ATECC508A

ATECC508A Summary Data Sheet

Features

- Cryptographic Co-processor with Secure Hardware-Based Key Storage
- Performs High-Speed Public Key (PKI) Algorithms
  - ECDSA: FIPS186-3 Elliptic Curve Digital Signature Algorithm
  - ECDH: FIPS SP800-56A Elliptic Curve Diffie-Hellman Algorithm
- NIST Standard P256 Elliptic Curve Support
- SHA-256 Hash Algorithm with HMAC Option
- Host and Client Operations
- 256-bit Key Length
- Storage for up to 16 Keys
- Two High-Endurance Monotonic Counters
- Guaranteed Unique 72-bit Serial Number
- Internal High-Quality FIPS Random Number Generator (RNG)
- 10 Kb EEPROM Memory for Keys, Certificates, and Data
- Multiple Options for Consumption Logging and One-Time Write Information
- Intrusion Latch for External Tamper Switch or Power-on Chip Enablement. Multiple I/O Options:
  - High-speed Single Pin Interface, with One GPIO Pin
  - 1 MHz Standard I^2C Interface
- 2.0V to 5.5V Supply Voltage Range
- 1.8V to 5.5V IO levels
- <150 nA Sleep Current
- 8-pad UDFN, 8-lead SOIC, and 3-lead CONTACT Packages

Applications

- IoT Node Security and ID
- Secure Download and Boot
- Ecosystem Control
- Message Security
- Anti-Cloning

Package Types

Table 1. Pin Configuration

Pin	Function
NC	No Connect
GND	Ground
SDA	Serial Data
SCL	Serial Clock Input
V_{CC}	Power Supply

Figure 1. Package Types

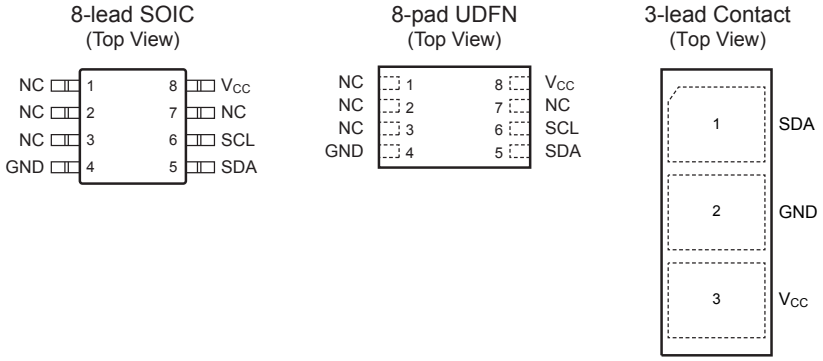


Table of Contents

1. Introduction

1.1 Applications

The ATECC508A device is a member of the Microchip CryptoAuthentication™ family of crypto engine authentication devices with highly secure hardware-based key storage.

The ATECC508A device has a flexible command set that allows use in many applications, including the following:

- **Network/IoT Node Protection** - Authenticates node IDs, ensures the integrity of messages, and supports key agreement to create session keys for message encryption.
- **Anti-Counterfeiting** - Validates that a removable, replaceable, or consumable client is authentic. Examples of clients could be system accessories, electronic daughter cards, or other spare parts. It can also be used to validate a software/firmware module or memory storage element.
- **Protecting Firmware or Media** - Validates code stored in flash memory at boot to prevent unauthorized modifications, encrypt downloaded program files as a common broadcast, or uniquely encrypt code images to be usable on a single system only.
- **Storing Secure Data** - Stores secret keys for use by crypto accelerators in standard microprocessors. Programmable protection is available using encrypted/authenticated reads and writes.
- **Checking User Password** - Validates user-entered passwords without letting the expected value become known, maps memorable passwords to a random number, and securely exchanges password values with remote systems.

1.2 Device Features

The ATECC508A includes an EEPROM array which can be used for storage of up to 16 keys, certificates, miscellaneous read/write, read-only or secret data, consumption logging, and security configurations. Access to the various sections of memory can be restricted in a variety of ways and then the configuration can be locked to prevent changes.

The ATECC508A 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 keys are used or generated provide further defense against certain styles of attack.

Access to the device is made through a standard I^2C Interface at speeds of up to 1 Mb/s. The interface is compatible with standard Serial EEPROM I^2C interface specifications. The device also supports a 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. If the Single-Wire Interface is enabled, the remaining pin is available for use as a GPIO, an authenticated output or tamper input.

Using either the I^2C or Single-Wire Interface, multiple ATECC508A devices can share the same bus, which saves processor GPIO usage in systems with multiple clients such as different color ink tanks or multiple spare parts, for example.

Each ATECC508A ships with a guaranteed unique 72-bit serial number. Using the cryptographic protocols supported by the device, a host system or remote server can verify a signature of the serial number to prove that the serial number is authentic and not a copy. Serial numbers are often stored in a

standard Serial EEPROM; however, these can be easily copied with no way for the host to know if the serial number is authentic or if it is a clone.

The ATECC508A can generate high-quality FIPS random numbers and employ them for any purpose, including usage as part of the device's crypto protocols. Because each random number is guaranteed to be essentially unique from all numbers ever generated on this or any other device, their inclusion in the protocol calculation ensures that replay attacks (i.e. re-transmitting a previously successful transaction) will always fail.

System integration is easy due to a wide supply voltage range (of 2.0V to 5.5V) and an ultra-low sleep current (of <150 nA). Complete DC parametrics are found in Section Electrical Characteristics. Multiple package options are available (see Sections Product Identification System and Package Drawings).

See Section Compatibility for information regarding compatibility with the Microchip ATSHA204A and ATECC108A devices.

1.3 Cryptographic Operation

The ATECC508A implements a complete asymmetric (public/private) key cryptographic signature solution based upon Elliptic Curve Cryptography and the ECDSA signature protocol. The device features hardware acceleration for the NIST standard P256 prime curve and supports the complete key life cycle from high quality private key generation, to ECDSA signature generation, ECDH key agreement, and ECDSA public key signature verification.

The hardware accelerator can implement such asymmetric cryptographic operations from ten to one-thousand times faster than software running on standard microprocessors, without the usual high risk of key exposure that is endemic to standard microprocessors.

The device is designed to securely store multiple private keys along with their associated public keys and certificates. The signature verification command can use any stored or an external ECC public key. Public keys stored within the device can be configured to require validation via a certificate chain to speed up subsequent device authentications.

Random private key generation is supported internally within the device to ensure that the private key can never be known outside of the device. The public key corresponding to a stored private key is always returned when the key is generated and it may optionally be computed at a later time.

The ATECC508A also supports a standard hash-based challenge-response protocol in order to simplify programming. In its most basic instantiation, the system sends a challenge to the device, which combines that challenge with a secret key via the `MAC`, `HMAC` or `SHA` commands and then sends the response back to the system. The device uses a SHA-256 cryptographic hash algorithm to make that combination so that an observer on the bus cannot derive the value of the secret key, but preserving the ability of a recipient to verify that the response is correct by performing the same calculation with a stored copy of the secret on the recipient's system.

Due to the flexible command set of the ATECC508A, these basic operation sets (i.e. ECDSA signatures, ECDH key agreement and SHA-256 challenge-response) can be expanded in many ways. Using the `GenDig` command, the values in other slots can be included in the response digest or signature, which provides an effective way of proving that a data read really did come from the device, as opposed to being inserted by a man-in-the-middle attacker. This same command can be used to combine two keys with the challenge, which is useful when there are multiple layers of authentication to be performed.

In a host-client configuration where the host (for instance, a mobile phone) needs to verify a client (for instance, an OEM battery), there is a need to store the secret in the host in order to validate the response

from the client. The CheckMac command allows the device to securely store the secret in the host system and hides the correct response value from the pins, returning only a yes or no answer to the system.

Finally, the hash combination of a challenge and secret key can be kept on the device and XORed with the contents of a slot to implement an encrypted Read command, or it can be XORed with encrypted input data to implement an encrypted Write command.

All hashing functions are implemented using the industry-standard SHA-256 secure hash algorithm, which is part of the latest set of high-security cryptographic algorithms recommended by various government agencies and cryptographic experts. The ATECC508A employs full-sized 256-bit secret keys to prevent any kind of exhaustive attack.

1.4 Commands

The ATECC508A is a command-based device which receives commands from the system, executes those commands, and then returns a result or error code. Within this document, the following nomenclature is used to describe the various commands:

- **Security Commands:**
  This group of commands generally access the EEPROM space and/or perform cryptographic computation. These commands are indicated with a special font in this document (e.g. GenDig) and are available from all interfaces.
- **Cryptographic Commands:**
  This subset of the security commands includes all the ECC commands which access the hardware ECC accelerator (GenKey, Sign, ECDH, and Verify) and the SHA commands which access the hardware SHA accelerator (CheckMac, DeriveKey, GenDig, HMAC, MAC, SHA, and Nonce).

2. Electrical Characteristics

2.1 Absolute Maximum Ratings

Operating Temperature	-40°C to +85°C
Storage Temperature	-65°C to +150°C
Maximum Operating Voltage	6.0V
DC Output Current	5 mA
Voltage on any pin	-0.5V to (V_{CC} + 0.5V)

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.

2.2 Reliability

The ATECC508A is fabricated with the Microchip high reliability of the CMOS EEPROM manufacturing technology.

Table 2-1. EEPROM Reliability

Parameter	Min	Typical	Max	Units
Write Endurance at +85°C (Each Byte)	400,000			Write Cycles
Data Retention at +55°C	10			Years
Data Retention at +35°C	30	50		Years
Read Endurance	Unlimited			Read Cycles

2.3 AC Parameters: All I/O Interfaces

Figure 2-1. AC Timing Diagram: All Interfaces

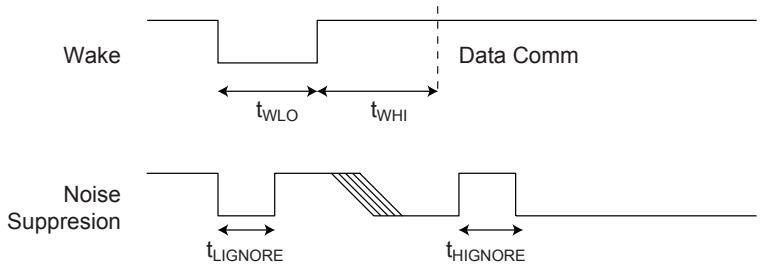


Table 2-2. AC Parameters: All I/O Interfaces

Parameter (Note)	Symbol	Direction	Min	Typ	Max	Unit	Conditions
Power-Up Delay	t_{PU}	To Crypto Authentication	100		—	µs	Minimum time between V_{CC} > V_{CC} min prior to measurement of t_{WLO}.
Wake Low Duration	t_{WLO}	To Crypto Authentication	60		—	µs	
Wake High Delay to Data Comm.	t_{WHI}	To Crypto Authentication	1500			µs	SDA should be stable high for this entire duration.
High Side Glitch Filter at Active	$t_{HIGNORE\_A}$	To Crypto Authentication	45(Note)			ns	Pulses shorter than this in width will be ignored by the device, regardless of its state when active.
Low Side Glitch Filter at Active	$t_{LIGNORE\_A}$	To Crypto Authentication	45(Note)			ns	Pulses shorter than this in width will be ignored by the device, regardless of its state when active.
Low Side Glitch Filter at Sleep	$t_{LIGNORE\_S}$	To Crypto Authentication	15(Note)			µs	Pulses shorter than this in width will be ignored by the device when in sleep mode.
Watchdog Timeout	$t_{WATCHDOG}$	To Crypto Authentication	0.7	1.3	1.7	s	Maximum time from wake until device is forced into sleep mode.

Note: These parameters are guaranteed through characterization, but not tested.

2.3.1 AC Parameters: Single-Wire Interface

Figure 2-2. AC Timing Diagram: Single-Wire Interface

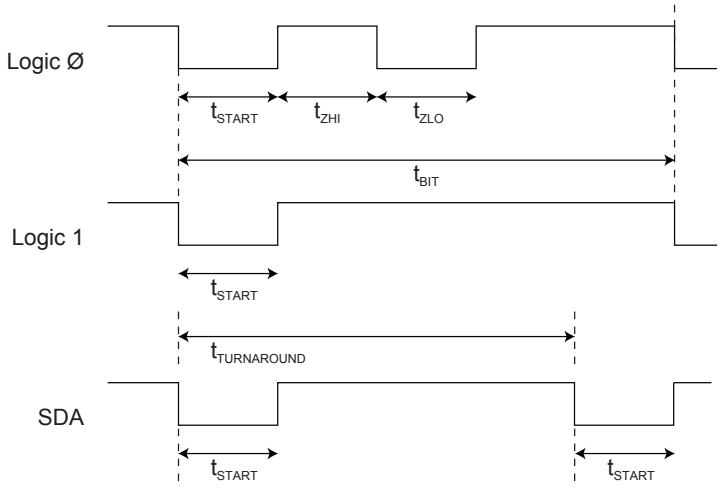


Table 2-3. AC Parameters: Single-Wire Interface

Unless otherwise specified, applicable from T_A = -40°C to +85°C, V_{CC} = +2.0V to +5.5V, CL =100 pF.

Parameter	Symbol	Direction	Min	Typ	Max	Unit	Notes
Start Pulse Duration	t_{START}	To Crypto Authentication	4.10	4.34	4.56	µs	
		From Crypto Authentication	4.60	6	8.60	µs	
Zero Transmission High Pulse	t_{ZHI}	To Crypto Authentication	4.10	4.34	4.56	µs	
		From Crypto Authentication	4.60	6	8.60	µs	
Zero Transmission Low Pulse	t_{ZLO}	To Crypto Authentication	4.10	4.34	4.56	µs	
		From Crypto Authentication	4.60	6	8.60	µs	
Bit Time(Note)	t_{BIT}	To Crypto Authentication	37	39	—	µs	If the bit time exceeds $t_{TIMEOUT}$ then ATECC508A may enter the sleep mode.
		From Crypto Authentication	41	54	78	µs	
Turn Around Delay	$t_{TURNAROUND}$	From Crypto Authentication	64	96	131	µs	ATECC508A will initiate the first low going transition after this time interval following the initial falling edge of the start pulse of the last bit of the transmit flag.
		To Crypto Authentication	93			µs	After ATECC508A transmits the last bit of a group, system must wait this interval before sending the first bit of a flag. It is measured from the falling edge of the start pulse of the last bit transmitted by ATECC508A.
IO Timeout	$t_{TIMEOUT}$	To Crypto Authentication	45	65	85	ms	ATECC508A may transition to the sleep mode if the bus is inactive longer than this duration.

Note: START, ZLO, ZHI, and BIT are designed to be compatible with a standard UART running at 230.4 Kbaud for both transmit and receive. The UART should be set to seven data bits, no parity and one stop bit.

2.3.2 AC Parameters: I²C Interface

Figure 2-3. I²C Synchronous Data Timing

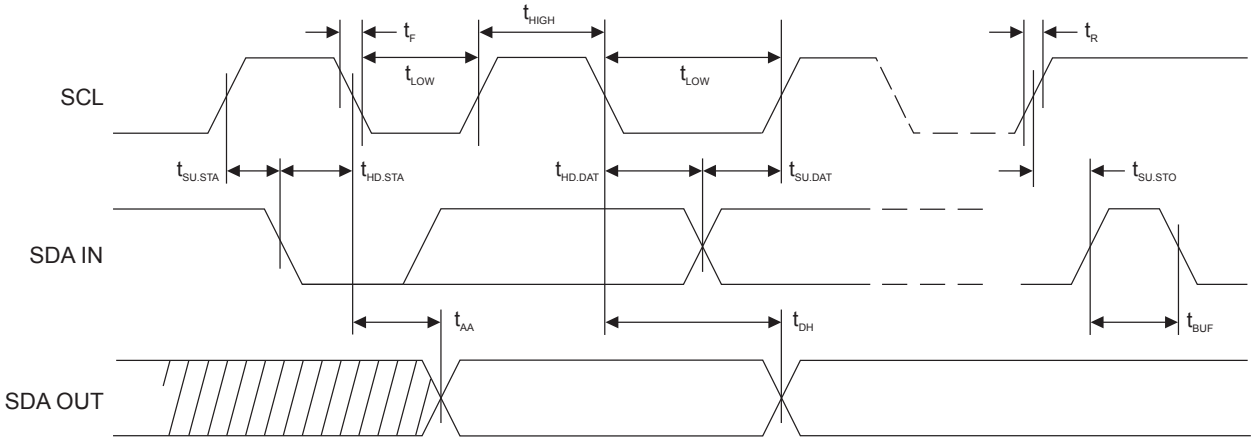


Table 2-4. AC Characteristics of I²C Interface

Unless otherwise specified, applicable over recommended operating range from T_A = -40°C to + 85°C, V_{CC} = +2.0V to +5.5V,
CL = 1 TTL Gate and 100 pF.

Parameter	Symbol	Min	Max	Units
SCK Clock Frequency	f_{SCK}	0	1	MHz
SCK High Time	t_{HIGH}	400		ns
SCK Low Time	t_{LOW}	400		ns
Start Setup Time	$t_{SU.STA}$	250		ns
Start Hold Time	$t_{HD.STA}$	250		ns
Stop Setup Time	$t_{SU.STO}$	250		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		100	ns
Clock Low to Data Out Valid	t_{AA}	50	550	ns
Data Out Hold Time	t_{DH}	50		ns
SMBus Timeout Delay	$t_{TIMEOUT}$	25	75	ms
Time bus must be free before a new transmission can start. (1)	t_{BUF}	500		ns

Note:

1. Values are based on characterization and are not tested
2. AC measurement conditions:
   - RL (connects between SDA and V_{CC}): 1.2 kΩ (for V_{CC} +2.0V to +5.0V)
   - Input pulse voltages: 0.3 V_{CC} to 0.7 V_{CC}
   - Input rise and fall times: ≤ 50 ns
   - Input and output timing reference voltage: 0.5V_{CC}

2.4 DC Parameters: All I/O Interfaces

Table 2-5. DC Parameters on All I/O Interfaces

Parameter	Symbol	Min	Typ	Max	Unit	Conditions
Ambient Operating Temperature	T_A	-40	—	85	°C	
Power Supply Voltage	V_{CC}	2.0	—	5.5	V	
Active Power Supply Current	I_{CC}	—	3	6	mA	Waiting for I/O during I/O transfers or execution of non-ECC commands.
		—	—	16	mA	During ECC command execution.
Idle Power Supply Current	I_{IDLE}	—	800	—	µA	When device is in idle mode, V_{SDA} and V_{SCL} < 0.4V or > V_{CC} – 0.4
Sleep Current	I_{SLEEP}	—	30	150	nA	When device is in sleep mode, V_{CC} ≤ 3.6V, V_{SDA} and V_{SCL} < 0.4V or > V_{CC} – 0.4, T_A ≤ +55°C
		—	—	2	µA	When device is in sleep mode.
Output Low Voltage	V_{OL}	—	—	0.4	V	When device is in active mode, V_{CC} = 2.5 – 5.5V
Output Low Current	I_{OL}	—	—	4	mA	When device is in active mode, V_{CC} = 2.5 – 5.5V, V_{OL} = 0.4V
Theta JA	Θ_{JA}	—	166	—	°C/W	SOIC (SSH)
		—	173	—	°C/W	UDFN (MAH)
		—	146	—	°C/W	RBH

2.4.1 V_{IH} and V_{IL} Specifications

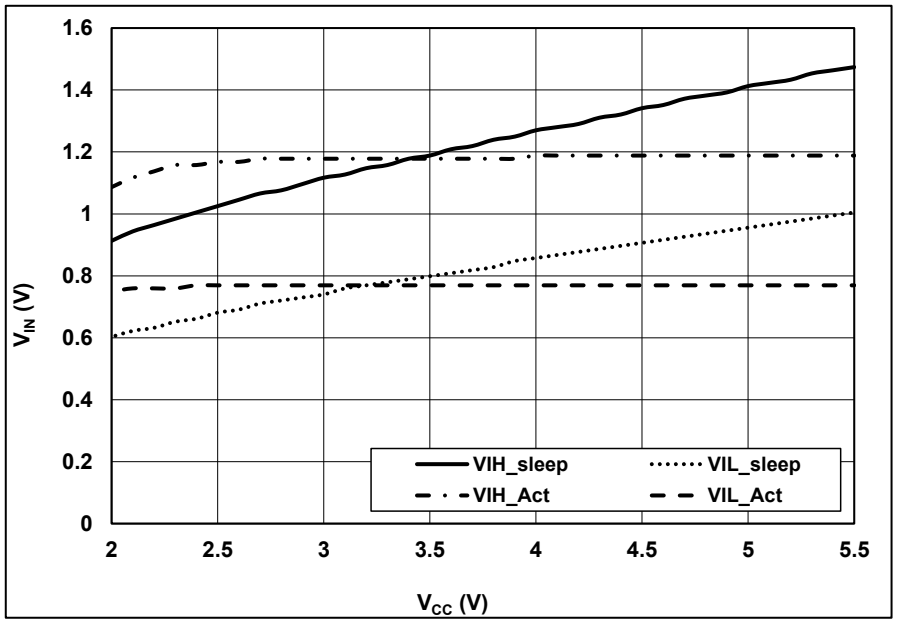
The input levels of the device will vary dependent on the mode and voltage of the device. The input voltage thresholds when in sleep or idle mode are dependent on the V_{CC} level as shown in Figure 2-4. When in sleep or idle mode the TTLenable bit has no effect.

When the device is active (i.e. not in sleep or idle mode), the input voltage thresholds are different depending upon the state of TTLenable (bit 1) within the ChipMode byte in the Configuration zone of the EEPROM. If the voltage supplied to the V_{CC} pin of the ATECC508A is different than the system voltage to which the input pull-up resistor is connected, then the system designer may choose to set TTLenable to zero, which enables a fixed input threshold shown by curves VIL_ACT and VIH_ACT in Figure 2-4. Table 2-6 which applies only when the device is active, presents the guaranteed levels of operation when operating in this mode.

Table 2-6. V_{IL}, V_{IH} on All I/O Interfaces (TTLenable = 0)

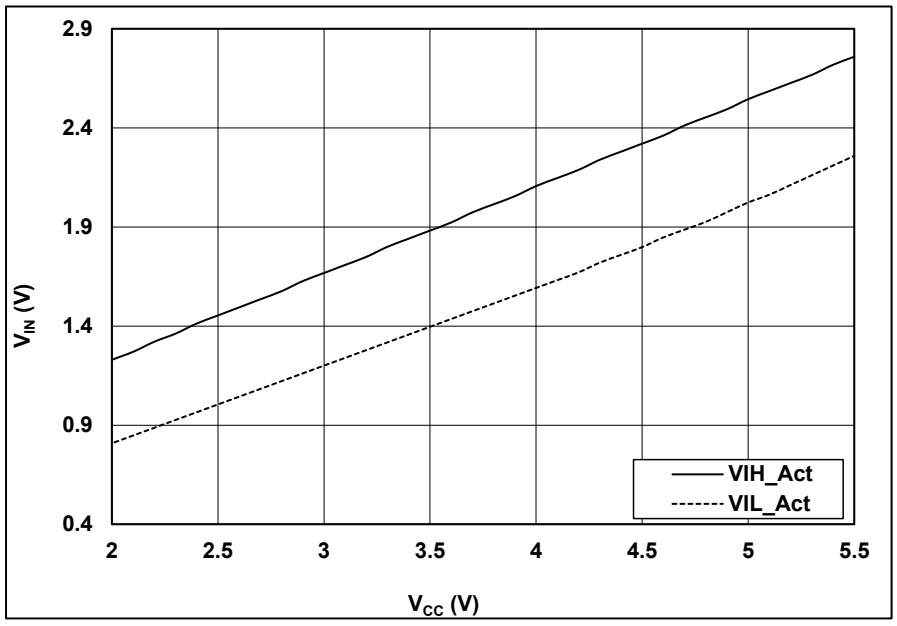
Parameter	Symbol	Min	Typ	Max	Unit	Conditions
Input Low Voltage	V_{IL}	-0.5		0.5	V	When device is active and TTLenable bit in configuration memory is zero; otherwise see above.
Input High Voltage	V_{IH}	1.5		V_{CC} + 0.5	V	When device is active and TTLenable bit in configuration memory is zero; otherwise see above.

Figure 2-4. V_{IH} and V_{IL} in Sleep and Idle Mode or When TTLenable = 0 on All I/O Interfaces



When a common voltage is used for the ATECC508A V_{CC} pin and the input pull-up resistor, then the TTLenable bit should be set to a one, which permits the input thresholds to track the supply as shown in Figure 2-5.

Figure 2-5. V_{IH} and V_{IL} When Active and TTLenable = 1 on All I/O Interfaces



3. Compatibility

3.1 Microchip ATSHA204A

ATECC508A is fully compatible with the ATSHA204 and ATSHA204A devices. If properly configured, it can be used in all situations where the ATSHA204 or ATSHA204A is currently employed. Because the configuration zone is larger, the personalization procedures for the device must be updated when personalizing the ATSHA204 or ATSHA204A. For proper compatibility, care should be taken with the KeyType, ReqRandom, and ReqAuth slots containing keys that are used with ATSHA204 or ATSHA204A sequences.

3.2 Microchip ATECC108A

ATECC508A is designed to be fully compatible with the ATECC108 and ATECC108A devices. If properly configured, it can be used in all situations where ATECC108 is currently employed. In many situations, the ATECC508A can also be used in an ATECC108 application without change. The new revisions provide significant advantages as outlined below:

- **Additional Features in ATECC508A vs. ATECC108A**
  - `ECDH` Command
  - High Endurance Monotonic Counters
  - Public Key Invalidation via Certificate
- **Minor Changes**
  - The `GenDig` command verifies that a random nonce is used when generating transport keys
  - The `Info` command DevRev mode now returns `0x1005` for ATECC108A and `0x5000` for ATECC508A. This value should not be used in the software as it will vary with each minor revision.

4. Package Marking Information

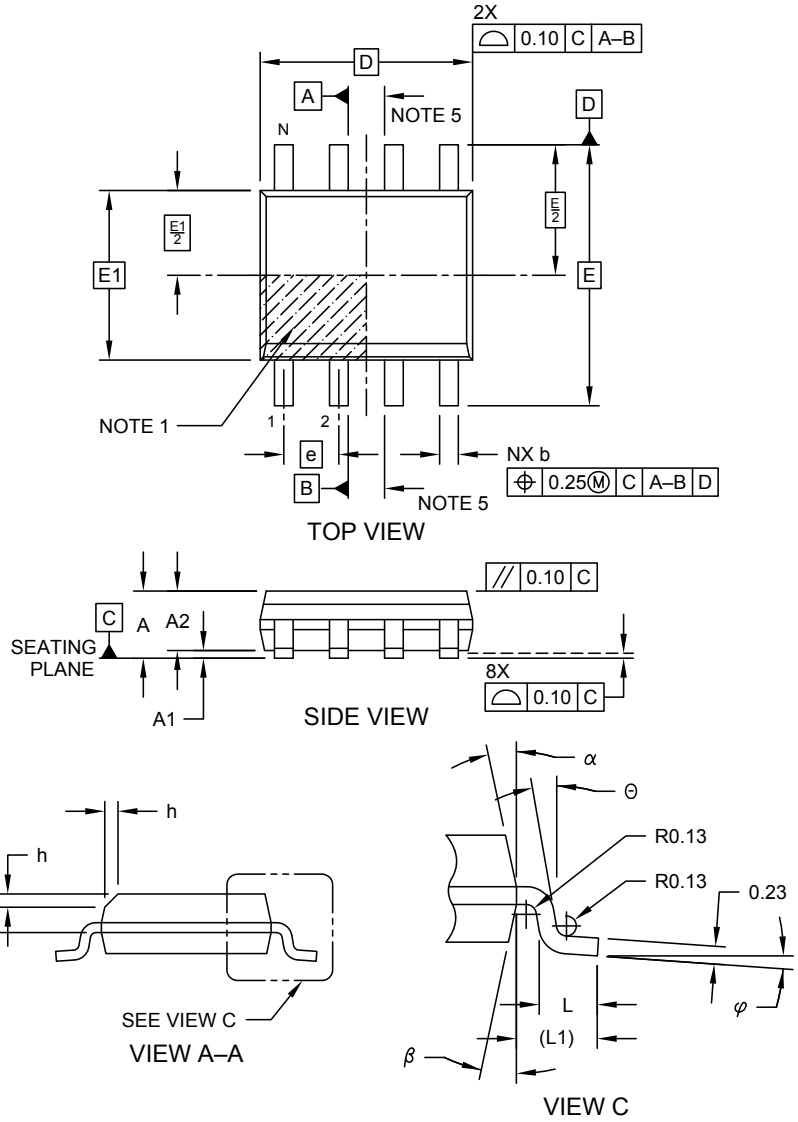
As part of Microchip's overall security features, the part mark for all crypto devices is intentionally vague. The marking on the top of the package does not provide any information as to the actual device type or the manufacturer of the device. The alphanumeric code on the package provides manufacturing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

5. Package Drawings

5.1 8-lead SOIC

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

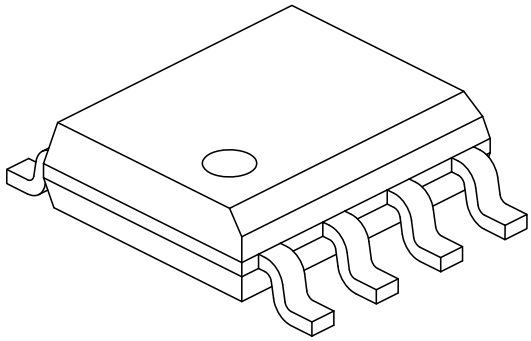
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing No. C04-057-Atmel Rev D Sheet 1 of 2

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

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	
Foot Angle	φ	0°	-	8°
Lead Thickness	c	0.17	-	0.25
Lead Width	b	0.31	-	0.51
Mold Draft Angle Top	α	5°	-	15°
Mold Draft Angle Bottom	β	5°	-	15°

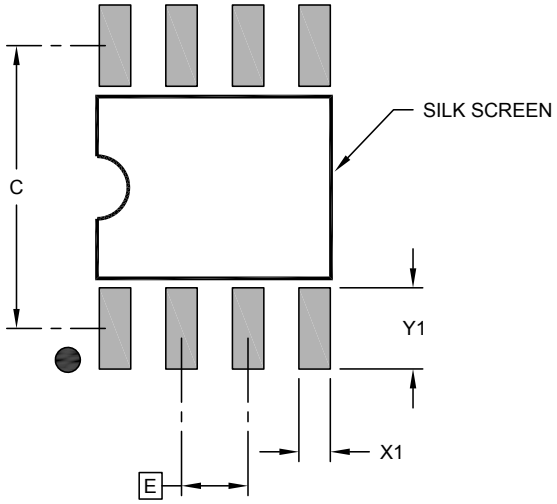
Notes:

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 D Sheet 2 of 2

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

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:

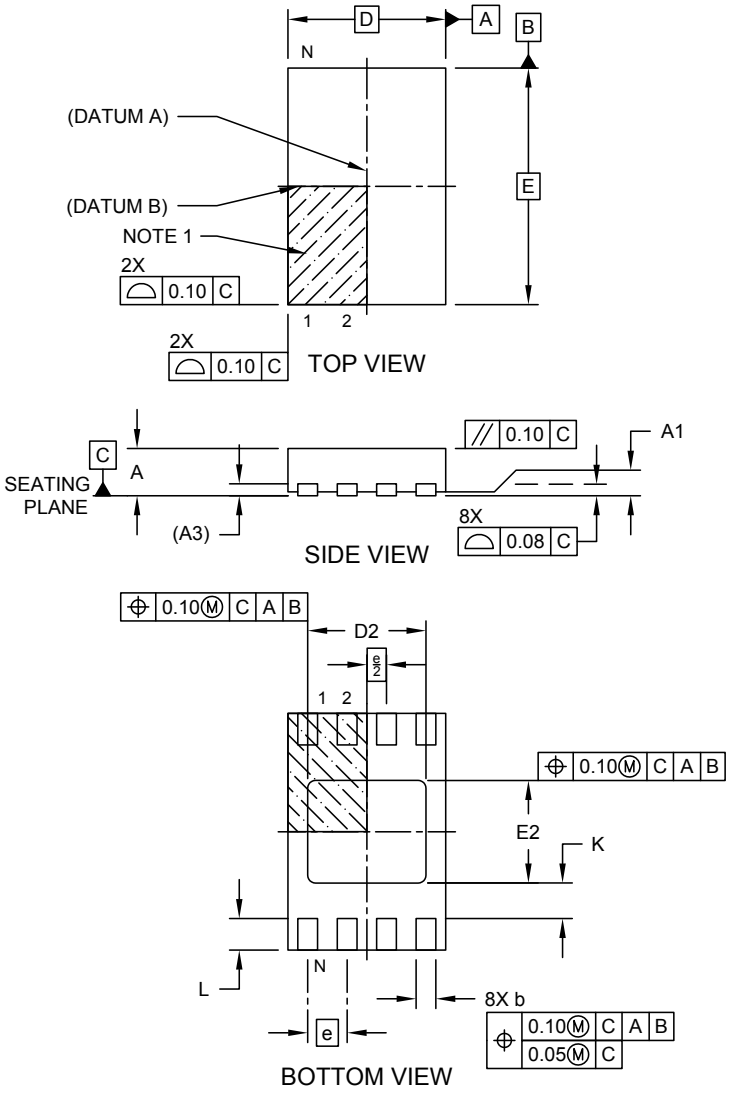
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-2057-M6B Rev B

5.2 8-pad UDFN

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

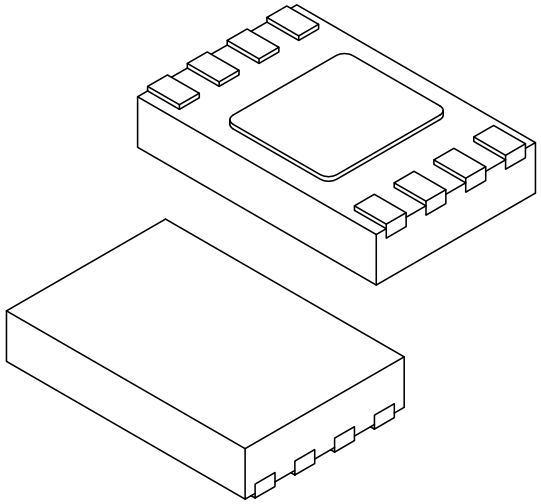
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



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

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

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	0.35	0.40	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

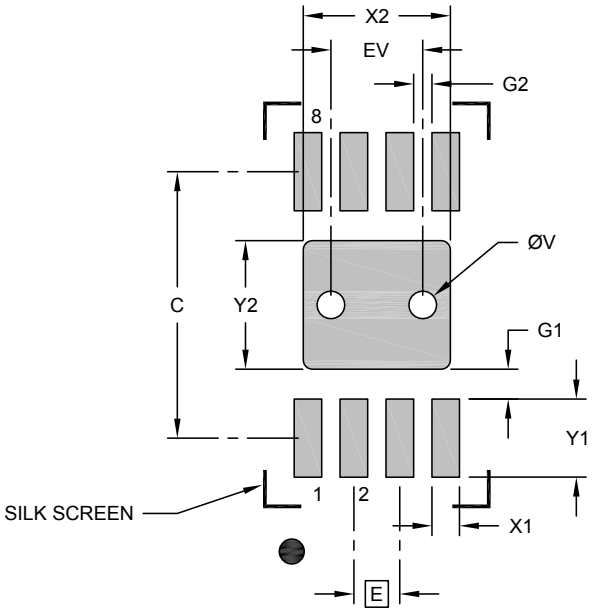
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

   REF: Reference Dimension, usually without tolerance, for information purposes only.

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

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

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	0.20		
Contact Pad to Contact Pad (X6)	G2	0.33		
Thermal Via Diameter	V		0.30	
Thermal Via Pitch	EV		1.00	

Notes:

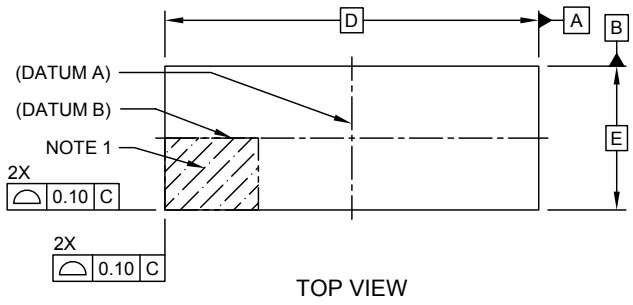
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
2. For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

Microchip Technology Drawing C04-21355-Q4B Rev A

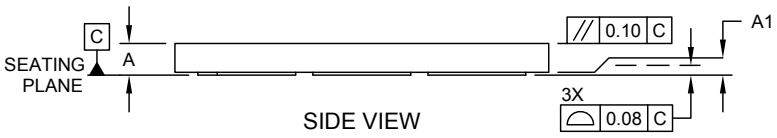
5.3 3-lead CONTACT

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

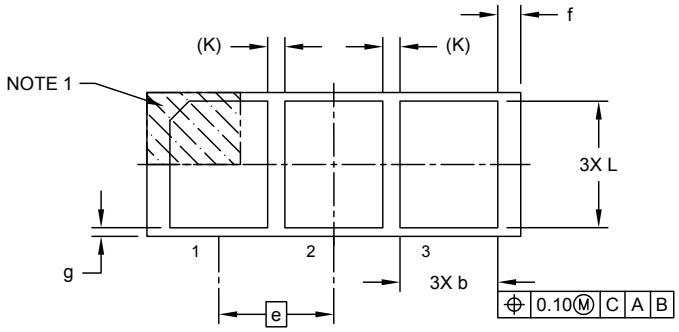
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



TOP VIEW



SIDE VIEW

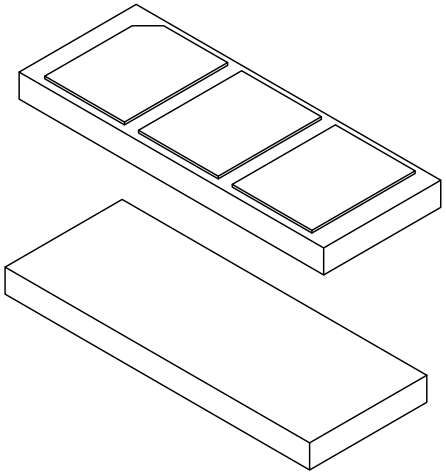


BOTTOM VIEW

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

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

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



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

Notes:

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

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

6. Revision History

Revision A (December 2017)
Original release of the document

This version replaces Atmel Document Revision 8923FX from 03.08.2016

The Microchip Web Site

Microchip provides online support via our web site at http://www.microchip.com/. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **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 (FAQ), technical support requests, online discussion groups, Microchip consultant 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

Customer Change Notification Service

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

To register, access the Microchip web site at http://www.microchip.com/. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: 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.	-XXX	XX	-X
Device	Package	I/O Type	Tape and Reel

Device:	ATECC508A: Cryptographic Co-processor with Secure Hardware-based Key Storage	
Package Options	SSH	= 8S1, 8-Lead (0.150” Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC)
	MAH	= 8MA2, 8-Pad 2 x 3 x 0.6 mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat No-Lead Package (UDFN)
	RBH	= 3RB, 3-Lead 2.5 x 6.5 mm Body, 2.0 mm pitch, CONTACT Package (Sawn).
I/O Type	CZ	= Single Wire Interface
	DA	= I^2C Interface
Tape and Reel Options	B	= Tube
	T	= Large Reel (Size varies by package type)
	S	= Small Reel (Only available for MAH)

Examples:

- ATECC508A-SSHCZ-T: Single-Wire, Tape and Reel, 4,000 per Reel, 8-Lead SOIC package
- ATECC508A-SSHCZ-B: Single-Wire, Tube, 100 per Tube, 8-Lead SOIC package
- ATECC508A-SSHDA-T: I^2C, Tape and Reel, 4,000 per Reel, 8-Lead SOIC package
- ATECC508A-SSHDA-B: I^2C, Tube, 100 per Tube, 8-Lead SOIC package
- ATECC508A-MAHCZ-T: Single-Wire, Tape and Reel, 15,000 per Reel, 8-Pad UDFN package
- ATECC508A-MAHDA-T: I^2C, Tape and Reel, 15,000 per Reel, 8-Pad UDFN package
- ATECC508A-MAHCZ-S: Single-Wire, Tape and Reel, 3,000 per Reel, 8-Pad UDFN package
- ATECC508A-MAHDA-S: I^2C, Tape and Reel, 3,000 per Reel, 8-Pad UDFN package
- ATECC508A-RBHCZ-T: Single-Wire, Tape and Reel, 5,000 per Reel, 3-Lead Contact Package
- ATECC508A-RBHCZ-B: Single-Wire, Tube, 56 per Tube, 3-Lead Contact Package

Note:

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 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 devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Information contained in this publication regarding device applications and the like 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. 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 ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. 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, AnyRate, AVR, AVR logo, AVR Freaks, BeaconThings, BitCloud, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Heldo, JukeBlox, KeeLoq, KeeLoq logo, Kleer, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, RightTouch, SAM-BA, SpyNIC, SST, SST Logo, SuperFlash, tinyAVR, UNI/O, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

ClockWorks, The Embedded Control Solutions Company, EtherSynch, Hyper Speed Control, HyperLight Load, IntelliMOS, mTouch, Precision Edge, and Quiet-Wire are registered trademarks of Microchip Technology Incorporated in the U.S.A.

ISBN: 978-1-5224-2485-7

Quality Management System Certified by DNV

ISO/TS 16949

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: http://www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4450-2828 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-67-3636 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-7289-7561 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820