



# SHA104

---

---

## SHA104 CryptoAuthentication™ Summary Data Sheet

---

---

### Introduction

---

The SHA104 is a member of the Microchip Technology Inc. CryptoAuthentication™ product family used in accessory or disposable applications. The device provides 128 bits of symmetric security targeted for disposable and ecosystem control applications, is intended to be used as a companion device and is microcontroller/microprocessor agnostic. The device can be used in systems where either the host can assist in the authentication through the use 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 can be used in conjunction with the SHA105 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°C
- 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<sup>2</sup>C interface
- Voltage Supply Range: 1.65V to 5.5V
- 130 nA Nominal Sleep Current
- Human Body Model (HBM) ESD: I<sup>2</sup>C 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

---

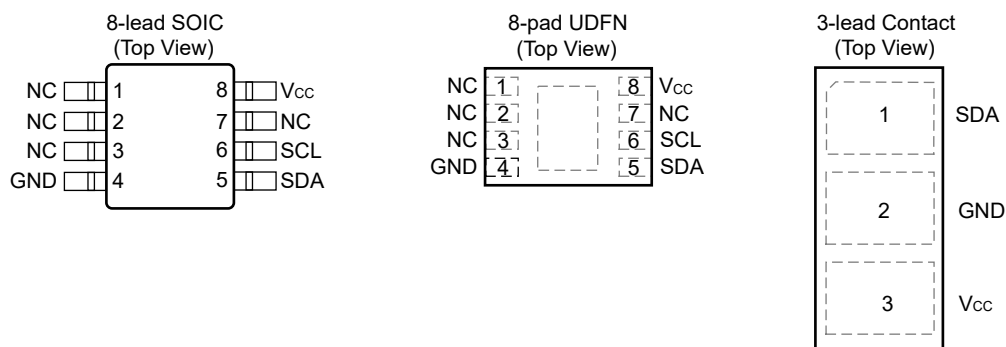
- Disposables and accessory authentication
- Ecosystem control
- Anti-cloning

## Pin Configuration and Pinouts

Table 1. Pin Configuration

Package = 8-PAD SOIC or 8-Lead UDFN				Package = 3-Lead Contact		
Pin #	Function	I <sup>2</sup> C	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	Serial I/O	SDA	SI/O	3	Supply	VCC
6	Serial Clock	SCL	NC	—	—	—
8	Supply	VCC	VCC	—	—	—

Figure 1. Pinouts<sup>(1)</sup>



**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. Security Information.....	6
2.1. Cryptographic Standards.....	6
2.1.1. SHA-256.....	6
2.2. Key Uses and Restrictions.....	6
2.2.1. Symmetric Keys.....	6
2.2.2. Monotonic Counter.....	6
2.2.3. Transport Keys.....	6
2.3. Security Features.....	6
2.3.1. Physical Security.....	6
2.3.2. Random Number Generator (RNG).....	6
3. Electrical Characteristics.....	7
3.1. Absolute Maximum Ratings.....	7
3.2. Reliability.....	7
3.3. DC Parameters.....	7
3.3.1. DC Parameters: All I/O Interfaces.....	7
3.3.2. DC Parameters: Single-Wire Interface.....	8
3.3.3. DC Parameters: Single-Wire Interface – Parasitic Power Mode.....	9
4. SHA104 Trust Platform Variants and Provisioning Services.....	10
5. Package Marking Information.....	11
6. Package Drawings.....	12
6.1. 8-Pad UDFN.....	12
6.2. 8-Lead SOIC.....	15
6.3. 3-Lead Contact.....	18
7. Revision History SHA104.....	20
Microchip Information.....	21
The Microchip Website.....	21
Product Change Notification Service.....	21
Customer Support.....	21
Product Identification System.....	22
Microchip Devices Code Protection Feature.....	22
Legal Notice.....	23

Trademarks..... 23  
Quality Management System..... 24  
Worldwide Sales and Service.....25

## 1. Overview

### 1.1 Use Cases

SHA104 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 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.
- **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 will be used on the accessory/disposable side of an application and the SHA105 will be used on the host side of that application.

### 1.2 Device Features

SHA104 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<sup>2</sup>C version of the device supports a standard I<sup>2</sup>C interface at speeds of up to 400 KHz. The interface is compatible with standard-mode and fast-mode I<sup>2</sup>C 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 unit ships with a unique 72-bit serial number. Also, SHA104 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 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. Security Information

### 2.1 Cryptographic Standards

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

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

### 2.2 Key Uses and Restrictions

#### 2.2.1 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.

#### 2.2.2 Monotonic Counter

SHA104 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.

#### 2.2.3 Transport Keys

The SHA104 includes an internal hardware set of keys that is used for secure personalization (i.e., transport keys). The values of the hardware keys are kept secret and are made available only to qualified customers upon request to Microchip. Microchip also offers secure personalization services through the Trust Platform provisioning services. Contact your local Microchip Sales Office for more information on such services.

### 2.3 Security Features

#### 2.3.1 Physical Security

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

#### 2.3.2 Random Number Generator (RNG)

The SHA104 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 <sub>CC</sub> + 0.5V)	-0.5V to (V <sub>CC</sub> + 0.5V)
<b>ESD Ratings:</b>	
Human Body Model (HBM) ESD I <sup>2</sup> C 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.

#### 3.2 Reliability

The SHA104 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:**

- 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<sub>CC</sub> Power Applied**

Unless otherwise indicated, these values are applicable over the specified operating range from T<sub>A</sub> = -40°C to +105°C, V<sub>CC</sub> = +1.65V to +5.5V.

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Ambient Operating Temperature	T <sub>A</sub>	-40	—	+105	°C	—
V <sub>CC</sub> Ramp Rate <sup>(4)</sup>	V <sub>RISE</sub>	—	—	0.1	V/μs	—

.....continued						
Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Output Low Voltage	V <sub>OL</sub>	—	—	0.4	V	When the device is in Active mode, V <sub>CC</sub> = 1.65V to 3.6V for output-low current = 4.0 mA
		—	—	0.4	V	V <sub>CC</sub> > 3.6V = 10.0 mA <sup>(4)</sup>
Input Low Threshold	V <sub>IL1</sub>	-0.5	—	0.3*V <sub>CC</sub>	V	Device is active and CMOSEnable = 1
Input High Threshold	V <sub>IH1</sub>	0.7*V <sub>CC</sub>	—	V <sub>CC</sub> +0.5	V	Device is active and CMOSEnable = 1
Input Low Threshold <sup>(1, 2)</sup>	V <sub>IL0</sub>	-0.5	—	0.5	V	Device is active and CMOSEnable = 0
Input High Threshold <sup>(1, 2)</sup>	V <sub>IH0</sub>	1.2	—	V <sub>CC</sub> +0.5	V	Device is active and CMOSEnable = 0
Input Leakage (I <sup>2</sup> C Signals)	I <sub>IN</sub>	-200	—	200	nA	V <sub>IN</sub> = V <sub>CC</sub> or GND
Sleep Current <sup>(3)</sup>	I <sub>SLEEP</sub>	—	130	325 <sup>(4)</sup>	nA	When the device is in Sleep mode, V <sub>CC</sub> ≤ 3.6V, I/O at either GND or V <sub>CC</sub> T <sub>A</sub> ≤ +55°C
		—	130	500	nA	V <sub>CC</sub> ≤ 3.6V, I/O at either GND or V <sub>CC</sub> Full temperature Range
		—	130	1000	nA	When the device is in Sleep mode Over full V <sub>CC</sub> and temperature range
Current Consumption in I/O Mode	I <sub>I/O</sub>	—	60	250	μA	Waiting for I/O
Theta JA	Θ <sub>JA</sub>	—	166	—	°C/W	8-lead SOIC
		—	173	—	°C/W	8-pad UDFN
		—	146	—	°C/W	3-lead Contact

**Notes:**

1. CMOSen = 0 must only be used when V<sub>CC</sub> 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<sub>IL</sub> and V<sub>IH</sub> levels are independent of the external V<sub>CC</sub> 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<sub>CC</sub> or allowed to be pulled up to V<sub>CC</sub> by the pull-up resistors on the signal lines.
4. This condition is characterized but not production tested.

### 3.3.2 DC Parameters: Single-Wire Interface

**Table 3-3. DC Parameters on Single-Wire Interface<sup>(1)</sup>**

Unless otherwise indicated, these values are applicable over the specified operating range from T<sub>A</sub> = -40°C to +105°C, V<sub>CC</sub> = +1.65V to +5.5V.

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Power Supply Voltage	V <sub>CC</sub>	1.65V	—	5.5V	V	—



.....continued

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Output Low Voltage	V <sub>OL</sub>	—	—	0.4	V	When the device is in Active mode, V <sub>CC</sub> = 1.65V to 3.6V for output-low current = 8.0 mA
		—	—	0.4	V	V <sub>CC</sub> > 3.6V 16.0 mA <sup>(3)</sup>
Input High Leakage	I <sub>IH</sub>	—	1.0	2.0	µA	V <sub>IN</sub> = V <sub>CC</sub>
Input Low Leakage	I <sub>IL</sub>	-200	—	200	nA	V <sub>IN</sub> = GND
Bus Capacitance	C <sub>BUS</sub>	—	—	500	pF	—

**Notes:**

1. All specifications not shown can be found in the All I/O Interfaces [Table 3-2](#).
2. The Single-Wire voltage must never be greater than V<sub>CC</sub>.
3. This condition is characterized but not production tested.
4. Operation over the C<sub>BUS</sub> range is ensured by design and is not production tested.

### 3.3.3 DC Parameters: Single-Wire Interface – Parasitic Power Mode

**Table 3-4. DC Parameters on Parasitic Single-Wire Interface**

Unless otherwise indicated, these values are applicable over the specified operating range from T<sub>A</sub> = -40°C to +105°C, CMOSen = '1'

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

**Notes:**

1. All specifications not shown can be found in the All I/O Interfaces [Table 3-2](#).
2. Single-Wire voltage (V<sub>PUP</sub>) must never be greater than the maximum V<sub>PUP</sub> operating voltage.
3. For the lowest system current, the SI/O signal must be driven to V<sub>PUP</sub> 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<sub>BUS</sub> range is ensured by design and is not production tested.

## 4. SHA104 Trust Platform Variants and Provisioning Services

Microchip offers secure provisioning services for the SHA104 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 SHA104 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.

### SHA104 Trust Platform Products

Trust Platform products are currently in development for the SHA104. Both TrustFLEX and TrustCUSTOM versions will be available.

**Table 4-1. SHA104 Trust Platform Ordering Codes<sup>(1)</sup>**

Trust Platform Type	Production Ordering Code	Package Type	Temperature Range
TrustFLEX <sup>(2)</sup>	SHA104-TFLXAUTHU	8-pad UDFN	Standard Industrial. -40°C to +105°C
	SHA104-TFLXAUTHS	8-pin SOIC	Standard Industrial. -40°C to +105°C
TrustCUSTOM <sup>(3)</sup>	SHA104-TCSMU	8-pad UDFN	Standard Industrial. -40°C to +105°C
	SHA104-TCSMS	8-pin SOIC	Standard Industrial. -40°C to +105°C

#### 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 SHA104 devices. SHA104-TCSMU/SHA104-TCSMS is equivalent to SHA104-MAHDA/SHA104-SSHDA, respectively.



**Attention:** For SWI TrustFLEX or TrustCUSTOM variants in a 3-lead contact package, contact Microchip sales to determine availability.

## **5. Package Marking Information**

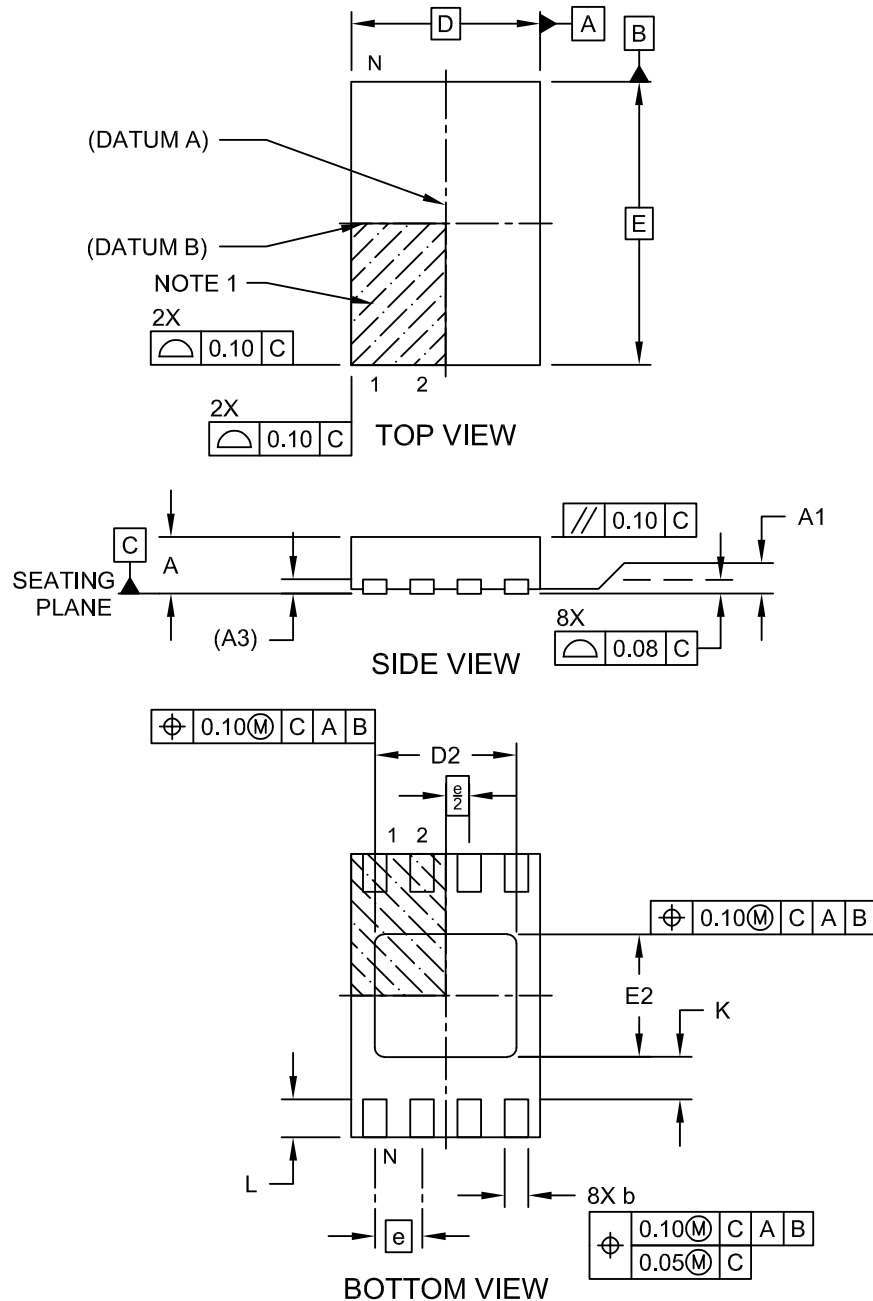
As part of Microchip's overall security features, the part marking for all crypto devices is intentionally vague. The marking on the top of the package does not provide any information as to the actual device type or the manufacturer of the device. The alphanumeric code on the package provides manufacturing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

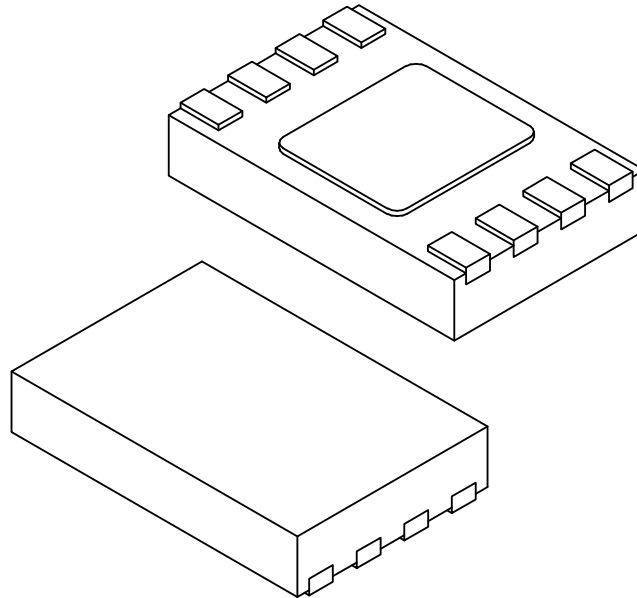
8-Lead Ultra Thin Plastic Dual Flat, No Lead Package (Q4B) - 2x3 mm Body [UDFN]  
Atmel Legacy Global Package Code YNZ

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



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

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



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

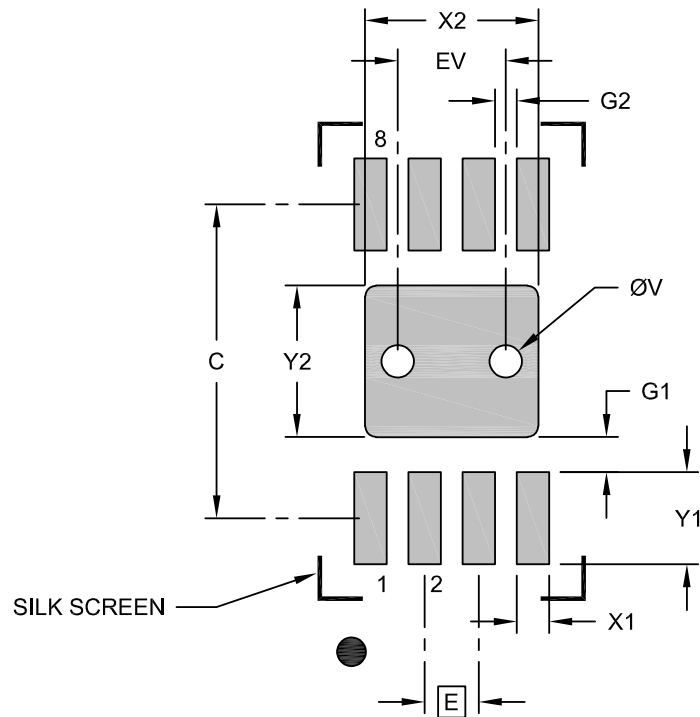
**Notes:**

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M
  - BSC: Basic Dimension. Theoretically exact value shown without tolerances.
  - REF: Reference Dimension, usually without tolerance, for information purposes only.

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

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

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



**RECOMMENDED LAND PATTERN**

Dimension Limits	Units	MILLIMETERS		
		MIN	NOM	MAX
Contact Pitch	E	0,50 BSC		
Optional Center Pad Width	X2			1,60
Optional Center Pad Length	Y2			1,40
Contact Pad Spacing	C		2,90	
Contact Pad Width (X8)	X1			0,30
Contact Pad Length (X8)	Y1			0,85
Contact Pad to Center Pad (X8)	G1	0,33		
Contact Pad to Contact Pad (X6)	G2	0,20		
Thermal Via Diameter	V		0,30	
Thermal Via Pitch	EV		1,00	

**Notes:**

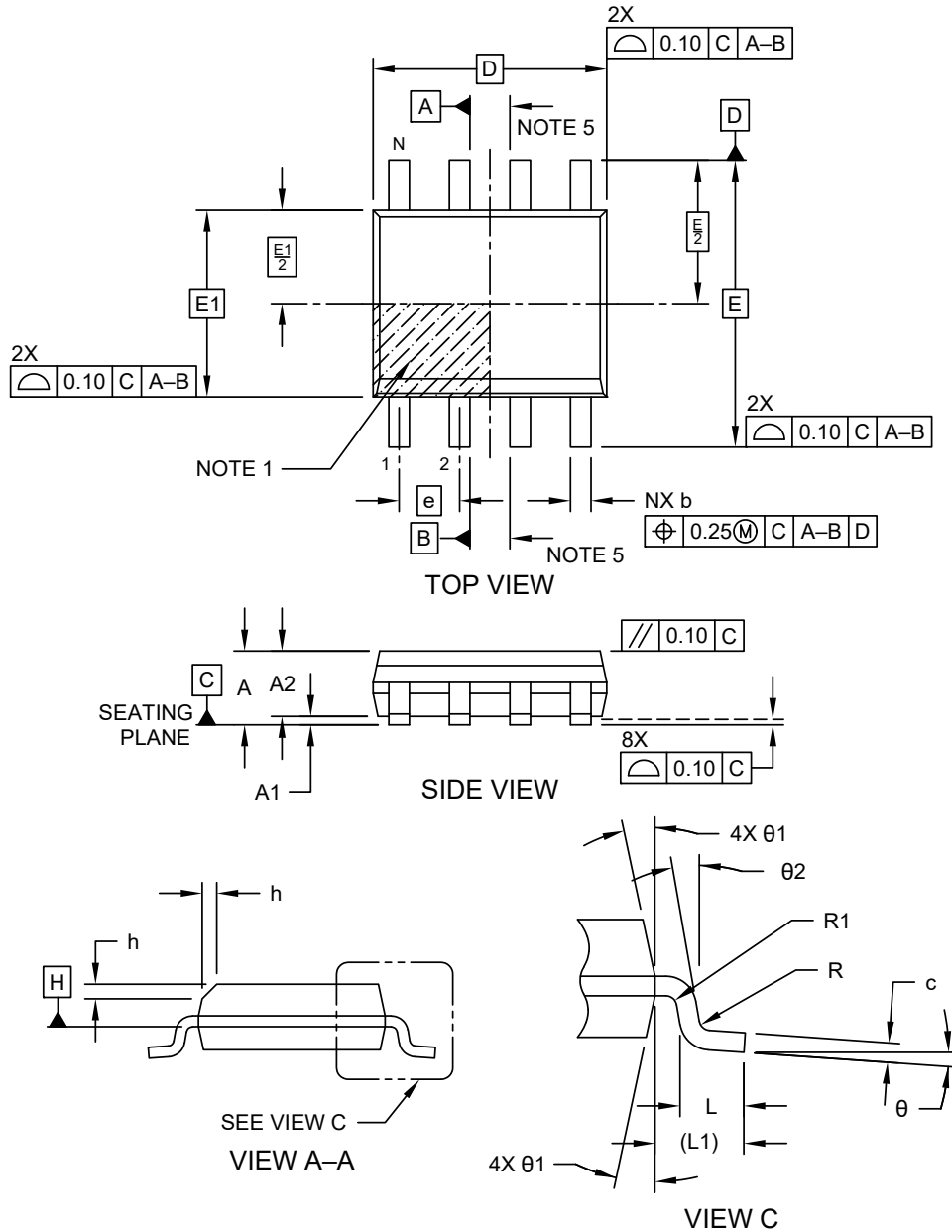
1. Dimensioning and tolerancing per ASME Y14.5M  
BSC: Basic Dimension. Theoretically exact value shown without tolerances.
2. For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

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]

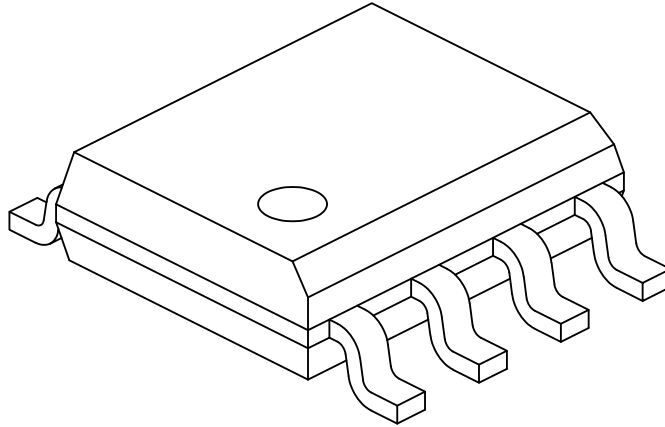
**Note:** For the most current package drawings, please see the Microchip Packaging Specification located at <http://www.microchip.com/packaging>



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>



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

**Notes:**

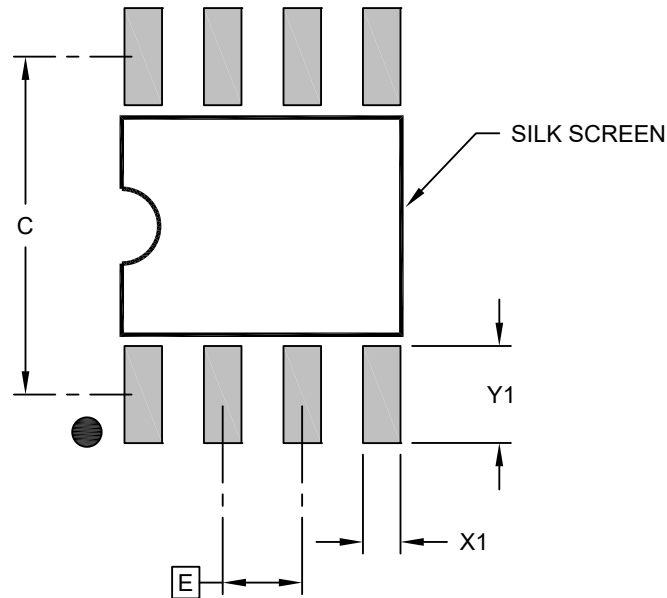
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. § Significant Characteristic
3. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.15mm per side.
4. Dimensioning and tolerancing per ASME Y14.5M
  - BSC: Basic 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

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

**Notes:**

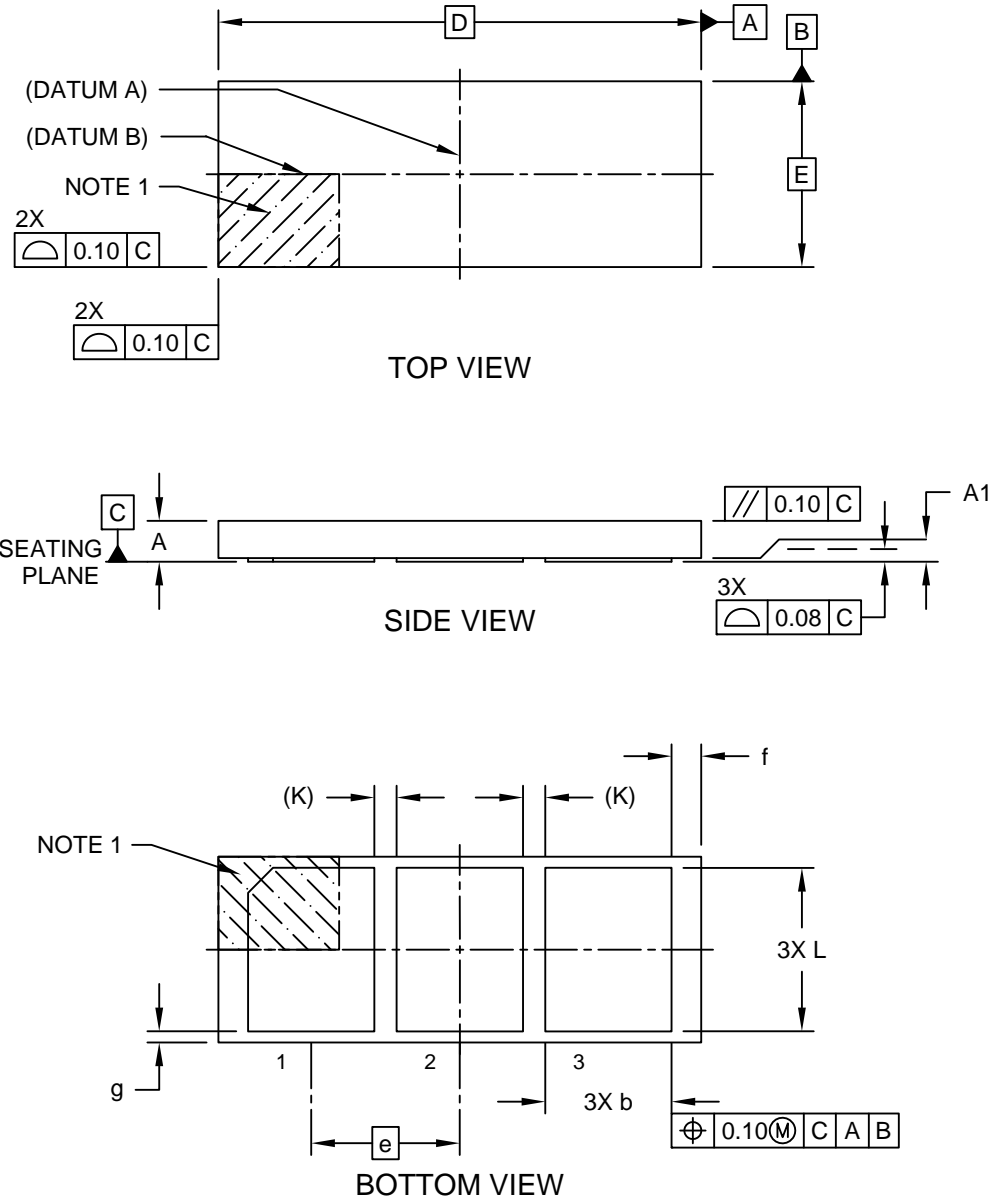
1. Dimensioning and tolerancing per ASME Y14.5M  
 BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-2057-OA Rev K

6.3 3-Lead Contact

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

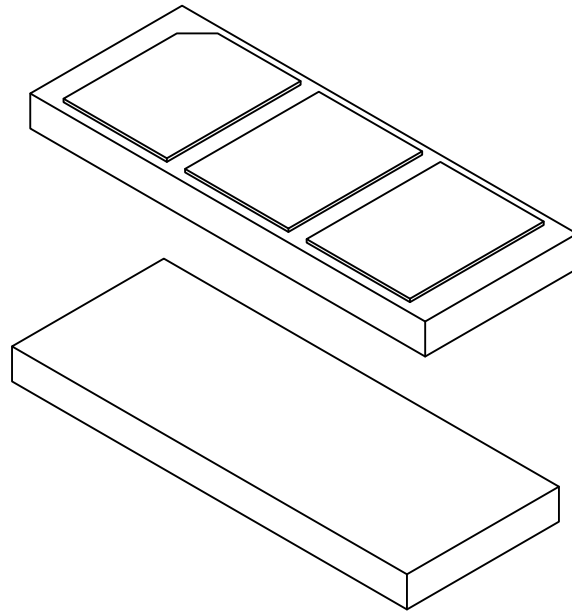
**Note:** For the most current package drawings, please see the Microchip Packaging Specification located at <http://www.microchip.com/packaging>



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.

## **7. Revision History SHA104**

### **Revision A (March 2023)**

- Initial data sheet release

---

## Microchip Information

---

### The Microchip Website

---

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

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

### Product Change Notification Service

---

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

To register, go to [www.microchip.com/pcn](http://www.microchip.com/pcn) and follow the registration instructions.

### Customer Support

---

Users of Microchip products can receive assistance through several channels:

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

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

Technical support is available through the website at: [www.microchip.com/support](http://www.microchip.com/support)

## Product Identification System

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

PART NO.	-XX	X	XX	-X
Device	Package	Temp Range	I/O Type	Tape and Reel

Device:	SHA104: 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)
	RB	3RB, 3-Lead 2.5 x 6.5 mm Body, 2.0 mm pitch, CONTACT Package (Sawn).
Temperature Option	V	Extended Industrial Temperature Range. -40°C to 105°C
I/O Type	CZ	Single Wire Interface
	DA	I <sup>2</sup> C Interface
Tape and Reel Options	B	Tube
	T	Tape and Reel (Size varies by package type)

### Examples:

- SHA104-SSVCZ-T: 8-Lead (0.150" Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC), Single-Wire, Tape and Reel, 3,300 per Reel
- SHA104-SSVDA-T: 8-Lead (0.150" Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC), I<sup>2</sup>C, Tape and Reel, 3,300 per Reel
- SHA104-MAVCZ-T: 8-Pad 2 x 3 x 0.6 mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat NoLead Package (UDFN), Single-Wire, Tape and Reel, 5,000 per Reel
- SHA104-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
- SHA104-RBVCZ-T: Single-Wire, Tape and Reel, 5,000 per Reel, 3-Lead Contact Package
- SHA104-RBVCZ-B: Single-Wire, Tube, 56 per Tube, 3-Lead Contact Package

### 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](http://www.microchip.com/packaging) for small-form factor package availability, or contact your local Sales Office.

## Microchip Devices Code Protection Feature

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

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

## Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at [www.microchip.com/en-us/support/design-help/client-support-services](http://www.microchip.com/en-us/support/design-help/client-support-services).

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

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

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

## Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, CryptoMemory, CryptoRF, dsPIC, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, 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, SQL, SuperSwitcher, SuperSwitcher II, Switchtec, SynchronPHY, 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.

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

© 2023, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.

ISBN: 978-1-6683-2004-4

## Quality Management System

---

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



## Worldwide Sales and Service

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