This is a summary document. A complete document is available under NDA. For more information, please contact your local Microchip sales office.

SHA105 CryptoAuthentication™ Summary Data Sheet

SHA105

www.microchip.com Product Pages: SHA105

Introduction

The SHA105 is a member of the Microchip Technology Inc. CryptoAuthentication™ product family. The device provides 128 bits of symmetric security targeted for disposable and ecosystem control applications and is intended to be used as a companion device and is microcontroller/microprocessor agnostic. The device is intended for use on the host side of symmetric authentication use cases and can provide secure key storage along with the ability to validate the MAC operation on an accessory/disposable security device through the use of a CheckMAC operation.

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 Random Number Generator (RNG). (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℃
- Monotonic Counter with Max Count Value of 10,000
- Unique 72-Bit Serial Number
- 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: >4 kV;
- Packaging Options: 8-Pad UDFN (2 mm x 3 mm), 8-Lead SOIC

Use Cases

Host side authentication support for:

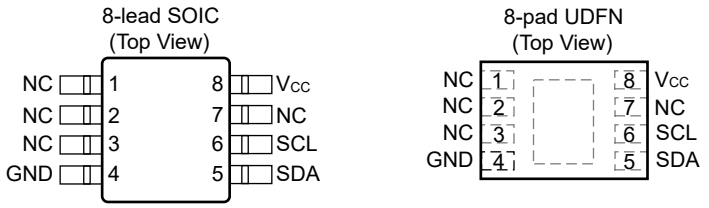
- Disposables and accessory authentication
- Ecosystem control
- Anti-cloning

Pin Configuration and Pinouts

Table 1. Pin Configuration

Package = 8-Pad SOIC or 8-Lead UDFN		
Pin #	**Function**	**I²C**
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

1. Overview

1.1 Use Cases

SHA105 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 has a command set that allows for its usage in multiple symmetric key applications where a host side device is required. The SHA105 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 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 I^2C interface at speeds of up to 400 KHz. The interface is compatible with standard-mode and fast-mode I^2C interface specifications.

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

2.1 Cryptographic Standards

SHA105 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.

2.1.1 SHA-256

The SHA105 computes the SHA-256 digest based on the algorithm documented here:

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

2.2 Security Features

2.2.1 Physical Security

The SHA105 incorporates a number of physical security features designed to protect the EEPROM contents from unauthorized exposure.

2.2.2 Random Number Generator (RNG)

The SHA105 device includes a high-quality cryptographic RNG implemented according to the NIST standards SP800-90A/B/C.

3. Electrical Characteristics

3.1 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.

3.2 Reliability

The SHA105 is fabricated with Microchip’s high-reliability CMOS EEPROM manufacturing technology.

Table 3-1. 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.

3.3 DC Parameters

3.3.1 DC Parameters: All I/O Interfaces

Table 3-2. 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[3]	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[3]
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

Table 3-2. DC Parameters on All I/O Interfaces with V_{CC} Power Applied (continued)

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
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[4]	V_{ILS}	-0.5	—	0.5	V	Device is in Sleep mode CMOSen= 0
Input High Threshold in Sleep mode[4]	V_{IHS}	1.35	—	V_{CC}+0.5	V	Device is in Sleep mode CMOSen= 0
Input Leakage (I^2C Signals)	I_{IN}	-200	—	200	nA	V_{IN} = V_{CC} or GND
Sleep Current[2]	I_{SLEEP}	—	130	325[3]	nA	When the device is in Sleep mode, V_{CC} ≤ 3.6V, I/O at either GND or V_{CC} T_A ≤ +55°C
		—	130	500	nA	V_{CC} ≤ 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
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. This condition is characterized but not production tested.
4. 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_{IL0}/ V_{IH0}.

4. SHA105 Trust Platform Variants and Provisioning Services

Microchip offers secure provisioning services for the SHA105 through the Trust Platform. It leverages the Trust Platform Design Suite set of tools (TPDS) and currently offers three provisioning flows:

- Trust&GO: Pre-configured and pre-provisioned Secure Elements for fix-function Use Cases
- TrustFLEX: Pre-configured and provisioned Secure Element with customer-unique credentials
- TrustCUSTOM: Fully customizable Secure Element including configuration and provisioning with customer-unique credentials

The Trust&GO flow provides pre-configured and pre-provisioned secure elements. These products are defined to meet common use case applications for customers that do not require unique credentials. These devices are provided as is and can be ordered directly from Microchip as easily as any standard product.

The TrustFLEX flow leverages the TrustFLEX configurator to input unique customer credentials into a pre-defined configuration and generate a Secure Exchange Package. This package is, then, deployed via the Microchip Secure Provisioning System to enable device ordering. Then, only the customer designated in the Secure Exchange Package can order these devices.

The TrustCUSTOM flow leverages the TrustCUSTOM configurator and provides the ability to fully configure the SHA105 device to meet the security requirements for a given application. At the end of the process, a Secure Exchange Package that is deployed to the Microchip Secure Provisioning System is generated. Then, only the customer designated in the Secure Exchange Package can order these devices.

Important: Microchip's test sites, that provide secure provisioning services, are equipped with Hardware Security Modules (HSMs) to ensure the security of customer data throughout the provisioning process.

SHA105 Trust Platform Products

Trust Platform products are currently in development for the SHA105. Both TrustFLEX and TrustCUSTOM versions will be available.

Table 4-1. SHA105 Trust Platform Ordering Codes[1]

Trust Platform Type	Production Ordering Code	Package Type	Temperature Range
TrustFLEX[2]	SHA105-TFLXAUTHU	8-pad UDFN	Standard Industrial. -40℃ to +105℃
	SHA105-TFLXAUTHS	8-pin SOIC	Standard Industrial. -40℃ to +105℃
TrustCUSTOM[3]	SHA105-TCSMU	8-pad UDFN	Standard Industrial. -40℃ to +105℃
	SHA105-TCSMS	8-pin SOIC	Standard Industrial. -40℃ to +105℃

Notes:

1. This table is a representative sample of Trust Platform Devices. Please refer to each Trust Platform Type for a more complete list.
2. For a complete list of ordering codes including sample devices, see the respective data sheets.
3. TrustCUSTOM sample devices correspond to the standard generic SHA105 devices. SHA105-TCSMU/SHA105-TCSMS is equivalent to SHA105-MAHDA/SHA105-SSHDA, respectively.

5. Package Marking Information

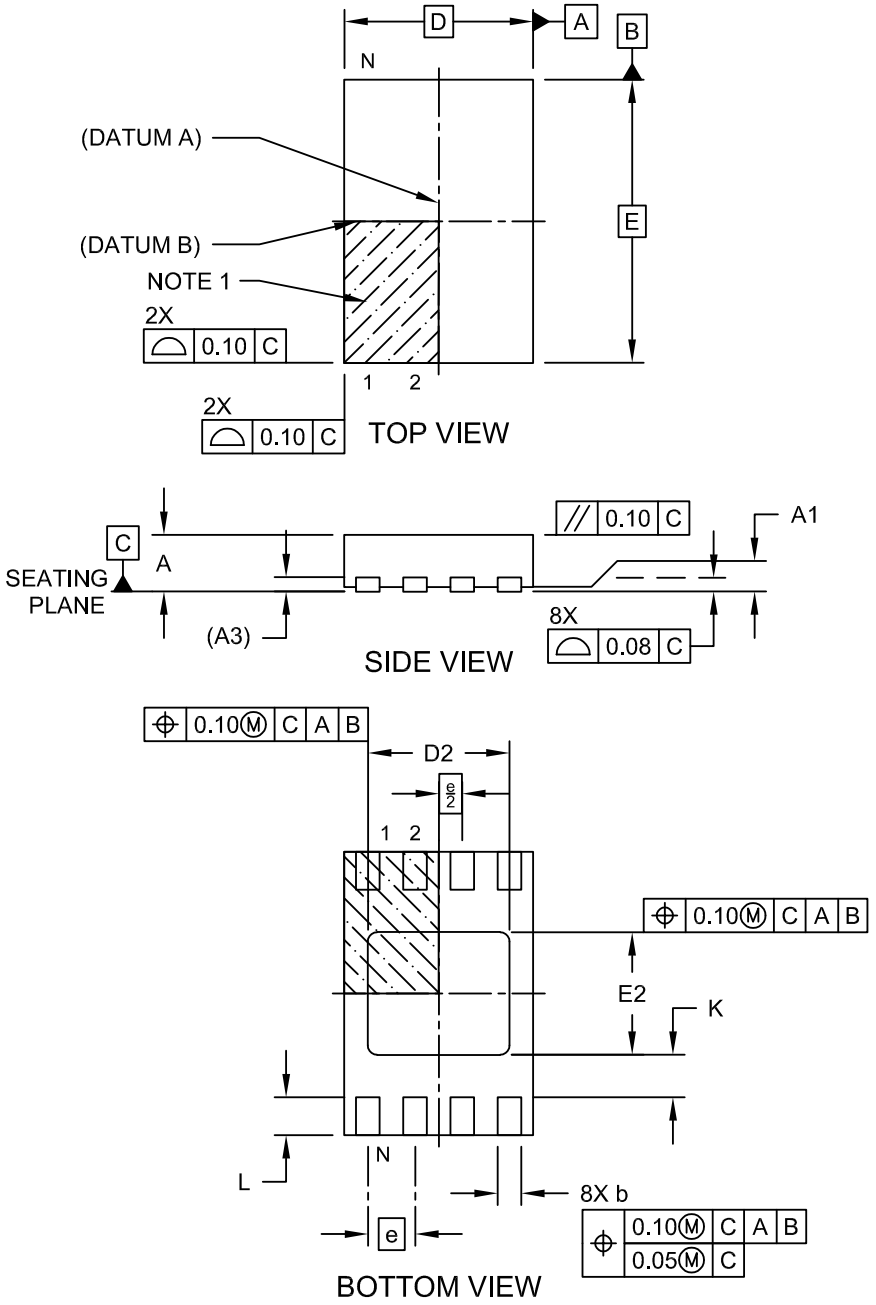
As part of Microchip's overall security features, the part marking for all crypto devices is intentionally vague. The marking on the top of the package does not provide any information as to the actual device type or the manufacturer of the device. The alphanumeric code on the package provides manufacturing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

6. Package Drawings

6.1 8-Pad UDFN

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

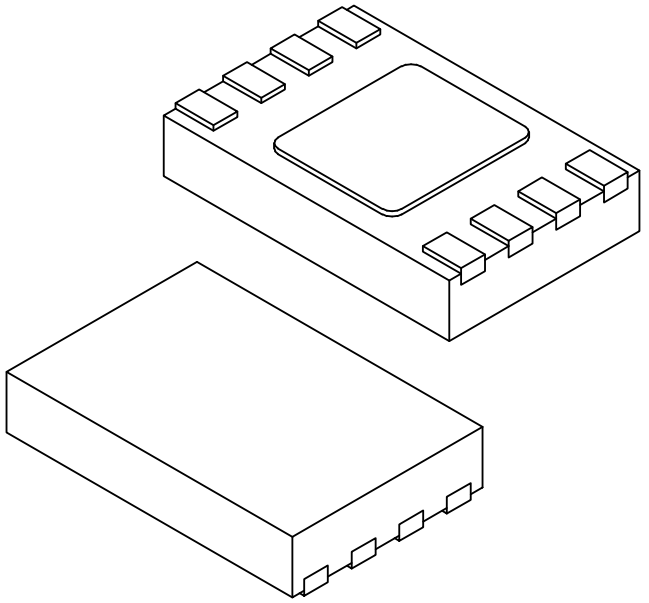
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



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:

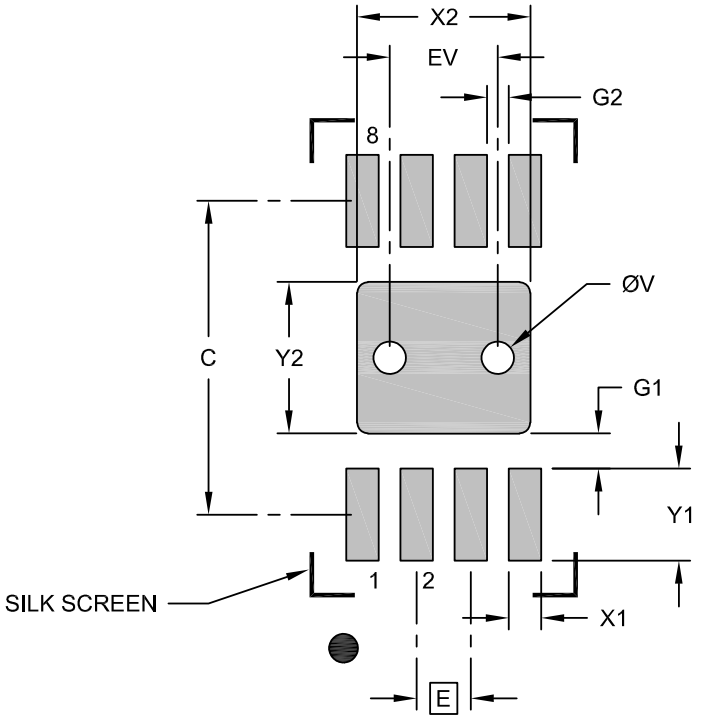
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M

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:

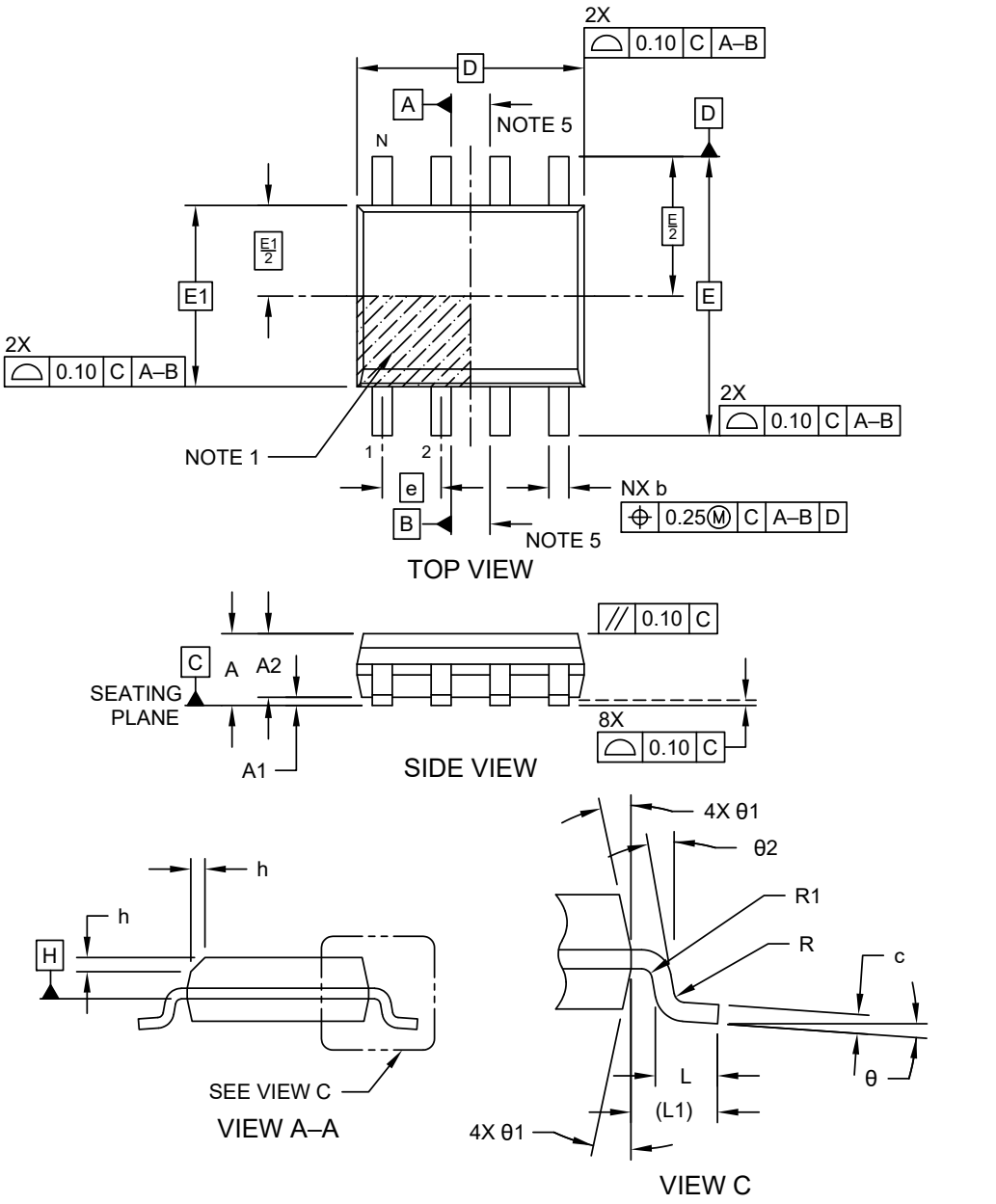
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
2. For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

Microchip Technology Drawing C04-23355-Q4B Rev C

6.2 8-Lead SOIC

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

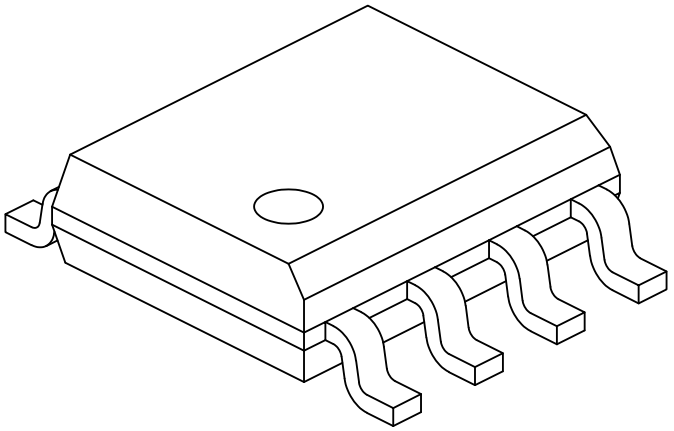
Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



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

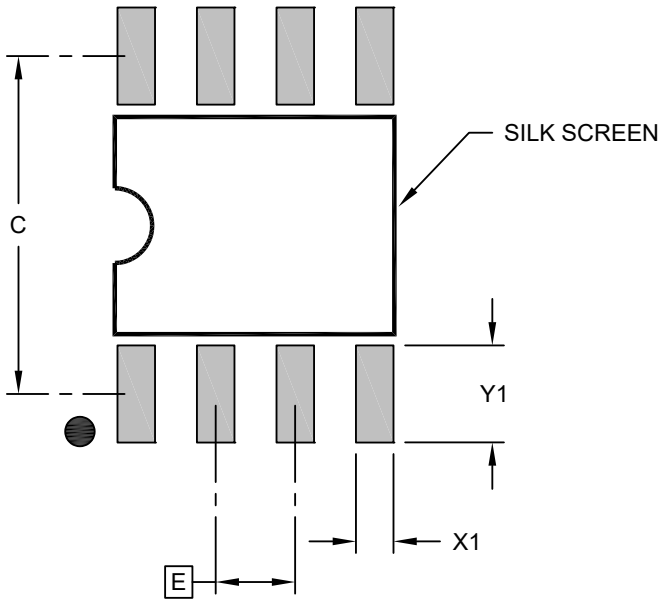
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

   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

7. 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.	-XX	X	XX	-X
Device	Package	Temp Range	I/O Type	Tape and Reel

Device:	SHA105: Cryptographic Co-processor with Secure Hardware-based Key Storage	
Package Options	SS	8-Lead (0.150” Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC)
	MA	8-Pad 2 x 3 x 0.6 mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat NoLead Package (UDFN)
Temperature Option	V	Extended Industrial Temperature Range. -40℃ to 105℃
I/O Type	DA	I^2C Interface
Tape and Reel Options	T	Tape and Reel (Size varies by package type)

Examples:

- SHA105-SSVDA-T: 8-Lead (0.150” Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC), I^2C, Tape and Reel, 3,300 per Reel
- SHA105-MAVDA-T: 8-Pad 2 x 3 x 0.6 mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat NoLead Package (UDFN), IC, Tape and Reel, 5,000 per Reel

Notes:

1. Tape and Reel identifier only appears in the catalog part number description. This identifier is used for ordering purposes and is not printed on the device package. Check with your Microchip Sales Office for package availability with the Tape and Reel option.
2. Small form-factor packaging options may be available. Please check www.microchip.com/packaging for small-form factor package availability, or contact your local Sales Office.
3. For customers that have interest in a SWI version of this device please contact Microchip Sales to determine availability.

8. Revision History SHA105

Revision B (April 2025)

NOTICE No changes were made to the actual silicon. Changes are only to the data sheet.

- Features
  - Corrected UDFN package dimension
  - Added (NIST Certified) to random number generator bullet.
- DC Parameters: All I/O Interfaces
  - Added input thresholds when in Sleep Mode (V_{ILS}, V_{IHS})
  - Updated Theta-JA values for SOIC and UDFN packages
- 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 (March 2023)

- Initial data sheet release

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: 979-8-3371-0733-2

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.