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

MICROCHIP

ATTPM20P

Trusted Platform Module (TPM) 2.0 - SPI Interface

Introduction

The Microchip ATTPM20P is a fully integrated security cryptoprocessor designed to be integrated into personal computers, embedded systems and IoT platforms. It implements version 2.0 of the Trusted Computing Group® (TCG) specification for Trusted Platform Modules (TPM).

Features

- Compliant to the Trusted Computing Group (TCG) Trusted Platform Module (TPM) Version 2.0, r116 Trusted Platform Module Library
- Single-Chip Turnkey Solution
- Hardware Asymmetric Crypto Engine
- Microchip ARM® M0+Microprocessor
- Internal FLASH Storage for Keys
- Serial Peripheral Interface (SPI) Protocol up to 36 MHz
- Secure Hardware and Firmware Design and Device Layout
- FIPS-140-2 Module Compliant Including the High-Quality Random Number Generator (RNG), HMAC, AES, SHA, ECC, and RSA Engines
- 8-pad UDFN Package for the Industry Smallest TPM 2.0 Device
- Offered in Commercial (0°C to +70°C) Temperature Range 1.8V to 3.3V Supply Voltage
- Offered in Industrial (-40°C to +85°C) Temperature Range 3.3V Supply Voltage
- Cryptographic Support for:
  - HMAC
  - AES-128
  - SHA-1
  - SHA-256
  - ECC BN_P256, ECCNIST_P256
  - RSA 1024-2048 bit keys
- 16 KB of User-Accessible Nonvolatile Memory
- X.509 EK Certificates (*Optional*)
- Pre-Generated Endorsement Keys

Table of Contents

1. Pin Configurations and Pinouts

Table 1-1. Pin Configuration

Pin Name	Function
V_{CC}	3.3V Supply Voltage
GND	Ground
MISO	SPI Slave Data Output
MOSI	SPI Slave Data Input
PIRQ#	SPI Interrupt Requests
SPI_CLK	SPI Clock Input
SPI_CS#	SPI Chip Select
SPI_RST#	SPI Reset Pin

Figure 1-1. 8-Pad UDFN Pinout Diagram

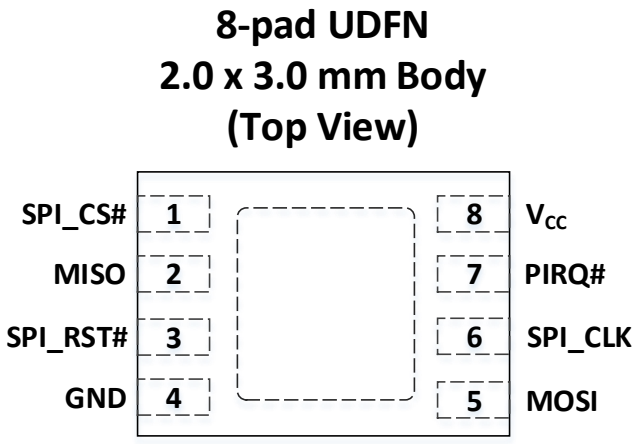


Table 1-2. Pin Descriptions

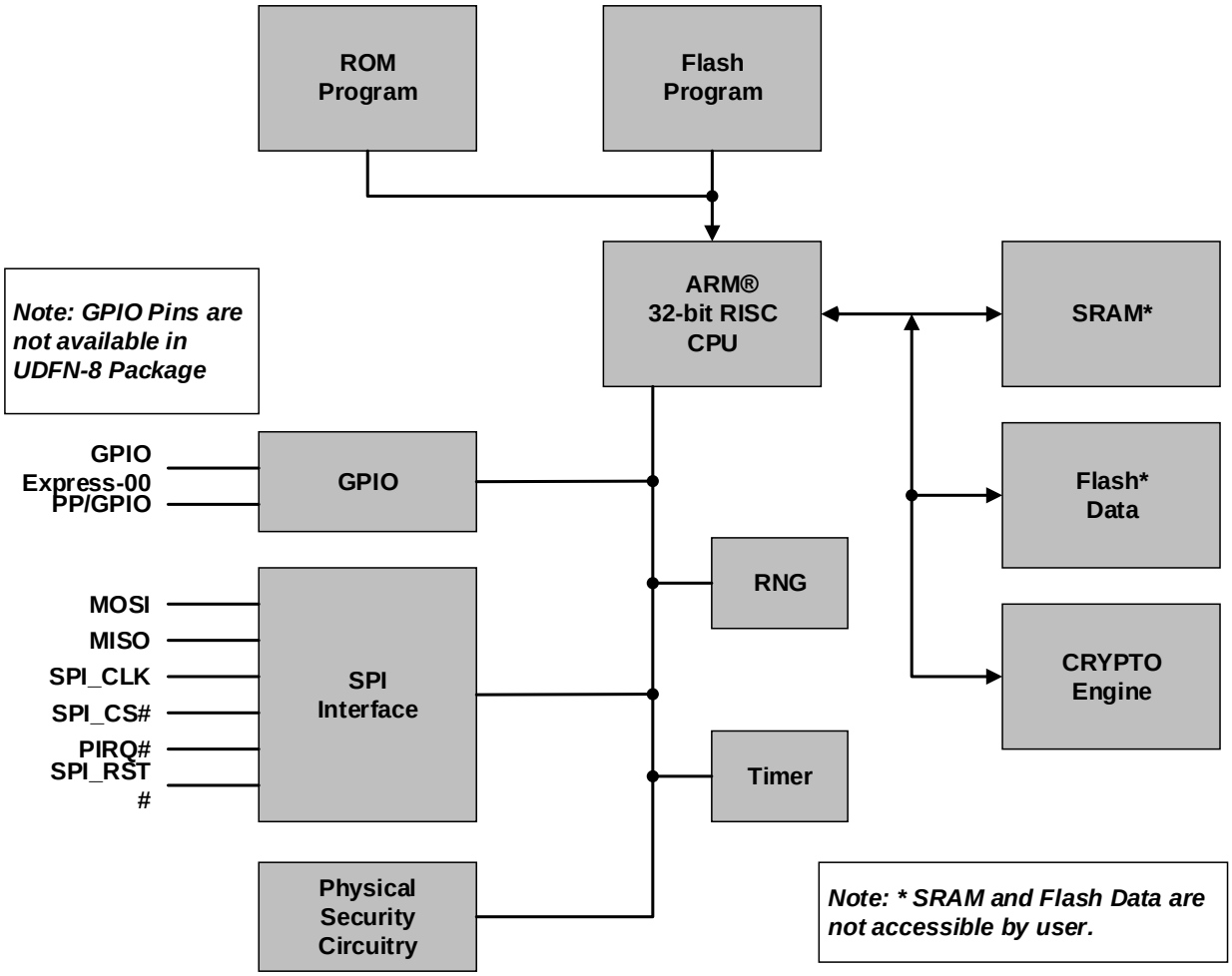
Pin	Pin Type	Description
V_{CC}	Power	Power Supply, 3.3V. Proper decoupling is required.
GND	Power	System Ground.
MISO	Output	Master In Slave Out. This pin serves as the SPI Data Output from the TPM.
MOSI	Input	Master Out Slave In. This pin serves as the SPI Data Input to the TPM.

.....continued

Pin	Pin Type	Description
PIRQ#	Open Drain Output	SPI Interrupt Pin, active-low. This pin is used by the TPM to assert interrupts. If unused, this pin should be tied to ground directly or through a 4.7 kΩ resistor.
SPI_CLK	Clock Input	Input Clock to drive the SPI bus. This pin should be asserted high for power savings when the TPM is not in use.
SPI_CS#	Input	SPI_CS# Chip Select, active-low. The TPM device will be selected when the chip select is asserted LOW.
SPI_RST#	Input	SPI Reset Pin, active-low. Pulsing this signal low resets the internal state of the TPM, and is equivalent to removal/restoration of power to the device. The required minimum reset pulse width is 2 µs. On power-up, it is critical that reset be kept active-low until V_{CC} and SPI_CLK stabilize. To be compliant with TCG requirements, this pin needs to be tied to system reset. TPM_Init is indicated by asserting this pin.

2. Block Diagram

Figure 2-1. Block Diagram



Random Number Generator

The ATTPM20P includes a hardware Random Number Generator (RNG), configured as a FIPS Deterministic Random Bit Generator (DRBG) that is used for key generation and TCG protocol functions. The RNG is also available to the system to generate random numbers that may be needed during normal operation.

Physical Security

The ATTPM20P has voltage and temperature tampers, an active shield and other physical security measures built into the device.

TCG Documentation

The ATTPM20P has been designed to be compliant with the Trusted Computing Group TPM 2.0 specification. Full documentation for TCG primitives can be found in the TCG Trusted Platform Module Library, Parts 1 to 3, on the TCG website: https://www.trustedcomputinggroup.org. TPM features specific

to PC client platforms are specified in TCG PC Client Platform TPM Profile (PTP) specification, also available on the TCG website.

Turnkey Solution

The ATTPM20P is offered to OEM and ODM manufacturers as a turnkey solution, including the firmware integrated on the chip. If custom firmware requirements are needed please contact Microchip Sales for more information.

3. Design Considerations

The following sections provide considerations when implementing the ATTPM20P into a given system.

3.1 SPI Bit Order

The bit order on the SPI Interface is Most Significant bit (MSb) first.

3.2 TPM SPI is Slave Only

The TPM SPI Interface is always configured to be in Slave mode.

3.3 Wait State

The TPM may insert Wait states per the TCG PC Client specification.

3.4 Available Key Storage

The ATTPM20P provides support for the loading of up to ten 2048-bit RSA or ECC keys. These key slots are in addition to the root keys allocated for the Platform, Storage, and Endorsement Hierarchies (i.e PPK, SRK, and EK).

3.5 Standard Mode Self-Test

Following a power-up event or a reset, the TPM will execute a series of self-tests of the TPM capabilities. ATTPM20P splits the TPM power-on self-tests into two groups as defined by the PTP. The initial group is executed immediately upon TPM power-up. The initial ATTPM20P self-test includes verification of the RNG and the SHA capabilities for secure boot operations.

The remaining tests of critical internal resources are performed at a later time, either:

- After the TPM2_SelfTest command is issued, or
- Upon receipt of the TPM2_IncrementalSelftest command, or
- Receipt of a command that requires TPM resources that were not tested.

In the event that a TPM command calls an untested resource, the TPM may return TPM_RC_TESTING and automatically complete internal self-test operations. The requesting software will then be required to resend the original command.

4. TCG PC Client Platform TPM Profile (PTP) Specification Summary

The Microchip TPM SPI communications protocol is implemented in accordance with the TCG PC Client Platform TPM Profile (PTP) Specification 1.3. A complete description of the protocol is contained in the specification available at www.trustedcomputinggroup.org. Application development and platform system design should be based on the TCG PTP specification.

Note: The TPM_DID_VID_x register contains Device ID (DID) and Vendor ID (VID) information. The VID register contents are assigned by the TCG Administration and contain the hex string 01 01 01 04. In the ATTPM20P, the DID register contains the device ID information and is set to 03 02 00 06. The ATTPM20P contains hardware and firmware revision information for the TPM in the TPM_RID_x register.

5. TCG TPM Command Data Bytes Transfer Format

5.1 TCG TPM Command Protocol

The TPM command protocol, as defined by the TCG TPM specification, specifies an initial predefined sequence of 10 data bytes for all commands transmitted to the TPM and also for all responses returned by the TPM. A required component of this 10-byte sequence is commandSize, which specifies the total number of data bytes in the command input or the response output.

The TPM uses a combination of commandSize and the master deasserting SPI_CS# inactive high to define the termination point of all input and output sequences. After the input or output sequence has completed, the TPM will automatically enter an Idle (Wait) state until the next communication is received from the master. A new input or output sequence is initiated by the master asserting SPI_CS# active-low.

5.2 TCG Command - Incoming Operands and Sizes

Every TCG command begins with 10 initial bytes that contain information common to all commands:

- tag (two bytes) — Specifies the authorization session type for the command.
- commandSize (four bytes) — Total number of input bytes including tag and commandSize.
- commandCode (four bytes) — Command code as defined in TCG TPM specification.

Following the 10-byte preamble, the SPI Master will continue to transmit the remaining command data bytes as specified by the TCG TPM specification until the total number of bytes reaches commandSize.

Table 5-1. Command Data Written to the TPM

tag<0>	tag<1>		
commandSize<0>	commandSize<1>	commandSize<2>	commandSize<3>
commandCode<0>	commandCode<1>	commandCode<2>	commandCode<3>

5.3 TCG Command - Outgoing Operands and Sizes

The TPM will respond to every TCG command with 10 initial bytes that contain information common to all commands:

- tag (two bytes) — Specifies the authorization session type for the command.
- responseSize (four bytes) — Total number of output bytes including tag and responseSize.
- responseCode (four bytes) — The return code of the operation.

Following the 10-byte preamble, the TPM will continue to output data until the total number of data bytes reaches responseSize. Depending on the command, zero bytes of data are possible. After output of the final data byte and the master writing Command_Ready to a one, the TPM will enter an Idle state until the next valid SPI command sequence is initiated by the master.

Table 5-2. Response Data Read from the TPM

tag<0>	tag<1>		
responseSize<0>	responseSize<1>	responseSize<2>	responseSize<3>
responseCode<0>	responseCode<1>	responseCode<2>	responseCode<3>
data<0>	data<1>	...	...
data<responseSize-3>	data<responseSize-2>	data<responseSize-1>	data<responseSize>

6. Background Operations

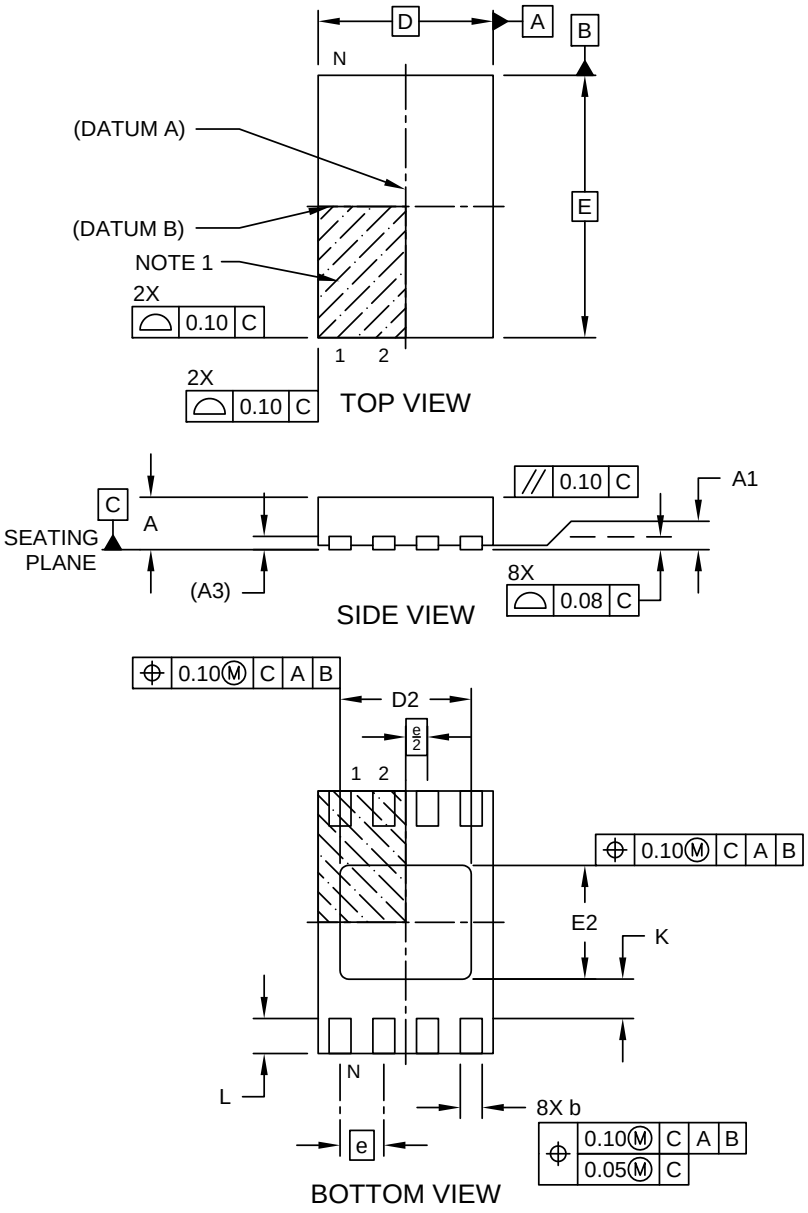
The ATTPM20P enters the Idle mode between the end of execution of an initial TCG command and preparation to receive the next command. During Idle mode, the TPM may automatically begin execution of background operations in order to reduce execution time when those capabilities are required in the future. Background operations are aborted if activity is detected on the data bus.

7. Package Drawings

7.1 8 Pin UDFN Package Drawing

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

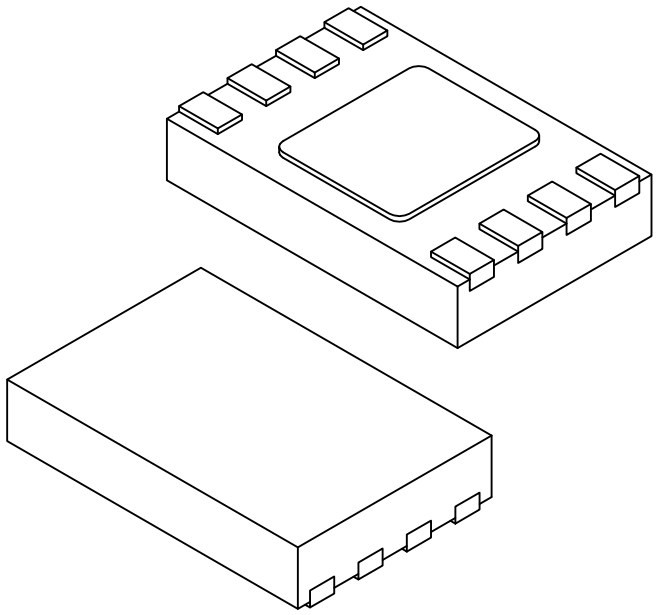
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



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

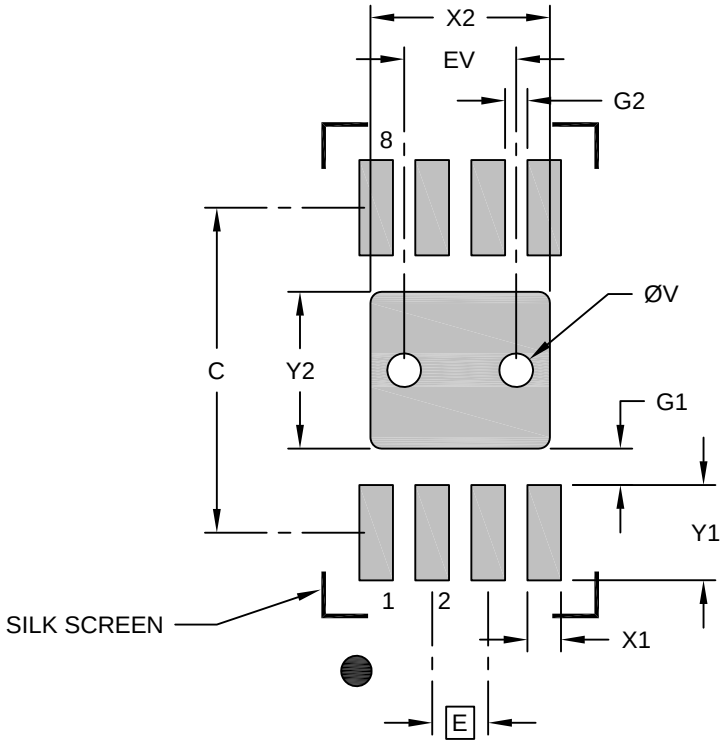
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

   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

7.2 TPM 2.0 Standard Packages

The TCG TPM 2.0 working group has defined an industry standard 32 QFN pinout. For more information on obtaining this product in a TCG standard package format please contact Microchip Sales.

7.3 Package Marking

As part of Microchip's overall security features, the part mark for all CryptoAuthentication™ 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. The packaging mark should not be used as part of any incoming inspection procedure.

8. Revision History

Revision A (December 2018)

- Original release of this document. Generated from the full version of the Trusted Platform Module (TPM) 2.0 - SPI Interface data sheet. Microchip Doc#: DS40002064.

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.	-XX	XXX	-XX	(-X)
Device	Temp Range	Package Code	Mfg ID	Shipping Option

Device:	ATTPM20P: TPM 2.0 Cryptographic processor with SPI Interface	
Temperature Range	G3	Commercial Range 0°C to +70°C
	H3	Industrial Range -40°C to +85°C
Package Options	MA1	8-Pad 2 x 3 x 0.6 mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat NoLead Package (UDFN)
MFG Code	-10	Pre-generated Endorsement Key
Tape and Reel Options		Tape and Reel in 3K quantity

PIS Examples:

ATTPM20P-G3MA1-10	ATTPM20P SPI Device, Commercial Temp Range, UDFN Package, Pre-generated Endorsement Key, 3K Tape and Reel
ATTPM20P-H3MA1-10	ATTPM20P SPI Device, Industrial Temp Range, UDFN Package, Pre-generated Endorsement Key, 3K Tape and Reel

PIS Notes:

1. No Special code for 3K Tape and Reel.

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

Trademarks

ISBN: 978-1-5224-3960-8

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: 47-72884388 **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

X-ON Electronics

Largest Supplier of Electrical and Electronic Components

Click to view similar products for Security ICs / Authentication ICs ***category:***

Click to view products by Microchip ***manufacturer:***

Other Similar products are found below :

A1007TL/TA4STZ DS2476Q+T DS28C36Q+T DS28C22Q+T DS2401-SL+T&R DS28E35P+ ATECC608B-RBHCZ-B DS28E18Q+T W74M12JWSSIQ ATECC508A-MAHAW-S SLB9656TT12FW432XUMA1 SLB9660XT12FW440XUMA2 SLS32AIA020A4USON10XTMA2 SLB9645XT12FW13332XUMA1 DS2401T&R DS1990R-F5# DS2411P+T&R A1006TL/TA1NXZ ATAES132A-SHER-B ATSHA204A-RBHCZ-B ATECC608A-SSHDA-T A1006UK/TA1NXZ ATAES132A-MAHEQ-S ATECC608A-MAHCZ-S IPL-CHP ATAES132A-MAHER-S AT88SC118-SH-CN-T AT88SC118-SH-CM-T SE050A2HQ1/Z01SHZ SE050A1HQ1/Z01SGZ SE050B2HQ1/Z01SFZ ATECC608A-MAHCZ-T AT88SC118-SH-CM AT88SC118-SH-CN ATAES132A-MAHER-T ATAES132-SH-EQ ATAES132-SH-ER-T ATECC508A-MAHCZ-T ATAES132A-SHEQ-B ATAES132A-MAHER-T ATECC108A-SSHDA-B ATECC508A-SSHCZ-B ATECC508A-SSHDA-B DS2460S+ SLB9645TT12FW13333XUMA2 SLB9665TT20FW563XUMA3 SLB9670VQ20FW785XTMA1 SLM9670AQ20FW1311XTMA1 SLS32AIA010MLUSON10XTMA2 SLS32AIA010MKUSON10XTMA2