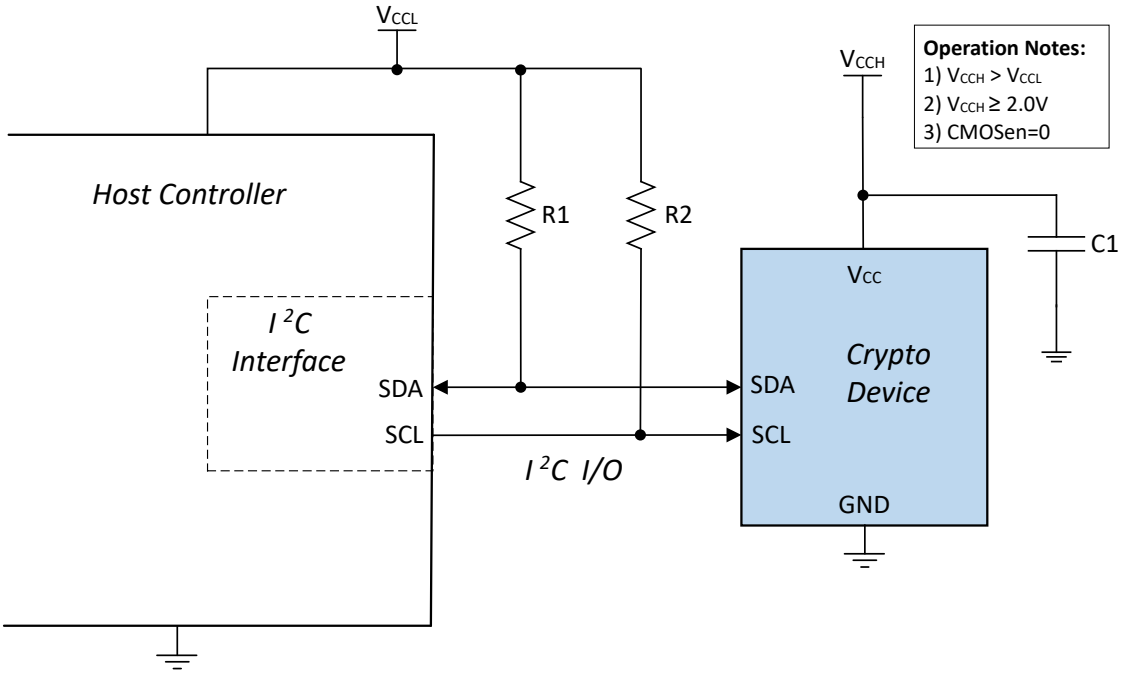


Figure 4-4. Application Diagram for using Using the I²C Interface with CMOSen=0



Related Links

4.2. Single-Wire Interface
4.3. I2C Interface

4.2 Single-Wire Interface

The SHA104-TFLXAUTH operates as a client device and utilizes a single-wire digital serial interface to communicate with a host controller. The host device controls all read and write operations to the

client devices on the serial bus. The device supports the High-Speed mode. This interface is designed to be compatible at the protocol level with the Microchip AT21CS01 and AT21CS11 Serial EEPROM operating at High-Speed mode.

Note: It is recommended that designers read the respective data sheets carefully.

The device utilizes an 8-bit data structure. Data are transferred to and from the device via the single-wire serial interface using the Serial Input/Output (SI/O) pin. Power to the device can also be provided via the SI/O pin, thus only the SI/O pin and the GND pin are required for device operation. Data sent to the device over the single-wire bus are interpreted by the state of the SI/O pin during specific time intervals or slots. Each time slot is referred to as a bit frame and lasts t_{BIT} in duration. The host initiates all bit frames by driving the SI/O line low. All commands and data information are transferred with the MSb first.

During bus communication, one data bit is transmitted in every bit frame, and after eight bits (one byte) of data are transferred, the receiving device must respond with either an Acknowledge (ACK) or a No Acknowledge (NACK) response bit during a ninth bit window. There are no unused clock cycles during any read or write operation, so there must not be any interruptions or breaks in the data stream during each data byte transfer and ACK or NACK clock cycle. In the event where an unavoidable system interrupt is required, refer to the requirements outlined in 4.2.2.7. Communication Interruptions.

Related Links

5.3.3. AC Parameters: Single-Wire Interface

4.2.1 I/O Conditions

The device responds to the following I/O conditions:

4.2.1.1 Device is Asleep

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

If the SHA104-TFLXAUTH detects a rising edge on the Single-Wire pin, it will exit Low-Power mode. No data must be sent to the SHA104-TFLXAUTH in single-wire mode during t_{PU} time interval.

4.2.1.2 Device is Awake

When the device is awake, it honors the conditions listed in 4.2.2. Single-Wire Bus Transactions. Data must not be sent when the device is actively doing computations or the device will go to sleep.

4.2.2 Single-Wire Bus Transactions

Types of data transmitted over the SI/O line:

- Reset and Discovery Response
- Logic '0' or Acknowledge (ACK)
- Logic '1' or No Acknowledge (NACK)
- Start condition
- Stop condition

The Reset and Discovery Response is not considered to be part of the data stream to the device, whereas, the remaining four transactions are all part of the data sequence being sent to or received from the device. The difference between the types of data stream transactions is the duration that SI/O is driven low within the bit frame.

4.2.2.1 Device Reset/Power-Up and Discovery Response

4.2.2.1.1 Resetting the Device

A Reset and Discovery Response sequence is used by the host to reset the client device as well as to perform a general bus call to determine if a device is present on the bus.

To begin the Reset portion of the sequence, the host must drive SI/O low for the minimum t_{RESET} time. If the device is busy, driving the SI/O signal low will interrupt the current operation and reset the device.

Upon SI/O being released for a sufficient amount of time to allow the device time to power-up and initialize, the host must always request a Discovery Response Acknowledge from the SHA104-TFLXAUTH prior to any commands being sent to the device. The host can, then, determine if the SHA104-TFLXAUTH is present by sampling for the Discovery Response Acknowledge from the device.

4.2.2.1.2 Device Response upon Reset or Power-Up

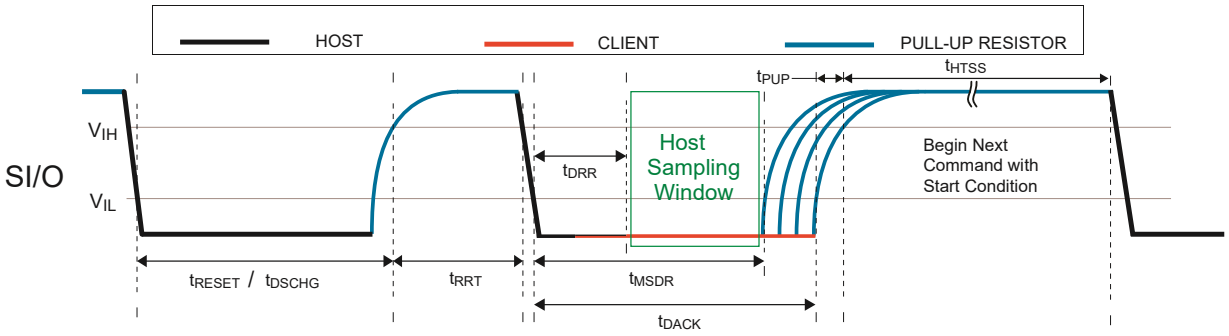
After the device is powered-up or after the host resets the device by holding the SI/O line low for t_{RESET} or t_{DSCHG}, the host must release the line, which will be pulled high by an external pull-up resistor. The host must, then, wait an additional minimum time of t_{RRT} before it can request a Discovery Response Acknowledge from the device.

The Discovery Response Acknowledge sequence begins with the host driving the SI/O line low, which will enable the SHA104-TFLXAUTH internal timing circuits. The host must continue to drive the line low for t_{DRR}.

During the t_{DRR} time, the SHA104-TFLXAUTH will respond by concurrently driving SI/O low. The device will continue to drive SI/O low for a total time of t_{DACK}. The host must sample the state of the SI/O line at t_{MSDR} past the initiation of t_{DRR}. By definition, the t_{DACK} minimum time is longer than the t_{MSDR} maximum time, thereby ensuring the host can always correctly sample the SI/O for a level less than V_{IL}. After the t_{DACK} time elapses, the SHA104-TFLXAUTH will release SI/O, which will, then, be pulled high by the external pull-up resistor.

The host must, then, wait t_{HTSS} to create a Start condition before continuing with the first command (see Start/Stop Condition for more details about Start conditions).

Figure 4-5. Reset and Discovery Response Waveform



4.2.2.2 Interrupting the Device During an Active Operation

If S/IO is brought low during Active operation, the SHA104-TFLXAUTH device will halt computation and enter Sleep mode. The SHA104-TFLXAUTH will wake up on the subsequent rising edge on the single-wire bus.

4.2.2.3 Data Input and Output Bit Frames

Communication with the SHA104-TFLXAUTH is conducted in time intervals referred to as bit frames and lasts t_{BIT} in duration. Each bit frame contains a single binary data value. Input bit frames are used to transmit data from the host to the SHA104-TFLXAUTH and can either be a logic '0' or a logic '1'. An output bit frame carries data from the SHA104-TFLXAUTH to the host. In all input and output cases, the host initiates the bit frame by driving the SI/O line low. Once the SHA104-TFLXAUTH detects the SI/O being driven below the V_{IL} level for a duration greater than t_{IGNORE_SWI} its internal timing circuits begin to run.

The duration of each bit frame is allowed to vary from bit to bit as long as the variation does not cause the t_{BIT} length to exceed the specified minimum and maximum values.

4.2.2.4 Data Input Bit Frame

A data input bit frame can be used by the host to transmit either a logic '0' or a logic '1' data bit to the SHA104-TFLXAUTH. The input bit frame is initiated when the host drives the SI/O line low. The length of time that the SI/O line is held low will dictate whether the host is transmitting a logic '0' or a logic '1' for that bit frame. For a logic '0' input, the length of time that the SI/O line must be held low is defined as t_{LOW0}. Similarly, for a logic '1' input, the length of time that the SI/O line must be held low is defined as t_{LOW1}.

The SHA104-TFLXAUTH will sample the state of the SI/O line after the maximum t_{LOW1} but prior to the minimum t_{LOW0} after SI/O is driven below the V_{IL} threshold to determine if the data input is a logic '0' or a logic '1'. If the host is still driving the line low at the sample time, the SHA104-TFLXAUTH will decode that bit frame as a logic '0' as SI/O will be at a voltage less than V_{IL}. If the host has already released the SI/O line, the SHA104-TFLXAUTH sees a voltage level greater than or equal to V_{IH} because of the external pull-up resistor, and that bit frame is decoded as a logic '1'.

A logic '0' condition has multiple uses similar to I^2C sequences. It is used to signify a '0' data bit and it is also used for an ACK response. Additionally, a logic '1' condition is used for a NACK response in addition to the nominal '1' data bit.

The figures below depict the logic '0' and logic '1' input bit frames.

Figure 4-6. Logic '0' Input Condition Waveform

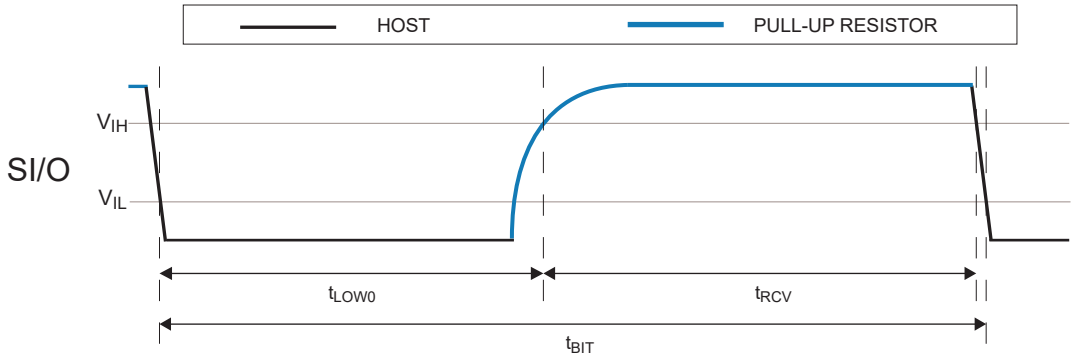
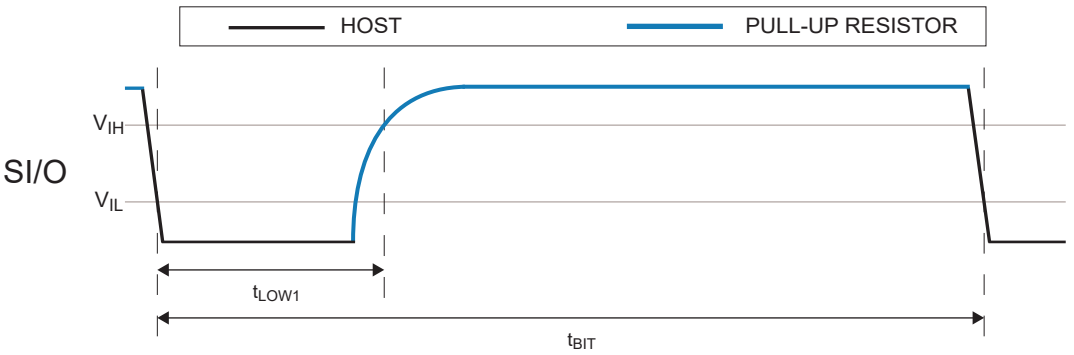


Figure 4-7. Logic '1' Input Condition Waveform



4.2.2.5 Data Output Bit Frame

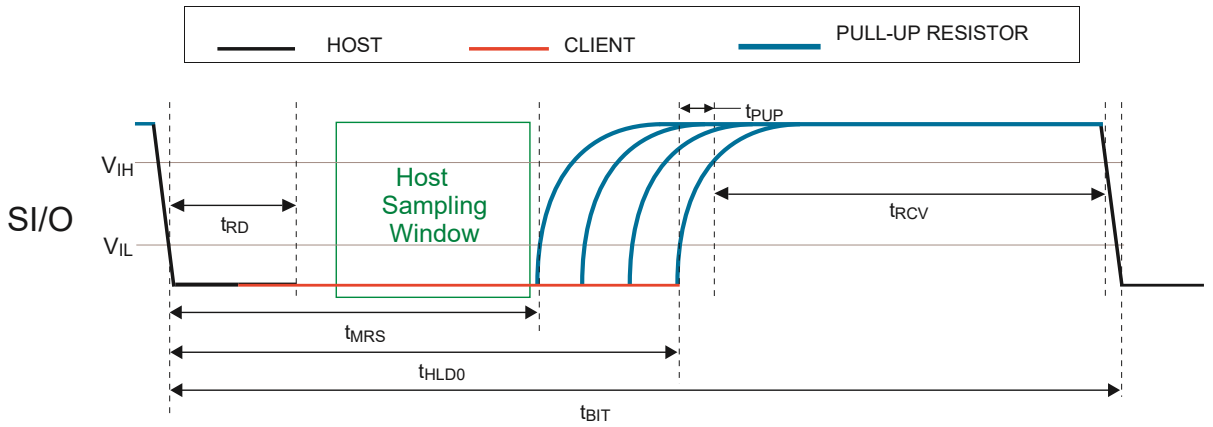
A data output bit frame is used when the host is to receive communication back from the SHA104-TFLXAUTH. Data output bit frames are used when reading any data out, as well as any ACK or

NACK responses from the device. Just as in the input bit frame, the host initiates the sequence by driving the SI/O line below the V_{IL} threshold, which engages the SHA104-TFLXAUTH internal timing generation circuit.

Within the output bit frame is the critical timing parameter t_{RD}, which is defined as the amount of time the host must continue to drive the SI/O line low after crossing below the V_{IL} threshold to request a data bit back from the SHA104-TFLXAUTH. Once the t_{RD} duration expires, the host must release the SI/O line.

If the SHA104-TFLXAUTH is responding with a logic '0' (for either a '0' data bit or an ACK response), it will begin to pull the SI/O line low concurrently during the t_{RD} window and continue to hold it low for a duration of t_{HLD0}, after which it will release the line to be pulled back up to V_{PUP} (see the following figure). Thus, when the host samples SI/O within the t_{MRS} window, it will see a voltage less than V_{IL} and decode this event as a logic '0'. By definition, the t_{HLD0} time is longer than the t_{MRS} time, and, therefore, the host is ensured to sample while the SHA104-TFLXAUTH is still driving the SI/O line low.

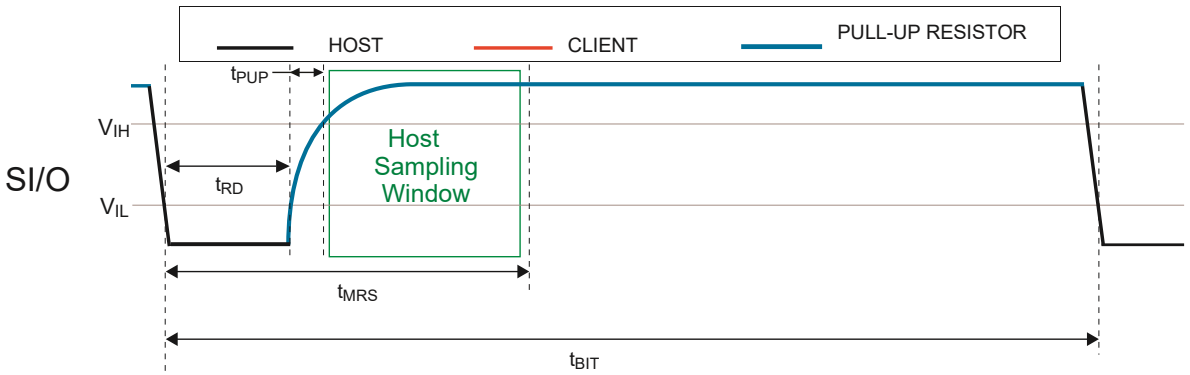
Figure 4-8. Logic '0' Data Output Bit Frame Waveform



If the SHA104-TFLXAUTH intends to respond with a logic '1' (for either a '1' data bit or a NACK response), it will not drive the SI/O line low at all. When the host releases the SI/O line after the maximum t_{RD} elapses, the line will be pulled up to V_{PUP}. Thus, when the host samples the SI/O line within the t_{MRS} window, it will detect a voltage greater than V_{IH} and decode this event as a logic '1'.

The data output bit frame is shown in detail below.

Figure 4-9. Logic 1 Data Output Bit Frame Waveform



4.2.2.6 Start/Stop Condition

All transactions to the SHA104-TFLXAUTH begin with a Start condition; therefore, a Start can only be transmitted by the host to the client. Likewise, all transactions are terminated with a Stop condition, and, thus, a Stop condition can only be transmitted by the host to the client.

The Start and Stop conditions require identical biasing of the SI/O line. The Start/Stop condition is created by holding the SI/O line at a voltage of V_{PUP} for a duration of t_{HTSS}.

The following figures depict the Start and Stop conditions.

Figure 4-10. Start Condition Waveform

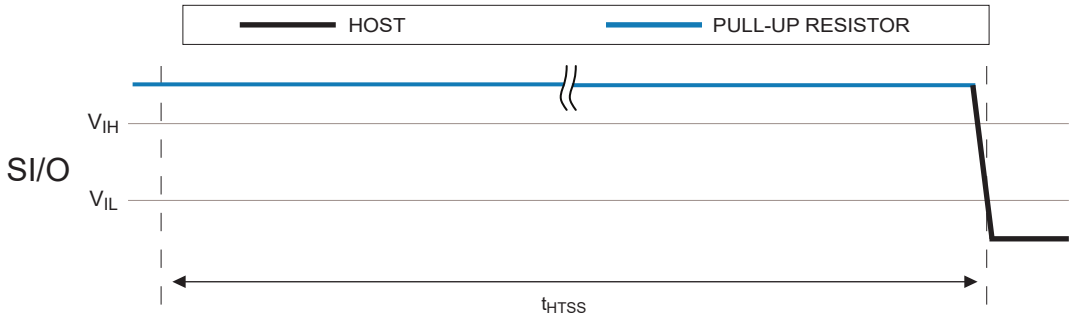
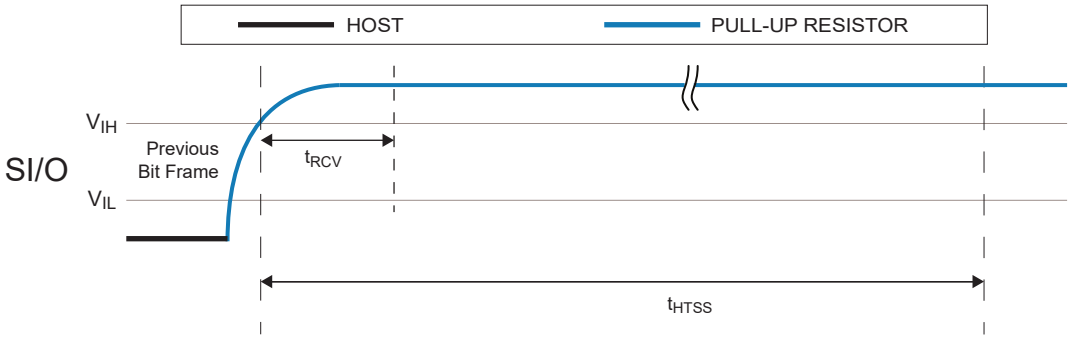


Figure 4-11. Stop Condition Waveform



4.2.2.7 Communication Interruptions

In the event that a protocol sequence is interrupted midstream, this sequence can be resumed at the point of interruption if the elapsed time of inactivity is less than the maximum t_{BIT} time. If the sequence is interrupted for longer than the maximum t_{BIT}, the host must wait at least the minimum t_{HTSS} before continuing. By waiting the minimum t_{HTSS} time, a new Start condition is created and the device is ready to receive a new command. It is recommended that the host start over and repeat the transaction that was interrupted midstream.

4.3 I²C Interface

This interface is designed to be compatible at the protocol level with the Microchip AT24C16 Serial EEPROM operating at 400 kHz.

Tip: There are some differences between the two devices (for example, the SHA104-TFLXAUTH and AT24C16 have different default I²C addresses); therefore, it is recommended that designers read the respective data sheets carefully.

The SDA pin is normally pulled high with an external pull-up resistor because the SHA104-TFLXAUTH only includes an open-drain driver on its output pin. The host system may use either an open-drain

or a totem pole driver. In the latter case, it must be tri-stated when the SHA104-TFLXAUTH 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 pulled high by an external resistor.

The serial interface is comprised of two signal lines: Serial Clock (SCL) and Serial Data (SDA). The SCL pin is used to receive the clock signal from the host, while the bidirectional SDA pin is used to receive command and data information from the host as well as to send data back to the host. Data are always latched into the SHA104-TFLXAUTH on the rising edge of SCL and always output from the device on the falling edge of SCL. Both SCL and SDA pins incorporate integrated glitch suppression filters and Schmitt Triggers to minimize the effects of input spikes and bus noise.

All command and data information is transferred with the MSb first. During bus communication, one data bit is transmitted every clock cycle and after eight bits (one byte) of data are transferred, the receiving device must respond with either an ACK or a NACK response bit during a ninth clock cycle (ACK/NACK clock cycle) generated by the host. Therefore, nine clock cycles are required for every one byte of data transferred. There are no unused clock cycles during any read or write operation, so there must not be any interruptions or breaks in the data stream during each data byte transfer and ACK or NACK clock cycle.

During data transfers, data on the SDA pin must only change while SCL is low, and the data must remain stable while SCL is high. If data on the SDA pin change while SCL is high, either a Start or a Stop condition will occur. Start and Stop conditions are used to initiate and end all serial bus communication between the host and the client devices. The number of data bytes transferred between a Start and a Stop condition is not limited and is determined by the host. For the serial bus to be idle, both the SCL and SDA pins must be in the logic high state at the same time.

4.3.1 I/O Conditions

The device responds to the following I/O conditions:

4.3.1.1 Device is Asleep

When the device is asleep, it ignores all but the Wake condition. The Wake condition is as follows:

- Send Start condition
- Send Device Address
- Expect NACK
- Send Stop condition

The SHA104-TFLXAUTH will only exit Low-Power mode if the device address sent by the system microprocessor contains a client address that matches the address stored in the Config: Device_Address byte. The SHA104-TFLXAUTH will NACK the device address and ignore all subsequent bytes until t_{PU} expires.

Related Links

4.3.2.1. Data Input and Output Frames
5.3.1. AC Parameters: All I/O Interfaces

4.3.1.2 Device is Awake

When the device is awake, it honors the conditions listed in 4.3.2. I2C Bus Transactions.

4.3.2 I²C Bus Transactions

Types of data transmitted over the I²C bus:

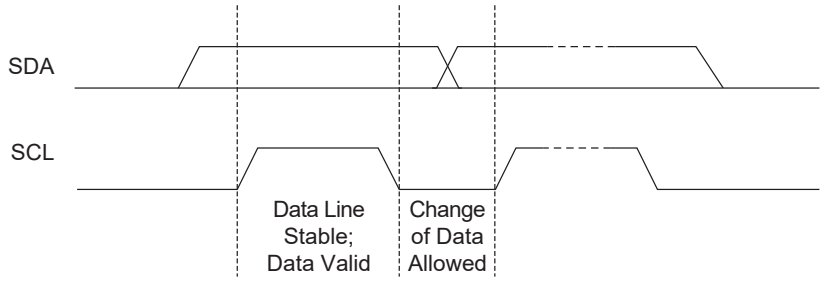
- Data ‘0’
- Acknowledge (ACK)
- Data ‘1’

- No Acknowledge (NACK)
- Start condition
- Stop condition

4.3.2.1 Data Input and Output Frames

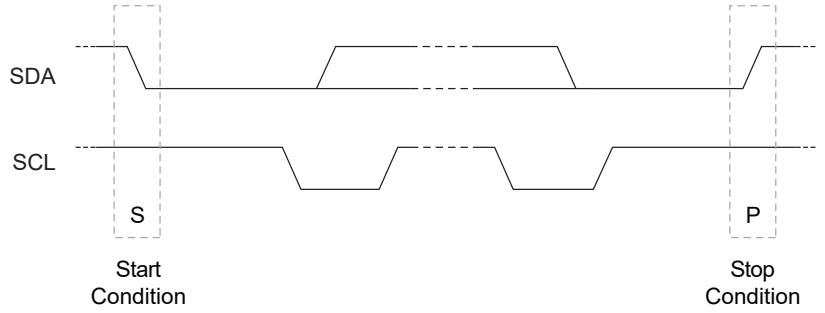
- **DATA Zero**: If SDA is low and stable while SCL goes from low to high to low, a zero bit is transferred on the bus. SDA can change while SCL is low.
- **DATA One**: If SDA is high and stable while SCL goes from low to high to low, a one bit is transferred on the bus. SDA can change while SCL is low.

Figure 4-12. Data Bit Transfer on the I^2C Interface



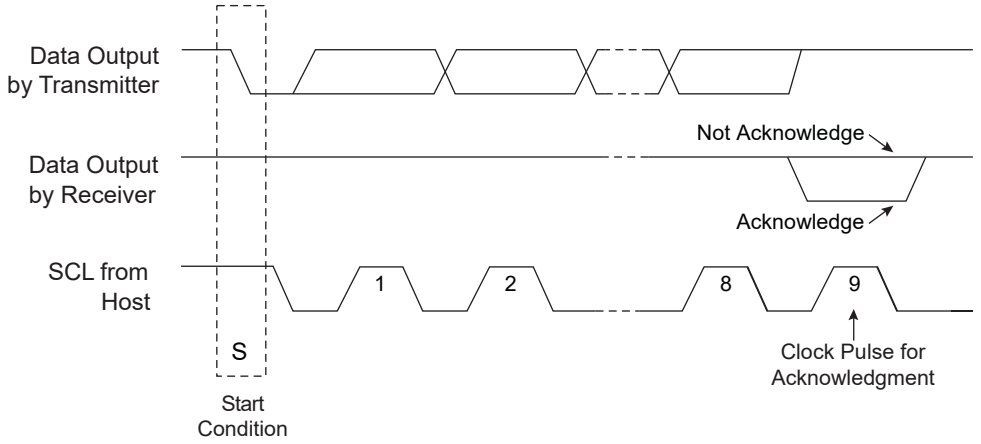
- **Start Condition**: A high-to-low transition of SDA with SCL high is a Start condition that must precede all commands.
- **Stop Condition**: A low-to-high transition of SDA with SCL high is a Stop condition. After this condition is received by the device, the current I/O transaction ends. On input, 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 4-13. Start and Stop Conditions on the I^2C 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 4-14. NACK and ACK Conditions on the I²C Interface



Multiple SHA104 devices can easily share the same I²C interface signals if the Device_Address byte in the Configuration zone is programmed differently for each device on the bus. All seven bits of the device address are programmable; therefore, the SHA104-TFLXAUTH can also share the I²C interface with any I²C device, including any Serial EEPROM.

4.3.3 Split I²C Transactions

System requirements sometimes limit the length of a transaction to a certain number of bytes. The SHA104-TFLXAUTH can accommodate this limitation and commands can be subdivided into multiple transactions. When the device receives the first portion of the command, which includes the total number of bytes being sent, the control logic of the device will be looking for that number of bytes before it will execute the command. Each portion of the command requires that the device address plus word address be sent for each partial packet. It is recommended that a Restart condition be sent between the partial packets without a Stop condition and only send the Stop condition after the last of the command bytes are sent. It is, however, acceptable to send a Stop condition between each portion of the command byte stream.

Beyond system level requirements that force the need to subdivide a command, it may simply be convenient to do so. For example, when executing a read transaction of an unknown length, it may be desirable to first read back only the initial payload byte to determine the length of the data being read back. This allows for the ability to dynamically allocate the size of the array being read back.

Legend: A = ACK N = NACK S = Start condition P = Stop condition Sr = Repeated Start Condition
The legend applies to all of the following diagrams.

Figure 4-15. 32-Byte Standard I²C Write

S	Address+W	A	Word Address	A	Count=39	A	OpCode	A	Mode	A	Param2[0]	A	Param2[1]	A	32-Bytes of Data	CRC0]	A	CRC[1]	A	P

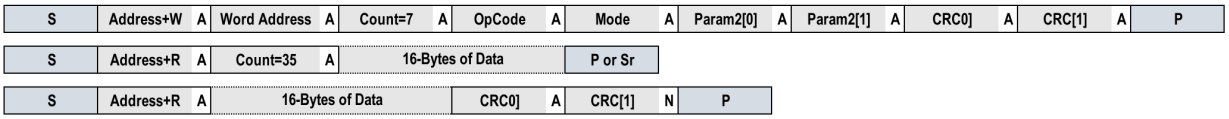
Figure 4-16. 32-Byte Split I²C Write

S	Address+W	A	Word Address	A	Count=39	A	OpCode	A	Mode	A	Param2[0]	A	Param2[1]	A	25-Bytes of Data	P or Sr
S	Address+W	A	Word Address	A	7-Bytes of Data				CRC0]	A	CRC[1]	A	P			

Figure 4-17. 32-Byte Standard I²C Read

S	Address+W	A	Word Address	A	Count=7	A	OpCode	A	Mode	A	Param2[0]	A	Param2[1]	A	CRC0]	A	CRC[1]	A	P
S	Address+R	A	Count=35	A	32-Bytes of Data				CRC0]	A	CRC[1]	N	P						

Figure 4-18. 32-Byte Split I²C Read



4.3.4 I²C Synchronization

It is possible for the system to lose synchronization with the I/O port on the SHA104-TFLXAUTH, perhaps due to a system reset, I/O noise or other conditions. Under this circumstance, the SHA104-TFLXAUTH 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 I²C 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

   A read sequence can now be issued, and, if synchronization is properly completed, the SHA104-TFLXAUTH 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 SHA104-TFLXAUTH to ignore any partial input command that was possibly 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 I²C wake condition and wait t_{PU}. 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.

4.4 I/O Transmission to the SHA104-TFLXAUTH

The transmission of data from the system to the SHA104-TFLXAUTH is summarized in the table below. This transmission sequence is valid for both the I²C and SWI. The order of transmission is as follows:

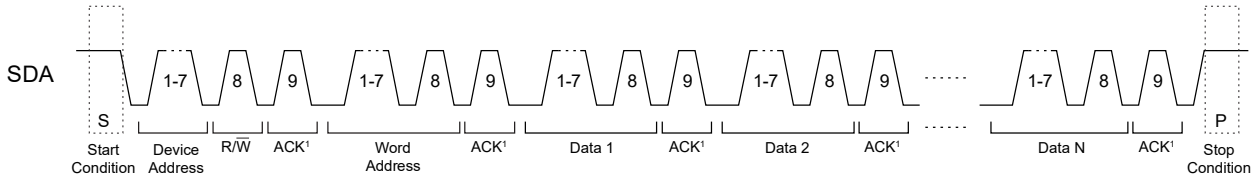
- Start condition
- Device Address byte
- Word Address byte
- Optional Data bytes (1 through N)
- Stop condition

Table 4-1. Transmission to the SHA104-TFLXAUTH

Name	I/O Name	Description
Device Address	Device Address	This byte selects a particular device on the I/O interface. SHA104-TFLXAUTH is selected if bits 1 through 7 of this byte match bits 1 through 7 of the Device_Address byte in the Configuration zone. Bit 0 of this byte is the R/$\overline{W}$ bit and must be zero to indicate a write operation (the bytes following the device address travel from the host to the client).

.....continued		
Name	**I/O Name**	**Description**
Word Address	Word Address	This byte must have a value of 0x03 for normal operation. See 4.4.1. Word Address Values for more information.
Command	Data 1, 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.

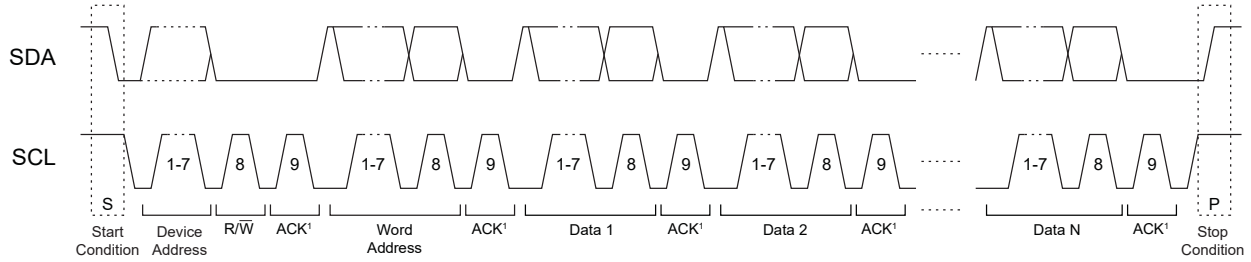
Figure 4-19. Normal Single-Wire Transmission to the SHA104-TFLXAUTH



Notes:

1. The SHA104-TFLXAUTH does not support the same client addressing scheme as Microchip AT21CS11.
2. Data is transferred MSb first. Numbers in diagram represent bit location, not bit number in the byte.

Figure 4-20. Normal I^2C Transmission to the SHA104-TFLXAUTH



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/O 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 execution is finished.

The system must send a Stop condition after the last command byte to ensure that the SHA104-TFLXAUTH will start the computation of the command. Failure to send a Stop condition may eventually result in a loss of synchronization.

4.4.1 Word Address Values

During an I/O write packet, the SHA104-TFLXAUTH interprets the second byte sent as the word address, which indicates the packet function as it is described in the table below:

Table 4-2. Word Address Values

Name	Value	Description
Reset	0x00	Resets the address counter. The next I/O read or write transaction will start with the beginning of the I/O buffer.
Sleep (low-power)	0x01 or 0x02	The SHA104-TFLXAUTH 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.

.....continued		
Name	Value	Description
Command	0x03	Writes subsequent bytes to sequential addresses in the input command buffer that follow previous writes. This is the normal operation.

Note: Only the lower two bits of the Word Address byte are decoded by the SHA104-TFLXAUTH.

4.4.2 Sleep Sequence

Upon completion of the use of the SHA104-TFLXAUTH 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.

4.4.3 Command Completion Polling

After a complete command is sent to the SHA104-TFLXAUTH, the device will be busy until the command computation completes. The system has options depending on the I/O, as noted below:

- **Polling**:
  It is recommended that the system wait t_{EXEC} (typical), then send a read sequence (see 4.5. I/O Transmission from the SHA104-TFLXAUTH). If the device NACKs the device address, then it is still busy. The system may delay for some time or immediately send another read sequence, looping on NACK again. After a total delay of t_{EXEC} (max.), the device will complete the computation and return the results.
- **Single Delay**:
  The system must wait t_{EXEC} (max.), after which the device will complete the execution, and the result can be read from the device using a normal read sequence.

Important: Polling can only be used when operating with the I^2C interface. For the SWI, Single Delay timing must be used.

4.5 I/O Transmission from the SHA104-TFLXAUTH

When the SHA104-TFLXAUTH is awake and not busy, the host can retrieve the current output buffer contents from the device using an I/O read. If valid command results are available, the size of the group returned is determined by the particular run command. Otherwise, the size of the group (and the first byte returned) will always be four: count, status/error and 2-byte CRC.

Table 4-3. I/O Transmission from the SHA104-TFLXAUTH

Name	I/O Name	Direction	Description
Device Address	Device Address	To client	This byte selects a particular device on the I/O interface and the SHA104-TFLXAUTH will be selected if bits 1 through 7 of this byte match bits 1 through 7 of the Device_Address byte in the Configuration zone. Bit 0 of this byte is the R/$\overline{W}$ bit and must be one to indicate that the bytes following the device address travel from the client to the host (read).
Data	Data 1, 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 SHA104-TFLXAUTH along the I/O 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 SHA104-TFLXAUTH is busy 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/$\overline{W}$ == R)] is sent to the device, the SHA104-TFLXAUTH will NACK the device address to indicate that no data are available to be read.

5. Electrical Characteristics

5.1 Absolute Maximum Ratings

Operating Temperature	-40°C to +105°C
Storage Temperature	-65°C to +150°C
Maximum Operating Voltage	6.0V
DC Output Low Current	20 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 I^2C Devices	>4 kV
Human Body Model (HBM) ESD SWI Devices	>7 kV
Charge Device Model (CDM) ESD	>2 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.

5.2 Reliability

The SHA104-TFLXAUTH is fabricated with Microchip's high-reliability CMOS EEPROM manufacturing technology.

Table 5-1. EEPROM Reliability

Parameter	Min	Typ.	Max.	Units
Data Retention at +55°C	>40	—	—	Years
Read Endurance	Unlimited			Read Cycles

Note:

1. The number of times that an EEPROM cell would be written is expected to be minimal for most use cases. Maximum EEPROM write cycles are expected to occur when the monotonic counter is used, which can be incremented up to 10,000 times. Similar devices in this technology have a write endurance of >100k.

5.3 AC Parameters

5.3.1 AC Parameters: All I/O Interfaces

Table 5-2. AC Parameters: All I/O Interfaces
Unless otherwise indicated, these values are applicable over the specified operating range from T_A = -40℃ to +105℃, V_{CC} =+1.65V to +5.5V.

Parameter	Sym.	Direction		Min.	Typ.	Max.	Units	Conditions
Power-up Delay	t_{PU}(1, 2)	To SHA104-TFLXAUTH	Clock Divider = 1x	1.0	—	—	ms	Minimum time prior to V_{CC} > V_{CC} min.
			Clock Divider = 2x	1.2	—	—	ms	
			Clock Divider = 4x	1.8	—	—	ms	
Watchdog Timer (WDT) Delay	t_{WDT}(1)	N/A		0.7	1	1.3	s	Time that the WDT will run after a command is sent, prior to automatically resetting the chip.

Notes:

1. These parameters are ensured through characterization but not production tested.
2. The Single-Wire pin must be stable high for the entire t_{PU} duration when in Parasitic Power mode.

5.3.2 AC Parameters: I²C Interface

Figure 5-1. I²C Synchronous Data Timing

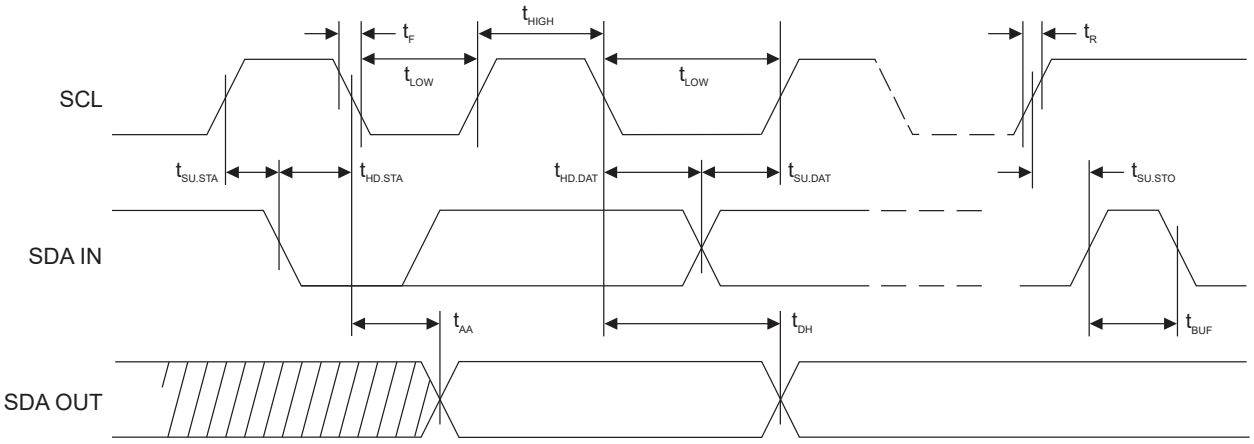


Table 5-3. AC Characteristics of I²C Interface
Unless otherwise indicated, these values are applicable over the specified operating range from T_A = -40℃ to +105℃, V_{CC} = +1.65V to +5.5V, C_L = 1 TTL Gate and 100 pF.

Parameter	Sym.	Min.	Max.	Units
SCL Clock Frequency	f_{SCL}	0	400	kHz
SCL High Time	t_{HIGH}	600	—	ns
SCL Low Time	t_{LOW}	1200	—	ns
Start Setup Time	$t_{SU.STA}$	600	—	ns
Start Hold Time	$t_{HD.STA}$	600	—	ns
Stop Setup Time	$t_{SU.STO}$	600	—	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	—	300	ns
Clock Low to Data Out Valid	t_{AA}	50	900	ns
Data Out Hold Time	t_{DH}	50	—	ns
Time Bus Must be Free before a New Transmission Can Start(1)	t_{BUF}	1200	—	ns
Glitch Filter(3)	t_{IGNORE_I2C}	50	250	ns

Notes:

1. Host system must ensure this timing is met.
2. AC measurement conditions:
   - R_L (connects between SDA and V_{CC}): 1.2 kΩ (for V_{CC} = +1.65V to +5.5V)
   - Input pulse voltages: 0.3V_{CC} to 0.7 V_{CC} with CMOSenable = 1
   - Input rise and fall times: ≤ 50 ns
   - Input and output timing reference voltage: 0.5 V_{CC}
3. The glitch filter ensures that all pulses below the min value will be suppressed but may suppress values as great as the max value over all process, voltage and temperature conditions.

5.3.3 AC Parameters: Single-Wire Interface

5.3.3.1 Reset and Discovery Response Timing

Table 5-4. Reset and Discovery Response Timing
Unless otherwise indicated, these values are applicable over the specified operating range from T_A = -40℃ to +105℃, V_{CC} = +1.65V to +5.5V, CL = 100 pF.

Parameter and Condition[1]		Sym.	Min.	Max.	Units
Reset Low Time, Device in Inactive State[4]		t_{RESET}	96	—	µs
Discharge Low Time, Device in Active Write Cycle (t_{WR})[4, 7]		t_{DSCHG}	150	—	µs
Reset Recovery Time[4, 6]	Clock Divider = 1x	t_{RRT}	1000	—	µs
	Clock Divider = 2x		1200	—	µs
	Clock Divider = 4x		1800	—	µs
Discovery Response Request[4]		t_{DRR}	1	2 – t_{PUP}[2]	µs
Discovery Response Acknowledge Time[5]		t_{DACK}	2	6[3]	µs
Host Strobe Discovery Response Time[4]		t_{MSDR}	t_{RD} + t_{PUP}[2]	2	µs
SI/O High Time for Start/Stop Condition[4]		t_{HTSS}	150	—	µs

Notes:

1. AC measurement conditions for the table above:
   - All parameters are production tested unless otherwise noted.
   - Loading capacitance on SI/O: 100 pF
   - V_{PUP}: Applied at minimum and maximum V_{CC}
   - In Parasitic Power mode, V_{PUP} minimum restricted to 2.4V
2. t_{PUP} is the time required to be pulled up from V_{IL} to V_{IH} when the SI/O line is released. This value is application-specific and is a function of the loading capacitance on the SI/O line as well as the R_{PUP} chosen.
3. Microchip's AT21CS11 supports a maximum of 24 µs and a minimum of 8 µs.
4. The host system must ensure the parameter timing values are met.
5. The SHA104-TFLXAUTH ensures by design this timing parameter is met.
6. Parameter is ensured through characterization but is not production tested.
7. This parameter is only relevant when operating in parasitic power mode.

5.3.3.2 Data Communication Timing

Table 5-5. Data Communication Timing
Unless otherwise indicated, these values are applicable over the specified operating range from T_A = -40℃ to +105℃, V_{CC} = +1.65V to +5.5V, C_L = 100 pF.

Parameter and Condition[1]	Sym.	Frame Type	Min.	Max.	Units
Bit Frame Duration[6, 7]	t_{BIT}	Input and Output Bit Frame	$t_{LOW0} + t_{PUP}$[2] + t_{RCV}	75	µs
SI/O High Time for Start/Stop Condition[6]	t_{HTSS}	Input Bit Frame	150	—	µs
SI/O Low Time, Logic '0' Condition[6]	t_{LOW0}	Input Bit Frame	6	16	µs
SI/O Low Time, Logic '1' Condition[6]	t_{LOW1}	Input Bit Frame	1	2	µs
Host SI/O Low Time during Read[6]	t_{RD}	Output Bit Frame	1	2 – t_{PUP}[2]	µs
Host Read Strobe Time[6]	t_{MRS}	Output Bit Frame	$t_{RD} + t_{PUP}$[2]	2	µs
Data Output Hold Time (Logic '0')[7]	t_{HLD0}	Output Bit Frame	2	6	µs
Client Recovery Time[6, 7]	t_{RCV}	Input and Output Bit Frame	4[3, 4]	—	µs
Glitch Filter[5]	t_{IGNORE_SWI}	Input Bit Frame	50	500	ns

Notes:

1. AC measurement conditions for the table above:
   - All parameters are production tested unless otherwise noted.
   - Loading capacitance on SI/O: 100 pF
   - V_{PUP}: Applied at minimum and maximum V_{CC}
   - In Parasitic Power mode, V_{PUP} minimum restricted to 2.4V
2. t_{PUP} is the time required to be pulled up from V_{IL} to V_{IH} when the SI/O line is released. This value is application-specific and is a function of the loading capacitance on the SI/O line as well as the R_{PUP} chosen.
3. The system designer must select a combination of R_{PUP}, C_{BUS} and t_{BIT} such that the minimum t_{RCV} is satisfied. The relationship of t_{RCV} within the bit frame can be expressed by the following formula: $t_{BIT} = t_{LOW0} + t_{PUP} + t_{RCV}$.
4. Microchip's AT21CS11 supports 2 µs.
5. The glitch filter is assured to suppress all pulses below the min value but may suppress values as great as the max value over all process, voltage and temperature conditions.
6. The host system must ensure the parameter timing values are met.
7. By design, the SHA104-TFLXAUTH ensures this timing parameter is met.

5.4 DC Parameters

5.4.1 DC Parameters: All I/O Interfaces

Table 5-6. DC Parameters on All I/O Interfaces with V_{CC} Power Applied
Unless otherwise indicated, these values are applicable over the specified operating range from T_A = -40°C to +105°C, V_{CC} = +1.65V to +5.5V.

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Ambient Operating Temperature	T_A	-40	—	+105	°C	—
V_{CC} Ramp Rate[6]	V_{RISE}	—	—	0.1	V/µs	—
Output Low Voltage	V_{OL}	—	—	0.4	V	When the device is in Active mode, V_{CC} = 1.65V to 3.6V for output-low current = 4.0 mA
		—	—	0.4	V	V_{CC} > 3.6V = 10.0 mA[6]
Input Low Threshold	V_{IL1}	-0.5	—	0.3*V_{CC}	V	Device is active and CMOSEnable = 1
Input High Threshold	V_{IH1}	0.7*V_{CC}	—	V_{CC}+0.5	V	Device is active and CMOSEnable = 1
Input Low Threshold[1, 2]	V_{IL0}	-0.5	—	0.5	V	Device is active and CMOSEnable = 0
Input High Threshold[1, 2]	V_{IH0}	1.2	—	V_{CC}+0.5	V	Device is active and CMOSEnable = 0

.....continued						
Parameter	**Sym.**	**Min.**	**Typ.**	**Max.**	**Units**	**Conditions**
Input Leakage (I^2C Signals)	I_{IN}	-200	—	200	nA	$V_{IN} = V_{CC}$ or GND
Sleep Current[3]	I_{SLEEP}	—	130	325[6]	nA	When the device is in Sleep mode, $V_{CC} \leq 3.6V$, I/O at either GND or V_{CC} $T_A \leq +55°C$
		—	130	500	nA	$V_{CC} \leq 3.6V$, I/O at either GND or V_{CC} Full temperature Range
		—	130	1000	nA	When the device is in Sleep mode Over full V_{CC} and temperature range
Current Consumption in I/O Mode	$I_{I/O}$	—	60	250	µA	Waiting for I/O
Current Consumption in Computation Mode	$I_{COMPUTE}$[4]	—	—	0.75	mA	During command execution 1x divider
		—	—	0.5	mA	During command execution 2x divider
		—	—	0.4	mA	During command execution 4x divider
EEPROM Write Current	I_{WRITE}[5]	—	0.6	1.5	mA	Current when writing to EEPROM -5°C to +105°C
EEPROM Write Current	I_{WRITE}[5]	—	0.6	4.0	mA	Current when writing to EEPROM full temperature range
Theta JA	Θ_{JA}	—	166	—	°C/W	8-lead SOIC
		—	173	—	°C/W	8-pad UDFN

Notes:

1. CMOSen = `0` must only be used when V_{CC} is between 2.0V and 5.5V and the host is running on a lower supply voltage than the client. In this mode, the input buffers are referenced to an internal supply and V_{IL} and V_{IH} levels are independent of the external V_{CC} supply over this range. For voltages lower than 2.0V, CMOSen must always be set to '`1`'.
2. CMOSen = `0` must not be used when SWI Parasitic Power mode is used.
3. The lowest system current will be achieved if the inputs are driven to V_{CC} or allowed to be pulled up to V_{CC} by the pull-up resistors on the signal lines.
4. Applies to all commands where an EEPROM write does not occur.
5. Applies to all commands where an EEPROM write occurs. This includes `Write`, `Lock`, `GenKey`, `Counter(Increment)`.
6. This condition is characterized but not production tested.

5.4.2 DC Parameters: Single-Wire Interface

Table 5-7. DC Parameters on Single-Wire Interface[1]
Unless otherwise indicated, these values are applicable over the specified operating range from T_A = -40℃ to +105℃, V_{CC} = +1.65V to +5.5V.

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Power Supply Voltage	V_{CC}	1.65V	—	5.5V	V	—
Output Low Voltage	V_{OL}	—	—	0.4	V	When the device is in Active mode, V_{CC} = 1.65V to 3.6V for output-low current = 8.0 mA
		—	—	0.4	V	V_{CC} > 3.6V 16.0 mA[3]
Input High Leakage	I_{IH}	—	1.0	2.0	uA	$V_{IN} = V_{CC}$
Input Low Leakage	I_{IL}	-200	—	200	nA	V_{IN} = GND

.....continued						
Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Bus Capacitance	C_{BUS}	—	—	500	pF	—

Notes:

1. All specifications not shown can be found in the All I/O Interfaces Table 5-6.
2. The Single-Wire voltage must never be greater than V_{CC}.
3. This condition is characterized but not production tested.
4. Operation over the C_{BUS} range is ensured by design and is not production tested.

5.4.3 DC Parameters: Single-Wire Interface – Parasitic Power Mode

Table 5-8. DC Parameters on Parasitic Single-Wire Interface
Unless otherwise indicated, these values are applicable over the specified operating range from T_A = -40℃ to +105℃, CMOSen = '1'

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Max. I/O Voltage(2)	V_{PUP}	2.5	—	5.5	V	—
Output Low Voltage	V_{OL}	—	—	0.4	V	When the device is in Active mode, V_{PUP} = 2.5V to 3.6V for output-low current = 8.0 mA
Input Low Leakage(4)	I_{IL}	-200	—	200	nA	V_{IN} = GND, V_{CC_DVC} ≥ 1.65V
Input Low Threshold	V_{IL1}	-0.5	—	0.3*V_{PUP}	V	—
Input High Threshold	V_{IH1}	0.7*V_{PUP}	—	V_{PUP}+0.5	V	—
Bus Capacitance	C_{BUS}	—	—	500	pF	—

Notes:

1. All specifications not shown can be found in the All I/O Interfaces Table 5-6.
2. Single-Wire voltage (V_{PUP}) must never be greater than the maximum V_{PUP} operating voltage.
3. For the lowest system current, the SI/O signal must be driven to V_{PUP} by the host or allowed to be pulled up by the pull-up resistors.
4. Input High leakage cannot be measured in parasitic power mode because the device and decoupling capacitor are charged via the SI/O signal. Low leakage is valid provided device was charged to be within the operational range.
5. Operation over the C_{BUS} range is ensured by design and is not production tested.

6. Command Descriptions

6.1 Counter Command

The Counter command reads or increments the binary count value from the monotonic counter located on the device within the Configuration zone. The maximum value of the counter is fixed at 10,000. The starting value of the counter is programmed during initial provisioning and, when CSZ2 is locked, it cannot be modified.

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.

The counter can be attached to the secret key in Slot 3 to limit its use. The counter will be incremented whenever the MAC command is called or until the counter has reached its maximum value, at which point, use of the key will no longer be permitted and an execution error will occur.

The number of legal uses for a key can also be controlled by initializing the counter to a non-zero value at configuration time. Contact Microchip for details.

Related Links

3.2.2. Monotonic Counter

6.2 Delete Command

The Delete command, when executed, will clear all of the Data zone slots and set all bytes of each slot to 0xFF. The Configuration zone will be untouched, except for the value of the Primary_Deleted byte.

6.3 Info Command

The Info command accesses some static or dynamic status information from the device depending upon the parameters input to the command. The specific command modes include:

Revision	Returns a value indicating the device identification byte and the revision number of the device. It is recommended that software not depend on the revision information as it may change over time.
LockStatus	Returns a value indicating if the Slot selected in either the Configuration or Data zone is locked or unlocked. After the Delete command has been run this mode will always fail.
ChipStatus	Returns a value. The first byte returned indicates if the Delete command has been used to clear the data slots.

Related Links

6.4. Lock Command

6.4 Lock Command

The Lock command prevents future modifications of the Configuration and/or Data zones. This command can be used to lock individual Configuration subzones or individual Data zone slots. Prior to locking or writing any Data zone slots, CSZ0 and CSZ1 must be locked. CSZ0 is pre-locked by Microchip prior to device shipment.

6.5 MAC Command

The MAC command computes a SHA-256 digest of a key stored in the device or a challenge. The output of this command is the digest of this message. If the message includes the serial number of the device, the response is said to be “diversified”.

6.6 Nonce Command

The Nonce command has multiple purposes. The command can be used to output a random number for use by the system, input a fixed value to be used by other commands, generate a random value for use by other commands or to generate a Session Key for use by a subsequent write command dependent upon the mode.

Related Links
3.3.2. Random Number Generator (RNG)

6.7 Read Command

The Read command is used to read data from either the Configuration zone or the EEPROM Data zone. The Configuration zone is always readable and can be read 16 bytes at a time. Data zone slots that allow reading can be read 32 bytes at a time. Multiple reads are required to completely read some data slots. Data slot 3 can never be read, and an execution error will occur if so attempted. Data slots 1 and 2 can always be read in the clear.

6.8 SelfTest Command

The SelfTest command performs on-demand testing of one or more of the cryptographic algorithms implemented in the SHA104-TFLXAUTH. The SHA-256 algorithm and the DRBG of the RNG each have a self-test routine to confirm their integrity. The SelfTest command can be run at any time after the initial start-up procedure is completed.

Related Links
3.3.2. Random Number Generator (RNG)

6.9 SHA Command

The SHA command computes a SHA-256 digest for general purpose use by the host system. The SHA command must be executed repetitively to calculate the digest over the entire message. Data can be sent to the command in 1-64-byte blocks. The maximum message length over which a digest can be calculated is limited to 2^{28} bytes.

Upon successful completion of the command, a 32-byte value is output on the bus. If this value is required for use in a SHA104-TFLXAUTH command, the value must first be stored in the system, then resubmitted as an input parameter to the command. There is no ability to store the value directly in the device.

6.10 Write Command

The Write command writes 16 bytes to one of the EEPROM Configuration subzones or 32 bytes to the EEPROM Data zone slots. Multiple writes may be required to completely write the data slots. Data in slots 1 and 2 can be written using a clear text write. The secret key in Slot 3 can be written either with a clear text write or with an encrypted write.

Modes of Operation:

1. Configuration subzone Write
2. Clear Text Data slot Write
3. Encrypted Key Write

Related Links
2.2. EEPROM Configuration Zone

7. Application Information

The SHA104-TFLXAUTH 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 SHA104-TFLXAUTH device was developed to take the guesswork out of adding security to accessory and disposable devices while maintaining a high level of security.

In addition to the secure element, Microchip has 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.

7.1 Development Tools

The SHA104-TFLXAUTH 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 SHA104-TFLXAUTH 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 SHA104-TFLXAUTH devices can be ordered through Microchip Direct.

7.1.1 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 SHA104-TFLXAUTH.

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

7.1.2 Hardware Tools

There are multiple hardware tools that can help in developing with the SHA104-TFLXAUTH. 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. With the exception of the EV97M19A, sample units must be acquired to use with the kit as they are not included.

DM320118 – CryptoAuthentication Trust Platform

The DM320118 is a compact development system consisting of an ATSAMD21 microcontroller, one each of the ATECC608B-TNGTLS, ATECC608B-TFLXTLS and ATECC608B-TCSM Trust devices, a USB Hub, a mikroBUS™ connector and an on-board debugger. Through use of the mikroBUS header, additional types of devices can be configured with the Trust Platform Design Suite of tools and

used to implement various use cases with a wide variety of devices. The kit can be used with either MPLAB® X or Microchip Studio Design environments to develop applications.

EV97M19A – SHA104/5 CryptoAuth

The EV97M19A development board is a mikroBUS accessory board for evaluating the SHA104 and SHA105 CryptoAuthentication Devices. These devices are generic devices that are not provisioned. The board has both SHA104 I^2C and SWI devices mounted and a SHA105 I^2C only. The board can be directly connected to a DM320118 or any host board that supports a mikroBUS host interface. The pass-through header allows additional mikroBus accessories to be used at the same time as the EV97M19A.

DM320109 – CryptoAuthentication Starter Kit

The DM320109 consists of an ATSAMD21-XPRO development board pre-programmed with firmware that can work with CryptoAuthentication devices and the TPDS tools. The kit comes with the AT88CKSCKTSOIC-XPRO socket board but can be used with the AT88CKSCKTUDFN-XPRO board as well. Samples of the SHA104-TFLXAUTH will need to be obtained separately as they are not included in the kit. Through the use of the ATMBUSAdapter, the mikroBUS accessory board can also be used with this board. The board has three XPRO extension sockets making it ideal for developing more complex systems.

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. Samples of the SHA104-TFLXAUTH will need to be obtained separately as they are not included in the kit.

7.1.3 CryptoAuthLib

CryptoAuthLib is a software library that supports Microchip's family of CryptoAuthentication devices. Microchip recommends working with this library when developing with the SHA104-TFLXAUTH. The library implements the API calls necessary to execute the commands detailed in this data sheet.

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

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

- CryptoAuthLib – Web Link
- CryptoAuthLib – GitHub

API Calls

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

Table 7-1. Example Commands to CryptoAuthLib API Calls

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

8. Package Marking Information

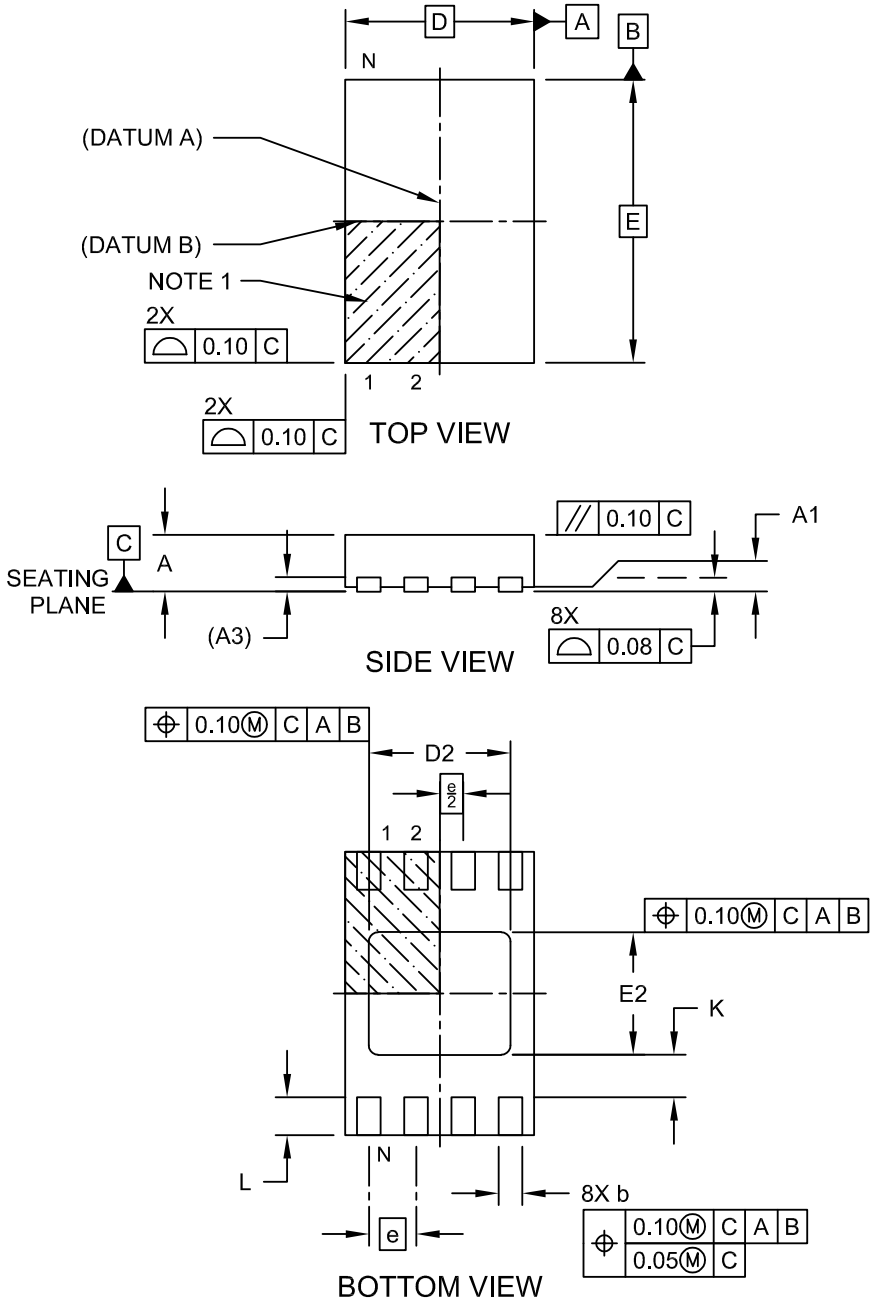
As part of Microchip's overall security features, the part marking for all crypto devices is intentionally vague. The marking on the top of the package does not provide any information as to the actual device type or the manufacturer of the device. The alphanumeric code on the package provides manufacturing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

9. Package Drawings

9.1 8-Pad UDFN

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

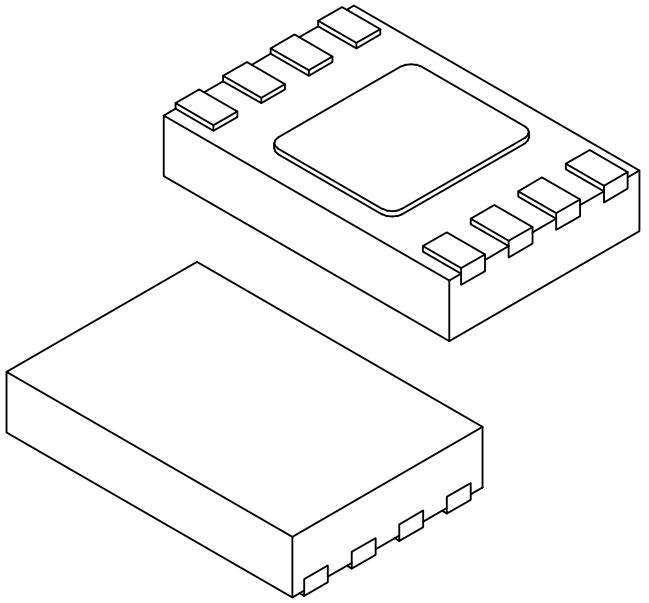
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



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

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

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



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	0.25	0.35	0.45
Terminal-to-Exposed-Pad	K	0.20	-	-

Notes:

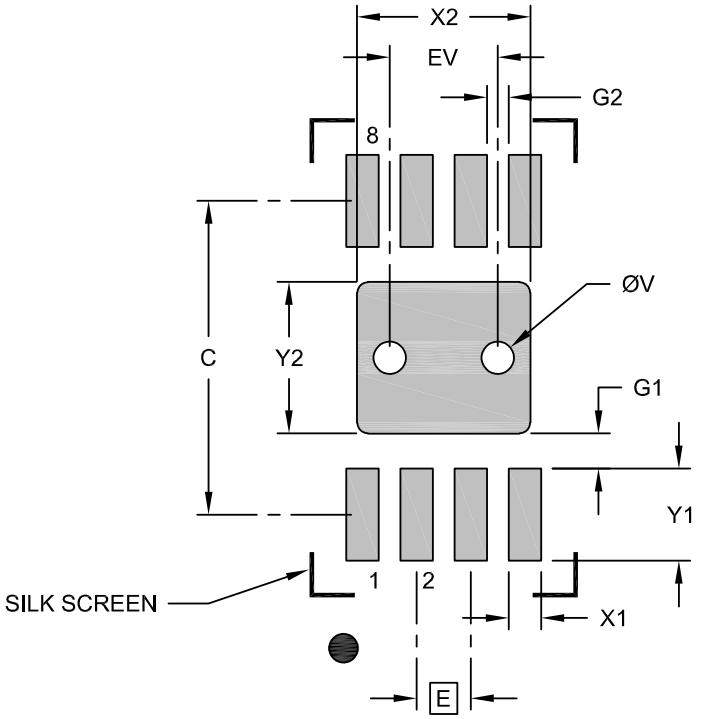
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M

BSC: Basic Dimension. Theoretically exact value shown without tolerances.
REF: Reference Dimension, usually without tolerance, for information purposes only.

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

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

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



RECOMMENDED LAND PATTERN

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:

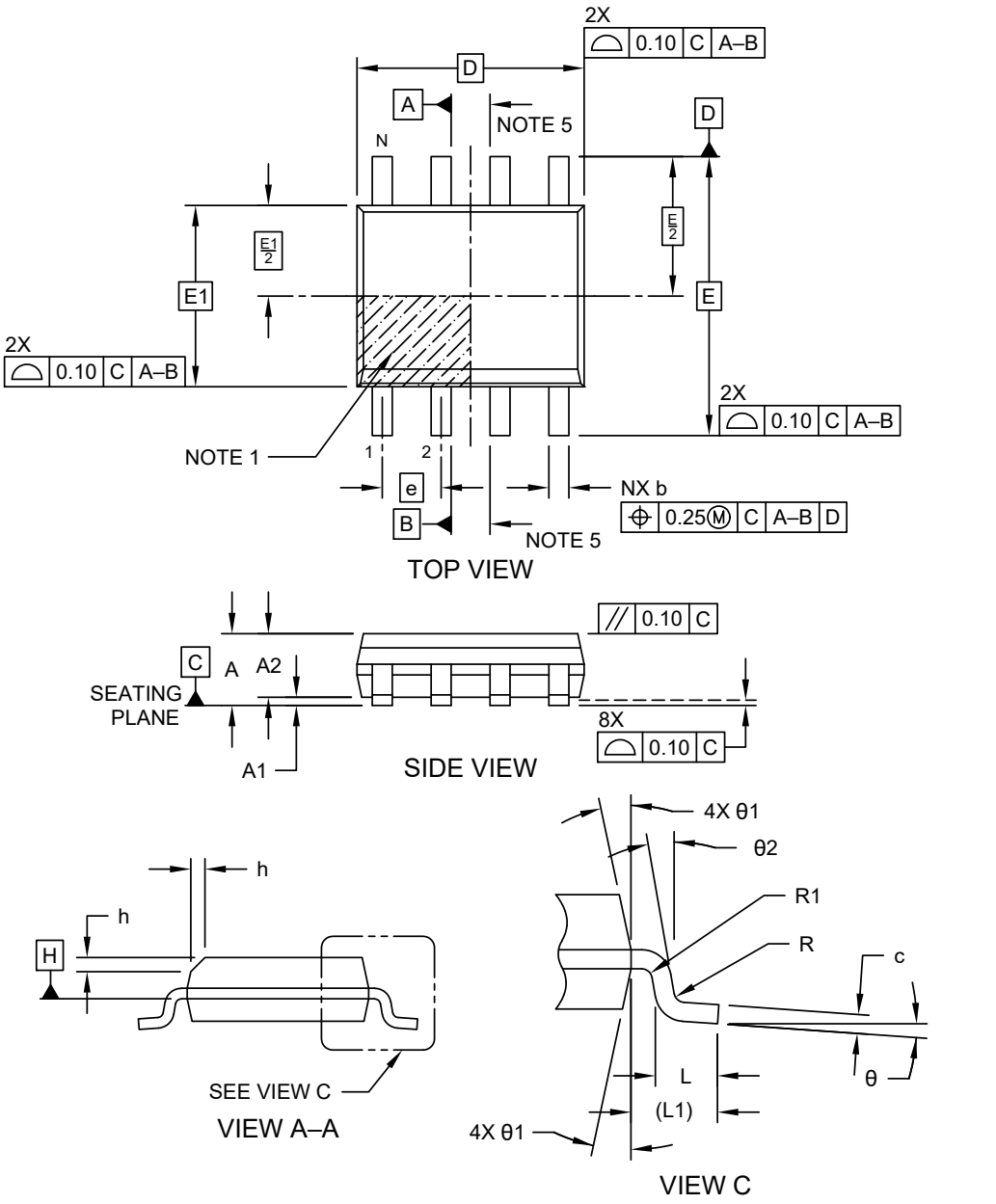
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
2. For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

Microchip Technology Drawing C04-23355-Q4B Rev C

9.2 8-Lead SOIC

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

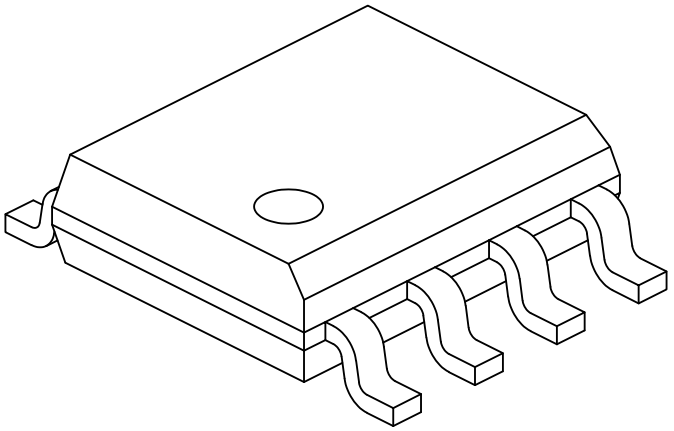
Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



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

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

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



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	
Lead Thickness	c	0.17	–	0.25
Lead Width	b	0.31	–	0.51
Lead Bend Radius	R	0.07	–	–
Lead Bend Radius	R1	0.07	–	–
Foot Angle	θ	0°	–	8°
Mold Draft Angle	θ1	5°	–	15°
Lead Angle	θ2	0°	–	–

Notes:

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

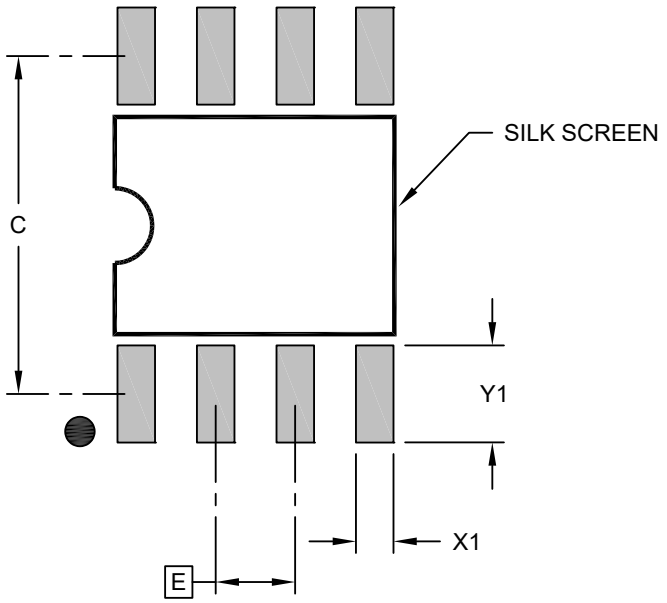
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

   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-OA Rev K Sheet 2 of 2

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

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



RECOMMENDED LAND PATTERN

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:

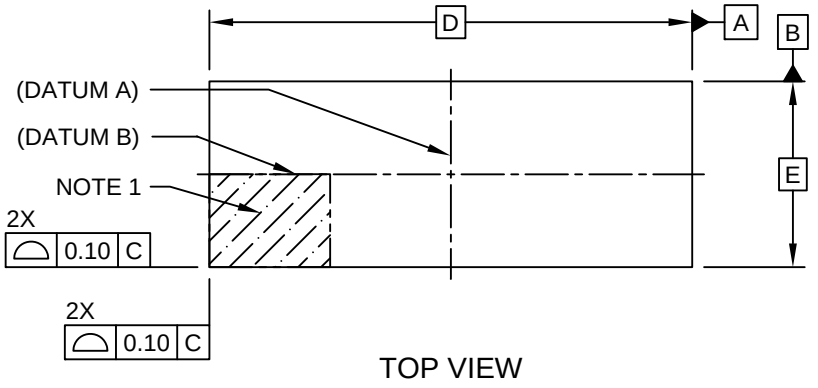
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-2057-OA Rev K

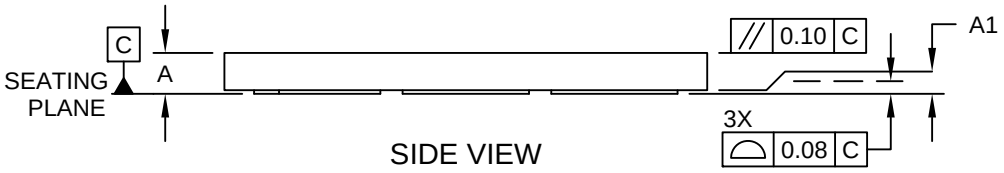
9.3 3-Lead Contact

3-Lead Contact Package (LAB) - 6.54x2.5 mm Body [Contact]
Atmel Legacy Global Package Code RHB

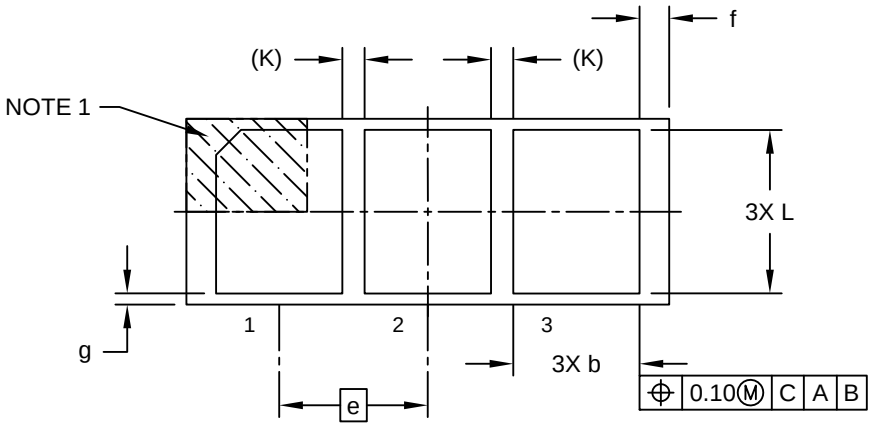
Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



TOP VIEW



SIDE VIEW

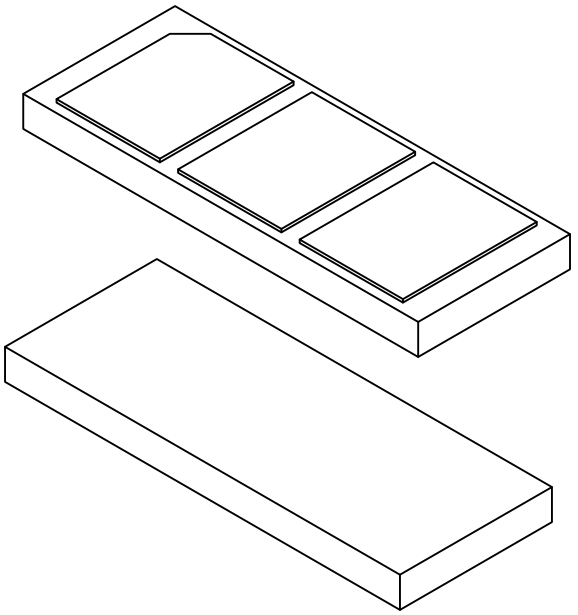


BOTTOM VIEW

Microchip Technology Drawing C04-21303 Rev A Sheet 1 of 2

3-Lead Contact Package (LAB) - 6.54x2.5 mm Body [Contact]
Atmel Legacy Global Package Code RHB

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		3	
Pitch	e		2.00 BSC	
Overall Height	A	0.45	0.50	0.55
Standoff	A1	0.00	0.02	0.05
Overall Length	D		6.50 BSC	
Overall Width	E		2.50 BSC	
Terminal Width	b	1.60	1.70	1.80
Terminal Length	L	2.10	2.20	2.30
Terminal-to-Terminal Spacing	K		0.30 REF	
Package Edge to Terminal Edge	f	0.30	0.40	0.50
Package Edge to Terminal Edge	g	0.05	0.15	0.25

Notes:

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. 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 C04-21303 Rev A Sheet 2 of 2

10. Revision History SHA104

Revision A (July 2023)

- Initial data sheet release

Microchip Information

The Microchip Website

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

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

Product Change Notification Service

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

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

Customer Support

Users of Microchip products can receive assistance through several channels:

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

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

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

Product Identification System

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

PART NO	-	Trust Type	Trust Option	Package Type	-	I/O Option
xxxxx	-	tttt	vvvv	p	-	yy

Part No	SHA104: Cryptographic Co-processor with Secure Hardware-based Key Storage	
Trust Type	TFLX	Type of Microchip Trust Product
Trust Option	AUTH	Configuration associated with Trust Product
Package Options(1,2)	S	8-Lead (0.150" Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC)
	U	8-Pad 2 mm x 3 mm x 0.6 mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat No Lead Package (UDFN)
Interface Options	—	I^2C Interface
	CZ	SWI Interface

Examples:

- SHA104-TFLXAUTHS: 8-Lead (0.150" Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC), I^2C MOQ 2k units
- SHA104-TFLXAUTHS-CZ: 8-Lead (0.150" Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC), SWI, MOQ 2k units
- SHA104-TFLXAUTHU: 8-Pad 2 mm x 3 mm x 0.6 mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat No Lead Package (UDFN), I^2C, MOQ 2k units
- SHA104-TFLXAUTHU-CZ: 8-Pad 2 mm x 3 mm x 0.6 mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat No Lead Package (UDFN), SWI, MOQ 2k units

Notes:

1. Product will be delivered as Tape and Reel. Actual size of reel will vary based on customer order. 2k units is the minimum order quantity (MOQ) allowed.
2. The 3-Lead Contact package can not be ordered through the low MOQ flow (2k units on Microchip Direct). The package option (SHA104-RBVCZ) can be selected through TPDS but must be ordered through the high volume flow. Contact Microchip sales for more information on the MOQ.

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

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

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided

only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

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

Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

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

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

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

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

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

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

ISBN: 978-1-6683-2774-6

Quality Management System

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

Worldwide Sales and Service

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