TA010-TFLXWPC CryptoAutomotive™ Data Sheet

TA010-TFLXWPC

Product Page Links

Introduction

The TA010-TFLXWPC is a pre-provisioned variant of the TA010 product family. The TrustFLEX secure element is part of Microchip's family of generically-provisioned, security-focused devices. The device configuration is designed to meet the authentication requirements of the Wireless Power Consortium (WPC) Qi® 1.3 and Qi 2.x standards.

The TA010-TFLXWPC configuration is defined to meet the basic authentication needs of Qi transmitters that provide authentication. The device supports a single WPC Slot. Each device data slot has a specific use and will be provisioned with the appropriate information.

This data sheet provides the data slot and subzone configuration information that is unique to the TA010-TFLXWPC. The majority of information is predefined, and only a limited number of configuration options can be specified. An application section discussing Microchip's hardware and software tools that can aid in developing an application is also provided, with additional links to the location of the tools.

Features

- Cryptographic Authentication Device with Secure Hardware-Based Key Storage:
  - Protected storage for private key, certificates 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 Digest Generation
- Internal Asymmetric Key Generation
- Internal High-Quality NIST SP 800-90A/B/C True Random Number Generator (TRNG) (NIST Certified)
- JIL High Rating – Validated to JIL Application of Attack Potential to Smartcards and Similar Devices, Version 3.1
  - Achieved through tamper-resistant countermeasures to resist environmental, non-invasive and invasive Fault attacks
    - Active shield to protect against invasive attacks
    - Internal memory encryption and scrambling
    - Low- and high-supply voltage tampers
    - Low- and high-temperature tampers
  - Clone-Resistant Features
- Compliant with WPC Qi 1.3 and Qi 2.x standards
  - WPC slot 0 P256 ECC private key
  - Full storage of WPC Slot 0 product unit certificate
  - Storage of WPC Slot 0 certificate chain digest for rapid authentication

© 2023-2025 Microchip Technology Inc. and its subsidiaries

- Monotonic Counter with the Maximum Count Value of 10,000
- Unique 72-bit Serial Number
- 400 kHz Fast mode I^2C interface
- Voltage Supply Range: 1.65V to 5.5V
- 130 nA Nominal Sleep Current
- AEC-Q100 Automotive Qualified
- Automotive Grade 1 Temperature Range: -40°C to +125°C Ambient Operating Range
- ESD >4 kV Human Body Model (HBM)
- Packaging Options: 8-Pad VDFN (2 mm x 3 mm) with wettable flanks, 8-lead SOIC

Use Cases

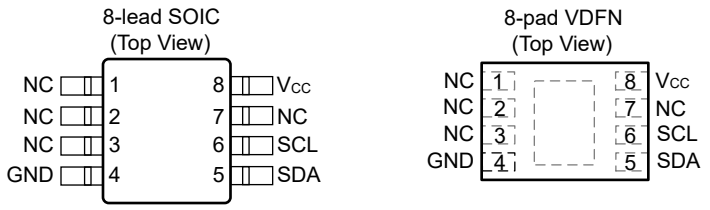
- WPC Qi Power Transmitter Authentication

Pin Configuration and Pinouts

Table 1. Pin Configuration

Package: 8-Lead SOIC or 8-Pad VDFN		
Pin #	Function	I^2C
1-3,7	No Connect	NC
4	Ground	GND
5	Serial I/O	SDA
6	Serial Clock	SCL
8	Supply	VCC

Figure 1. Pinouts[1]



Note:

1. Connecting the exposed backside paddle of the VDFN package to GND is recommended.

NOTICE The UDFN Package has been deprecated for use with the TA010-TFLXWPC in favor of the VDFN package with wettable flanks. The board land pattern is identical for both packages. The UDFN package will continue to be supported for existing customers on existing programs.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

Table of Contents

Introduction....1

Features....1

Use Cases....2

Pin Configuration and Pinouts....2

1. Wireless Power Consortium....5
   - 1.1. Wireless Power Consortium Terminology....5

2. Overview....7
   - 2.1. Device Features....7
   - 2.2. Cryptographic Operation....7

3. EEPROM Memory....8
   - 3.1. EEPROM Data Zone....8
   - 3.2. EEPROM Configuration Zone....8

4. Security Information....10
   - 4.1. Cryptographic Standards....10
     - 4.1.1. SHA-256....10
     - 4.1.2. HMAC/SHA-256....10
     - 4.1.3. Elliptic Curve Digital Signature Algorithm (ECDSA)....10
   - 4.2. Security Features....10
     - 4.2.1. Physical Security....10
     - 4.2.2. Random Number Generator (RNG)....10

5. I/O Interfaces....11
   - 5.1. General I/O Information....11
   - 5.2. I^2C Interface....12
     - 5.2.1. I/O Conditions....13
       - 5.2.1.1. Device is Asleep....13
       - 5.2.1.2. Device is Awake....13
     - 5.2.2. I^2C Bus Transactions....13
       - 5.2.2.1. Data Input and Output Frames....13
     - 5.2.3. Split I^2C Transactions....15
     - 5.2.4. I^2C Synchronization....15
   - 5.3. I/O Transmission to the TA010-TFLXWPC....16
     - 5.3.1. Word Address Values....17
     - 5.3.2. Sleep Sequence....17
     - 5.3.3. Command Completion Polling....17
   - 5.4. I/O Transmission from the TA010-TFLXWPC....17

6. Electrical Characteristics....19
   - 6.1. Absolute Maximum Ratings....19
   - 6.2. Reliability....19
   - 6.3. AC Parameters....19
     - 6.3.1. AC Parameters: All I/O Interfaces....19

© 2023-2025 Microchip Technology Inc. and its subsidiaries

6.3.2. AC Parameters: I²C Interface....20
6.4. DC Parameters....21
6.4.1. DC Parameters: All I/O Interfaces....21

7. Command Descriptions....23
7.1. `Counter` Command....23
7.2. `Delete` Command....23
7.3. `GenKey` Command....23
7.4. `Info` Command....23
7.5. `Lock` Command....24
7.6. `Nonce` Command....24
7.7. `Read` Command....24
7.8. `SelfTest` Command....24
7.9. `SHA` Command....24
7.10. `Sign` Command....24
7.11. `Write` Command....24

8. Application Information....26
8.1. Use Cases....26
8.2. WPC Engagement....26
8.3. Development Tools....27
8.3.1. Trust Platform Design Suite....27
8.3.2. Hardware Tools....27
8.3.3. CryptoAuthLib....28

9. Package Marking Information....30

10. Package Drawings....31
10.1. 8-Pad VDFN....31
10.2. 8-Lead SOIC....34

11. Revision History....37

12. Product Identification System....39

Microchip Information....40
Trademarks....40
Legal Notice....40
Microchip Devices Code Protection Feature....40

Product Page Links....41

© 2023-2025 Microchip Technology Inc. and its subsidiaries

1. Wireless Power Consortium

The Wireless Power Consortium has developed wireless power standards to support multiple ecosystems. The Qi standard defines a complete ecosystem for the deployment of wireless charging for mobile devices.

Starting with version 1.3 of the Qi specification, authentication was defined as a requirement for chargers that wish to charge at a power level higher than 5W. Version 1.3 of the specification allows charging of mobile devices up to 15W. All chargers are allowed to initially charge at the 5W level without authentication. Authentication must occur to allow charging at a level of higher than 5W. Starting with the Qi 2.2 specification, the power level can be increased up to 25W, with even higher power level standards in definition and development. Qi 2.x also supports the Magnetic Power profile. There is no difference in the authentication requirements.

Each of these ecosystems requires the following to create a chain of trust from the root to the WPC transmitter.

1. WPC root certificate – Consists of the root public key and root certificate.
2. WPC manufacturing certificate – Consists of a manufacturing certificate signed by the private key of the root certificate.
3. WPC product unit certificate – Consists of the product unit certificate signed by the private key of the WPC manufacturing certificate.

The WPC certificates follow the X.509 format. For WPC Slots 0 and 1, the certificate format is fixed. For WPC Slots 2 and 3, the format is not defined and allows for proprietary use of these certificate chain slots.

To participate in one or both of the WPC wireless charging ecosystems, one must be a member of the Wireless Power Consortium. Each ecosystem is unique and requires a separate membership fee. Additional information on the standards and on the consortium can be found on the WPC website: www.wirelesspowerconsortium.com/.

1.1. Wireless Power Consortium Terminology

The following terminology used in this data sheet is included to aid in understanding items associated with the WPC Qi authentication standard. This section is intended to reflect the information in the WPC standard but, in all cases, the standard takes precedence over this section of the document.

Power Receiver	The device that is charged by the power transmitter and provides communication to the power transmitter for the purpose of authentication or to control the power charging of the power receiver.
Power Transmitter	The device that is used to communicate with and provide power to the power receiver. The secure storage subsystem resides within the power transmitter.
Qi (pronounced "chee")	The designator used by the WPC for the standards associated with wireless charging of mobile devices.
Revocation Sequential Identifier (RSID)	The RSID is a unique identifier stored in the WPC device unit certificate that uniquely identifies a given transmitter and can be used to revoke high power or complete operational use of a power transmitter for noncompliance reasons.
Secure Storage Subsystem (SSS)	The device used to store the security information used to authenticate a wireless power transmitter. This can be considered a secure element or secure crypto device.
WPC Manufacturer	A company or entity licensed by the WPC to produce certified WPC power transmitters. All WPC manufacturers are required to sign a WPC manufacturer agreement.
WPC Manufacturing CA	A company licensed by the WPC to produce secure storage subsystems for use in certified WPC power transmitters. Microchip is a licensed manufacturing CA.
Wireless Power Consortium (WPC)	The standard body responsible for defining all aspects of wireless charging associated with the Qi standards and for licensing and certifying Qi-certified

© 2023-2025 Microchip Technology Inc. and its subsidiaries

	products. Membership in the WPC is required to produce Qi-compliant power transmitters or receivers. More information on the WPC can be found on the website: www.wirelesspowerconsortium.com/.
WPC Root Authority	The WPC Root Authority is the head of the WPC Qi certificate chain. All WPC manufacturing certificates will be signed by the Qi WPC Root authority.
WPC Slot	The WPC authentication specification defines a slot as the element that holds a WPC certificate chain. There are four possible slots (Slots 0-3) defined by the WPC authentication specification, but only Slot 0 is required and must hold a WPC certificate chain. If used, Slot 1 is also reserved for use as a WPC certificate chain. The format of Slots 2 and 3 is undefined and they are reserved for optional proprietary extensions. For the purpose of this document, the term “WPC Slot” will always be used when referring to a WPC certificate chain to distinguish it from the term “slot” used to indicate a data slot in the TA010-TFLXWPC device.
WPC Slot Digest	A 32-byte digest of the entire certificate chain stored in a WPC Slot.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

2. Overview

2.1. Device Features

The TA010-TFLXWPC does not support all the capabilities defined in the WPC Authentication specification. The device was developed to support the most common use case and only supports WPC Slot 0. The EEPROM array can be used to store the WPC Slot 0, ECC P-256 key, a full WPC Device Unit Certificate and the WPC Slot 0 digest. Write access to the various data zone slots and configuration subzones of memory can be restricted once written.

The device has an I^2C serial interface that operates at speeds up to 400 kHz. The interface is compatible with the Standard and Fast modes' I^2C interface specifications.

Each TA010-TFLXWPC unit is shipped with a unique 72-bit serial number. The TA010-TFLXWPC 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.

The TA010-TFLXWPC has a monotonic counter that can be used by the host system. The counter default programming allows it to be incremented up to 10,000 times. If so desired, this value can be set to a lower value.

The host system can also use the SHA command to generate either a SHA or HMAC Digest. If an HMAC digest needs to be generated, then an HMAC key needs to be written to the device.

2.2. Cryptographic Operation

The TA010-TFLXWPC 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 TA010-TFLXWPC 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 TA010-TFLXWPC 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

© 2023-2025 Microchip Technology Inc. and its subsidiaries

3. EEPROM Memory

The EEPROM memory is divided into data zone with slots and a configuration zone made up of several subzones. Each data slots or configuration subzones can be locked independently.

Terms discussed within this document will have the following meanings:

Table 3-1. Document Terms

Term	Meaning
Block	A single 256-bit (32-byte) area of a slot in the Data zone. Data slots will have between 1 and 10 blocks. The industry SHA-256 documentation also uses the term “block” to indicate a 512-bit section of the message input. Within this document, this convention is used only when describing hash input messages.
Configuration Subzone	A portion of the Configuration zone that stores device identification or configuration information. Each subzone can be individually locked.
Data Zone Slot	A separate portion of the Data zone that stores customer-specific data. Each slot can be individually locked.
KeyID	KeyID is equivalent to the slot number for those slots designated to hold key values.
mode[b]	Indicates bit b of the parameter mode.
SRAM	Contains input and output buffers.
LSB/MSB	Least Significant Byte/Most Significant Byte.
LSb/MSb	Least Significant bit/Most Significant bit.

3.1. EEPROM Data Zone

The Data Zone is defined to support WPC Slot 0 requirements for the Product Unit Certificate. The following table shows how the device is specified to meet the WPC requirements.

Table 3-2. Data Zone

Slot	Blocks	Bytes	Bits	Use	Notes
0	1	32	256	WPC Slot 0 ECC Private Key	No read/write access.
1	10	320	2560	WPC Slot 0 Product Unit Certificate	Writes allowed unless slot is locked. Slot is always readable.
2	2	64	512	WPC Slot 0 Digest	Writes allowed unless slot is locked. Slot is always readable.
3	1	32	256	HMAC Secret Key	Writes allowed unless slot is locked. No read access.

3.2. EEPROM Configuration Zone

The TA010-TFLXWPC configuration is largely fixed and cannot be modified by the customer. Relevant information about how the device is configured is shown below as well as the parameters that may be modified with the TPDS tools.

Remember: The configuration zone is divided into four subzones. These are designated throughout the document by CSZn, where n can be a value between 0 to 3 inclusive.

Device Configuration Information

- The serial number for each device is unique and stored in bytes [0:8] of configuration subzone #1. Default values of bytes [0:1] are 0x01 0x23 and byte [8] is 0xEE. All other bytes are unique.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

- The default 7-bit I^2C address is `0x38`. The I^2C address can be overwritten by writing CSZ3.
- The I/O levels are set to be V_{CC} referenced by default. This allows for the full operating voltage range to be available.
- Maximum command speed is enabled by setting the clock speed of the device to divide by 1.
- An HMAC key can be programmed into the device to allow for calculation of an HMAC Digest using the `SHA` command. The HMAC Key is not required for correct WPC operation.
- Monotonic counters are available for use by the system. By default, the counter is not attached to any keys.
- A Health Test Failure will be cleared after any time that a command fails as a result of a health test failure. If the failure symptom is transient, the command may pass when run a second time.

Modifiable Configuration Information

Through use of the TPDS tools, the following parameters may be modified provided the zones were not already locked.

- I^2C address
- I/O levels can be modified to have a fixed reference. This allows for the I^2C Bus to run at a lower voltage level than the TA010-TFLXWPC supply.
- The initial Counter value can be limited to something less than 10,000.
- The HMAC Key can be attached to the counter for limited use.
- Serial Number bytes [0:1] and byte [8] can be modified from their default values to uniquely identify a given customer or application, but the specific values used will be specified by Microchip.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

4. Security Information

4.1. Cryptographic Standards

TA010-TFLXWPC 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.

4.1.1. SHA-256

The TA010-TFLXWPC computes the SHA-256 digest based on the algorithm documented here:

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

Related Links

Command Descriptions

4.1.2. HMAC/SHA-256

TA010-TFLXWPC 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

4.1.3. Elliptic Curve Digital Signature Algorithm (ECDSA)

TA010-TFLXWPC 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

4.2. Security Features

4.2.1. Physical Security

The TA010-TFLXWPC incorporates a number of physical security features designed to protect the EEPROM contents from unauthorized exposure.

4.2.2. Random Number Generator (RNG)

The TA010-TFLXWPC 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.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

5. I/O Interfaces

The I²C interface uses the SDA and SCL pins to transfer commands/data/status to and from the TA010-TFLXWPC device. Data flow is controlled by the host controller.

Interface Terminology

Host:	The host MCU generates the command and controls the data flow on the bus to one or more client devices.
Client:	The TA010-TFLXWPC device always operates as a client device on the bus and cannot take control of the bus.
Device Address:	7-bit address used to address a client device. This is part of the first byte sent to a client device for each write or read transaction.
Open-Drain:	The TA010-TFLXWPC device has an open-drain output buffer where the bus is actively pulled low by the output buffer when data are read from the device but are passively pulled high by an external pull-up resistor.

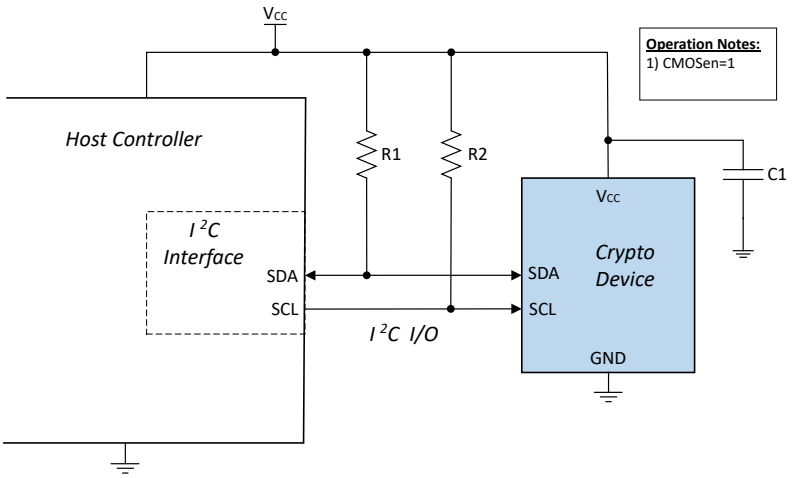
Remember: The I²C standard uses the terminology "Master" and "Slave". The equivalent Microchip terminology used in this document is "Host" and "Client", respectively.

5.1. General I/O Information

The TA010-TFLXWPC operates as a client device and utilizes an I²C to communicate with a host controller. The host device controls all read and write operations to the client device(s) on the serial bus.

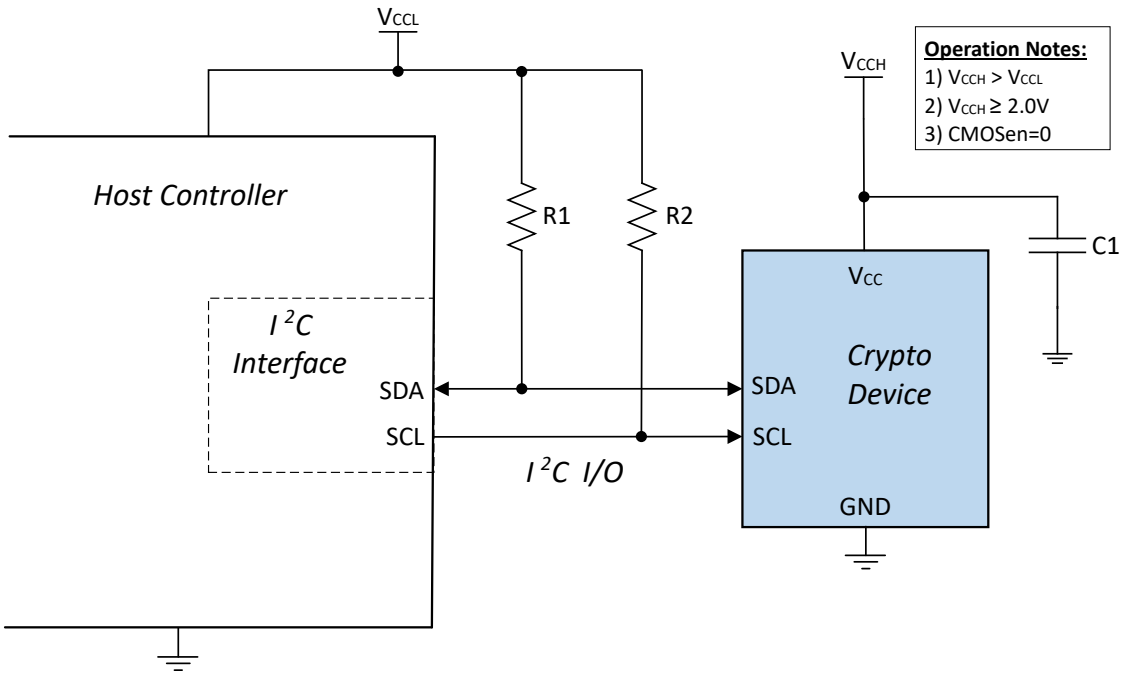
- **I²C Interface:**
  This mode is compatible with the I²C standard and with the Microchip AT24C16 Serial EEPROM interface. Two pins, Serial Data (SDA) and Serial Clock (SCL), are required. The I²C interface supports a bit rate of up to 400 kbps.

Figure 5-1. Application Diagram for Using the I²C Interface with CMOSen=1



© 2023-2025 Microchip Technology Inc. and its subsidiaries

Figure 5-2. Application Diagram for using Using the I²C Interface with CMOSen=0



Related Links
I2C Interface

5.2. I²C Interface

This interface is designed to be compatible at the protocol level with the Microchip AT24C16 Serial EEPROM operating at 400 kHz.

Tip: There are some differences between the two devices (for example, the TA010-TFLXWPC and AT24C16 have different default I²C addresses); therefore, it is recommended that designers read the respective data sheets carefully.

The SDA pin is normally pulled high with an external pull-up resistor because the TA010-TFLXWPC only includes an open-drain driver on its output pin. The host system may use either an open-drain or a totem pole driver. In the latter case, it must be tri-stated when the TA010-TFLXWPC is driving results on the bus. The SCL pin is an input and must be driven both high and low at all times by an external device or pulled high by an external resistor.

The serial interface is comprised of two signal lines: Serial Clock (SCL) and Serial Data (SDA). The SCL pin is used to receive the clock signal from the host, while the bidirectional SDA pin is used to receive command and data information from the host as well as to send data back to the host. Data are always latched into the TA010-TFLXWPC on the rising edge of SCL and always output from the device on the falling edge of SCL. Both SCL and SDA pins incorporate integrated glitch suppression filters and Schmitt Triggers to minimize the effects of input spikes and bus noise.

All command and data information is transferred with the MSb first. During bus communication, one data bit is transmitted every clock cycle and after eight bits (one byte) of data are transferred, the receiving device must respond with either an ACK or a NACK response bit during a ninth clock

© 2023-2025 Microchip Technology Inc. and its subsidiaries

cycle (ACK/NACK clock cycle) generated by the host. Therefore, nine clock cycles are required for every one byte of data transferred. There are no unused clock cycles during any read or write operation, so there must not be any interruptions or breaks in the data stream during each data byte transfer and ACK or NACK clock cycle.

During data transfers, data on the SDA pin must only change while SCL is low, and the data must remain stable while SCL is high. If data on the SDA pin change while SCL is high, either a Start or a Stop condition will occur. Start and Stop conditions are used to initiate and end all serial bus communication between the host and the client devices. The number of data bytes transferred between a Start and a Stop condition is not limited and is determined by the host. For the serial bus to be idle, both the SCL and SDA pins must be in the logic high state at the same time.

5.2.1. I/O Conditions

The device responds to the following I/O conditions:

5.2.1.1. Device is Asleep

When the device is asleep, it ignores all but the Wake condition. The Wake condition is as follows:

- Send Start condition
- Send Device Address
- Expect NACK
- Send Stop condition

The TA010-TFLXWPC will only exit Low-Power mode if the device address sent by the system microprocessor contains a client address that matches the address stored in the Config: Device_Address byte. The TA010-TFLXWPC will NACK the device address and ignore all subsequent bytes until t_{PU} expires.

Related Links

Data Input and Output Frames
AC Parameters: All I/O Interfaces

5.2.1.2. Device is Awake

When the device is awake, it honors the conditions listed in I2C Bus Transactions.

5.2.2. I²C Bus Transactions

Types of data transmitted over the I²C bus:

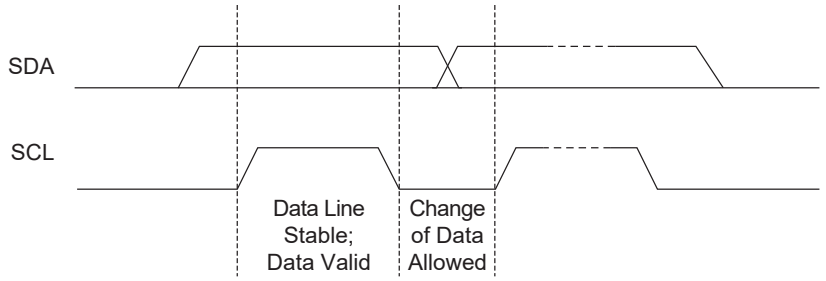
- Data '0'
- Acknowledge (ACK)
- Data '1'
- No Acknowledge (NACK)
- Start condition
- Stop condition

5.2.2.1. Data Input and Output Frames

- **DATA Zero**: If SDA is low and stable while SCL goes from low to high to low, a zero bit is transferred on the bus. SDA can change while SCL is low.
- **DATA One**: If SDA is high and stable while SCL goes from low to high to low, a one bit is transferred on the bus. SDA can change while SCL is low.

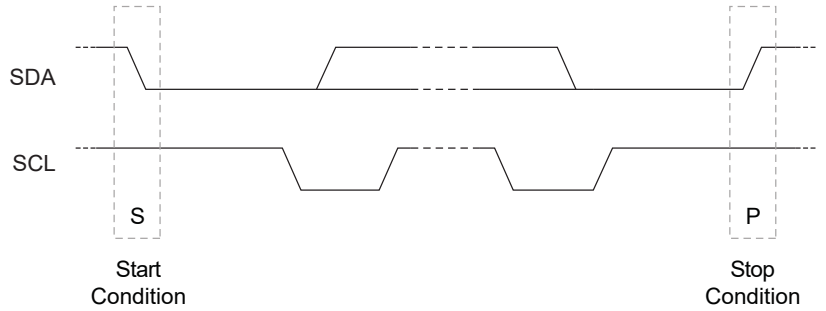
© 2023-2025 Microchip Technology Inc. and its subsidiaries

Figure 5-3. Data Bit Transfer on the I²C Interface



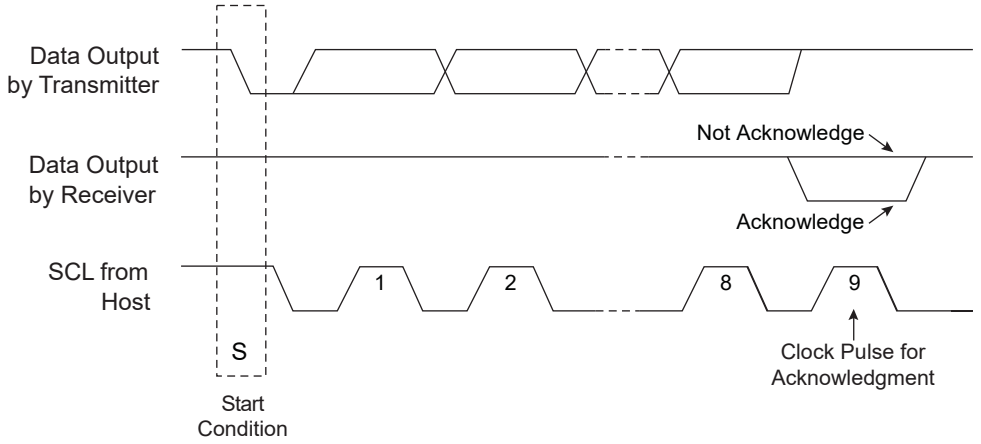
- **Start Condition**: A high-to-low transition of SDA with SCL high is a Start condition that must precede all commands.
- **Stop Condition**: A low-to-high transition of SDA with SCL high is a Stop condition. After this condition is received by the device, the current I/O transaction ends. On input, if the device has sufficient bytes to execute a command, the device transitions to the busy state and begins execution. The Stop condition must always be sent at the end of any packet sent to the device.

Figure 5-4. Start and Stop Conditions on the I²C Interface



- **Acknowledge (ACK)**: On the ninth clock cycle after every address or data byte is transferred, the receiver will pull the SDA pin low to acknowledge proper reception of the byte.
- **Not Acknowledge (NACK)**: Alternatively, on the ninth clock cycle after every address or data byte is transferred, the receiver can leave the SDA pin high to indicate that there was a problem with the reception of the byte or that this byte completes the group transfer.

Figure 5-5. NACK and ACK Conditions on the I²C Interface



Multiple TA010-TFLXWPC devices can easily share the same I²C interface signals if the Device_Address byte in the Configuration zone is programmed differently for each device on the

© 2023-2025 Microchip Technology Inc. and its subsidiaries

bus. Because all seven bits of the device address are programmable, the TA010-TFLXWPC can also share the I²C interface with any I²C device, including any Serial EEPROM.

5.2.3. Split I²C Transactions

System requirements sometimes limit the length of a transaction to a certain number of bytes. The TA010-TFLXWPC can accommodate this limitation and commands can be subdivided into multiple transactions. When the device receives the first portion of the command, which includes the total number of bytes being sent, the control logic of the device will be looking for that number of bytes before it will execute the command. Each portion of the command requires that the device address plus word address be sent for each partial packet. It is recommended that a Restart condition be sent between the partial packets without a Stop condition and only send the Stop condition after the last of the command bytes are sent. It is, however, acceptable to send a Stop condition between each portion of the command byte stream.

Beyond system level requirements that force the need to subdivide a command, it may simply be convenient to do so. For example, when executing a read transaction of an unknown length, it may be desirable to first read back only the initial payload byte to determine the length of the data being read back. This allows for the ability to dynamically allocate the size of the array being read back.

Legend:	A = ACK	N = NACK	S = Start condition	P = Stop condition	Sr = Repeated Start Condition
The legend applies to all of the following diagrams.					

Figure 5-6. 32-Byte Standard I²C Write

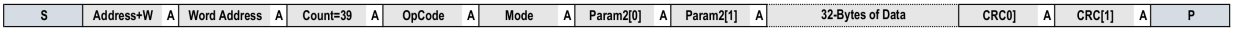


Figure 5-7. 32-Byte Split I²C Write

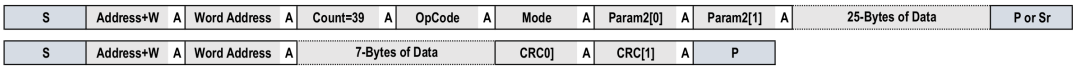


Figure 5-8. 32-Byte Standard I²C Read

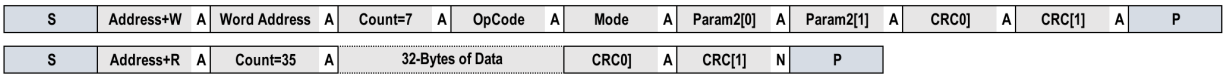
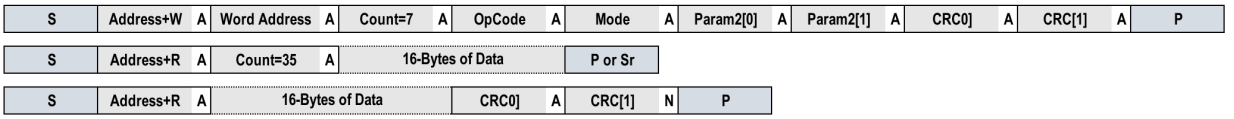


Figure 5-9. 32-Byte Split I²C Read



5.2.4. I²C Synchronization

It is possible for the system to lose synchronization with the I/O port on the TA010-TFLXWPC, perhaps due to a system reset, I/O noise or other conditions. Under this circumstance, the TA010-TFLXWPC may not respond as expected, may be asleep or may be transmitting data during an interval when the system is expecting to send data. To resynchronize, the following procedure can be followed:

1. To ensure an I/O channel reset, the system must send the standard I²C software reset sequence, as follows:
   - A Start bit condition
   - Nine cycles of SCL with SDA held high by the system pull-up resistor

© 2023-2025 Microchip Technology Inc. and its subsidiaries

- Another Start bit condition
- A Stop bit condition

A read sequence can now be issued, and, if synchronization is properly completed, the TA010-TFLXWPC will ACK the device address. The device may return data or may leave the bus floating (which the system will interpret as a data value of `0xFF`) during the data periods.

If the device does ACK the device address, the system must reset the internal address counter to force the TA010-TFLXWPC to ignore any partial input command that was possibly sent. This can be accomplished by sending a write sequence to word address `0x00` (Reset) followed by a Stop condition.

2. If the device does not respond to the device address with an ACK, then it may be asleep. In this case, the system must send a complete I^2C wake condition and wait t_{PU}. The system may, then, send another read sequence, and, if synchronization is complete, the device will ACK the device address.
3. If the device still does not respond to the device address with an ACK, then it may be busy executing a command. The system must wait the longest t_{EXEC} (max.), then send the read sequence, which will be acknowledged by the device.

5.3. I/O Transmission to the TA010-TFLXWPC

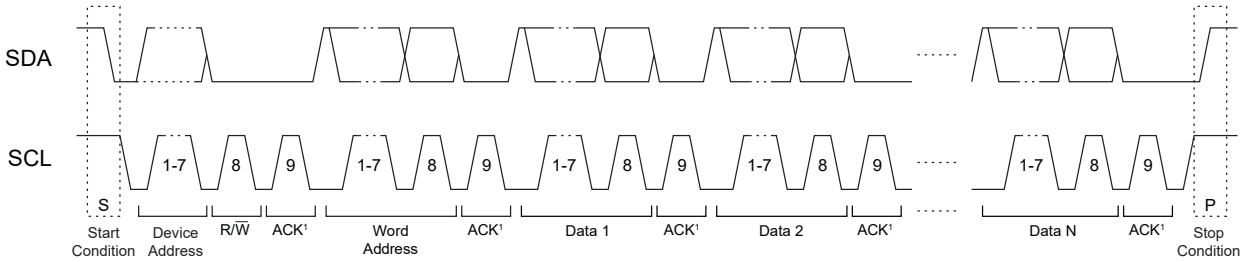
The transmission of data from the system to the TA010-TFLXWPC is summarized in the table below. The order of transmission is as follows:

- Start condition
- Device Address byte
- Word Address byte
- Optional Data bytes (1 through N)
- Stop condition

Table 5-1. Transmission to the TA010-TFLXWPC

Name	I/O Name	Description
Device Address	Device Address	This byte selects a particular device on the I/O interface. TA010-TFLXWPC is selected if bits 1 through 7 of this byte match bits 1 through 7 of the Device_Address byte in the Configuration zone. Bit 0 of this byte is the R/$\overline{W}$ bit and must be zero to indicate a write operation (the bytes following the device address travel from the host to the client).
Word Address	Word Address	This byte must have a value of `0x03` for normal operation. See Word Address Values for more information.
Command	Data 1, N	The command group, consisting of the count, command packet and the 2-byte CRC. The CRC is calculated over the size and packet bytes.

Figure 5-10. Normal I^2C Transmission to the TA010-TFLXWPC



Because the device treats the command input buffer as a FIFO, the input group can be sent to the device in one or many I/O command groups. The first byte sent to the device is the count, so after the device receives that number of bytes, it will ignore any subsequently received bytes until execution is finished.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

The system must send a Stop condition after the last command byte to ensure that the TA010-TFLXWPC will start the computation of the command. Failure to send a Stop condition may eventually result in a loss of synchronization.

Related Links

I2C Synchronization
Word Address Values

5.3.1. Word Address Values

During an I/O write packet, the TA010-TFLXWPC interprets the second byte sent as the word address, which indicates the packet function as it is described in the table below:

Table 5-2. Word Address Values

Name	Value	Description
Reset	`0x00`	Resets the address counter. The next I/O read or write transaction will start with the beginning of the I/O buffer.
Sleep (low-power)	`0x01` or `0x02`	The TA010-TFLXWPC goes into the low-power Sleep mode and ignores all subsequent I/O transitions until the next Wake flag. The entire volatile state of the device is reset.
Command	`0x03`	Writes subsequent bytes to sequential addresses in the input command buffer that follow previous writes. This is the normal operation.

Note: Only the lower two bits of the Word Address byte are decoded by the TA010-TFLXWPC.

5.3.2. Sleep Sequence

Upon completion of the use of the TA010-TFLXWPC by the system, it is recommended that the system issue a sleep sequence to put the device into Low-Power mode. This sequence consists of the proper device address followed by the value of `0x01` as the word address followed by a Stop condition. This transition to the Low-Power state causes a complete reset of the device's internal command engine and input/output buffer. It can be sent to the device at any time when it is awake and not busy.

5.3.3. Command Completion Polling

After a complete command is sent to the TA010-TFLXWPC, the device will be busy until the command computation completes. The system has options depending on the I/O, as noted below:

- **Polling**:
  It is recommended that the system wait t_{EXEC} (typical), then send a read sequence (see I/O Transmission from the TA010-TFLXWPC). If the device NACKs the device address, then it is still busy. The system may delay for some time or immediately send another read sequence, looping on NACK again. After a total delay of t_{EXEC} (max.), the device will complete the computation and return the results.
- **Single Delay**:
  The system must wait t_{EXEC} (max.), after which the device will complete the execution, and the result can be read from the device using a normal read sequence.

5.4. I/O Transmission from the TA010-TFLXWPC

When the TA010-TFLXWPC is awake and not busy, the host can retrieve the current output buffer contents from the device using an I/O read. If valid command results are available, the size of the group returned is determined by the particular run command. Otherwise, the size of the group (and the first byte returned) will always be four: count, status/error and 2-byte CRC.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

Table 5-3. I/O Transmission from the TA010-TFLXWPC

Name	I/O Name	Direction	Description
Device Address	Device Address	To client	This byte selects a particular device on the I/O interface and the TA010-TFLXWPC will be selected if bits 1 through 7 of this byte match bits 1 through 7 of the Device_Address byte in the Configuration zone. Bit 0 of this byte is the R/$\overline{W}$ bit and must be one to indicate that the bytes following the device address travel from the client to the host (read).
Data	Data 1, N	To host	The output group, consisting of the count, status/error byte or the output packet followed by the 2-byte CRC.

The status, error or command outputs can be read repeatedly by the host. Each time a `Read` command is sent to the TA010-TFLXWPC along the I/O interface, the device transmits the next sequential byte in the output buffer. See the following section for details on how the device handles the address counter.

If the TA010-TFLXWPC is busy or asleep, it will NACK the device address on a read sequence. If a partial command is sent to the device and a read sequence `[Start + DeviceAddress(R/`$\overline{W}$` == R)]` is sent to the device, the TA010-TFLXWPC will NACK the device address to indicate that no data are available to be read.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

6. Electrical Characteristics

6.1. Absolute Maximum Ratings

Operating Temperature	-40°C to +125°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	>4 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.

6.2. Reliability

The TA010-TFLXWPC is fabricated with Microchip's high-reliability CMOS EEPROM manufacturing technology.

Table 6-1. EEPROM Reliability

Parameter	Min	Typ.	Max.	Units
Data Retention at +55°C	>40	—	—	Years
Read Endurance	Unlimited			Read Cycles

Note:

1. The number of times that an EEPROM cell would be written is expected to be minimal for most use cases. Maximum EEPROM write cycles are expected to occur when the monotonic counter is used, which can be incremented up to 10,000 times. Similar devices in this technology have a write endurance of >100k.

6.3. AC Parameters

6.3.1. AC Parameters: All I/O Interfaces

Table 6-2. AC Parameters: All I/O Interfaces

Unless otherwise indicated, these values are applicable over the specified operating range from T_A = -40°C to +125°C, V_{CC} =+1.65V to +5.5V.

Parameter	Sym.	Direction		Min.	Typ.	Max.	Units	Conditions
Power-up Delay	t_{PU}[1]	To TA010-TFLXWPC	Clock Divider = 1x	1.0	—	—	ms	Minimum time prior to V_{CC} > V_{CC} min.
			Clock Divider = 2x	1.2	—	—	ms	
			Clock Divider = 4x	1.8	—	—	ms	

© 2023-2025 Microchip Technology Inc. and its subsidiaries

Table 6-2. AC Parameters: All I/O Interfaces (continued)

Parameter	Sym.	Direction	Min.	Typ.	Max.	Units	Conditions
Watchdog Timer (WDT) Delay	t_{WDT}[1]	N/A	0.7	1	1.3	s	Time that the WDT will run after a command is sent, prior to automatically resetting the chip.

Note:

1. These parameters are ensured through characterization but not production tested.

6.3.2. AC Parameters: I²C Interface

Figure 6-1. I²C Synchronous Data Timing

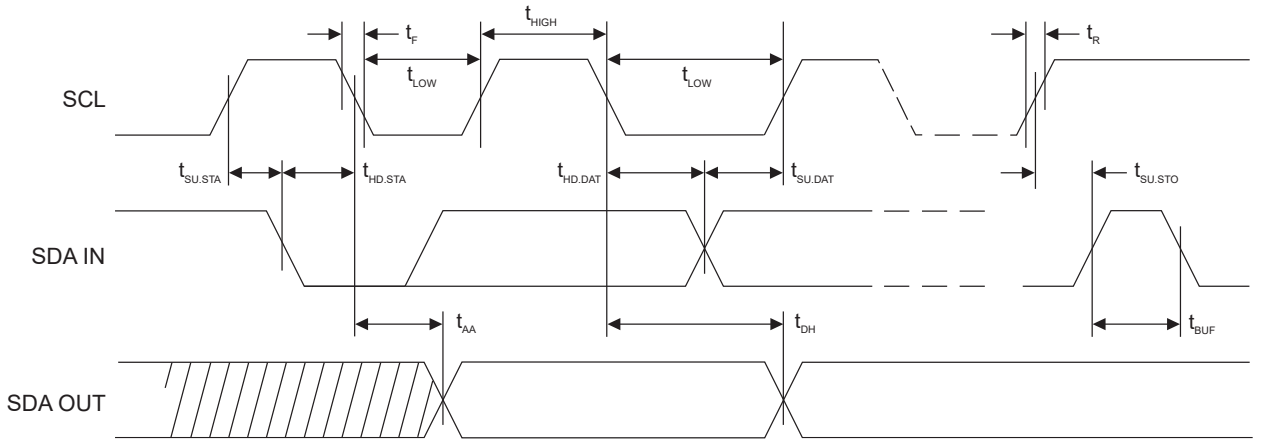


Table 6-3. AC Characteristics of I²C Interface

Unless otherwise indicated, these values are applicable over the specified operating range from T_A = -40°C to +125°C, V_{CC} = +1.65V to +5.5V, C_L = 1 TTL Gate and 100 pF.

Parameter	Sym.	Min.	Max.	Units
SCL Clock Frequency	f_{SCL}	0	400	kHz
SCL High Time	t_{HIGH}	600	—	ns
SCL Low Time	t_{LOW}	1200	—	ns
Start Setup Time	$t_{SU.STA}$	600	—	ns
Start Hold Time	$t_{HD.STA}$	600	—	ns
Stop Setup Time	$t_{SU.STO}$	600	—	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	—	300	ns
Clock Low to Data Out Valid	t_{AA}	50	900	ns
Data Out Hold Time	t_{DH}	50	—	ns
Time Bus Must be Free before a New Transmission Can Start[1]	t_{BUF}	1200	—	ns
Glitch Filter[3]	t_{IGNORE_I2C}	50	250	ns

© 2023-2025 Microchip Technology Inc. and its subsidiaries

Notes:

1. Host system must ensure this timing is met.
2. AC measurement conditions:
   - R_L (connects between SDA and V_{CC}): 1.2 kΩ (for V_{CC} = +1.65V to +5.5V)
   - Input pulse voltages: 0.3V_{CC} to 0.7 V_{CC} with CMOSenable = 1
   - Input rise and fall times: ≤ 50 ns
   - Input and output timing reference voltage: 0.5 V_{CC}
3. The glitch filter ensures that all pulses below the min value will be suppressed but may suppress values as great as the max value over all process, voltage and temperature conditions.

6.4. DC Parameters

6.4.1. DC Parameters: All I/O Interfaces

Table 6-4. 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 +125°C, V_{CC} = +1.65V to +5.5V.

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Ambient Operating Temperature	T_A	-40	—	+125	°C	—
V_{CC} Ramp Rate(5)	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(5)
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)	V_{IL0}	-0.5	—	0.5	V	Device is active and CMOSEnable = 0
Input High Threshold(1)	V_{IH0}	1.2	—	V_{CC}+0.5	V	Device is active and CMOSEnable = 0
Input Low Threshold in Sleep mode(6)	V_{ILS}	-0.5	—	0.5	V	Device is in Sleep mode CMOSen= 0
Input High Threshold in Sleep mode(6)	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
Sleep Current(2)	I_{SLEEP}	—	130	325(5)	nA	When the device is in Sleep mode, V_{CC} ≤ 3.6V, I/O at either GND or V_{CC} T_A ≤ +55°C
		—	130	800	nA	V_{CC} ≤ 3.6V, I/O at either GND or V_{CC} Full temperature Range
		—	130	2000	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	300	µA	Waiting for I/O

© 2023-2025 Microchip Technology Inc. and its subsidiaries

Table 6-4. DC Parameters on All I/O Interfaces with V_{CC} Power Applied (continued)

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Current Consumption in Computation Mode	$I_{COMPUTE}$(3)	—	—	0.75	mA	During command execution 1x divider
		—	—	0.5	mA	During command execution 2x divider
		—	—	0.4	mA	During command execution 4x divider
EEPROM Write Current	I_{WRITE}(4)	—	0.6	1.5	mA	Current when writing to EEPROM -5°C to +125°C
EEPROM Write Current	I_{WRITE}(4)	—	0.6	4.0	mA	Current when writing to EEPROM full temperature range
Theta JA	θ_{JA}	—	99.1	—	°C/W	8-lead SOIC
		—	82.1	—	°C/W	8-pad VDFN

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. 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.
3. Applies to all commands where an EEPROM write does not occur.
4. Applies to all commands where an EEPROM write occurs. This includes `Write`, `Lock`, `GenKey`, `Counter(Increment)`.
5. This condition is characterized but not production tested.
6. 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}.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

7. Command Descriptions

7.1. `Counter` Command

The `Counter` command reads or increments the count value of the monotonic counter. The counter value is stored in CSZ2. The maximum value of the counter is fixed at 10,000. The starting value of the counter is programmed during initial provisioning, and when the Configuration zone slot is locked, it cannot be modified.

The counter is designed to never lose counts even if the power is interrupted during the counting operation. In some power loss conditions, the counter may increment by a value of more than one.

The counter can be attached to the HMAC key to limit its use. The counter will be incremented with the respective key until the counter reaches its maximum value, at which point the use of the key will no longer be permitted.

The number of legal uses for a key can be controlled by initializing the `Counter` to a nonzero value at configuration time. Contact Microchip for details.

7.2. `Delete` Command

The `Delete` command, when executed, will clear all of the Data zone slots and set all bytes of each slot to `0xFF`. The Configuration zone will be untouched, except for the value of the Primary_Deleted byte.

Related Links

Nonce Command

7.3. `GenKey` Command

The `GenKey` command performs the following operations:

- **Private Key Creation**:
  Creates a new random ECC private key. The command writes the generated key into the slot specified by the KeyID parameter.
- **Public Key Computation**:
  Outputs an ECC public corresponding to the private key stored in Slot 0. This mode of the command may be used to avoid storing the public key on the device at the expense of the time required to regenerate it.

Related Links

Random Number Generator (RNG)

7.4. `Info` Command

The `Info` command accesses some static or dynamic status information from the device, depending on the parameters input to the command.The specific modes of information include:

Revision	Returns a value indicating the device identification byte and the revision number of the device. It is recommended that software not depend on the revision information as it may change over time.
KeyValid	Returns a value indicating the validity of an ECC private key . An ECC private key status can either be valid or invalid.
LockStatus	Returns a value indicating if the slot selected in either the Configuration or Data zone is locked or unlocked. After the `Delete` command has been run this mode will always fail.
ChipStatus	Returns a value. The first byte returned indicates if the `Delete` command has been used to clear the data slots.

Related Links

Lock Command

© 2023-2025 Microchip Technology Inc. and its subsidiaries

7.5. Lock Command

The Lock command prevents future modifications of the Configuration and/or Data zones. This command can be used to lock individual Configuration subzones or individual Data zone slots. Prior to locking or writing any Data zone slots, CSZ0 and CSZ1 must be locked. CSZ0 is pre-locked by Microchip prior to device shipment.

7.6. Nonce Command

The Nonce command can output a random number for use by the system. A single invocation of the Nonce command will result in the following:

- A random number will be generated and output on the bus for use by the host system.
- An internal nonce value will be generated for use internally by the TA010-TFLXWPC.

Related Links

GenKey Command
Random Number Generator (RNG)

7.7. Read Command

The Read command is used to read data from either the Configuration zone or the EEPROM Data zone. The Configuration zone is always readable and can be read 16 bytes at a time. Data zone slots that allow reading can be read 32 bytes at a time. Multiple reads are required to completely read some data slots. Data slots 0 and 3 can never be read and an execution error will occur if so attempted. Data slots 1 and 2 can always be read in the clear.

7.8. SelfTest Command

The SelfTest command performs on-demand testing of one or more of the cryptographic algorithms implemented in the TA010-TFLXWPC. The algorithms HMAC (SHA-256), ECDSA and the DRBG of the RNG each have a self-test routine to confirm their integrity. The SelfTest command can be run at any time after the initial start-up procedure is completed.

Related Links

Random Number Generator (RNG)

7.9. SHA Command

The SHA command computes a SHA-256 or HMAC digest for general purpose use by the host system. The SHA command must be executed repetitively to calculate the digest over the entire message. Data can be sent to the command in 1-64-byte blocks. The maximum message length over which a digest can be calculated is limited to 2^{28} bytes.

Upon successful completion of the command, a 32-byte value is output on the bus. If this value is required for use in a subsequent TA010-TFLXWPC command, the value must first be stored in the system, then resubmitted as an input parameter to the command. There is no ability to store the value directly into the device.

7.10. Sign Command

The Sign command generates a signature over the 32-byte SHA-256 digest of an externally-generated message. The digest of the message is passed into the device as part of the Sign command. The ECC private key in Slot 0 is used to generate the signature. Signing of internal messages is not an option with the device.

If so desired, a monotonic counter can be configured for limited key use with the Sign command.

7.11. Write Command

The Write command writes 16 bytes to one of the EEPROM Configuration subzones or 32 bytes to the EEPROM Data zone slots. This command cannot be used to write a slot used for an ECC private

© 2023-2025 Microchip Technology Inc. and its subsidiaries

key. When writing the HMAC key, it is recommended, but not required, that an encrypted write be performed.

Modes of Operation:

1. Configuration Subzone Write
2. Clear Text Data Slot Write
3. Encrypted HMAC Key Write

Related Links

Nonce Command

© 2023-2025 Microchip Technology Inc. and its subsidiaries

8. Application Information

The TA010-TFLXWPC is a member of the Microchip's Trust CryptoAuthentication™ family of products. The TrustFLEX products are easy to use, simple to implement and allow even low-volume users to implement security into their end system, while leveraging Microchip's expertise and infrastructure in secure provisioning.

The TA010-TFLXWPC device was developed to take the guesswork out of adding security to Qi-compliant wireless charging transmitters. The product is pre-configured to readily store the WPC device unit certificate of the WPC Slot 0 chain. The WPC Slot 0 digest of the full certificate chain is also stored, allowing for rapid authentication by just comparing the digest value to a previously stored value in the host device.

In addition to the actual secure subsystem, Microchip developed a series of tools that seamlessly integrate with their hardware devices to provide an easy path to developing an entire security solution. When developers use Microchip's software security tools, they eliminate the complexity of setting up their own infrastructure and provide a rapid path to initial prototypes and production.

Important: Automotive versions of the TrustFLEX products currently require that the Microchip high-volume Trust flow be followed. The TPDS tools can still be used to develop the configuration and obtain initial prototypes of the devices. Part ordering codes will, however, be uniquely assigned for each customer for production units. Contact Microchip for more information on Automotive grade TrustFLEX products.

8.1. Use Cases

The TA010-TFLXWPC is specifically designed to address the authentication needs of the WPC Qi charging market. For Qi the power transmitter is required to be authenticated for Qi standards 1.3 and 2.x and beyond. Microchip is an authorized Manufacturing CA for the WPC. In addition to security ICs, Microchip offers a complete power receiver and power transmitter reference designs for Qi mobile charging markets with authentication.

8.2. WPC Engagement

All companies selling Qi-certified products must be members of the Wireless Power Consortium. All products intended to be sold as Qi-certified must go through the appropriate validation, testing and certification procedures. Products are not allowed to claim compliance if they do not undergo the proper validation and test procedures. Manufacturers of Qi-certified products must be in good standing with Wireless Power Consortium.

For products that require authentication, additional measures are also required. An entity that wishes to manufacture products with authentication must be licensed as a Qi-certified manufacturer. Products that need to be authenticated must have a Secure Storage Subsystem (SSS) that securely stores the ECC P-256 private key. A corporation that provides the SSS must be a WPC Licensed Manufacturing Certificate Authority. Microchip has several products that meet the requirements of an SSS, and the TA010-TFLXWPC is one such product. Microchip is a Qi-certified Manufacturing CA.

Note that it is the responsibility of the manufacturer to select an SSS from a certified provider and the responsibility of the manufacturer CA to verify that a manufacturer is in good standing with the WPC.

Secure Production Provisioning Flow

The following is a typical provisioning flow for WPC production units:

1. The customer begins development work using the TA010-TFLXWPC.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

2. The customer opens a Microchip Sales Force support ticket for provisioned SSS.
3. The customer provides the PTMC and Qi ID to Microchip through the support ticket system.
4. Microchip validates the PTMC and Qi ID with the WPC to validate ownership.
5. Once validated, Microchip generates the appropriate certificates and sets up a certificate signing request to sign the manufacturing certificate with the WPC Root CA. Microchip will initiate the key signing ceremony with WPC on behalf of the customer through the WPC automated CSR submission process once all of the WPC requirements have been met.
6. Once the signing ceremony is completed, Microchip will generate a limited number of validation units for the customer to evaluate. Evaluation consists of verifying that the units are programmed correctly and meet all requirements of the customer.
7. The customer provides notification to Microchip that the validation units are accepted.
8. The customer proceeds with completion of WPC certification testing.
9. Upon successful completion, the customer can request full production units and quantities.

8.3. Development Tools

The TA010-TFLXWPC is supported with multiple hardware and software tools and backend services that provide a path to rapidly develop applications. Initial development can start by using a family of easy-to-use Trust Platform Design Suite tools. These tools provide a graphical way to implement your use case and end with the C code necessary to implement your application.

If your application differs from what the predefined Trust Platform Design Suite tools can provide, then through use of the CryptoAuthLib or the Python® version of CryptoAuthLib and CryptoAuthTools, an application can be developed. CryptoAuthLib is also the backbone of the code that is output from the Trust Platform Design Suite tools.

Full verification of your application can be implemented via hardware tools along with samples of the TA010-TFLXWPC device. The access policies of the device are already set, therefore, the focus revolves just around developing the system level code.

Once the application is complete, the TA010-TFLXWPC devices can be ordered through Microchip Direct.

8.3.1. Trust Platform Design Suite

To simplify the implementation process, Microchip developed a web-based Trust Platform Design Suite of tools that will allow developers to go from concept to production via a guided flow. The tools allow you to develop and construct the transaction diagrams and code necessary to implement a particular application within the constraints of the configuration and defined access policies of the TA010-TFLXWPC.

Note: More information on these tools can be found on Microchip's Trust Platform information page.

8.3.2. Hardware Tools

There are multiple hardware tools that can help in developing with the TA010-TFLXWPC. Check the Microchip website for the availability of additional tools that are not mentioned here. Specific tools are also mentioned with the specific use case examples.

DM320118 – CryptoAuthentication™ Trust Platform

The DM320118 is a compact development system consisting of an ATSAMD21 microcontroller, one each of the ATECC608B-TNGTLS, ATECC608B-TFLXTLS and ATECC608B-TCSM Trust devices, a USB hub, a mikroBUS™ connector and the NEDBG on-board debugger. Through use of the mikroBUS header, additional types of devices can be configured with the Trust Platform Design Suite of tools and used to implement various use cases with a wide variety of devices. The kit can be used with MPLAB® X IDE to develop applications.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

EV89U05A – CryptoAuthentication™ Pro Trust Platform

The CryptoAuth Pro Trust Platform kit extends the CryptoAuth Trust Platform with a more powerful Cortex M4 microcontroller, four on-board CryptoAuthentication devices, two mikroBUS™ sockets, and an on-board 10/100 Mbit Ethernet PHY. The board also contains the Microchip Technology PKoB4 debugger, which is compatible with MPLAB®X IDE. The application microcontroller has been configured to readily make use of many of the features provided on the board.

Similar to the DM320118, additional CryptoAuthentication™ and CryptoAutomotive™ devices can be used with the board through the mikroBUS header. Additionally, two user-programmable switches and LEDs are provided to aid in the development of demonstrations and applications.

EV74C12A – TA010 CryptoAuto

The EV74C12A is a mikroBUS extension board that contains one TA010 I^2C device, one TA010 SWI device and one TA100 host device with both a SPI and I^2C interface. These devices are generic devices that have not been provisioned. The board can be directly connected to a DM320118 or any host board that supports a mikroBUS host interface.

Secure UDFN(SOIC) Click Boards SOIC

The SECURE-UDFN-CLICK and SECURE-SOIC-CLICK are generic CryptoAuthentication socket kits that can be used with any microcontroller development board with a mikroBUS interface. These kits have been developed by MikroElektronika and are available through their website. TA010-TFLXWPC samples for use with these boards will need to be obtained separately as they are not included in the kits.

DM320109 – CryptoAuthentication Starter Kit

The DM320109 consists of an ATSAMD21-XPRO development board pre-programmed with firmware that can work with CryptoAuthentication devices. The kit comes with the AT88CKSCKTSOIC-XPRO socket board, but you will need to obtain the UDFN version of the board to work with the sample devices that are currently provided only in the UDFN package. Specific samples of the TA010-TFLXWPC will need to be obtained separately.

AT88CKSCKTUDFN(SOIC)-XPRO

The AT88CKSCKTUDFN-XPRO and AT88CKSCKTSOIC-XPRO are generic CryptoAuthentication socket kits that can be used with any microcontroller development board with an XPRO interface. Specific samples of the TA010-TFLXWPC must be acquired to be used with these kits.

8.3.3. CryptoAuthLib

CryptoAuthLib is a software library that supports Microchip's family of CryptoAuthentication devices. Microchip recommends working with this library when developing with the TA010-TFLXWPC. The library implements the API calls necessary to execute the commands detailed in this data sheet.

The library was implemented to readily work with many of Microchip's microcontrollers but can easily be extended through a Hardware Abstraction Layer (HAL) to other microcontrollers, including those made by other vendors.

For more details on these tools, check the information on:

- CryptoAuthLib – Web Link
- CryptoAuthLib – GitHub

API Calls

Each of the commands in the data sheet have one or more API calls that are associated with them. Typically, there is a base API call of the command where all input parameters can be specified. The parameter shown in the commands and subsections can be used with this command. There are also mode variants of each of the API calls. The table below shows examples of commands and base API calls. For the most accurate API information, refer to the GitHub information.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

Table 8-1. Example Commands to CryptoAuthLib API Calls

Device Command	API Call	Comments
`Info`	atcab_info_base()	
`Write`	atcab_write()	
`Read`	atcab_read_zone()	
`SHA`	atcab_sha_base()	
`Sign`	atcab_sign_base()	

© 2023-2025 Microchip Technology Inc. and its subsidiaries

9. 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.

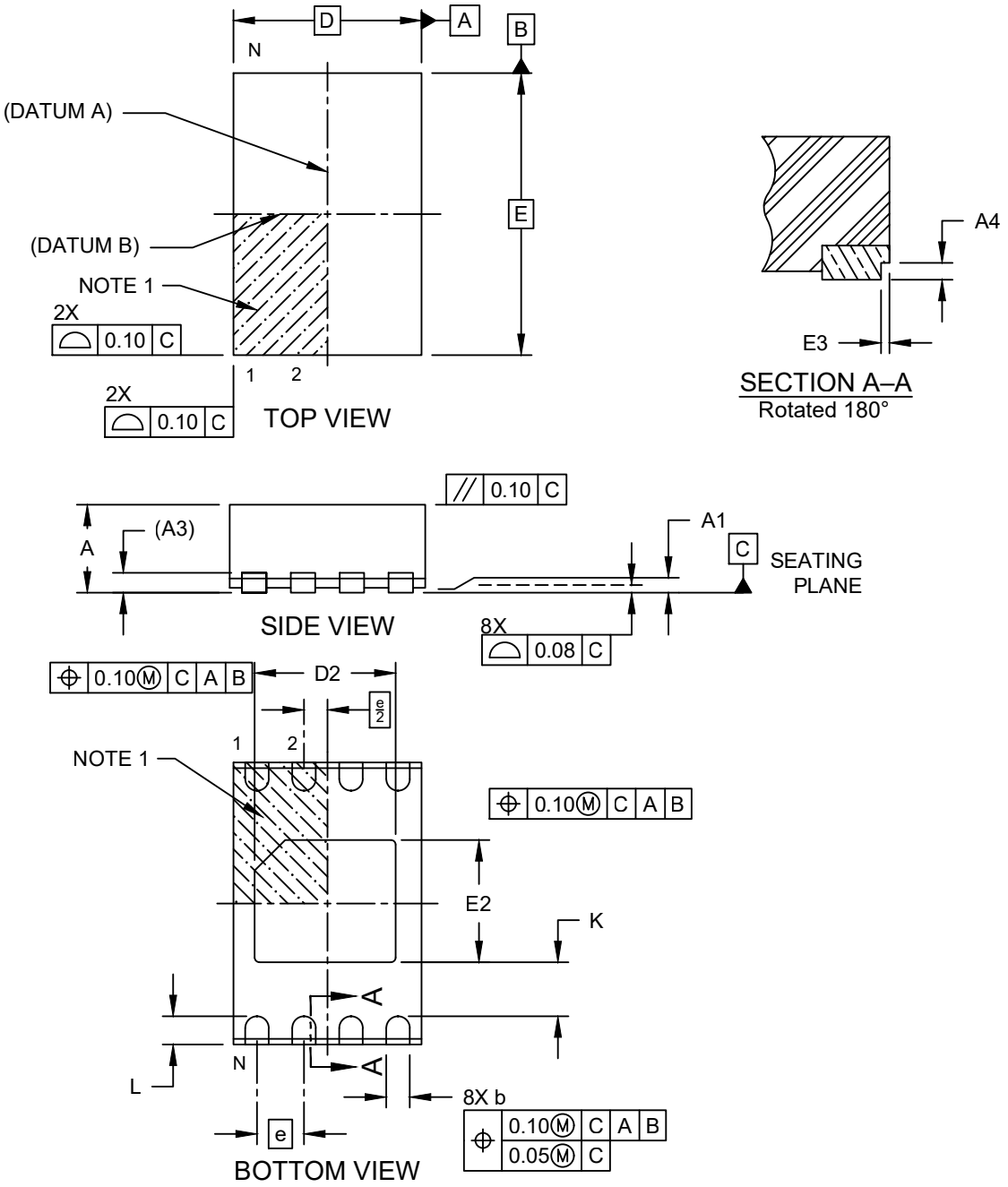
© 2023-2025 Microchip Technology Inc. and its subsidiaries

10. Package Drawings

10.1. 8-Pad VDFN

8-Lead Very Thin Plastic Dual Flat, No Lead Package (MWF) - 2x3x1.0 mm Body [VDFN] 1.5x1.3 mm Exposed Pad Wettable Step Cut Flanks

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

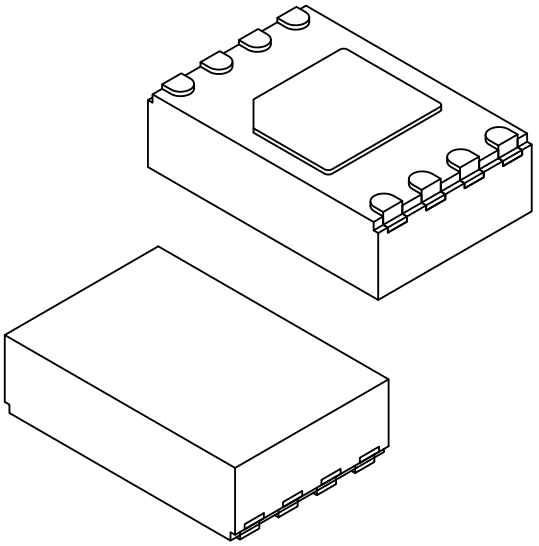


Microchip Technology Drawing C04-00598 Rev E Sheet 1 of 2

© 2023-2025 Microchip Technology Inc. and its subsidiaries

8-Lead Very Thin Plastic Dual Flat, No Lead Package (MWF) - 2x3x1.0 mm Body [VDFN] 1.5x1.3 mm Exposed Pad Wettable Step Cut Flanks

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	008		
Pitch	e	0.50 BSC		
Overall Height	A	0.80	0.90	1.00
Standoff	A1	0.00	0.02	0.05
Terminal Thickness	A3	0.203 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	0.20	0.25	0.30
Terminal Length	L	0.25	0.35	0.45
Terminal-to-Exposed-Pad	K	0.20	–	–
Wettable Flank Step Cut Width	E3	0.035	0.06	0.085
Wettable Flank Step Cut Depth	A4	0.100	–	0.190

Notes:

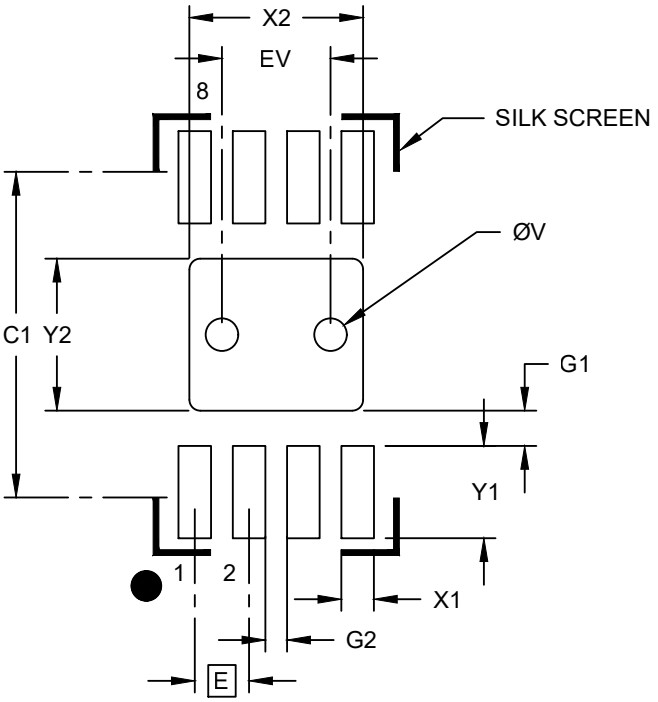
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
   REF: Reference Dimension, usually without tolerance, for information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

Microchip Technology Drawing C04-00598 Rev E Sheet 2 of 2

© 2023-2025 Microchip Technology Inc. and its subsidiaries

8-Lead Very Thin Plastic Dual Flat, No Lead Package (MWF) - 2x3x1.0 mm Body [VDFN] 1.5x1.3 mm Exposed Pad Wettable Step Cut Flanks

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	
Center Pad Width	X2			1.60
Center Pad Length	Y2			1.40
Contact Pad Spacing	C1		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

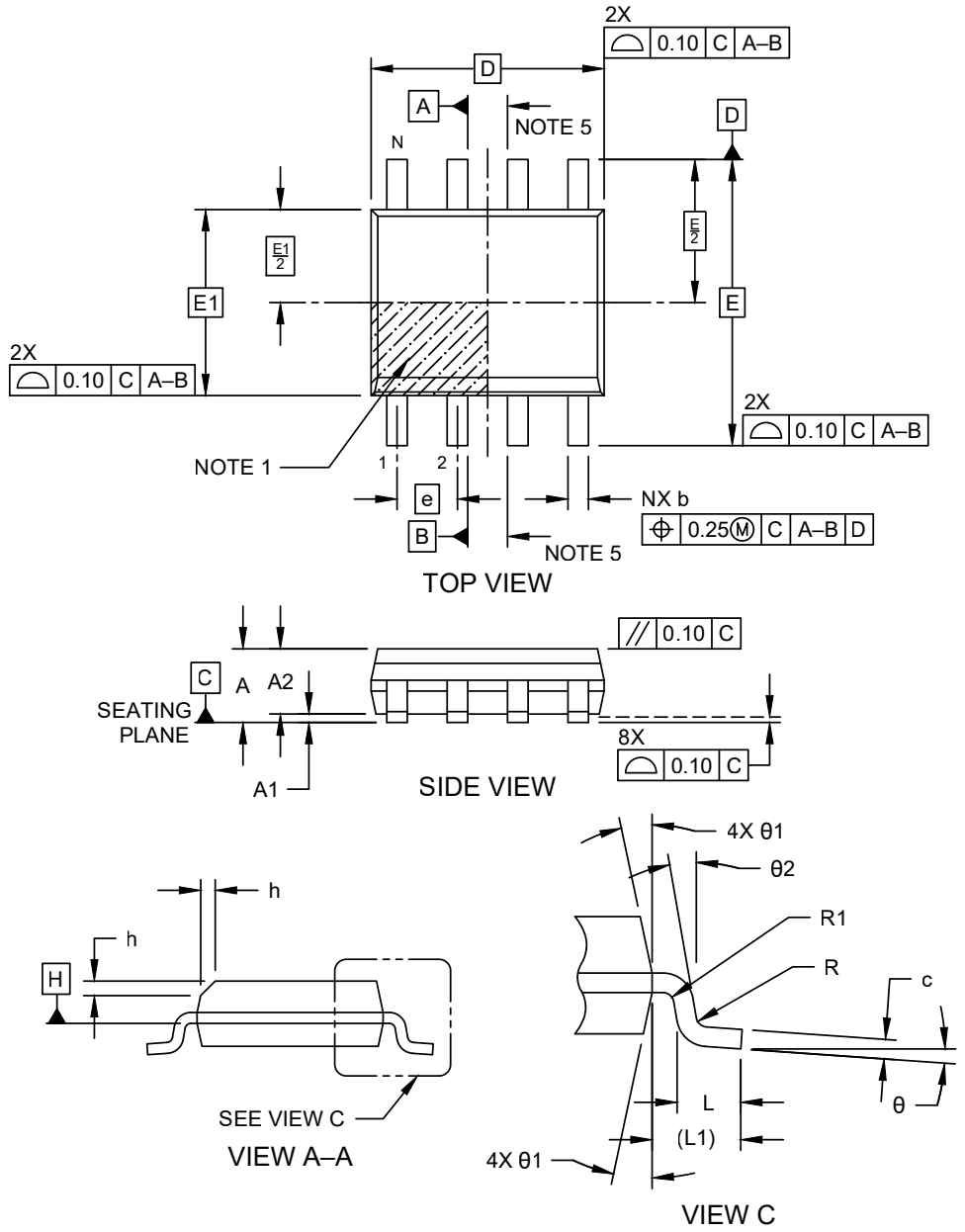
Microchip Technology Drawing C04-02598 Rev E

© 2023-2025 Microchip Technology Inc. and its subsidiaries

10.2. 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

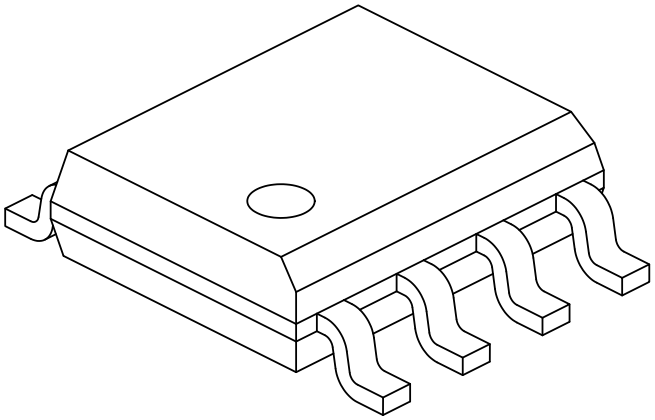


Microchip Technology Drawing No. C04-00057-OA Rev L Sheet 1 of 2

© 2023-2025 Microchip Technology Inc. and its subsidiaries

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:

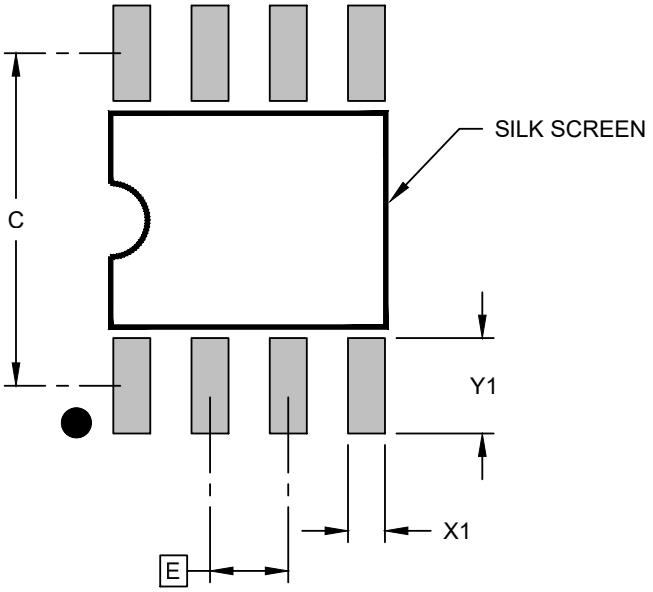
1. The Pin 1 visual index feature may vary, but it must be located within the hatched area.
2. § Significant Characteristic
3. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.15mm per side.
4. Dimensioning and tolerancing per ASME Y14.5M
   BSC: 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

© 2023-2025 Microchip Technology Inc. and its subsidiaries

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

© 2023-2025 Microchip Technology Inc. and its subsidiaries

11. Revision History

Revision D (November 2025)

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

- Introduction: Removed references to Ki 1.x.
- Features: Updated WPC bullet, removing support for Ki 1.x standards.
- Use Cases: Removed Ki use cases.
- Wireless Power Consortium: Removed Ki references.
- Wireless Power Consortium Terminology: Removed Ki term.
- Use Cases: Removed Ki references.
- WPC Engagement: Removed Ki references.

Revision C (October 2025)

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

- Features: Added AEC-Q100 bullet to Features list.
- Random Number Generator (RNG): Updated SP 800-90C to the released version of the spec.
- 8-Lead SOIC: Updated SOIC package drawings to latest version.

Revision B (June 2025)

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

- Introduction: WPC updates to indicate support for Qi 2.x and Ki 1.x.
- Features:
  - Added NIST certified to TRNG bullet.
  - Updated WPC bullet indicating support for Qi2.x and Ki 1.x standards.
  - Added VDFN package option.
- Use Cases: Added Ki use cases.
- Pin Configuration and Pinouts: Updated for VDFN package.
- Wireless Power Consortium: Updated for Qi 2.x and Ki 1.x.
- Wireless Power Consortium Terminology: Added Ki term.
- Random Number Generator (RNG): Added specification information. Added ESV information.
- DC Parameters: All I/O Interfaces:
  - Added input thresholds when in Sleep mode (V_{ILS}, V_{IHS}).
  - Updated Theta J_A values. Added VDFN value.
- GenKey Command: Removed MAC calculation from TFLX data sheet versions.
- Nonce Command: Removed session key information.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

- Use Cases: Updated use case information to cover Qi and Ki.
- WPC Engagement: Updated to cover Qi and Ki.
- Hardware Tools: Added/updated tool descriptions.
- Package Drawings: Added VDFN package information.
- Product Identification System: Product Identification now separate section and not part of Back Matter. Updated ordering codes. Added VDFN package information.
- Microchip Information: Back Matter simplified per Microchip's new standard.

Revision A (March 2023)

- Initial data sheet release.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

12. 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	-	Trust Type	Trust Option	Package Type	-	Device Type	-	Product Identifier
xxxxx	-	tttt	vvvv	p	-	dd	-	Vxx

Device:	TA010: Pre-configured Cryptographic Coprocessor with secure hardware-based key storage	
Trust Type	TFLX	Type of Microchip Trust Product
Trust Product Configuration	WPC	Configuration associated with Trust Product
Package Options	W	8-Pad 2 x 3 x 1.0 mm Body, Thermally Enhanced with Wettable Flanks Very Thin Dual Flat no Lead Package (VDFN)
	S	8-Lead (0.150" Wide Body), Plastic Gull Wing Small Outline (JEDEC® SOIC)
Device Type	—	Production Units
	HV	Hardware Validation Units(1)
Product Identifier	VAO(1)	Standard Product Identifier
	Vxx(2)	Customer Specific Product Identifier

Part Numbers used for Quoting(1)

- TA010-TFLXWPCW-HV-VAO: TrustFLEX WPC, Provisioned, 8-VDFN, I^2C Interface
- TA010-TFLXWPCS-HV-VA0: TrustFLEX WPC, Provisioned, 8-SOIC, I^2C Interface

Production Unit Examples(2)

Production unit ordering codes follow the format of standard TA010 ordering code with the -Vxx code being unique.

- TA010-MWYDAT-WPC-Vxx: TrustFLEX WPC, Provisioned, 8-VDFN, I^2C Interface
- TA010-SSYDAT-WPC-Vxx: TrustFLEX WPC, Provisioned, 8-SOIC, I^2C Interface

Notes:

1. Currently, no standard automotive product offering is available for this device. As part of the development process, customers will receive validation units to verify that the devices have been provisioned correctly. These units are only available in small quantities and must not be used for production.
2. Automotive products are not available in volume through the programming center. Each product will receive a unique customer-assigned ordering code defined by Microchip. The format of this ordering code follows the standard part numbering with the -Vxx code being unique for each product or customer.

NOTICE The UDFN Package has been deprecated for use with the TA010-TFLXWPC in favor of the VDFN package with wettable flanks. The board land pattern is identical for both packages. The UDFN package will continue to be supported for existing customers on existing programs.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

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: 979-8-3371-2318-9

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.

© 2023-2025 Microchip Technology Inc. and its subsidiaries

Product Page Links

TA010, TA010-TFLXWPC

© 2023-2025 Microchip Technology Inc. and its subsidiaries