

Introduction

The SHA105-TFLXAUTH is a member of the Microchip Technology Inc. Trust Platform product family. The device is a pre-provisioned SHA105 targeted for use in symmetric authentication applications and is ideally suited for use in consumable and disposable applications as the host-side security device. The device can be used in systems where the host-side security device performs a CheckMAC operation. The SHA105-TFLXAUTH can be used in conjunction with the SHA104-TFLXAUTH or other Microchip CryptoAuthentication™ client-side devices.

Features

- Cryptographic Authentication Device with Secure Hardware-Based Key Storage:
 - Protected storage for symmetric key
- Hardware Support for CheckMAC Validation of Client-Generated MAC
- Internal High-Quality NIST SP 800-90A/B/C True Random Number Generator (TRNG) (NIST Certified)
- Extensive Security Measures Against Attacks
- Strong Physical Protection Mechanisms Against Invasive Attacks
- Field-Programmable EEPROM
 - Single symmetric secret key
 - I/O protection key
 - 384-byte user memory
 - 40-year data retention at +55°C
- Monotonic Counter with Max Count Value of 10,000
- Unique 72-Bit Serial Number
- Interface: 400 kHz Fast-Mode I²C Interface
- Voltage Supply Range: 1.65V to 5.5V
- 130 nA Nominal Sleep Current
- Human Body Model (HBM) ESD: >4 kV;
- Packaging Options: 8-Pad UDFN (2 mm x 3 mm), 8-Lead SOIC

Use Cases

Host side authentication support for:

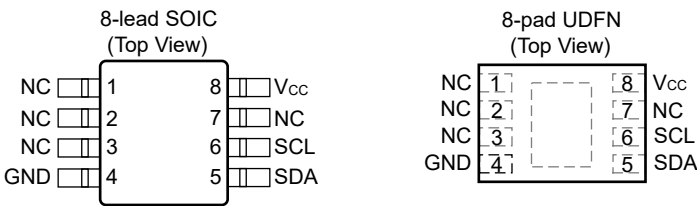
- Disposables and accessory authentication
- Ecosystem control
- Anti-cloning

Pin Configuration and Pinouts

Table 1. Pin Configuration

Package = 8-Pad SOIC or 8-Lead UDFN		
Pin #	Function	I ² C
1-3, 7	No Connect	NC
4	Ground	GND
5	Serial I/O	SDA
6	Serial Clock	SCL
8	Supply	VCC

Figure 1. Pinouts⁽¹⁾



Note:

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

Table of Contents

Introduction.....	1
Features.....	1
Use Cases.....	1
Pin Configuration and Pinouts.....	2
1. Overview.....	5
1.1. Use Cases.....	5
1.2. Device Features.....	5
2. EEPROM Memory.....	6
2.1. EEPROM Data Zone.....	6
2.2. EEPROM Configuration Zone.....	6
3. Security Information.....	8
3.1. Cryptographic Standards.....	8
3.1.1. SHA-256.....	8
3.2. Key Uses and Restrictions.....	8
3.2.1. Symmetric Keys.....	8
3.2.2. Monotonic Counter.....	8
3.3. Security Features.....	8
3.3.1. Physical Security.....	8
3.3.2. Random Number Generator (RNG).....	9
4. I/O Interfaces.....	10
4.1. General I/O Information.....	10
4.2. I ² C Interface.....	11
4.2.1. I/O Conditions.....	12
4.2.1.1. Device is Asleep.....	12
4.2.1.2. Device is Awake.....	12
4.2.2. I ² C Bus Transactions.....	12
4.2.2.1. Data Input and Output Frames.....	12
4.2.3. Split I ² C Transactions.....	14
4.2.4. I ² C Synchronization.....	14
4.3. I/O Transmission to the SHA105-TFLXAUTH.....	15
4.3.1. Word Address Values.....	16
4.3.2. Sleep Sequence.....	16
4.3.3. Command Completion Polling.....	16
4.4. I/O Transmission from the SHA105-TFLXAUTH.....	16
5. Electrical Characteristics.....	18
5.1. Absolute Maximum Ratings.....	18
5.2. Reliability.....	18
5.3. AC Parameters.....	18
5.3.1. AC Parameters: All I/O Interfaces.....	18
5.3.2. AC Parameters: I ² C Interface.....	19
5.4. DC Parameters.....	20

5.4.1. DC Parameters: All I/O Interfaces.....	20
6. Command Descriptions.....	22
6.1. CheckMac Command.....	22
6.2. Counter Command.....	22
6.3. Delete Command.....	22
6.4. GenDivKey Command.....	22
6.5. Info Command.....	22
6.6. Lock Command.....	23
6.7. Nonce Command.....	23
6.8. Read Command.....	23
6.9. SelfTest Command.....	23
6.10. SHA Command.....	23
6.11. Write Command.....	23
7. Application Information.....	25
7.1. Development Tools.....	25
7.1.1. Trust Platform Design Suite.....	25
7.1.2. Hardware Tools.....	25
7.1.3. CryptoAuthLib.....	26
8. Package Marking Information.....	28
9. Package Drawings.....	29
9.1. 8-Pad UDFN.....	29
9.2. 8-Lead SOIC.....	32
10. Revision History SHA105.....	35
11. Product Identification System.....	36
Microchip Information.....	37
Trademarks.....	37
Legal Notice.....	37
Microchip Devices Code Protection Feature.....	37
Product Page Links.....	38

1. Overview

1.1. Use Cases

SHA105-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.

SHA105-TFLXAUTH has a command set that allows for its usage in multiple symmetric key applications where a host side device is required. The SHA105-TFLXAUTH will perform a CheckMAC operation to validate the MAC that was executed on the SHA104-TFLXAUTH or other client side device. The primary uses include the following:

- **Accessory/Disposable Authentication**
 - **Shared Key authentication** – Requires integrating a SHA104 on the accessory/disposable and a 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.

1.2. Device Features

SHA105-TFLXAUTH includes an EEPROM array that can be used for storage of one secret key, one I/O protection 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 SHA105 supports a standard I²C interface at speeds of up to 400 KHz. The interface is compatible with standard-mode and fast-mode I²C interface specifications.

Each SHA105-TFLXAUTH unit ships with a unique 72-bit serial number. Also, SHA105-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 SHA105-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.

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

[EEPROM Data Zone](#)

2.1. EEPROM Data Zone

The data zone has a total of 4 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
0	1	32	256	I/O Protection Key	Key can be written in the clear. When written, it is recommended that this slot be locked. No Read access.
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	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 slot 3 of the SHA105-TFLXAUTH must be the same as the key stored in the client device or the key that was used to generate a diversified key in the client device.

2.2. EEPROM Configuration Zone

The SHA105-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 I²C address is 0x42. The I²C 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.
- A symmetric key can be programmed into the device to allow for CheckMac operations and to allow for calculation of a diversified key.
- 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.

- I²C address
- I/O levels can be modified to have a fixed reference. This allows for the I²C Bus to run at a lower voltage level than the SHA105-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.
- 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

SHA105-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 SHA105-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.

For enhanced symmetric security, it is recommended that a host side security device be added to the system and that diversified keys be used for the disposable/accessory device. Diversified keys are generated by the provisioning system, by hashing a common parent key, with the unique serial number of each of the disposable device and some additional information. The host device securely stores the parent key. With the help of the host microcontroller, the serial number from the disposable device will be read, loaded into the host security device and the diversified key of the disposable is regenerated. Once this has been done, a random challenge can be initiated and MAC/CHECKMAC operations can be performed to verify the authenticity of the disposable device in a highly secure fashion.

Storing the parent key in a secure host device makes it more difficult to compromise the security of the system. Utilizing diversified keys, limits any security exposure to an individual disposable device. Because the host regenerates the diversified key from a disposable device it is not limited in terms of the disposable devices it can be used with. The SHA105 has the ability to regenerate and authenticate the diversified key of the client device when the Parent key is stored in Slot 3. The TPDS tools can assist with this process.

I/O Protection Key

For the SHA105, Slot 0 may be configured with an I/O Protection key. This key can be used to generate the MAC response for the `CheckMac` command.

3.2.2. Monotonic Counter

SHA105-TFLXAUTH supports one nonvolatile monotonic counter that can count to a value of 10,000.

The monotonic counter can only be used as a system counter and can not be connected to any keys :

Related Links

[Counter Command](#)

3.3. Security Features

3.3.1. Physical Security

The SHA105-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 SHA105-TFLXAUTH device includes a high-quality cryptographic True Random Number Generator (TRNG) implemented according to the NIST standards SP800-90A/B/C.

The NRBG output is evaluated using the methods in NIST SP 800-90B. The DRBG is designed using the SHA-256 variant specified within NIST SP 800-90A. The combination of the two creates the TRNG output following the methods specified in NIST SP 800-90C:

- [NIST SP800-90A](#): Certified as part of the NIST Cryptographic Algorithm Validation Program (CAVP) certification process ([Hash DRBG CAVP Certification](#))
- [NIST SP 800-90B](#): Certified as part of the NIST [Entropy Source Validation](#) (ESV) process ([ESV Certificate #E194 - Operating Environment 59V02 A3](#))
- [NIST SP 800-90C](#): Currently a draft specification with implementation recommendations and does not have a specific certification procedure

4. I/O Interfaces

The I²C interface uses the SDA and SCL pins to transfer commands/data/status to and from the SHA105-TFLXAUTH device. Data flow is controlled by the host controller.

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 SHA105-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 SHA105-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 I²C standard uses the terminology “Master” and “Slave”. The equivalent Microchip terminology used in this document is “Host” and “Client”, respectively.

4.1. General I/O Information

The SHA105-TFLXAUTH operates as a client device and utilizes an I²C digital serial interface to communicate with a host controller. The host device controls all read and write operations to the client device(s) on the serial bus.

- **I²C Interface:**
This mode is compatible with the I²C standard and with the Microchip AT24C16 Serial EEPROM interface. Two pins, Serial Data (SDA) and Serial Clock (SCL), are required. The I²C interface supports a bit rate of up to 400 kbps.

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

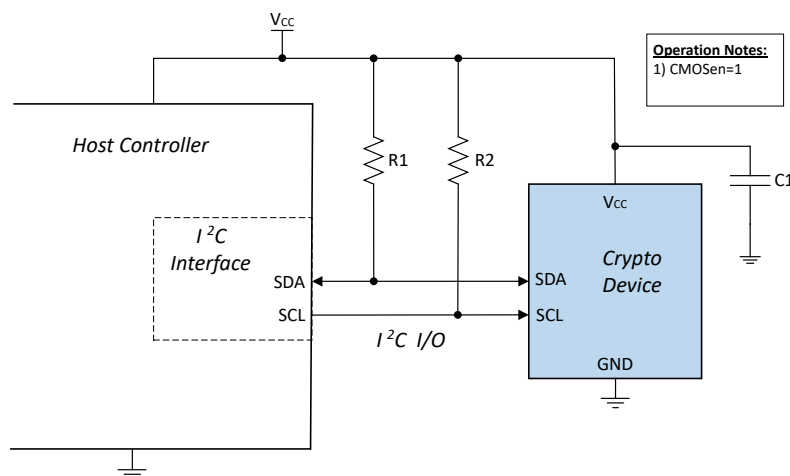
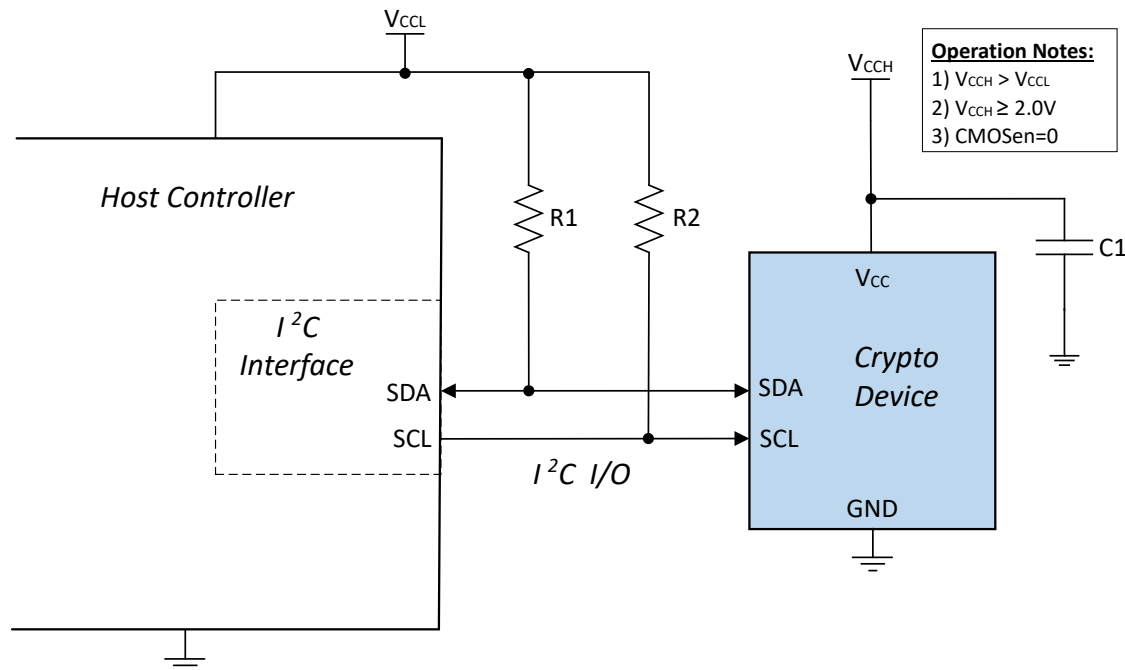


Figure 4-2. Application Diagram for using Using the I²C Interface with CMOSen=0**Related Links**[I2C Interface](#)**4.2. I²C Interface**

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 SHA105-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 SHA105-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 SHA105-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 SHA105-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.

4.2.1. 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 but the Wake condition. The Wake condition is as follows:

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

The SHA105-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 SHA105-TFLXAUTH will NACK the device address and ignore all subsequent bytes until t_{PU} expires.

Related Links

[Data Input and Output Frames](#)

[AC Parameters: All I/O Interfaces](#)

4.2.1.2. Device is Awake

When the device is awake, it honors the conditions listed in [I2C Bus Transactions](#).

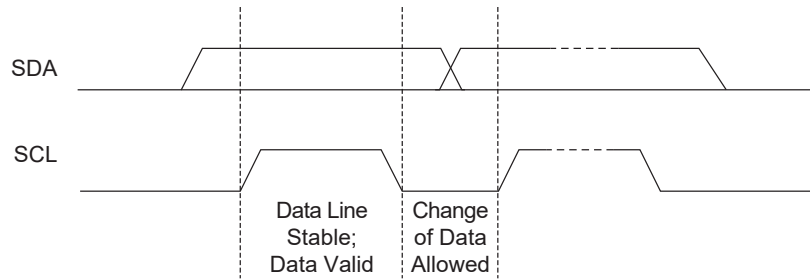
4.2.2. I²C Bus Transactions

Types of data transmitted over the I²C bus:

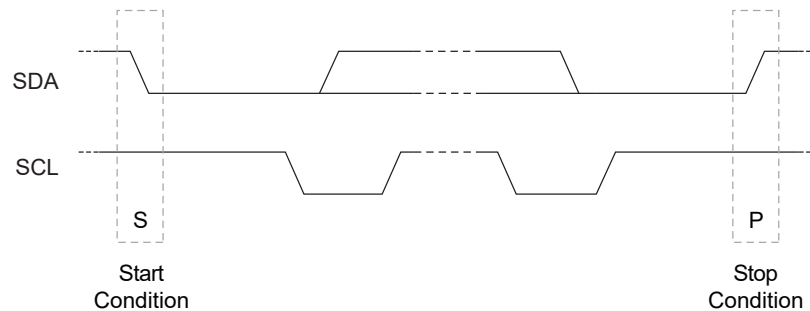
- Data '0'
- Acknowledge (ACK)
- Data '1'
- No Acknowledge (NACK)
- Start condition
- Stop condition

4.2.2.1. Data Input and Output Frames

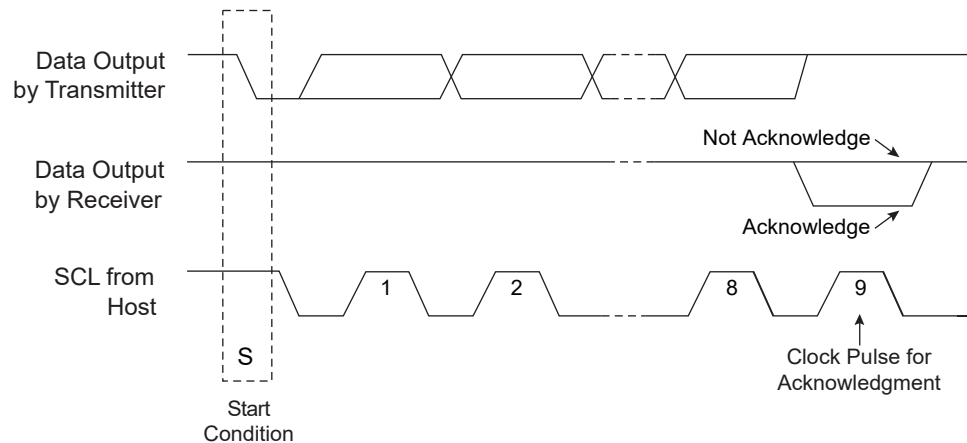
- **DATA Zero:** If SDA is low and stable while SCL goes from low to high to low, a zero bit is transferred on the bus. SDA can change while SCL is low.
- **DATA One:** If SDA is high and stable while SCL goes from low to high to low, a one bit is transferred on the bus. SDA can change while SCL is low.

Figure 4-3. Data Bit Transfer on the I²C 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 4-4. Start and Stop Conditions on the I²C 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 4-5. NACK and ACK Conditions on the I²C Interface

Multiple SHA105 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 SHA105-TFLXAUTH can also share the I²C interface with any I²C device, including any Serial EEPROM.

4.2.3. Split I²C Transactions

System requirements sometimes limit the length of a transaction to a certain number of bytes. The SHA105-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 4-6. 32-Byte Standard I²C Write

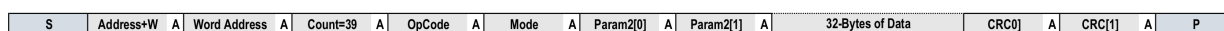


Figure 4-7. 32-Byte Split I²C Write

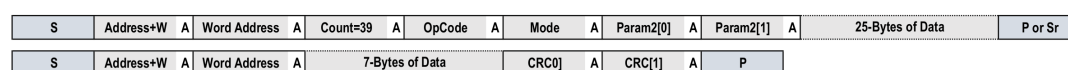


Figure 4-8. 32-Byte Standard I²C Read

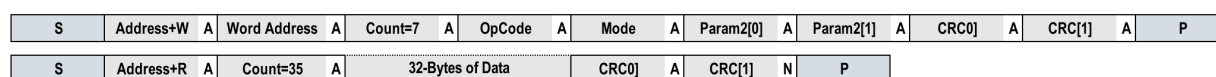
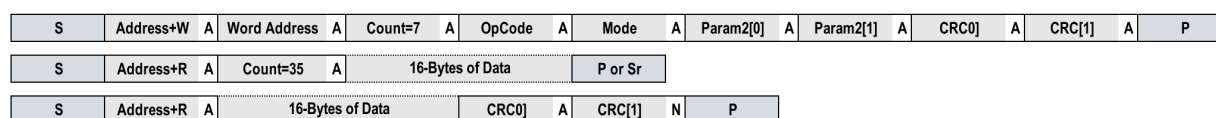


Figure 4-9. 32-Byte Split I²C Read



4.2.4. I²C Synchronization

It is possible for the system to lose synchronization with the I/O port on the SHA105-TFLXAUTH, perhaps due to a system reset, I/O noise or other conditions. Under this circumstance, the SHA105-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 SHA105-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 $0 \times FF$) during the data periods.

If the device does ACK the device address, the system must reset the internal address counter to force the SHA105-TFLXAUTH to ignore any partial input command that was possibly sent. This can be accomplished by sending a write sequence to word address 0×00 (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.

4.3. I/O Transmission to the SHA105-TFLXAUTH

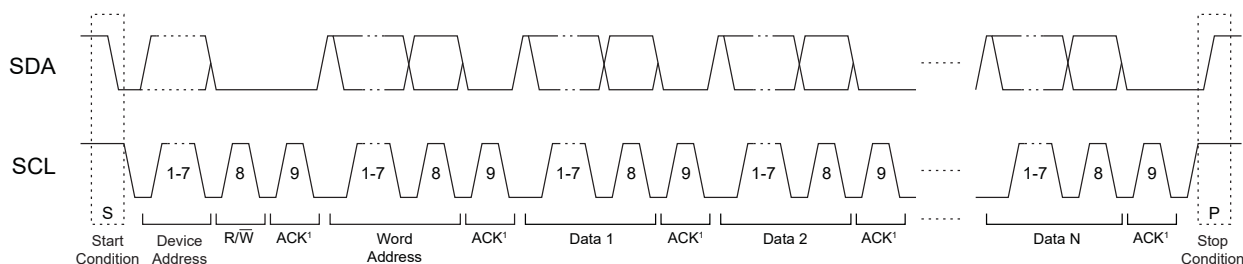
The transmission of data from the system to the SHA105-TFLXAUTH is summarized in the table below. This transmission sequence is valid for I²C communications. The order of transmission is as follows:

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

Table 4-1. Transmission to the SHA105-TFLXAUTH

Name	I/O Name	Description
Device Address	Device Address	This byte selects a particular device on the I/O interface. SHA105-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/W bit and must be zero to indicate a write operation (the bytes following the device address travel from the host to the client).
Word Address	Word Address	This byte must have a value of 0×03 for normal operation. See 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 4-10. Normal I²C Transmission to the SHA105-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 SHA105-TFLXAUTH will start the computation of the command. Failure to send a Stop condition may eventually result in a loss of synchronization.

4.3.1. Word Address Values

During an I/O write packet, the SHA105-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 SHA105-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.
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 SHA105-TFLXAUTH.

4.3.2. Sleep Sequence

Upon completion of the use of the SHA105-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.

4.3.3. Command Completion Polling

After a complete command is sent to the SHA105-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 [I/O Transmission from the SHA105-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.

4.4. I/O Transmission from the SHA105-TFLXAUTH

When the SHA105-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 SHA105-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 SHA105-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/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 SHA105-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 SHA105-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 SHA105-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 ($V_{CC} + 0.5V$)
ESD Ratings:	
Human Body Model (HBM) ESD	>4 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 SHA105-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 $T_A = -40^{\circ}\text{C}$ to $+105^{\circ}\text{C}$, $V_{CC} = +1.65\text{V}$ to $+5.5\text{V}$.

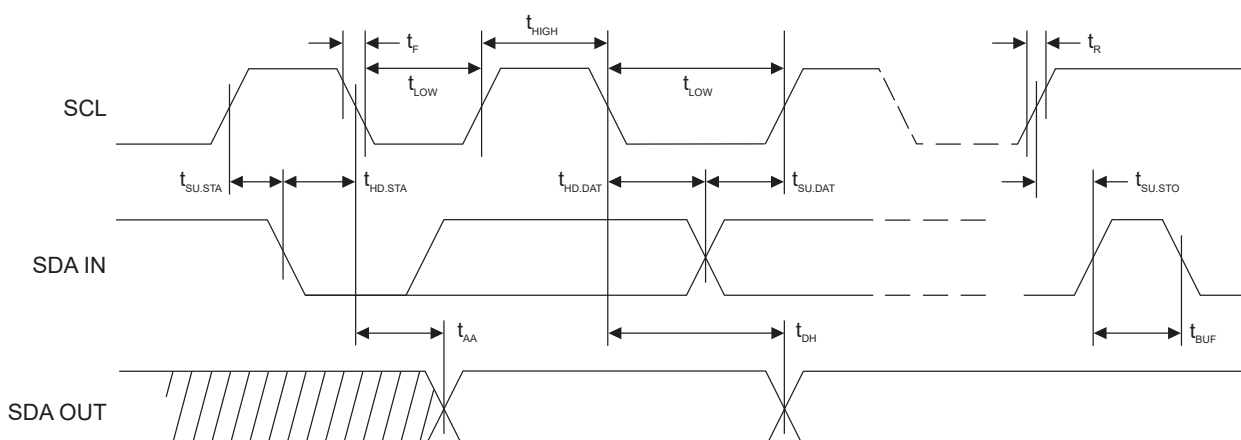
Parameter	Sym.	Direction	Min.	Typ.	Max.	Units	Conditions
Power-up Delay	$t_{PU}^{(1)}$	To SHA105-TFLXAUTH	Clock Divider = 1x	1.0	—	—	ms Minimum time prior to $V_{CC} > V_{CC\text{ min.}}$
			Clock Divider = 2x	1.2	—	—	
			Clock Divider = 4x	1.8	—	—	

Table 5-2. AC Parameters: All I/O Interfaces (continued)

Parameter	Sym.	Direction	Min.	Typ.	Max.	Units	Conditions
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.

Note:

- These parameters are ensured through characterization but not production tested.

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 $T_A = -40^{\circ}\text{C}$ to $+105^{\circ}\text{C}$, $V_{CC} = +1.65\text{V}$ to $+5.5\text{V}$, $C_L = 1$ 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:

- Host system must ensure this timing is met.
- AC measurement conditions:
 - R_L (connects between SDA and V_{CC}): 1.2 k Ω (for V_{CC} = +1.65V to +5.5V)
 - Input pulse voltages: $0.3V_{CC}$ to $0.7V_{CC}$ with CMOSEnable = 1
 - Input rise and fall times: ≤ 50 ns
 - Input and output timing reference voltage: $0.5V_{CC}$
- 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.

5.4. DC Parameters**5.4.1. DC Parameters: All I/O Interfaces****Table 5-4.** 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 ⁽⁵⁾	V_{RISE}	—	—	0.1	V/ μ s	—
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 ⁽⁵⁾
Input Low Threshold	V_{IL1}	-0.5	—	$0.3 \cdot V_{CC}$	V	Device is active and CMOSEnable = 1
Input High Threshold	V_{IH1}	$0.7 \cdot V_{CC}$	—	$V_{CC} + 0.5$	V	Device is active and CMOSEnable = 1
Input Low Threshold ⁽¹⁾	V_{IL0}	-0.5	—	0.5	V	Device is active and CMOSEnable = 0
Input High Threshold ⁽¹⁾	V_{IH0}	1.2	—	$V_{CC} + 0.5$	V	Device is active and CMOSEnable = 0
Input Low Threshold in Sleep mode ⁽⁶⁾	V_{ILS}	-0.5	—	0.5	V	Device is in Sleep mode CMOSen = 0
Input High Threshold in Sleep mode ⁽⁶⁾	V_{IHS}	1.35	—	$V_{CC} + 0.5$	V	Device is in Sleep mode CMOSen = 0
Input Leakage (I ² C Signals)	I_{IN}	-200	—	200	nA	$V_{IN} = V_{CC}$ or GND
Sleep Current ⁽²⁾	I_{SLEEP}	—	130	325 ⁽⁵⁾	nA	When the device is in Sleep mode, $V_{CC} \leq 3.6V$, I/O at either GND or V_{CC} $T_A \leq +55^\circ C$
		—	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	μ A	Waiting for I/O

Table 5-4. DC Parameters on All I/O Interfaces with V_{CC} Power Applied (continued)

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Current Consumption in Computation Mode	$I_{COMPUTE}^{(3)}$	—	—	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	$I_{WRITE}^{(4)}$	—	0.6	1.5	mA	Current when writing to EEPROM -5°C to +105°C
EEPROM Write Current	$I_{WRITE}^{(4)}$	—	0.6	4.0	mA	Current when writing to EEPROM full temperature range
Theta JA	θ_{JA}	—	99.1	—	°C/W	8-lead SOIC
		—	89.5	—	°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. 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.
3. Applies to all commands where an EEPROM write does not occur.
4. Applies to all commands where an EEPROM write occurs. This includes `Write`, `Lock`, `GenKey`, `Counter(Increment)`.
5. This condition is characterized but not production tested.
6. When coming out of Sleep mode when $CMOSen=0$, the initial input thresholds are V_{ILS}/V_{IHS} . When the device is awake, the thresholds will transition to V_{ILO}/V_{IHO} .

6. Command Descriptions

6.1. CheckMac Command

The `CheckMac` command calculates a MAC response that was generated on a SHA104, SHA106, ATECC608x, ATECC508A, ATECC108A, ATSHA204A or ATSHA206A CryptoAuthentication device and compares the result to the `ClientResp` value. It returns a Boolean result to indicate the success or failure of the comparison. An optional MAC may be appended to the response for enhanced security.

If the optional MAC is included in the output response, then this value must be checked by the host micro for validity. The host micro must calculate the value of the MAC and compare it against the value output by the `CheckMac` command.

6.2. 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 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

[Monotonic Counter](#)

6.3. 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.

6.4. GenDivKey Command

The `GenDivKey` command is used to generate the diversified key that is equivalent to the one programmed into the SHA104 or other client-side device. The command is similar to the `GenDig` command of other CryptoAuthentication devices but is much more limited in scope.

This command only makes sense to run when using a system with diversified keys. Upon completion, the value of the client side diversified key will be loaded into `TempKey` for use by the `CheckMac` command.

Related Links

[Nonce Command](#)

6.5. 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 <code>Delete</code> 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[Lock Command](#)

6.6. 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.

6.7. Nonce Command

The **Nonce** command has multiple purposes. The **Nonce** command can output a random number for use by the system, input a fixed value to be used by other commands or generate a random value for use by other commands.

Related Links[Random Number Generator \(RNG\)](#)

6.8. 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 slots 0 and 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.

6.9. SelfTest Command

The **SelfTest** command performs on-demand testing of one or more of the cryptographic algorithms implemented in the SHA105-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[Random Number Generator \(RNG\)](#)

6.10. 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 SHA105-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.

6.11. 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. The I/O Protection key in slot 0 and 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

[EEPROM Configuration Zone](#)

7. Application Information

The SHA105-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 SHA105-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 SHA105-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 SHA105-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 SHA105-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 SHA105-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 SHA105-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.

EV89U05A – CryptoAuthentication™ Pro Trust Platform

The CryptoAuth Pro Trust Platform kit extends the CryptoAuth Trust Platform with a more powerful Cortex M4 microcontroller, four on-board CryptoAuthentication devices, two mikroBUS™ sockets, and an on-board 10/100 Mbit Ethernet PHY. The board also contains the Microchip Technology PKoB4 debugger, which is compatible with MPLAB® X IDE. The application microcontroller has been configured to readily make use of many of the features provided on the board.

Similar to the DM320118, additional CryptoAuthentication and CryptoAutomotive™ devices can be used with the board through the mikroBUS header. Additionally, two user-programmable switches and LEDs are provided to aid in the development of demonstrations and applications.

EV97M19A – SHA104/SHA105 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 I²C and SWI devices mounted and a SHA105 I²C 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.

Secure UDFN(SOIC) Click Boards SOIC

The SECURE-UDFN-CLICK and SECURE-SOIC-CLICK are generic CryptoAuthentication socket kits that can be used with any microcontroller development board with a mikroBUS interface. These kits have been developed by MikroElektronika and are available through their website. SHA105-TFLXAUTH samples for use with these boards will need to be obtained separately as they are not included in the kits.

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 SHA105-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 SHA105-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 SHA105-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

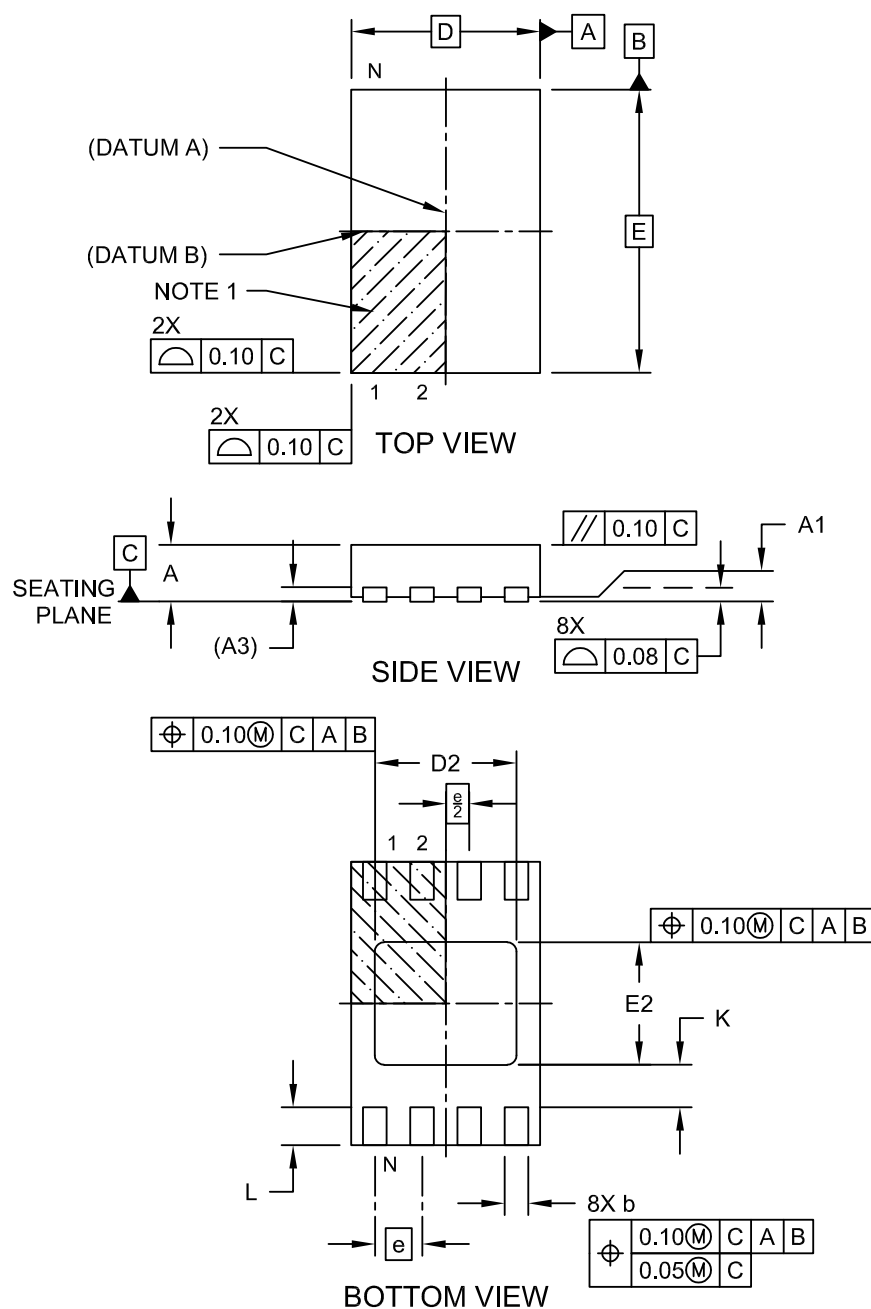
As part of Microchip's overall security features, the part marking for all crypto devices is intentionally vague. The marking on the top of the package does not provide any information as to the actual device type or the manufacturer of the device. The alphanumeric code on the package provides manufacturing 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

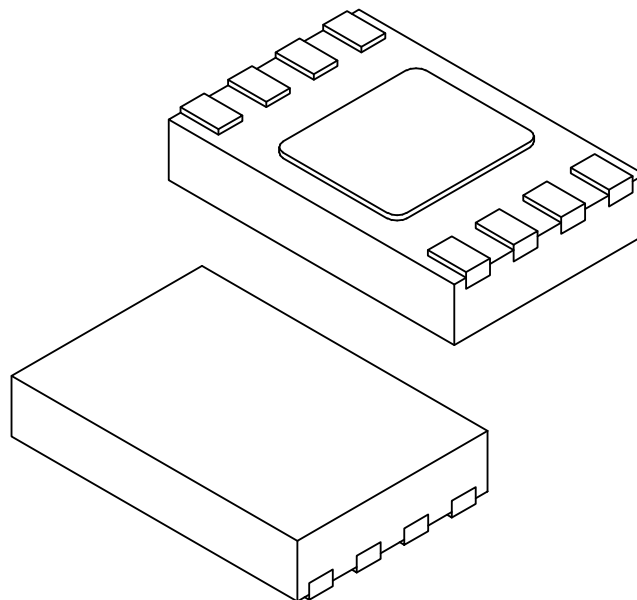
Note: For the most current package drawings, please see the Microchip Packaging Specification located at <http://www.microchip.com/packaging>



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

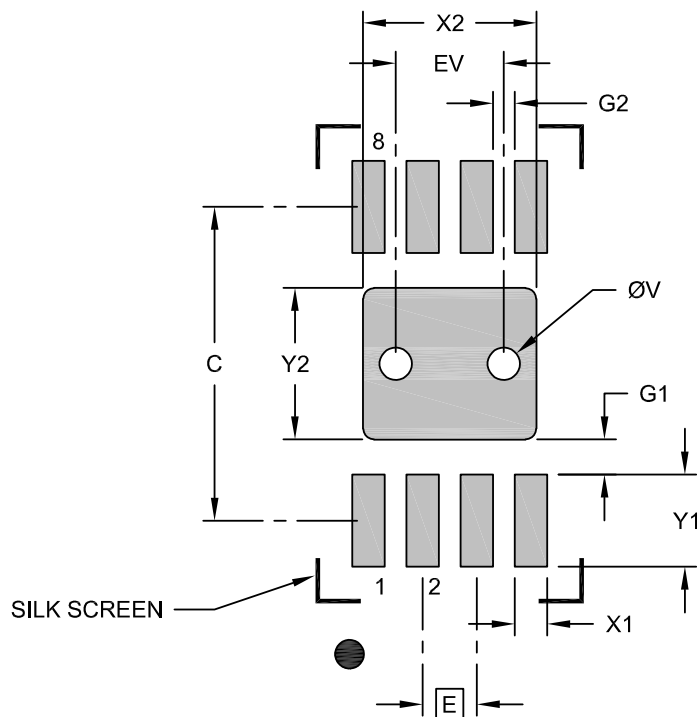
BSC: Basic Dimension. Theoretically exact value shown without tolerances.

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:

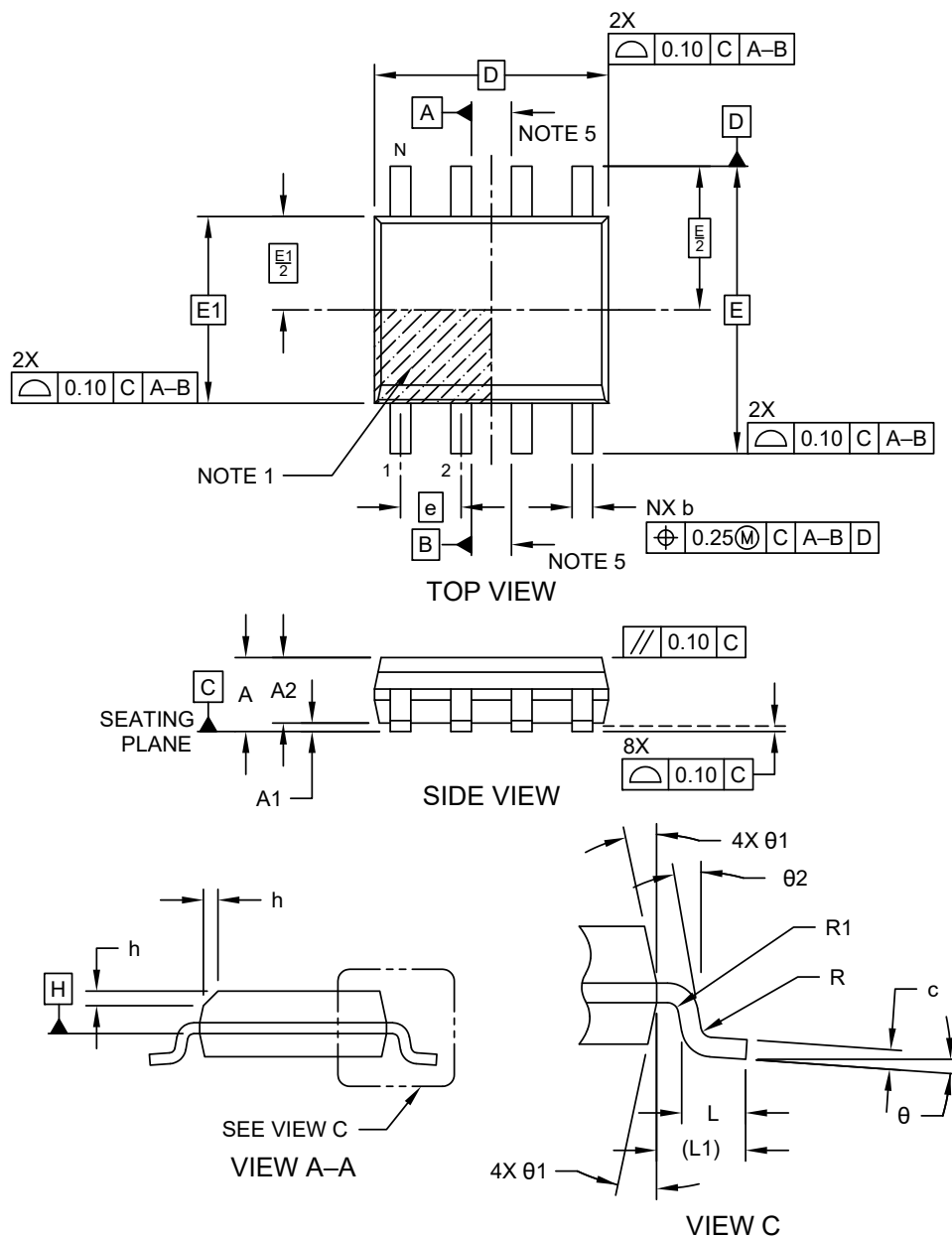
- Dimensioning and tolerancing per ASME Y14.5M
BSC: Basic Dimension. Theoretically exact value shown without tolerances.
- For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

Microchip Technology Drawing C04-23355-Q4B Rev C

9.2. 8-Lead SOIC

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

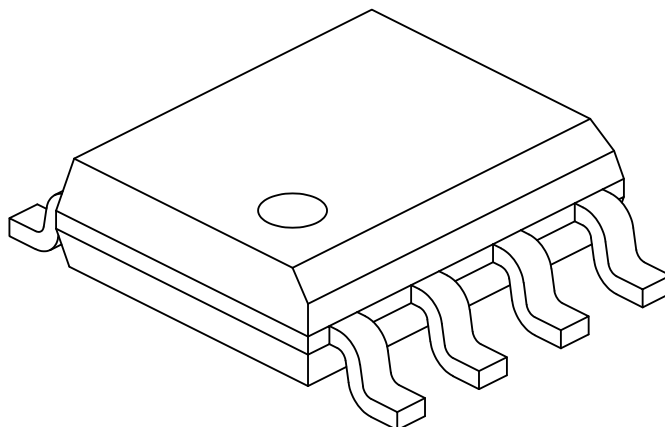
Note: For the most current package drawings, please see the Microchip Packaging Specification located at <http://www.microchip.com/packaging>



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°	–	–

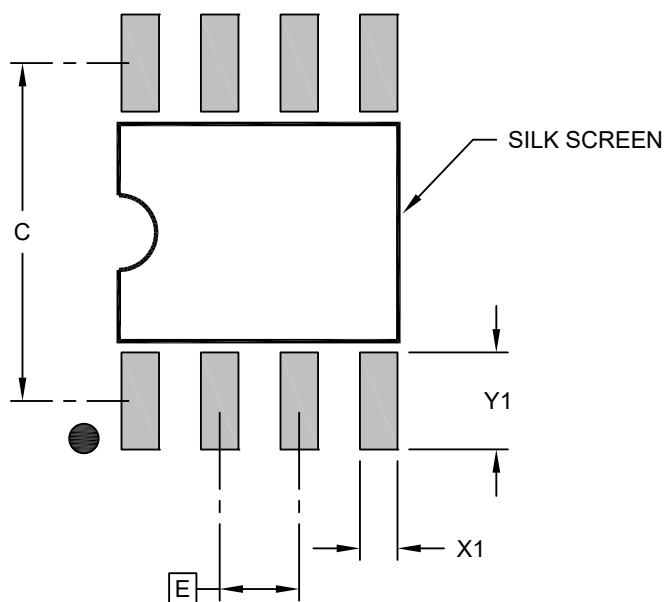
Notes:

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

Microchip Technology Drawing No. C04-057-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

10. Revision History SHA105

Revision B (June 2025)

NOTICE

No changes have been made to the actual silicon. Changes are only to the data sheet.

- **Features:**
 - Added NIST certified information to TRNG bullet.
 - Corrected UDFN package dimension.
- **Symmetric Keys:** Added information on diversified keys.
- **Random Number Generator (RNG):** Added specification information. Added ESV information.
- **DC Parameters: All I/O Interfaces:**
 - Added input thresholds when in Sleep mode (V_{ILS} , V_{IHS}).
 - Updated Theta J_A values.
- **Nonce Command:** Removed session key information.
- **Hardware Tools:** Added CryptoAuth Pro Trust Platform board and MikroElektronica Secure UDFN/SOIC Click boards.
- **Product Identification System:** Product Identification now separate section and not part of Back Matter.
- **Microchip Information:** Back Matter simplified per Microchip's new standard.

Revision A (July 2023)

- Initial data sheet release.

11. 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
xxxxx - tttt vvvv p

Part No	SHA105: 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⁾	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)

Examples:

- SHA105-TFLXAUTHS: 8-Lead (0.150" Wide Body), Plastic Gull Wing Small Outline (JEDEC® SOIC), I²C, MOQ 2k units
- SHA105-TFLXAUTHU: 8-Pad 2 mm x 3 mm x 0.6 mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat No Lead Package (UDFN), I²C, MOQ 2k units

Note:

1. Product will be delivered as Tape and Reel. Actual size of reel will vary based on customer order. The minimum order quantity (MOQ) allowed is 2k units.

Microchip Information

Trademarks

The “Microchip” name and logo, the “M” logo, and other names, logos, and brands are registered and unregistered trademarks of Microchip Technology Incorporated or its affiliates and/or subsidiaries in the United States and/or other countries (“Microchip Trademarks”). Information regarding Microchip Trademarks can be found at <https://www.microchip.com/en-us/about/legal-information/microchip-trademarks>.

ISBN: 979-8-3371-1196-4

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.

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 products are 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.

Product Page Links

[SHA105](#)