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

ECC206 CryptoAuthentication™ Summary Data Sheet

ECC206

Product Page Links

Introduction

The ECC206 is part of Microchip Technology Inc.'s CryptoAuthentication™ product family. This 2-pin device is powered parasitically and supports a single-wire interface. It is specifically designed for disposable and anti-cloning applications where a printed circuit board (PCB) is not required. The device is intended to serve as a companion device and is microcontroller/microprocessor agnostic.

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
- Interface: 100 kbps Pulse Width Modulated (PWM) Single-Wire Serial Interface with internal capacitor
- 130 nA Nominal Sleep Current
- Extended Industrial Temperature Range: -40°C to +105°C Ambient Operating Range
- Human Body Model (HBM) ESD: >7 kV
- Package Options: Contact Packages
  - 2-Lead VSFN 2 mm x 2.35 mm, 2-Lead XSFN 5 mm x 3.5 mm

Use Cases

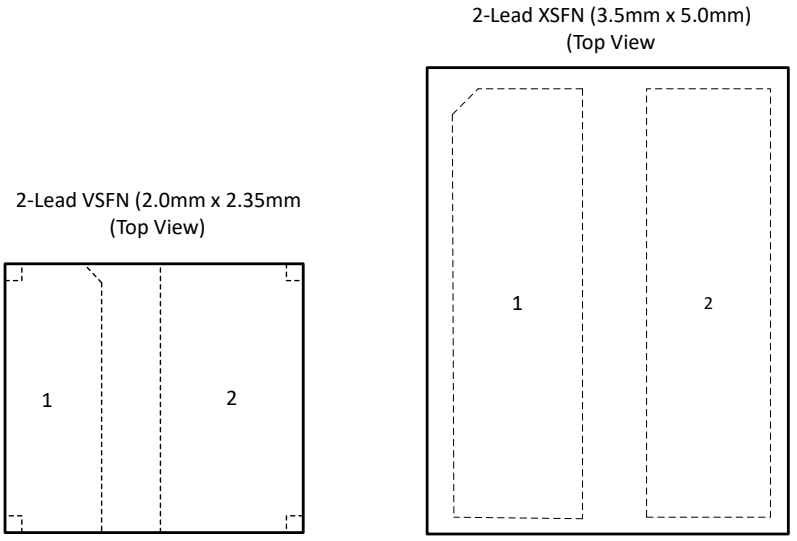
- Medical Disposables and Accessory Authentication
- Anti-cloning
- Medical Drug Delivery
- Battery Authentication
- Ecosystem Control

Pin Configuration and Pinouts

Table 1. Pin Configuration

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

Figure 1. Pinout



Related Links

2-Lead VSFN and XSFN Contact Packages

Table of Contents

1. Overview

1.1. Use Cases

The ECC206 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 ECC206 device has a command set that allows for its usage in many applications. The primary uses include the following:

- **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 ECC206 but is not exhaustive. Contact Microchip Technical Support to determine if a use case outside of these can be implemented.

1.1.1. 2-Lead VSFN and XSFN Contact Packages

The 2-Lead VSFN and XSFN contact packages are unique solutions designed for disposable and accessory applications, where cartridges or accessories are frequently replaced. Unlike traditional integrated circuit packages, which require soldering onto a printed circuit board (PCB) that typically contains multiple ICs and passive components, these contact packages are tailored for scenarios where electronics are added solely for authentication purposes.

In such disposable applications, the requirement is often limited to a single cryptographic IC and a decoupling capacitor. The ECC206 integrates both components within a single package, ensuring that all necessary electronics for the disposable accessory are fully contained.. This design enables alternative connection methods that can eliminate the need for a PCB in the system.

Contact packages offer a distinctive solution by allowing the device to be attached to the accessory using adhesive, with the package's pads exposed for future connection to the host system. Commonly, a 2-pin contactor or pogo pin connection is used to connect the accessory with the host device. This approach provides a simple and reliable connection, while reducing the cost of implementing authentication in disposable accessories.

1.2. Device Features

ECC206 includes an EEPROM array that can be used for storage of one private ECC P-256 key, 2 certificates, one symmetric secret key, miscellaneous read/write data, consumption logging and security configurations. Write access to the various data zone slots and configuration sub-zones of memory can be restricted.

The device 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. The chip operates in parasitic power mode, reducing the total pin count to just 2 pins.

Each ECC206 unit ships with a unique 72-bit serial number. Also, ECC206 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.

For those customers interested in a FIPS 140-3-compliant mode version of the device, a special CMP_Mode compliance bit is available in the configuration zone.

The ECC206 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 those keys. If so desired, the monotonic counter can also be used by the system and not be attached to any of the ECC206 keys.

1.3. Cryptographic Operation

The ECC206 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 ECC206 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 ECC206 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

ECC206 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 ECC206 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

ECC206 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)

ECC206 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 ECC206 incorporates a number of physical security features designed to protect the EEPROM contents from unauthorized exposure.

2.2.2. Random Number Generator (RNG)

The ECC206 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.

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. DC Parameters

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

Table 3-1. DC Parameters on Parasitic Single-Wire Interface
Unless otherwise indicated, 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
Ambient Operating Temperature	T_A	-40	—	+105	°C	—
Max. I/O Voltage(1)	V_{PUP}	2.4	—	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} = 2.4V 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
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. ECC206 Trust Platform Variants and Provisioning Services

Microchip offers secure provisioning services for the ECC206 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 ECC206 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.

ECC206 Trust Platform Products

The ECC206 is supported by Microchip's Trust Platform provisioning flow. TPDS tools are available to assist with device configuration for prototyping, design evaluation and secure provisioning services, such as onboarding. The device is offered exclusively in the 2-Lead VSFN package and supports only the Single-Wire Interface (SWI). Configuration and programming can be performed using the EV98D91A 2-Lead VSFN Socket Kit in combination with the DM320118 Trust Platform development board. For applications utilizing the 2-Lead XSFN package, the EV14Y33A Evaluation Kit is recommended. For additional Trust Platform products with similar capabilities, please refer to the ECC204 and ECC204-TFLXAUTH products available on the Microchip website.

5. Package Marking Information

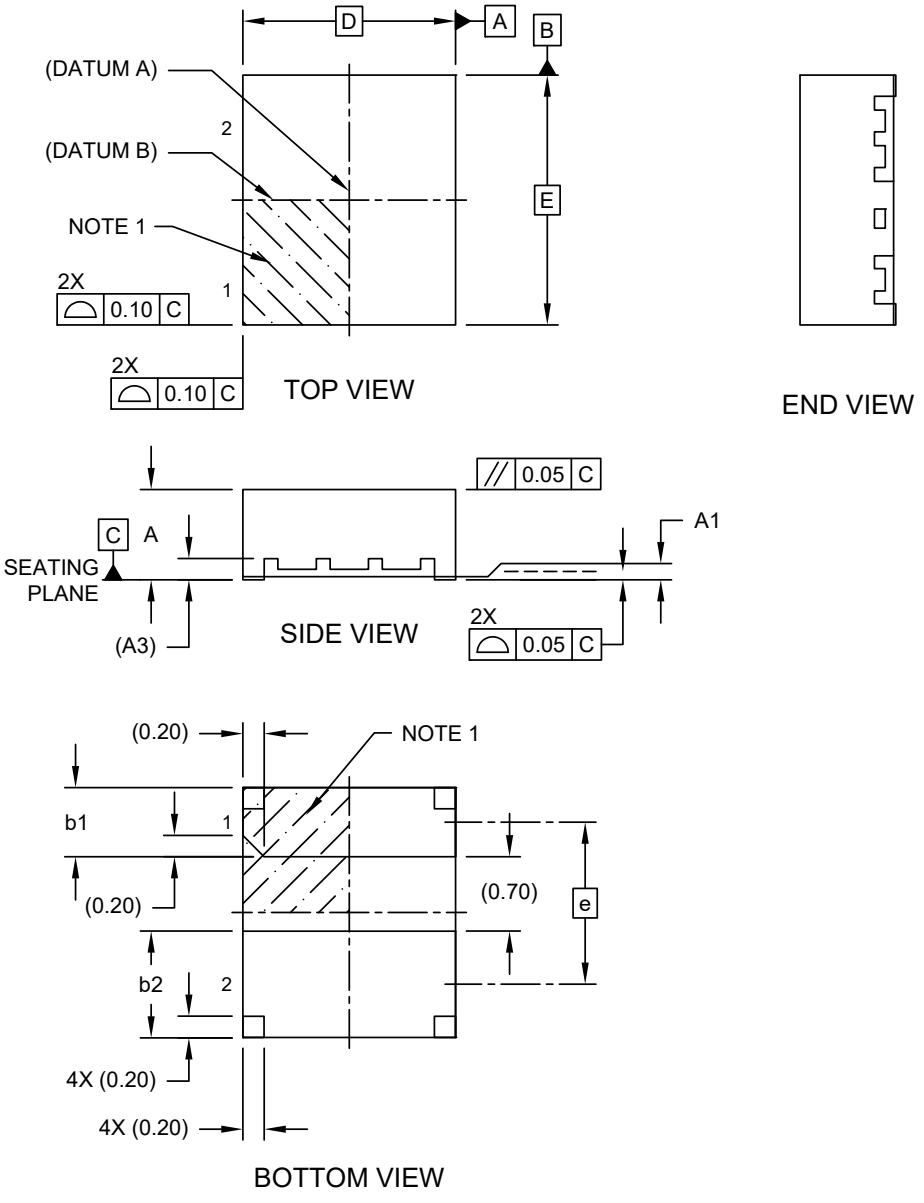
As part of Microchip's overall security features, the part marking for all crypto devices is intentionally vague. The marking on the top of the package does not provide any information as to the actual device type or the manufacturer of the device. The alphanumeric code on the package provides manufacturing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

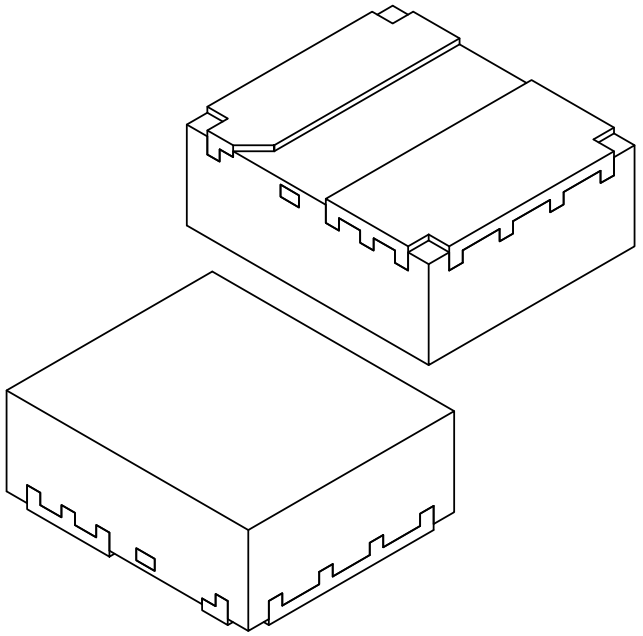
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



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

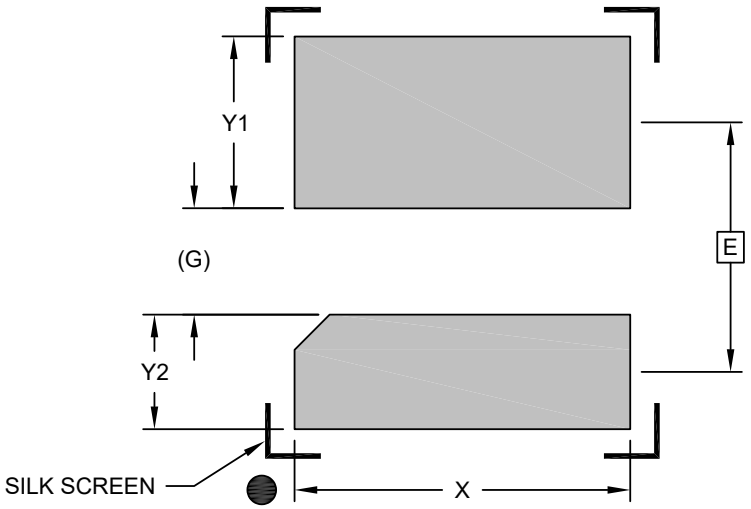
Notes:

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:

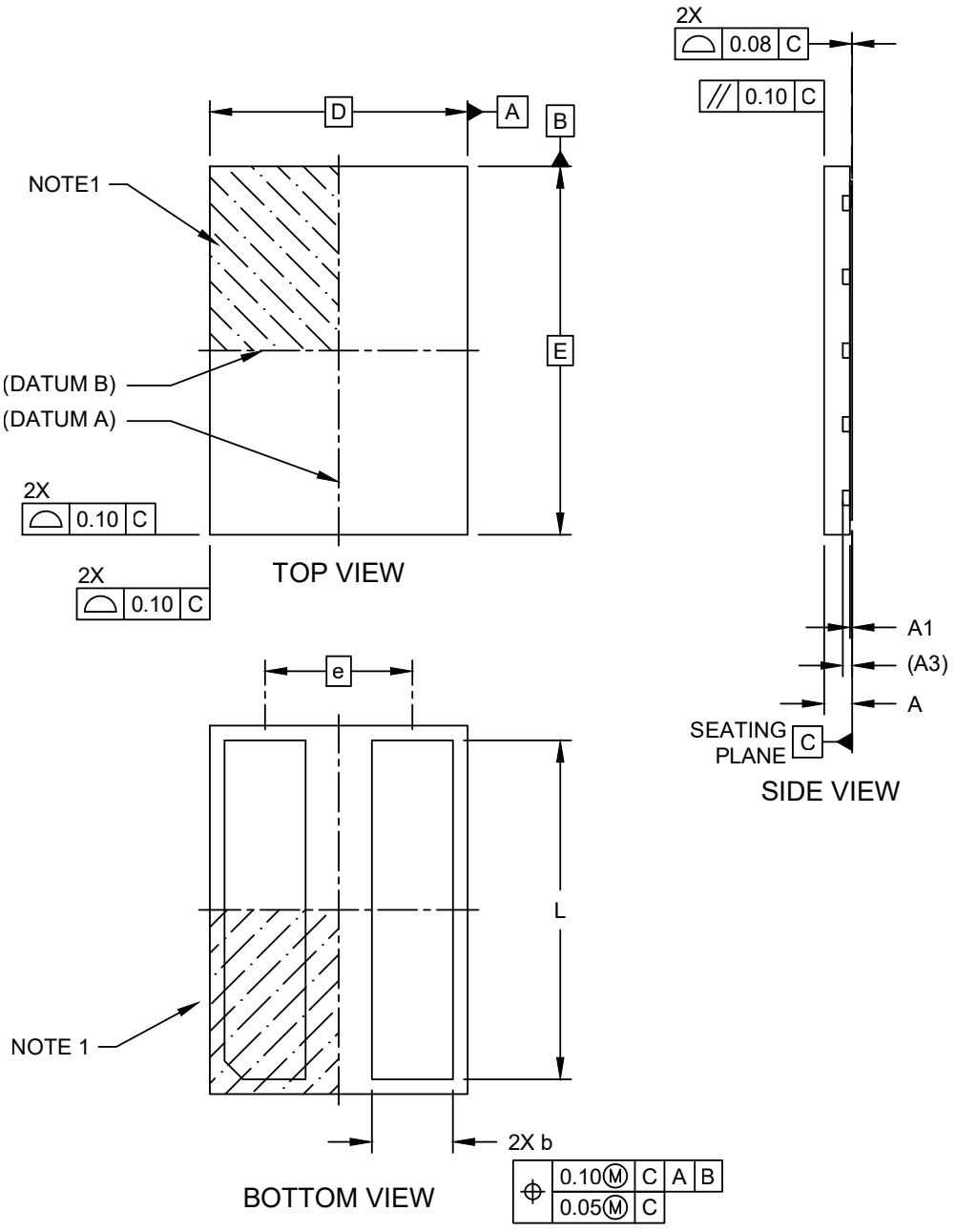
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
2. For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

Microchip Technology Drawing C04-2540 Rev A

6.2. 2-Lead XSFN Contact Package

2-Lead Extremely-Thin Single Flatpack No-Leads (9TW) 5x3.5x0.43mm [XSFN]

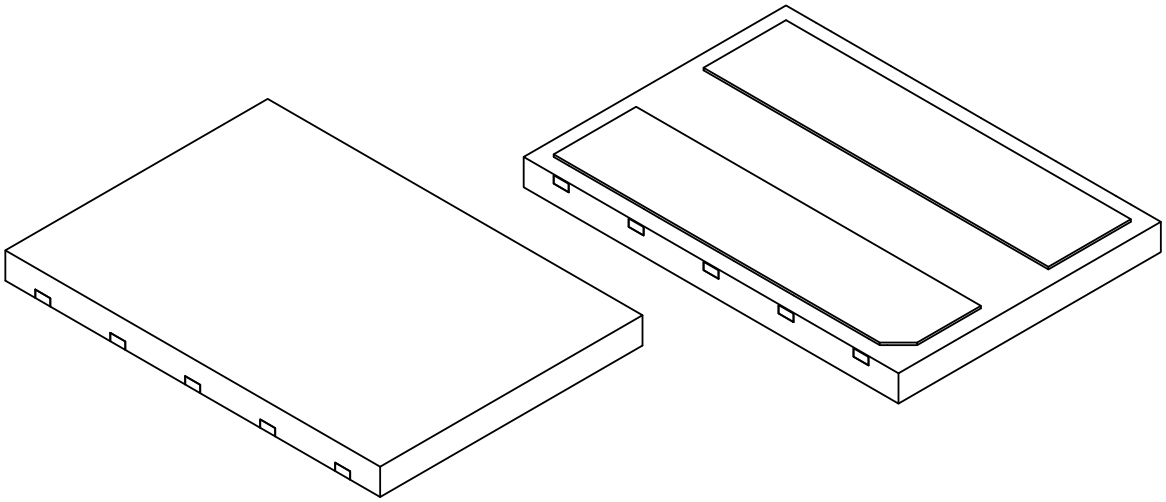
Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing C04-00689 Rev A Sheet 1 of 2

2-Lead Extremely-Thin Single Flatpack No-Leads (9TW) 5x3.5x0.43mm [XSFN]

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		2.00 BSC	
Overall Height	A	0.33	0.38	0.43
Standoff	A1	0.00	-	0.05
Terminal Thickness	A3		0.127 REF	
Overall Length	D		3.50 BSC	
Overall Width	E		5.00 BSC	
Terminal Width	b	1.00	1.10	1.20
Terminal Length	L	4.50	4.60	4.70

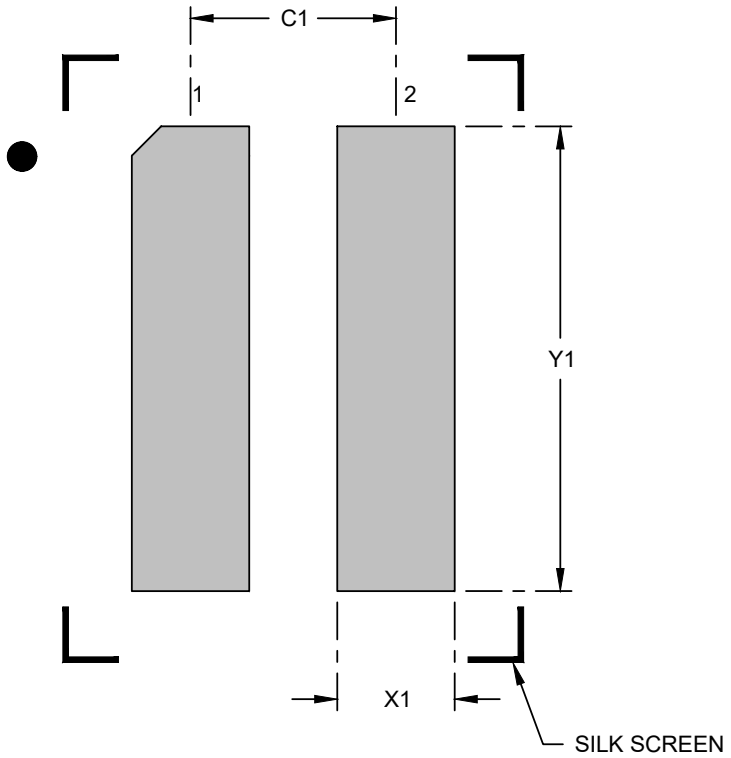
Notes:

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

Microchip Technology Drawing C04-00689 Rev A Sheet 2 of 2

2-Lead Extremely-Thin Single Flatpack No-Leads (9TW) 5x3.5x0.43mm [XSFN]

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 Pad Spacing	C1		2.10	
Contact Pad Width (X2)	X1			1.20
Contact Pad Length (X2)	Y1			4.75

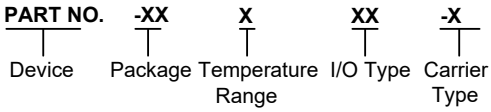
Notes:

1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. The theoretically exact value is shown without tolerances.
2. For best soldering results, please refer to the current industry standard IPC-7093.

Microchip Technology Drawing C04-02689 Rev A

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.



Device:	ECC206: Cryptographic Co-processor with Secure Hardware-based Key Storage	
Package Options	MC	2-Pad VSFN 2 mm x 2.35 mm Contact Package
	MX	2-Pad XSFN 5 mm x 3.5 mm Contact Package
Temperature Range	V	Extended Industrial Temperature Range. -40°C to 105°C
I/O Type	CZ	Single Wire Interface
Carrier Type	B	Bulk units in Canister

Examples:

- ECC206-MCVCZ-B: 2-Pad VSFN Contact package, Singe-Wire, Bulk, 10,000 devices per canister
- ECC206-MXVCZ-B: 2-Pad XSFN Contact package, Singe-Wire, Bulk, 10,000 devices per canister

Notes:

1. Carrier Type 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. Check www.microchip.com/packaging for small-form factor package availability or contact your local Sales Office.

8. Revision History

Revision C (February 2026)

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

- Features:
  - Updated random number generator bullet to indicate a True Random Number Generator (TRNG)
  - Corrected SWI-PWM speed to 100 kbps
  - Added XSFN package
- Use Cases: Updated Use Cases
- Random Number Generator (RNG):
  - Updated to indicate that the RNG is a TRNG
  - Added ESV and CAVP certification information
  - Updated SP 800-90C to the released version of the spec
- ECC206 Trust Platform Variants and Provisioning Services: Added EV14Y33A Evaluation Kit
- Package Drawings: Added XSFN package outline drawings
- Product Identification System
  - Updated for XSFN package
  - Updated ordering information to “Carrier Type”

Revision B (February 2025)

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

- DC Parameters: Single-Wire Interface – Parasitic Power Mode: Added Theta-JA for 2-Pad VSFN package
- Product Identification System: Product identification is now a separate section and not part of the 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: 979-8-3371-2706-4

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

ECC206