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

SHA106 CryptoAuthentication™ Summary Data Sheet

SHA106

www.microchip.com Product Pages: SHA106

Introduction

The SHA106 is a member of Microchip Technology Inc. CryptoAuthentication™ product family used in accessory or disposable applications. The device is a parasitically-powered Single-Wire Interface (SWI) version of the SHA104. 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 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 SHA106 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). (NIST Certified)
- Extensive Security Measures Against Attacks
- Strong Physical Protection Mechanisms Against Invasive Attacks
- Field-Programmable EEPROM
  - Single symmetric secret key
  - 384-byte user memory
  - 40-year data retention at +55℃
- Monotonic Counter with Max Count Value of 10,000
  - Counter can be attached to key for limited use
- Unique 72-Bit Serial Number
- Interface: 125 kbps Pulse Width Modulated (PWM) SWI
- Parasitically Powered through SIO Signal. Input Range 2.5 to 5.5 volts
- 130 nA Nominal Sleep Current
- Human Body Model (HBM) ESD: >7 kV
- Packaging Options: 2-Lead VSFN (2.0 mm x 2.35 mm) Contact Package

Use Cases

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

Pin Configuration and Pinouts

Table 1. Pin Configuration

2-PAD VSFN		
Pin #	Function	SWI-PWM
1	Ground	GND
2	Serial I/O	SI/O

Figure 1. Pinout

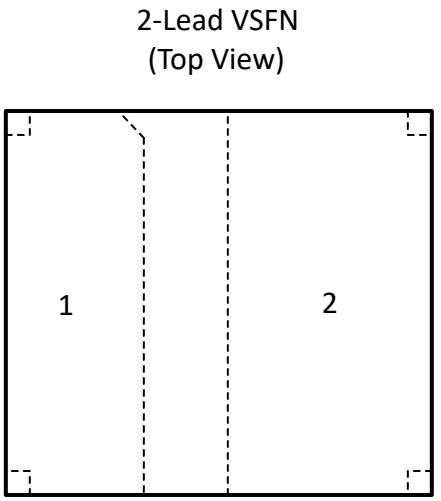


Table of Contents

1. Overview

1.1 Use Cases

SHA106 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.

SHA106 has a command set that allows for its usage in multiple symmetric key applications. The primary uses include the following:

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

In typical applications, the SHA106 will be used on the accessory/disposable side of an application and the SHA105 will be used on the host side of that application. SHA106 can be ordered as either an I^2C or SWI I/O option. If an SWI device is implemented in a given application, it can optionally be used in parasitic power mode.

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

1.1.1 2-Lead VSFN Contact Package

The 2-Lead VSFN contact package is a unique package that is especially suited for disposable and accessory applications where a cartridge or accessory is replaced on a regular basis. Typical integrated circuit packages require the package to be soldered down to a PCB. Most often this board has multiple ICs and/or passive devices.

For disposable applications where the only reason to add electronics is to authenticate the disposable, the requirement is often reduced to a single cryptographic IC plus a decoupling capacitor. The SHA106 contains both the IC and the decoupling capacitor so all electronics needed by the disposable are entirely contained in the packaged device. An alternative method to connect to the package, then, can eliminate the need for a PCB in the system.

Contact packages provide a unique solution where, instead of soldering the pads of the device down to a PCB board, the package is, instead, attached to the accessory by gluing the top side of the package to the accessory. The pads of the package are left exposed for future connection to the

host system. Typically, some sort of a 2-pin contactor or pogo pin connections are used to connect the accessory device to the host system. This approach allows for a simple and reliable connection between the disposable and the host device, while minimizing the cost to add authentication to the accessory.

1.2 Device Features

SHA106 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 SHA106 supports a Microchip proprietary PWM SWI operating in parasitic power mode. This reduces the total pin count of the interface to just two pins: a Ground Signal and the Serial I/O Signal. Power is provided to the device through the Serial I/O signal and a capacitor internal to the package.

Each SHA106 unit ships with a unique 72-bit serial number. Also, SHA106 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 SHA106 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

SHA106 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 SHA106 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 SHA106 incorporates a number of physical security features designed to protect the EEPROM contents from unauthorized exposure.

2.2.2 Random Number Generator (RNG)

The SHA106 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:	
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 SHA106 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: Single-Wire Interface – Parasitic Power Mode

Table 3-2. DC Parameters on Parasitic Single-Wire Interface

Unless otherwise indicated, values are applicable over the specified operating range from T_A = -40℃ to +105℃, CMOSen=1

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Ambient Operating Temperature	T_A	-40	—	+105	℃	—
Max. I/O Voltage(1)	V_{PUP}	2.5	—	5.5	V	R_{PUP} must be chosen such that $V_{PUP} - R_{PUP}*I_{CC} \geq 2.0V$
Output Low Voltage	V_{OL}	—	—	0.4	V	When the device is in Active mode, V_{PUP} = 2.5V to 3.6V for output-low current = 8.0 mA
Input Low Leakage(3)	I_{IL}	-200	—	200	nA	V_{IN} = GND
Input Low Threshold	V_{IL1}	-0.5	—	0.3*V_{SIO}	V	CMOSen = 1
Input High Threshold	V_{IH1}	0.7*V_{SIO}	—	V_{SIO}+0.5	V	CMOSen = 1

Table 3-2. DC Parameters on Parasitic Single-Wire Interface (continued)

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Sleep Current[2]	I_{SLEEP}	—	130	325[4]	nA	When the device is in Sleep mode, $V_{SIO} \leq 3.6V$, I/O at GND $T_A \leq +55°C$
		—	130	500	nA	When the device is in Sleep mode, $V_{SIO} \leq 3.6V$, I/O at GND Full Temperature Range
		—	130	1000	nA	When the device is in Sleep mode. Over full V_{SIO} and temperature range.
Current Consumption in I/O Mode	$I_{I/O}$	—	80	250	µA	Waiting for I/O
Bus Capacitance	C_{BUS}	—	—	500	pF	—
Theta JA[5]	Θ_{JA}	—	173.8	—	°C/W	2-PAD VSFN

Notes:

1. Single-Wire voltage (V_{PUP}) must never be greater than the maximum V_{PUP} operating voltage.
2. For the lowest system current, the SI/O signal must be driven to V_{PUP} by the host or allowed to be pulled up by the pull-up resistors.
3. Input High leakage can not be measured because the device and decoupling capacitor is charged via the SI/O signal.
4. This condition is characterized but not production tested.
5. The Theta-JA for this package is applicable when the device is soldered to a board. Typically this package is not mounted this way.

4. SHA106 Trust Platform Variants and Provisioning Services

Microchip offers secure provisioning services for the SHA106 through the Trust Platform. It leverages the Trust Platform Design Suite (TPDS) set of tools, and currently offers 3 provisioning flows:

- Trust&GO: Pre-configured and pre-provisioned Secure Elements for fix-function Use Cases
- TrustFLEX: Pre-configured & 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 SHA106 device to meet the security requirements for a given application. At the end of the process, a Secure Exchange Package is generated that is deployed to the Microchip Secure Provisioning System. 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.

SHA106 Trust Platform Products

The SHA106 is supported by Microchip's Trust Platform provisioning flow. The TPDS tools can be used to support configuring the devices for the purpose of prototyping, design evaluation and secure provisioning services (i.e., onboarding). The device is only available in the 2-Lead VSFN package and only the SWI is possible. Through use of the EV98D91A 2-Lead VSFN Socket Kit, combined with the DM320118 Trust Platform development board, units can be configured and programmed. For Trust Products with similar capabilities to the SHA106, review the SHA104 and SHA104-TFLXAUTH products on the Microchip website.

5. Package Marking Information

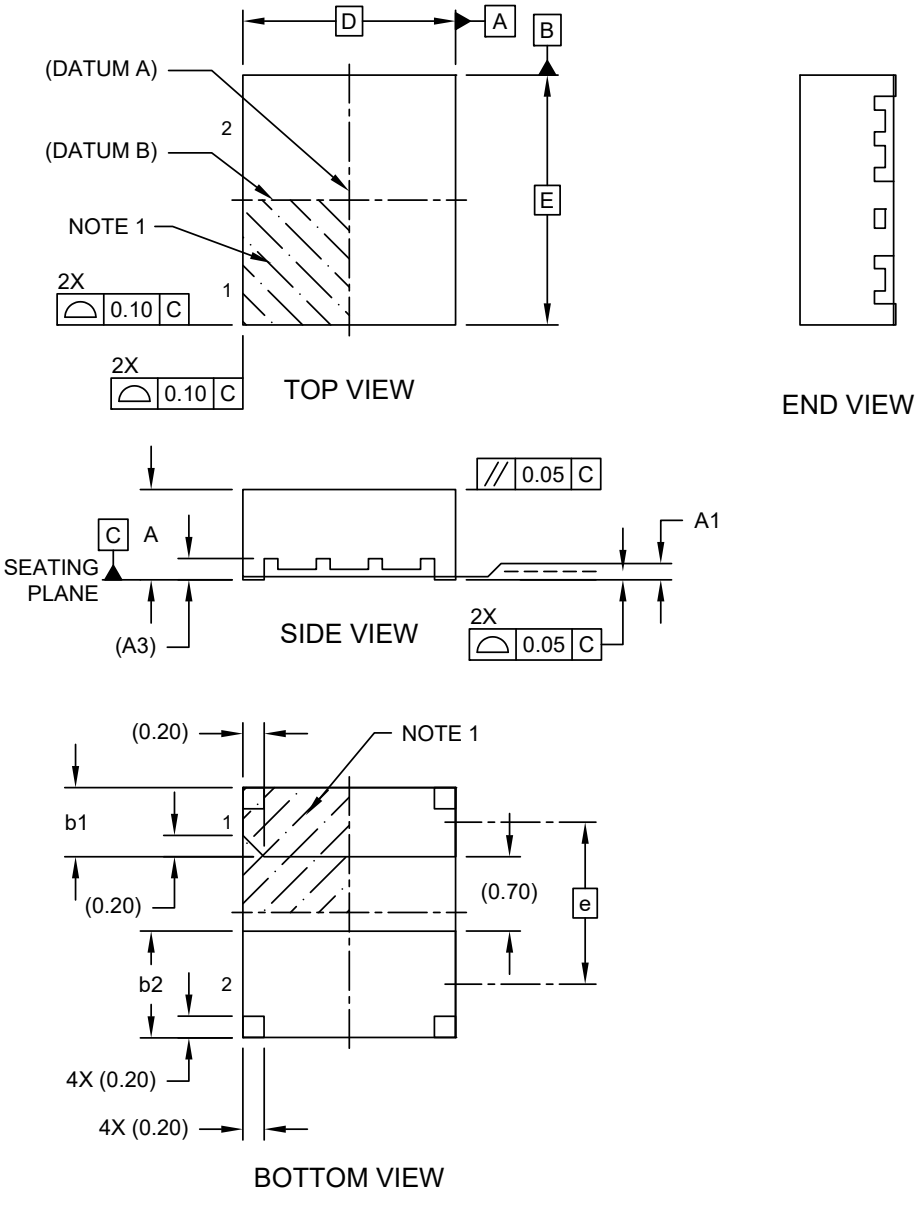
As part of Microchip's overall security features, the part marking for all crypto devices is intentionally vague. The marking on the top of the package does not provide any information as to the actual device type or the manufacturer of the device. The alphanumeric code on the package provides manufacturing 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 2-Lead VSFN Contact Package

2-Lead Very Thin Single Flatpack No Lead Package (2EW) - 2.0x2.35x0.9 mm Body [VSFN]

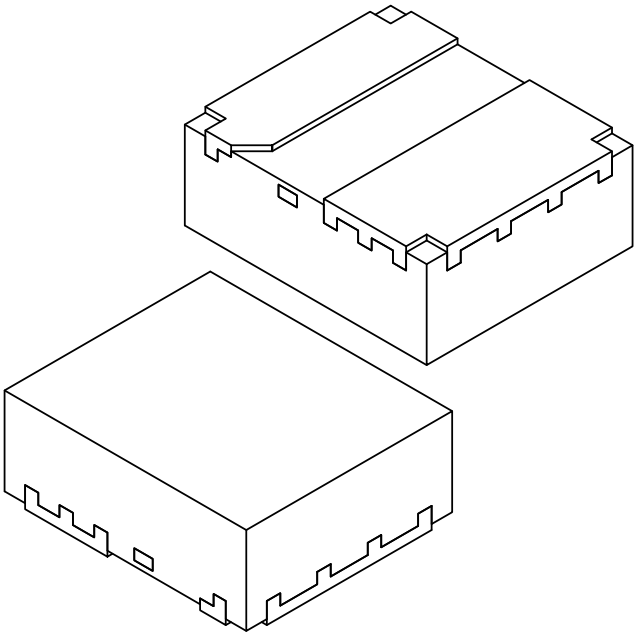
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing C04-540 Rev A Sheet 1 of 2

2-Lead Very Thin Single Flatpack No Lead Package (2EW) - 2.0x2.35x0.9 mm Body [VSFN]

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		2	
Pitch	e		1.525 BSC	
Overall Height	A	0.80	0.85	0.90
Standoff	A1	0.00	0.02	0.05
Terminal Thickness	A3		0.203 REF	
Overall Length	D		2.00 BSC	
Overall Width	E		2.35 BSC	
Terminal Width	b1	0.60	0.65	0.70
Terminal Width	b2	0.95	1.00	1.05

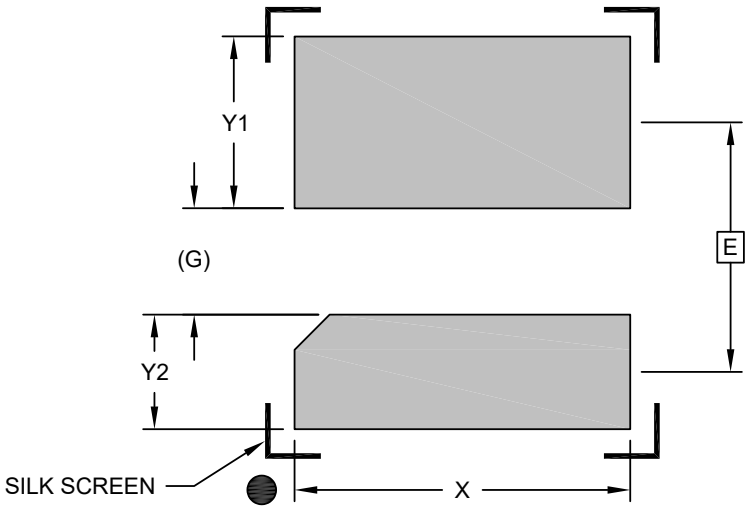
Notes:

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 C04-540 Rev A Sheet 2 of 2

2-Lead Very Thin Single Flatpack No Lead Package (2EW) - 2.0x2.35x0.9 mm Body [VSFN]

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	1.525 BSC		
Contact Pad Length (X2)	X			2.10
Contact Pad Width	Y1			1.05
Contact Pad Width	Y2			0.70
Contact Pad to Center Pad (Xnn)	G	0.587 REF		

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 C04-2540 Rev A

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:	SHA106: Cryptographic Co-processor with Secure Hardware-based Key Storage	
Package Options	MC	2-Pad VSFN 2.0 x 2.35mm Contact package
Temperature Option	V	Extended Industrial Temperature Range. -40℃ to 105℃
I/O Type	CZ	Single Wire Interface
Tape and Reel Options	B	Bulk units in Canister

Examples:

- SHA106-MCVCZ-B: 2-Pad VSFN Contact package, Singe-Wire, Bulk, 10,000 devices per canister.

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.
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.

8. Revision History

Revision B (April 2025)

- Features: Added (NIST Certified) to random number generator bullet.
- Removed Sections on Key Uses and SRAM memory
- DC Parameters: Single-Wire Interface – Parasitic Power Mode: Added Theta-JA value for 2-pad S-VSFN Contact Package
- 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: 979-8-3371-0736-3

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.