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

ECC204 CryptoAuthentication™ Summary Data Sheet

ECC204

Product Page Links

Introduction

The ECC204 is a member of the Microchip Technology Inc. CryptoAuthentication™ product family. The device is targeted for disposable and ecosystem control applications and is intended to be used as a companion device with Microchip or other vendors' microcontrollers.

Features

- Cryptographic Authentication Device with Secure Hardware-Based Key Storage:
  - Protected storage for private key, certificates, symmetric key or user data
- Hardware Support for the Asymmetric Sign:
  - ECDSA: FIPS186-4 Elliptic Curve Digital Signature
  - NIST standard P-256 Elliptic Curve Support
- Hardware Support for SHA-256 and HMAC
- Internal Asymmetric Key Generation
- Internal High-Quality NIST SP 800-90A/B/C True Random Number Generator (TRNG) (NIST Certified)
- Joint Interpretation Laboratory (JIL) Score for Resistance to Attackers with Attack Potential – High
  - Evaluated to the standard "Jil-Application-of-Attack-Potential-to-Smartcards-V3.1"
  - Achieved through tamper-resistant countermeasures to resist environmental, non-invasive and invasive Fault attacks
- FIPS 140-3 Compliance Mode Configuration Option
- Field-Programmable EEPROM:
  - Single ECC private key
  - One device certificate and one CA signer certificate
  - Single symmetric secret key
  - 64-byte user memory
  - >40-year data retention at +55°C
- Monotonic Counter with the Maximum Count Value of 10,000
- Unique 72-bit Serial Number
- Two Interface Options Available:
  - 100 kbps Pulse-Width Modulated (PWM) single-wire serial interface (SWI)
  - Parasitic power support for single-wire interface with External Capacitor
  - 400 kHz Fast mode I^2C interface
- 130 nA Nominal Sleep Current
- Extended Industrial Temperature Range: -40°C to +105°C Ambient Operating Range
- Human Body Model (HBM) ESD: I^2C Devices >4 kV; SWI Devices >7 kV

- Packaging Options:
  - 8-pad UDFN (2x3 mm), 8-lead SOIC, 3-lead Contact (2.5x6.5 mm)

Use Cases

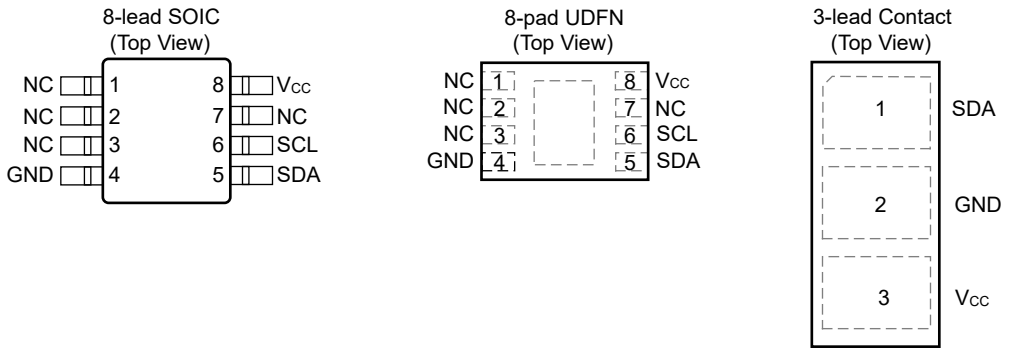
- Ecosystem Control Through asymmetric authentication / PKI
- Disposables and Accessory Authentication
- Disposable applications with limited use through programmable usage counter
- Symmetric Authentication through use of an HMAC Key

Pin Configuration and Pinouts

Table 1. Pin Configuration

Package = 8-PAD SOIC or 8-Lead UDFN				Package = 3-Lead Contact		
Pin #	Function	I²C	SWI	Pin #	Function	SWI
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(1)



Note:

1. Exposed backside paddle of the UDFN package is recommended to be connected to GND.

Table of Contents

Introduction....1

Features....1

Use Cases....2

Pin Configuration and Pinouts....2

1. Overview....4
   - 1.1. Use Cases....4
   - 1.2. Device Features....4
   - 1.3. Cryptographic Operation....4

2. Security Information....6
   - 2.1. Cryptographic Standards....6
     - 2.1.1. SHA-256....6
     - 2.1.2. HMAC/SHA-256....6
     - 2.1.3. Elliptic Curve Digital Signature Algorithm (ECDSA)....6
   - 2.2. Security Features....6
     - 2.2.1. Physical Security....6
     - 2.2.2. Random Number Generator (RNG)....6
     - 2.2.3. Compliance Mode....6

3. Electrical Characteristics....7
   - 3.1. Absolute Maximum Ratings....7
   - 3.2. DC Parameters....7
     - 3.2.1. DC Parameters: All I/O Interfaces....7
     - 3.2.2. DC Parameters: Single-Wire Interface....8
     - 3.2.3. DC Parameters: Single-Wire Interface – Parasitic Power Mode....9

4. ECC204 Trust Platform Variants and Provisioning Services....10

5. Package Marking Information....12

6. Package Drawings....13
   - 6.1. 8-Pad UDFN....13
   - 6.2. 8-Lead SOIC....16
   - 6.3. 3-Lead Contact....19

7. Product Identification System....21

8. Revision History....22

Microchip Information....23
- Trademarks....23
- Legal Notice....23
- Microchip Devices Code Protection Feature....23

Product Page Links....24

1. Overview

1.1. Use Cases

The ECC204 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.

The ECC204 device has a command set that allows for its usage in many applications. The primary uses include the following:

- **Disposables and Accessory Authentication**
  Authenticates that add-on accessories are authorized for use with a given host system. Both asymmetric and symmetric options can be implemented. Usage can be limited through the monotonic counter built into the device.
- **Ecosystem Control and Anti-Counterfeiting**
  Validates that a system or component is authentic and comes from the OEM shown on the nameplate

Tip: The use cases shown are examples of what can be implemented with the ECC204 but is not exhaustive. Contact Microchip Technical Support to determine if a use case outside of these can be implemented.

1.2. Device Features

The ECC204 includes an EEPROM array that can be used to store one private ECC P-256 key, two encoded certificates, one symmetric 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 device comes in one of two possible serial interfaces. The I^2C version of the device supports a standard I^2C interface at speeds of up to 400 kHz. The interface is compatible with the Standard and Fast modes I^2C 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 ECC204 can be operated in Parasitic Power mode, reducing the pin count to just two pins.

Each ECC204 unit is shipped with a unique 72-bit serial number. The ECC204 also 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 how a key is used or generated provide further defense against certain styles of attack.

For those users interested in a higher level of security, a Compliance mode bit is available in the Configuration zone. If the Compliance bit is set, compliance with various aspects of FIPS 140-3 is enforced by the device.

The ECC204 also has a monotonic counter that can be attached to either the ECC P-256 private key or the HMAC key to limit the use of one of these keys. If so desired, the monotonic counter can also be used by the host system.

1.3. Cryptographic Operation

The ECC204 device 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 P-256 prime curve and supports high-quality private key generation and ECDSA signature generation.

The hardware accelerator can implement asymmetric cryptographic operations faster than software running on standard microcontrollers without the usual high risk of key exposure, which is endemic to standard microcontrollers.

The ECC204 also implements SHA-256 and its derivative HMAC hash. SHA-256 can be used to facilitate message hashing for ECDSA signature generation. The device is designed to securely store a private key along with its associated public keys and certificates. Random private key generation is done 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 can also be requested at a future point in time.

The ECC204 can generate high-quality random numbers using its internal physical random number generator. This sophisticated function includes run-time health testing designed to ensure that values generated from the internal noise source contain sufficient entropy at the time of use. The RNG is designed to meet the requirements documented in the NIST SP 800-90A, SP 800-90B and SP 800-90C documents.

These random numbers can be employed for any purpose, including for use as part of the device's cryptographic protocols. Each random number is assured to be essentially unique from all numbers ever generated on this or any other device; therefore, their inclusion in the protocol calculation ensures that replay attacks (i.e., re-transmitting a previously-successful transaction) will always fail.

Related Links

Cryptographic Standards

2. Security Information

2.1. Cryptographic Standards

ECC204 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 ECC204 computes the SHA-256 digest based on the algorithm documented here:

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

2.1.2. HMAC/SHA-256

ECC204 can compute an HMAC digest based upon SHA-256 using a key stored in the EEPROM as documented below:

http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

2.1.3. Elliptic Curve Digital Signature Algorithm (ECDSA)

ECC204 computes the Elliptic Curve signatures according to the algorithm documented in:

- ANSI X9.62-2005 www.ansi.org/
- FIPS 186-5 specification nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf

2.2. Security Features

2.2.1. Physical Security

The ECC204 incorporates a number of physical security features designed to protect the EEPROM contents from unauthorized exposure.

2.2.2. Random Number Generator (RNG)

The ECC204 device includes a high-quality cryptographic True Random Number Generator (TRNG) implemented according to the NIST standards SP 800-90A/B/C.

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

- NIST SP 800-90A: Certified as part of the NIST Cryptographic Algorithm Validation Program (CAVP) certification process (Hash DRBG CAVP Certification)
- NIST SP 800-90B: Certified as part of the NIST Entropy Source Validation (ESV) process (ESV Certificate #E194 - Operating Environment 59V02 A2)
- NIST SP 800-90C: Provides recommendations on the creation of random bit generators that include DRBG mechanisms, as specified in SP 800-90A, and use entropy sources, as specified in SP 800- 90B.

2.2.3. Compliance Mode

For enhanced security, a Compliance mode is included in the ECC204 device. This mode is enabled through use of a configuration bit. If the Compliance bit is set, compliance with various aspects of FIPS140-3 is enforced by the device.

3. Electrical Characteristics

3.1. Absolute Maximum Ratings

Operating Temperature	-40°C to +105°C
Storage Temperature	-65°C to +150°C
Maximum Operating Voltage	6.0V
DC Output Low Current	20 mA
Voltage on any Pin	-0.5V to (V_{CC} + 0.5V)
ESD Ratings:	
Human Body Model (HBM) ESD I^2C 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. DC Parameters

3.2.1. DC Parameters: All I/O Interfaces

Table 3-1. DC Parameters on All I/O Interfaces with V_{CC} Power Applied
Unless otherwise indicated, these values are applicable over the specified operating range from T_A = -40°C to +105°C, V_{CC} = +1.65V to +5.5V.

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Ambient Operating Temperature	T_A	-40	—	+105	°C	—
V_{CC} Ramp Rate(4)	V_{RISE}	—	—	0.1	V/µs	—
Output Low Voltage	V_{OL}	—	—	0.4	V	When the device is in Active mode, V_{CC} = 1.65V to 3.6V for output-low current = 4.0 mA
		—	—	0.4	V	V_{CC} > 3.6V = 10.0 mA(4)
Input Low Threshold	V_{IL1}	-0.5	—	0.3*V_{CC}	V	Device is active and CMOSEnable = 1
Input High Threshold	V_{IH1}	0.7*V_{CC}	—	V_{CC}+0.5	V	Device is active and CMOSEnable = 1
Input Low Threshold(1, 2)	V_{IL0}	-0.5	—	0.5	V	Device is active and CMOSEnable = 0
Input High Threshold(1, 2)	V_{IH0}	1.2	—	V_{CC}+0.5	V	Device is active and CMOSEnable = 0
Input Low Threshold in Sleep mode(5)	V_{ILS}	-0.5	—	0.5	V	Device is in Sleep mode CMOSen= 0
Input High Threshold in Sleep mode(5)	V_{IHS}	1.35	—	V_{CC}+0.5	V	Device is in Sleep mode CMOSen= 0
Input Leakage (I^2C Signals)	I_{IN}	-200	—	200	nA	V_{IN} = V_{CC} or GND

Table 3-1. DC Parameters on All I/O Interfaces with V_{CC} Power Applied (continued)

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Sleep Current[3]	I_{SLEEP}	—	130	325[4]	nA	When the device is in Sleep mode, $V_{CC} \leq 3.6V$, I/O at either GND or V_{CC} $T_A \leq +55°C$
		—	130	500	nA	$V_{CC} \leq 3.6V$, I/O at either GND or V_{CC} Full temperature Range
		—	130	1000	nA	When the device is in Sleep mode Over full V_{CC} and temperature range
Current Consumption in I/O Mode	$I_{I/O}$	—	60	250	µA	Waiting for I/O
Theta JA	Θ_{JA}	—	99.1	—	°C/W	8-lead SOIC
		—	89.5	—	°C/W	8-pad UDFN
		—	91.5	—	°C/W	3-lead Contact[6]

Notes:

1. CMOSen = 0 must only be used when V_{CC} is between 2.0V and 5.5V and the host is running on a lower supply voltage than the client. In this mode, the input buffers are referenced to an internal supply and V_{IL} and V_{IH} levels are independent of the external V_{CC} supply over this range. For voltages lower than 2.0V, CMOSen must always be set to '1'.
2. 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_{CC} or allowed to be pulled up to V_{CC} by the pull-up resistors on the signal lines.
4. This condition is characterized but not production tested.
5. When coming out of Sleep mode when CMOSen=0, the initial input thresholds are V_{ILS}/V_{IHS}. When the device is awake, the thresholds will transition to V_{IL0}/ V_{IH0}.
6. For the 3-lead contact package, the Theta-JA applies when the device is soldered down to a board. Typically, this package is not mounted this way.

3.2.2. DC Parameters: Single-Wire Interface

Table 3-2. DC Parameters on Single-Wire Interface[1]

Unless otherwise indicated, these values are applicable over the specified operating range from T_A = -40°C to +105°C, V_{CC} = +1.65V to +5.5V.

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Power Supply Voltage	V_{CC}	1.65V	—	5.5V	V	—
Output Low Voltage	V_{OL}	—	—	0.4	V	When the device is in Active mode, V_{CC} = 1.65V to 3.6V for output-low current = 8.0 mA
		—	—	0.4	V	V_{CC} > 3.6V 16.0 mA[3]
Input High Leakage	I_{IH}	—	1.0	2.0	uA	$V_{IN} = V_{CC}$
Input Low Leakage	I_{IL}	-200	—	200	nA	V_{IN} = GND
Bus Capacitance	C_{BUS}	—	—	500	pF	—

Notes:

1. All specifications not shown can be found in the All I/O Interfaces Table 3-1.
2. The Single-Wire voltage must never be greater than V_{CC}.
3. This condition is characterized but not production tested.
4. Operation over the C_{BUS} range is ensured by design and is not production tested.

3.2.3. DC Parameters: Single-Wire Interface – Parasitic Power Mode

Table 3-3. DC Parameters on Parasitic Single-Wire Interface
Unless otherwise indicated, these values are applicable over the specified operating range from T_A = -40°C to +105°C, CMOSen = '1'

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Max. I/O Voltage(2)	V_{PUP}	2.5	—	5.5	V	—
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(4)	I_{IL}	-200	—	200	nA	V_{IN} = GND, V_{CC_DVC} ≥ 1.65V
Input Low Threshold	V_{IL1}	-0.5	—	0.3*V_{PUP}	V	—
Input High Threshold	V_{IH1}	0.7*V_{PUP}	—	V_{PUP}+0.5	V	—
Bus Capacitance	C_{BUS}	—	—	500	pF	—

Notes:

1. All specifications not shown can be found in the All I/O Interfaces Table 3-1.
2. Single-Wire voltage (V_{PUP}) must never be greater than the maximum V_{PUP} operating voltage.
3. 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.
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_{BUS} range is ensured by design and is not production tested.

4. ECC204 Trust Platform Variants and Provisioning Services

Microchip offers secure provisioning services for the ECC204 through the Trust Platform. It leverages the Trust Platform Design Suite set of tools (TPDS) 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 ECC204 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: The Microchip Secure Provisioning System is based on Hardware Security Modules (HSMs).

ECC204 Trust Platform Products

For the ECC204, only TrustFLEX and TrustCUSTOM variants of the products are currently available. The following devices are currently released versions of ECC204 Trust products. Additional products may be added in the future.

ECC204-TFLXWPC

- The ECC204-TFLXWPC was developed to meet the authentication requirements for Power Transmitters developed for the Wireless Power Consortium. Microchip is an authorized manufacturing CA of the Wireless Power Consortium.

ECC204-TFLXAUTH

- The ECC204-TFLXAUTH was developed to meet the authentication requirements for disposable and accessory applications. The devices provide the ability to do either asymmetric or symmetric authentication.

Table 4-1. ECC204 Trust Platform Ordering Codes[1]

Trust Platform Type	Production Ordering Code	Package Type	Temperature Range
TrustFLEX[2]	ECC204-TFLXWPCU	8-Pad UDFN	Extended Industrial. -40°C to +105°C
	ECC204-TFLXWPCS	8-Pin SOIC	Extended Industrial. -40°C to +105°C
	ECC204-TFLXAUTHU	8-Pad UDFN	Extended Industrial. -40°C to +105°C
	ECC204-TFLXAUTHS	8-Pin SOIC	Extended Industrial. -40°C to +105°C
TrustCUSTOM[3]	ECC204-TCSMU	8-Pad UDFN	Extended Industrial. -40°C to +105°C
	ECC204-TCSMS	8-Pin SOIC	Extended Industrial. -40°C to +105°C

Notes:

1. This table is a representative sample of Trust Platform Devices. 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 ECC204 devices. ECC204-TCSMU/ECC204-TCSMS is equivalent to ECC204-MAVDA-T/ECC204-SSVDA-T respectively.

5. Package Marking Information

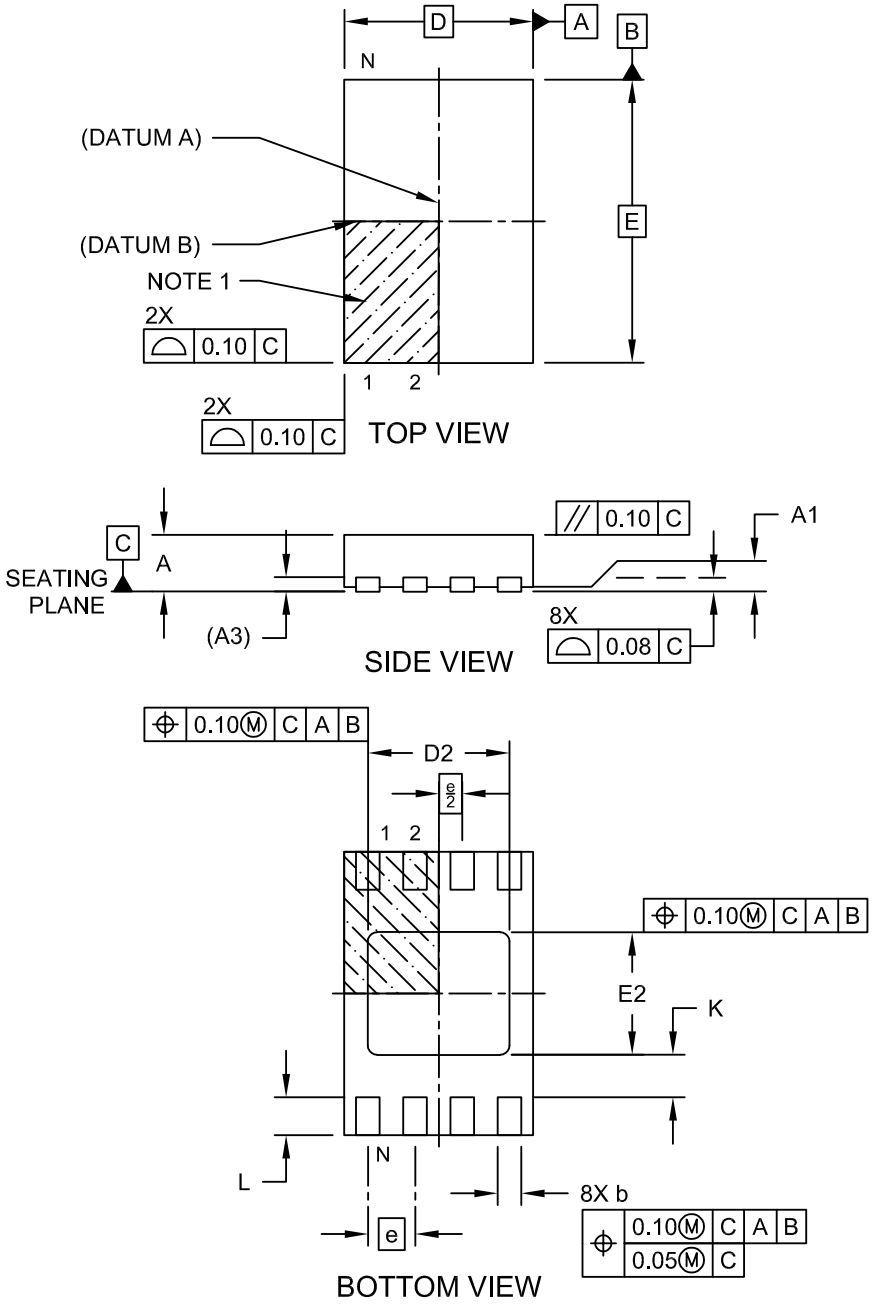
As part of Microchip's overall security features, the part marking for all crypto devices is intentionally vague. The marking on the top of the package does not provide any information as to the actual device type or the manufacturer of the device. The alphanumeric code on the package provides manufacturing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

6. Package Drawings

6.1. 8-Pad UDFN

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

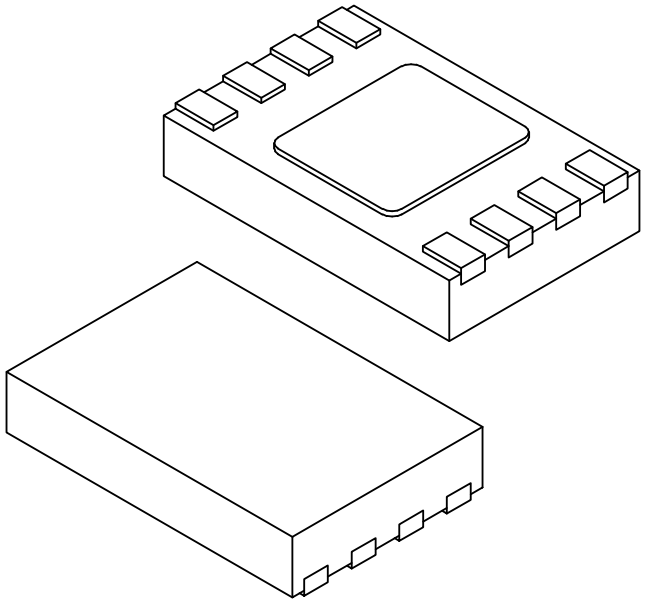
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



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

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

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



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

Notes:

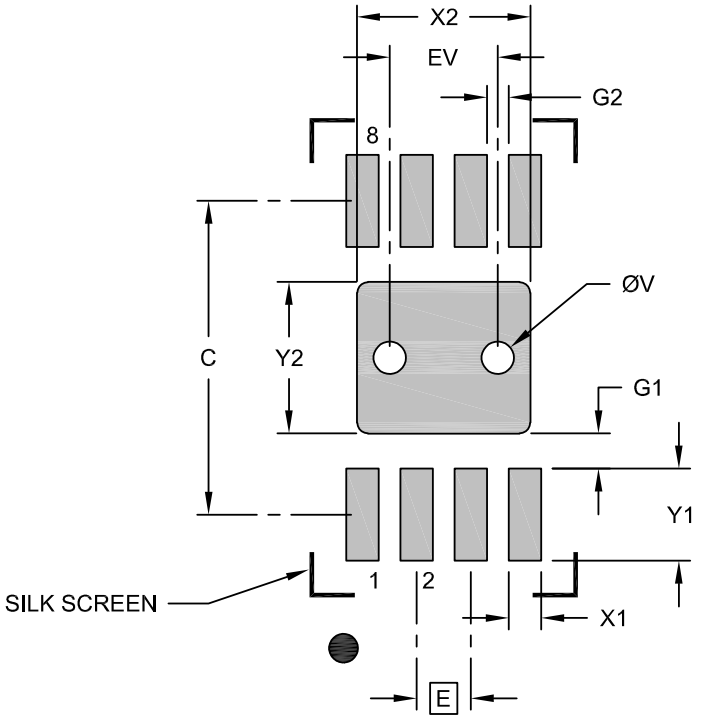
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M

BSC: Basic Dimension. Theoretically exact value shown without tolerances.
REF: Reference Dimension, usually without tolerance, for information purposes only.

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

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

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



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		0.50 BSC	
Optional Center Pad Width	X2			1.60
Optional Center Pad Length	Y2			1.40
Contact Pad Spacing	C		2.90	
Contact Pad Width (X8)	X1			0.30
Contact Pad Length (X8)	Y1			0.85
Contact Pad to Center Pad (X8)	G1	0.33		
Contact Pad to Contact Pad (X6)	G2	0.20		
Thermal Via Diameter	V		0.30	
Thermal Via Pitch	EV		1.00	

Notes:

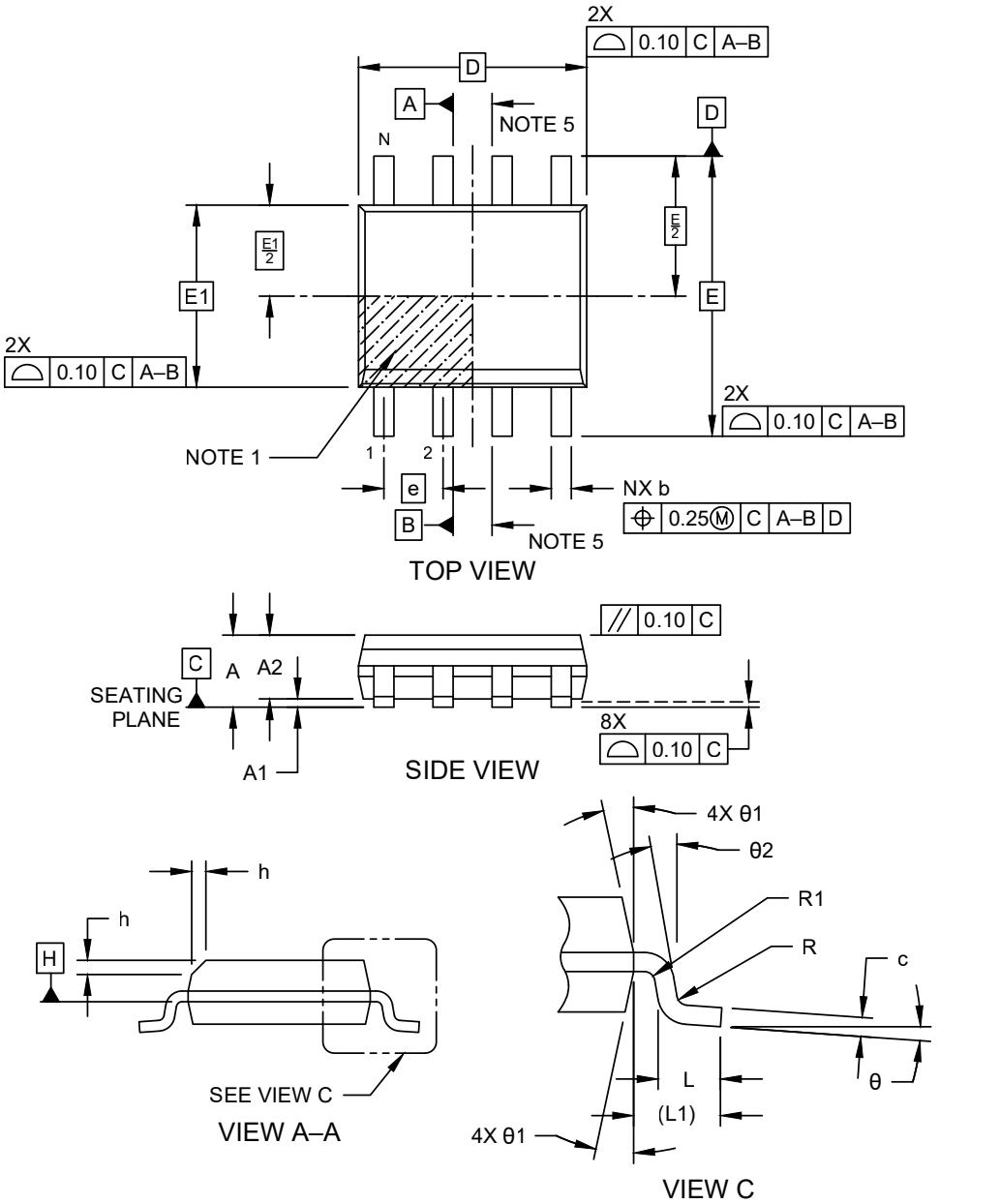
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
2. For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

Microchip Technology Drawing C04-23355-Q4B Rev C

6.2. 8-Lead SOIC

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

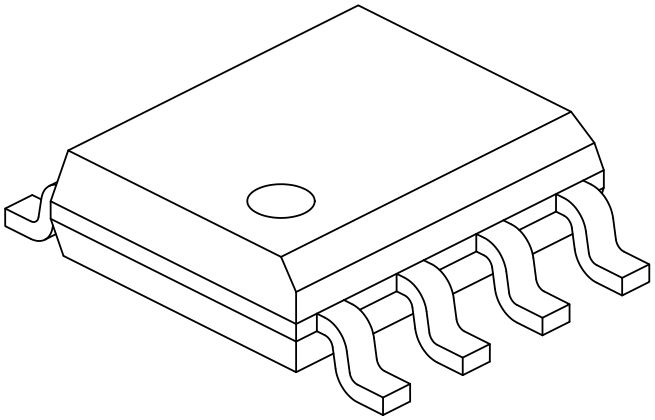
Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing No. C04-00057-OA Rev L Sheet 1 of 2

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

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



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

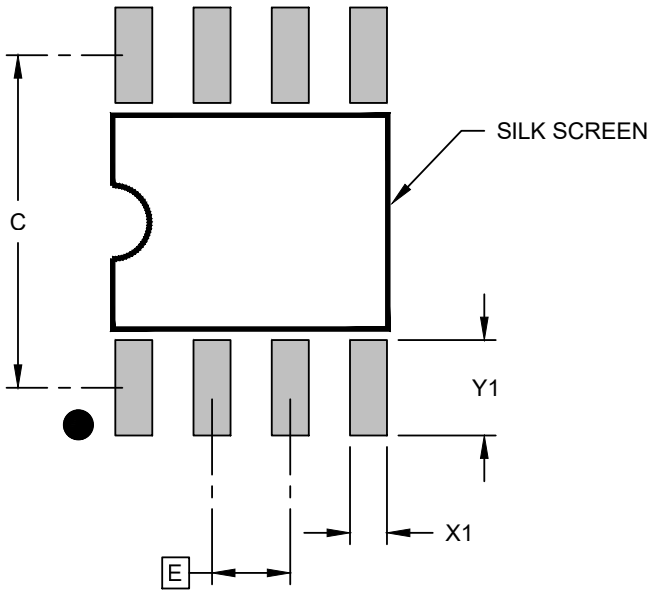
Notes:

1. The Pin 1 visual index feature may vary, but it 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. C04-00057-OA Rev L Sheet 2 of 2

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

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



RECOMMENDED LAND PATTERN

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

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M

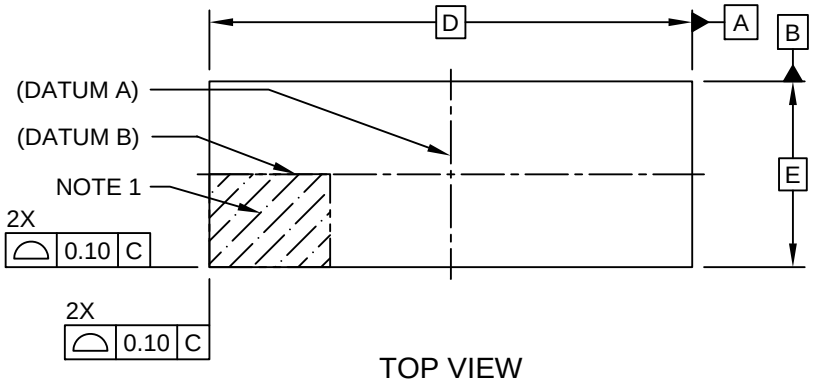
BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-02057-OA Rev L

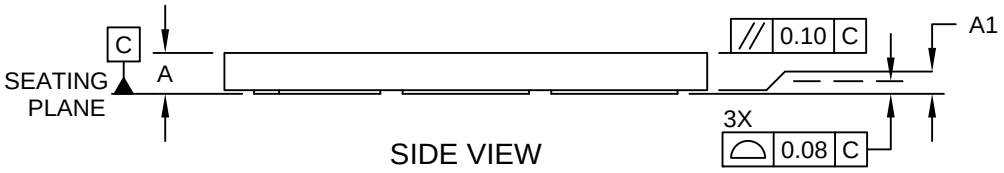
6.3. 3-Lead Contact

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

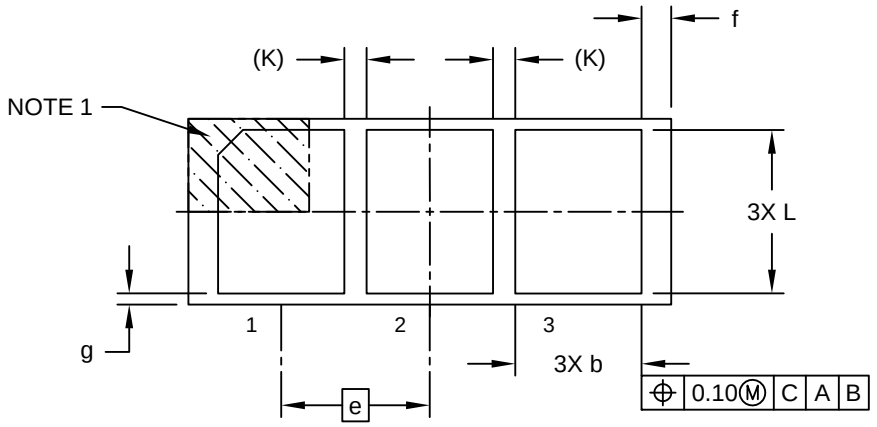
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



TOP VIEW



SIDE VIEW

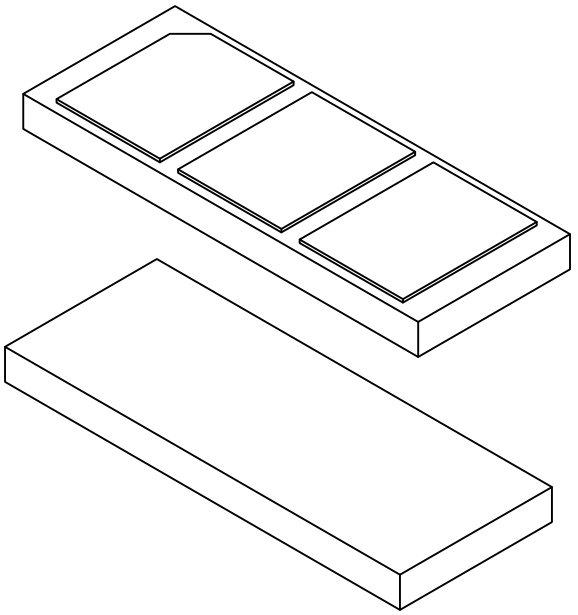


BOTTOM VIEW

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

7. Product Identification System

To order or obtain information, for example, on pricing or delivery, contact Microchip: https://www.microchip.com/en-us/about/contact-us.

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

Device:	ECC204: Cryptographic Coprocessor with Secure Hardware-Based Key Storage	
Package Options	SS	8-Lead (0.150" 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 No Lead 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^2C Interface
Tape and Reel Options	B	Tube
	T	Tape and Reel (size varies by package type)

Examples:

- ECC204-SSVCZ-T: 8-Lead (0.150" Body), Plastic Gull Wing Small Outline (JEDEC® SOIC), -40°C to +105°C, Single-Wire, Tape and Reel, 3,300 per Reel.
- ECC204-SSVDA-T: 8-Lead (0.150" Body), Plastic Gull Wing Small Outline (JEDEC SOIC), -40°C to +105°C, I^2C, Tape and Reel, 3,300 per Reel.
- ECC204-MAVCZ-T: 8-Pad (2 x 3 x 0.6 mm Body), Thermally Enhanced Plastic Ultra Thin Dual Flat No Lead Package (UDFN), -40°C to +105°C, Single-Wire, Tape and Reel, 5,000 per Reel.
- ECC204-MAVDA-T: 8-Pad (2 x 3 x 0.6 mm Body), Thermally Enhanced Plastic Ultra Thin Dual Flat No Lead Package (UDFN), -40°C to +105°C, I^2C, Tape and Reel, 5,000 per Reel.
- ECC204-RBVCZ-T: 3-Lead Contact Package, -40°C to +105°C, Single-Wire, Tape and Reel, 5,000 per Reel.
- ECC204-RBVCZ-B: 3-Lead Contact Package, -40°C to +105°C, Single-Wire, Tube, 56 per Tube.

Notes:

1. Tape and Reel identifier only appears in the catalog part number description. This identifier is used for ordering purposes and is not printed on the device package. Check with your Microchip Sales Office for package availability with the Tape and Reel option.
2. Small form-factor packaging options may be available. Please check www.microchip.com/packaging for small-form factor package availability or contact your local Sales Office.

8. Revision History

Revision C (December 2025)

NOTICE No changes have been made to the functional operation or electrical characteristics of the device.

- Features
  - Updated random number generator bullet to indicate a True Random Number Generator (TRNG)
  - Corrected SWI-PWM speed to 100 kbps
- Random Number Generator (RNG)
  - Updated to indicate that the RNG is a TRNG
  - Added certification information associated with the RNG
  - Updated SP 800-90C to the released version of the spec
- Package Drawings
  - Updated SOIC package outline drawings to latest version

Revision B (February 2025)

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

- DC Parameters: All I/O Interfaces
  - Added input thresholds when in Sleep mode (V_{ILS}, V_{IHS})
  - Updated the UDFN, SOIC and 3-Lead Contact θ_{JA} values
- Product Identification System: Product identification is now a separate section and not part of Back Matter
- Microchip Information: Back Matter simplified per Microchip's new standard

Revision A (March 2023)

Original release of the document

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: 979-8-3371-2406-3

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.

Product Page Links

ECC204