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

# TA100 (B5)

# CryptoAutomotive™ TA100 (B5) Summary Data Sheet

## Description

The Microchip Technology Inc. Trust Anchor security device TA100 is intended for automotive, industrial, or commercial systems and can provide support for code authentication (secure boot), Message Authentication Code (MAC) generation, support for trusted firmware updates, multiple key management protocols including Transport Layer Security (TLS), and other root-of-trust-based operations.

It is typically a companion device to an MCU or MPU on the same board.

## Features

- Advanced Crypto Engine (ACE) for Execution of All Cryptography Commands
- Fast Crypto Engine for SHA-256, HMAC and AES-CMAC Algorithms
- Sign/Verify Support:
  - ECDSA – P224, P256, P384 and 256-bit Brainpool elliptic curves
  - ECDSA – SECP256K1 (Bitcoin/Blockchain) curve
  - RSA 2048-bit signature generation and verification
  - RSA 3072-bit signature verification only
- ECDH/ECDHE/ECBD Key Agreement Support
  - Elliptic-Curve Diffie-Hellman (ECDH) Support for P224, P256, P384 and 256-bit Brainpool
  - Elliptic-Curve Burmeiseter-Desmedt (ECBD) Support for P224 Curve
- Internal Symmetric and Asymmetric Key Generation and Derivation:
  - P224, P256, P384 and 256-Bit Brainpool
  - 2048-bit RSA keys
  - AES 16-byte keys
- AES and RSA Encryption / Decryption Support
  - AES ECB/GCM Encryption/Decryption Supported directly
  - RSA 1024-bit and 2048-bit Keys Encryption/Decryption Support
- NIST SP800-90 A/B/C Random Number Generator (RNG)
- Multiple I/O Options for Security Commands Include:
  - 1 MHz standard I$^2$C interface
  - 16 MHz SPI interface
- Package Options:
  - 8-lead SOIC
  - 14-lead SOIC
- Voltage Supply Range: 2.7V to 5.5V
- Automotive Temperature Range: -40°C to +125°C Ambient Operating Range

## Applications

- Full and Partial Secure Boot

© 2020-2021 Microchip Technology Inc.
and its subsidiaries

- Secure Firmware Update
- CAN Message Authentication
- WPC 1.3 Qi High Power Transmitter Authentication
- High-Bandwidth Digital Content Protection (HDCP) Cryptographic Support
- Network Authentication and Session Establishment using TLS
- Electric Vehicle (EV) Battery Authentication

## Table of Contents

# 1. Pin Configuration

The TA100 device comes in three package configuration options based on the desired I/O interface. These include:

- SPI only interface in 8-pin SOIC
- I$^2$C only interface in 8-pin SOIC
- SPI and I$^2$C interfaces in 14-pin SOIC

Based on the configuration selected, different GPIO options are available.

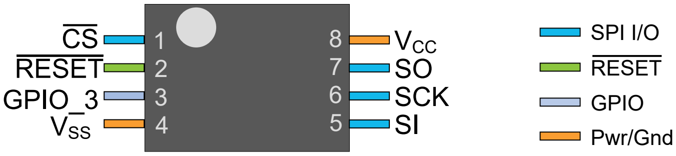
## 1.1 SOIC-8 Pinout with SPI Interface

The 8-pin SOIC SPI interface consists of the four SPI signals, a Reset signal and GPIO_3.

**Table 1-1. 8-Pin SOIC SPI Pin Configuration**

| Pin Name | Pin Number | Function |
|---|---|---|
| $\overline{\text{CS}}$ | 1 | Chip Select for SPI |
| $\overline{\text{RESET}}$ | 2 | Reset Input, active low |
| GPIO_3 | 3 | GPIO_3 |
| $V_{SS}$ | 4 | Ground |
| SI | 5 | SPI Serial Data Input |
| SCK | 6 | SPI Clock |
| SO | 7 | SPI Serial Data Output |
| $V_{CC}$ | 8 | 2.7V-5.5V Power Supply |

**Figure 1-1. Pinout**



## 1.2 SOIC-8 Pinout with I$^2$C Interface

Pull-up resistors are required for proper operation of the I$^2$C bus, sized according to the board configuration and bus speed per the I$^2$C specification.

**Table 1-2. 8-Pin SOIC I$^2$C Pin Configuration**

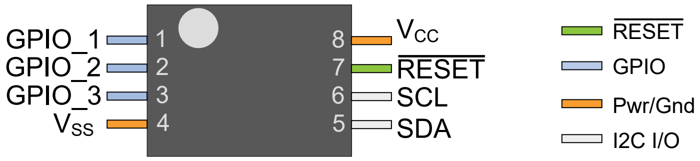
| Pin Name | Pin Number | Function |
|---|---|---|
| GPIO_1 | 1 | GPIO_1 |
| GPIO_2 | 2 | GPIO_2 |
| GPIO_3 | 3 | GPIO_3 |
| $V_{SS}$ | 4 | Ground |

© 2020-2021 Microchip Technology Inc.
and its subsidiaries

...........continued

| Pin Name | Pin Number | Function |
|---|---|---|
| SDA | 5 | $I^2C$ Data |
| SCL | 6 | $I^2C$ Clock |
| $\overline{\text{RESET}}$ | 7 | Reset Input, active low |
| $V_{CC}$ | 8 | 2.7V-5.5V Power Supply |

**Figure 1-2. Pinout**



## 1.3 SOIC-14 Pinout with $I^2C$ and SPI Interface

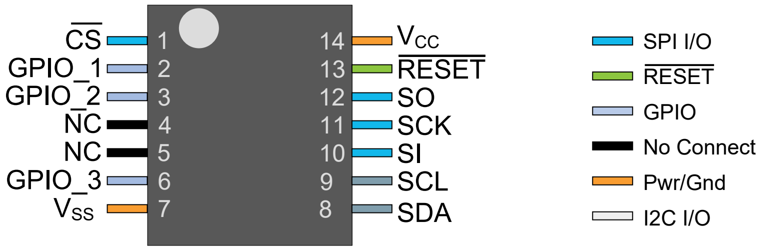
In the 14-pin package, there is access to both the $I^2C$ and SPI bus pins. Both can be used simultaneously. However, any concurrent transactions must be to different blocks in the device.

Pull-up resistors are required for proper operation of the $I^2C$ bus, sized according to the board configuration and bus speed required per the $I^2C$ specification.

**Table 1-3. 14-Pin SOIC Pin Configuration**

| Pin Name | Pin Number | Function |
|---|---|---|
| $\overline{\text{CS}}$ | 1 | Chip Select for SPI |
| GPIO_1 | 2 | General Purpose I/O pin |
| GPIO_2 | 3 | General Purpose I/O pin |
| NC | 4, 5 | Not Internally Connected |
| GPIO_3 | 6 | General Purpose I/O pin |
| $V_{SS}$ | 7 | Ground |
| SDA | 8 | $I^2C$ Data |
| SCL | 9 | $I^2C$ Clock |
| SI | 10 | SPI Serial Data Input |
| SCK | 11 | SPI Clock |
| SO | 12 | SPI Serial Data Output |
| $\overline{\text{RESET}}$ | 13 | Reset Input, active low |
| $V_{CC}$ | 14 | 2.7V-5.5V Power Supply |

**Figure 1-3. Pinout**



© 2020-2021 Microchip Technology Inc.
and its subsidiaries

# 2. Overview

The TA100 security device interfaces with a host MCU to provide a hardened root of trust with symmetric and asymmetric computation ability to facilitate a number of security-related capabilities within an automotive system.

- Secure boot support:
  - Host code image and signature validation
  - Secure encryption key storage and image encryption
  - Authenticated update of the code validation public key
- X.509 certificate storage, parsing, validation and revocation, supporting both ECC and RSA
- Fully internal random key generation for RSA, ECC and AES
- Monotonic counters protected against tearing
- Elliptic curves support:
  - P224 – ECDSA sign, verify, ECDH and ECBD
  - P256 – ECDSA sign, verify and ECDH
  - SECP256K1 (Bitcoin/Blockchain) – ECDSA support
  - 256-bit Brainpool – ECDSA and ECDH
  - P384 – ECDSA sign and verify
- RSA support:
  - 1024-bit and 2048-bit RSA OAEP/MGF encrypt/decrypt
  - 2048-bit RSA signature generation and verification
  - 3072-bit RSA verification
- ECDH key management capability with integrated KDF, either PRF or HKDF
- NIST SP800-90 A/B/C high-quality cryptographic random number generation
- TLS V1.2/V1.3 – Full session establishment support in conjunction with host SW
- AES-CMAC calculation and validation
- AES-ECB and GCM encrypt/decrypt for general purpose use
- SHA-256 and SHA-HMAC digest calculation
- Input/output encryption and authentication using AES-GCM, AES-CMAC and/or SHA-HMAC
- Flexible self-test support to meet FIPS 140 requirements
- Cryptographic support for High-Bandwidth Digital Content Protection (HDCP) V2.2

The TA100 device contains two processing blocks:

1. A main command processor that implements an Advanced Crypto Engine along with the management and session establishment functionality. The ACE can implement all symmetric and asymmetric crypto functions.
2. A Fast Crypto Engine capable of implementing AES and SHA calculations in parallel with the operation of the main command processor.

# 3. Device Features

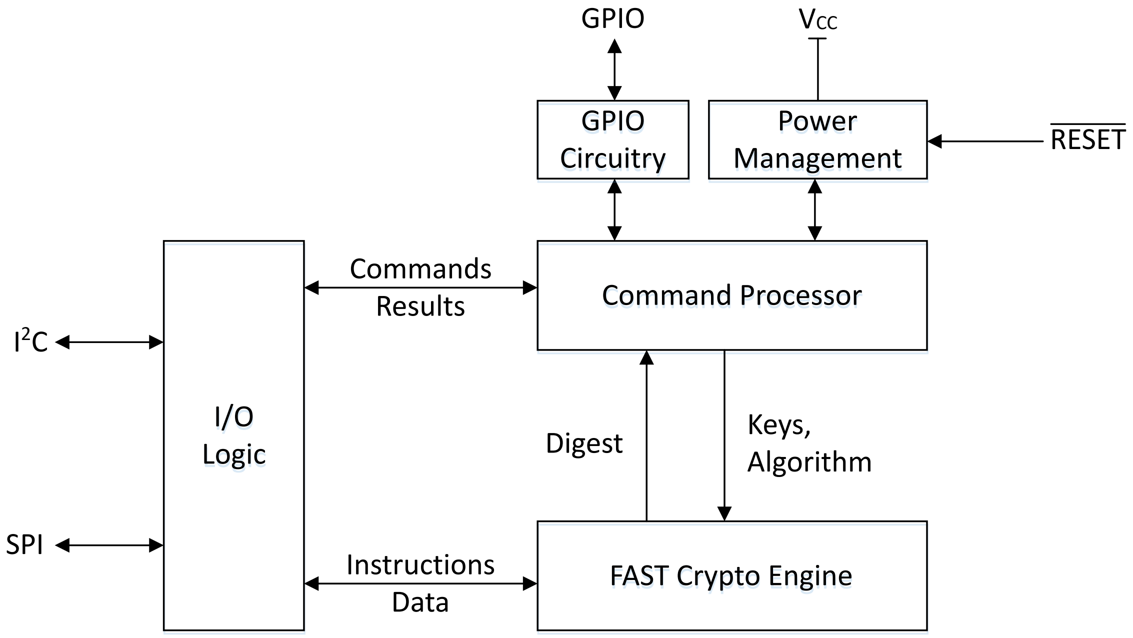
The TA100 device supports several broad features, including secure boot (host code authentication), MAC generation, secure key and certificate storage and management.

Public information stored within the protected memory, such as code digests, certificate validation status, public keys, etc., can only be modified when properly authorized by using the specified protocols in this data sheet.

The TA100 is powered by an internal microcontroller running dedicated software loaded into the ROM and nonvolatile memory during chip manufacture. Nonvolatile memory is used for certificate storage and secret/private key storage. There is no direct access to the memories from the external pins of the device and there is no available programming or debug interface.

The block diagram of the TA100 shows the major architectural features of the device.

**Figure 3-1. TA100 Block Diagram**



# 4. Nonvolatile Memory

The nonvolatile memory within the TA100 device is split into three pieces:

**Configuration Memory:** In general, this area is expected to be written prior to the placement of the TA100 device on the application board. Once the configuration is complete, this area must be locked to prevent further modification and for proper device operation.

**Shared Data Memory:** This area can be used for keys, secrets, certificates, and/or data. The TA100 does not place any requirements on the arrangement or distribution of items stored within this block other than the overall limit on the space available to all the shared elements.

**Dedicated Data Memory:** Certain other items are stored within the device and are managed directly by various commands.

© 2020-2021 Microchip Technology Inc.
and its subsidiaries

# 5. Security Features

The TA100 device includes protection against both active (invasive) and passive (noninvasive) attacks on the certificates, private and symmetric keys stored within the device. Specific hardware and firmware elements are included to prevent environmental (voltage, temperature and frequency) attacks, emissions attacks, fault attacks, physical attacks, cloning and many other attack methodologies. All internal memory for private/symmetric keys or other secret data is encrypted.

# 6. Electrical Characteristics

## 6.1 Absolute Maximum Ratings

| | |
|---|---|
| Ambient Temperature under Bias[1] | -40°C to +125°C |
| Storage Temperature (without Bias) | -65°C to +150°C |
| Maximum Supply Voltage | 6.0V |
| DC Voltage on Any Pin[4] | -0.5 to $V_{CC}$ + 0.5 |
| ESD Ratings | |
| — Human Body Model (HBM) ESD[2] | ≥ ±4 kV |
| — Charged Device Model (CDM) ESD[3] | ≥ ±750V |

**Notes:**

1. Recent Partial Networking Transceivers from Microchip and others use a spec throughout the document called the Virtual Junction Temperature, measured in accordance with IEC60747-1. An alternate definition is $T_{VJ} = T_A + P \times R_{th(j-a)}$, where P is the power and $R_{th(j-a)}$ is the thermal resistance from virtual junction to ambient. $T_{VJ}$ would be higher than +125°C (maximum).
2. Specified by: JEDEC® Standard JS-001-2017
3. Specified by: JEDEC® Standard JS-002-2014
4. $V_{CC}$ is the supply voltage to which the device is driven and must be within the specified operating voltage range.

**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 is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

## 6.2 DC Characteristics

**Table 6-1. DC Characteristics – All Interfaces**

*Applicable over the recommended operating range from $T_A$ = -40°C to +125°C, $V_{CC}$ = +2.7V to +5.5V.*

| Parameters | Test Conditions | Symbol | Min. | Typ. | Max. | Units | Type[1] |
|---|---|---|---|---|---|---|---|
| Supply Voltage on Pin $V_{CC}$ | — | $V_{CC}$ | 2.7 | — | 5.5 | V | A |
| Supply Current on Pin $V_{CC}$ | Active mode[4] | $I_{IO\_Active}$ | — | 25 | 40 | mA | A |
| | Idle mode[2] ($T_A$ = +85°C) | $I_{IO\_Idle}$ | — | — | 10 | mA | B |
| | Sleep mode | $I_{IO\_Sleep}$ | — | 7 | 15 | uA | B |
| $V_{CC}$ Rise Rate | — | $V_{RISE}$ | — | — | 0.1 | V/µs | C |
| High-Level Input Voltage | — | $V_{IH}$ | 0.7 x $V_{CC}$ | — | $V_{CC}$ + 0.3 | V | A |
| Low-Level Input Voltage | — | $V_{IL}$ | -0.3 | — | 0.3 x $V_{CC}$ | V | A |

© 2020-2021 Microchip Technology Inc.
and its subsidiaries

**Notes:**

1. Type means: A = 100% tested, B = characterized, C = design parameter.
2. Idle means that power is applied, the device is NOT in Sleep mode and no commands nor instructions are running.
3. The state of the $V_{CC}$ latches will be retained so long as $V_{CC}$ remains above the $V_{POR}$ level.
4. Active current is measured with all GPIO pins either driven to ground or configured as inputs. Active current also excludes any DC load on the I/O pins.

**Table 6-2. DC Characteristics – SPI Interface, $\overline{\text{RESET}}$ and GPIO Pins**

*Applicable over the recommended operating range from $T_A$ = -40°C to +125°C, $V_{CC}$ = +2.7V to +5.5V.*

| Parameters | Test Conditions | Symbol | Min. | Typ. | Max. | Units | Type[1] |
|---|---|---|---|---|---|---|---|
| Input Current[2] | $0.1V_{CC} < Vi < 0.9V_{CC}$ | $I_L$ | -2 | — | +2 | µA | A |
| Programmable Pull-Up | — | $R_{PU}$ | 24k | 40k | 62k | Ω | A |
| High-Level Output Voltage | $I_{OH}$ = -4 mA | $V_{OH}$ | $V_{CC}$ – 0.4 | — | — | V | A |
| Low-Level Output Voltage | $I_{OL}$ = 4 mA | $V_{OL}$ | — | — | 0.4 | V | A |

**Notes:**

1. Type means: A = 100% tested
2. This specification is only valid when the internal pull-ups are disabled. Otherwise, the input current is determined by the internal pull-up resistance value $R_{PU}$.

**Table 6-3. DC Characteristics of SDA and SCL Pins for I²C Interface**

*Applicable over the recommended operating range from $T_A$ = -40°C to +125°C, $V_{CC}$ = +2.7V to +5.5V.*

| Parameters | Test Conditions | Symbol | Min. | Typ | Max. | Units | Type[1] |
|---|---|---|---|---|---|---|---|
| Input Current[2] | $0.1V_{CC} < Vi < 0.9V_{CC}$ | Ii | -10 | — | +10 | µA | A |
| Low-Level Output Voltage | $I_{OL}$ = 20 mA<br>$V_{CC}$ > 3.6V to 5.5V | $V_{OL}$ | 0 | — | 0.4 | V | B |
| | $I_{OL}$ = 14 mA<br>$V_{CC}$ = 2.7V to 3.6V | $V_{OL}$ | 0 | — | 0.4 | V | B |
| Programmable Pull-Up | — | $R_{PU}$ | 2.3k | 3.0k | 4.5k | Ω | A |

**Notes:**

1. Type means: A = 100% tested, B = characterized on samples
2. The input current specification is only valid when the internal pull-ups are disabled. Otherwise, the input current is determined by the internal pull-up resistance value $R_{PU}$.

## 6.3 AC Characteristics

### 6.3.1 All Interfaces

**Table 6-4. AC Timing Characteristics – All Interfaces**

*Applicable over the recommended operating range from $T_A$ = -40°C to +125°C, $V_{CC}$ = +2.7V to +5.5V.*

| Parameters | Symbol | Min. | Typ. | Max. | Units | Type[4] |
|---|---|---|---|---|---|---|
| Wake-up Time from Sleep State. $V_{CC}$ > 2.7V | $t_{PU.SLEEP}$[1] | — | 3 | 5 | ms | A |
| Power-up Time from $V_{CC}$ < 2.7V | $t_{PU.POWERON}$[1] | — | 4 | 6 | ms | A |

© 2020-2021 Microchip Technology Inc.
and its subsidiaries

...........continued

| Parameters | Symbol | Min. | Typ. | Max. | Units | Type[4] |
|---|---|---|---|---|---|---|
| Idle Tmer | $t_{IDLE}$[2] | 0.85 | 1 | 1.15 | s | B |
| Rate at which the Nonvolatile Portion of Monotonic Counter Increments | $t_{MONOTONIC}$ | 42 | 51 | 60 | s | B |
| Noise Suppression on $\overline{\text{RESET}}$ Input Pin | $t_{RESET\_NOISE}$[3] | 0 | — | 0.150 | µs | A |
| Minimum Allowed Reset Pulse | $t_{RESET\_MIN}$[3] | 1.0 | — | — | µs | A |
| GPIO_3 Transition Ignored, Measured Starting with the Last Bit of Power (Sleep) | $t_{SLEEP\_WAKE}$ | — | — | 250 | µs | A |
| Low-Pulse Width for GPIO_3 High to Wake TA100 | $t_{WAKE\_GPIO\_LOW}$ | 40 | — | — | µs | A |
| Watchdog Time-out Value | $t_{WATCHDOG}$ | 900 | 1000 | 1100 | ms | B |

**Notes:**

1. Various situations can cause the power-up delays to exceed these parameters as follows:
   – If the power-on or the wake self-test functions are enabled in the configuration area, the execution of those self-test operations will increase the delay.
   – If an internal failure occurs to cause a boot event, then, there may be an additional delay during the boot to write the internal failure log in the nonvolatile memory within the chip.
   – If a device update is started but does not complete due to a power interruption, on the next power-up, some cleanup may be required and may take additional time.
   – If the 1 minute timer is enabled and is being updated in the nonvolatile memory concurrent with the wake event, the device will accept an `Input` command after $t_{PU\_SLEEP}/t_{PU\_POWERON}$, but will not start the execution of that command until the nonvolatile update is complete.
2. The idle timer specifications here assume that the idle timer is enabled and configured for 1 second. It is recommended that these times be multiplied by the delay time value set in the idle timer configuration field if that is not 1.
3. All noise pulses ≤ $t_{RESET\_NOISE}$ are assured to be suppressed. All pulse widths ≥ $t_{RESET\_MIN}$ are assured to pass to the device. Pulses in between these values may or may not be suppressed.
4. Type Means: A = 100% Tested, B = Characterized.

### 6.3.2 I²C Interface Timing

**Table 6-5. AC Characteristics of I²C Interface**

*Applicable over the recommended operating range from $T_A$ = -40°C to +125°C, $V_{CC}$ = +2.7V to +5.5V.*

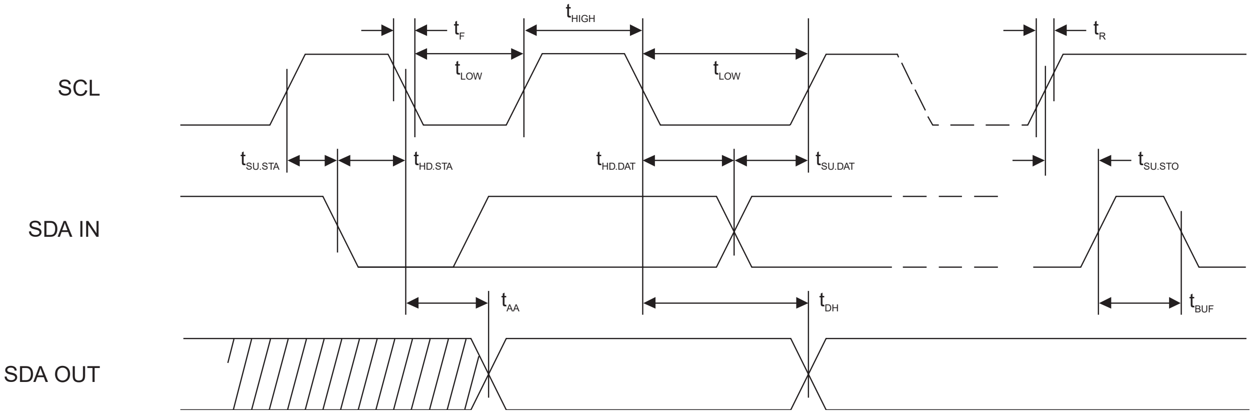
| Parameters | Symbol | Fast-Mode Plus | | Units |
|---|---|---|---|---|
| | | Min. | Max. | |
| SCL Clock Frequency | $f_{SCL}$ | — | 1000 | kHz |
| SCL High Time | $t_{HIGH}$ | 260 | — | ns |
| SCL Low Time | $t_{LOW}$ | 500 | — | ns |
| Start Setup Time | $t_{SU.STA}$ | 260 | — | ns |
| Start Hold Time | $t_{HD.STA}$ | 260 | — | ns |
| Stop Setup Time | $t_{SU.STO}$ | 260 | — | ns |
| Data in Setup Time | $t_{SU.DAT}$ | 50 | — | ns |
| Data in Hold Time | $t_{HD.DAT}$ | 0 | — | ns |
| Input Rise Time[1, 3] | $t_R$ | — | 120 | ns |

| ...........continued | | | | |
|---|---|---|---|---|
| Parameters | Symbol | Fast-Mode Plus | | Units |
| | | Min. | Max. | |
| Input Fall Time[1, 3] | $t_F$ | 20 x ($V_{DD}$/5.5V)[5] | 120 | ns |
| Clock Low to Data Out Valid | $t_{AA}$ | — | 450 | ns |
| Time bus must be free before a new transmission can start [1] | $t_{BUF}$ | 500 | — | ns |
| Pulse width of spikes that must be suppressed by the input filter[4] | $t_{SP}$ | — | 50 | ns |

**Notes:**

1. Values are based on characterization and are not tested.
2. AC measurement conditions: input pulse voltages: 0.3 x $V_{CC}$ to 0.7 x $V_{CC}$, input rise and fall times: ≤ 50 ns.
3. System designers must ensure that all AC parametrics are met. Rise fall times shown are for the Fast Mode Plus (1 MHz) of operation. For slower clock speeds, the rise and fall times may be increased but must still meet the industry standard I$^2$C specification UM10204.
4. Input filters on the SDA and SCL pins will suppress noise spikes of less than 50 ns.
5. Backwards compatibility is necessary for the Fast mode (400 kHz) specifications.

**Figure 6-1. I$^2$C Synchronous Data Timing**



### 6.3.3 SPI Interface Timing

**Table 6-6. AC Characteristics of SPI Interface**

*Applicable over the recommended operating range from $T_A$ = -40°C to +125°C, $V_{CC}$ = +2.7V to +5.5V.*

| Parameters | Symbol | Min. | Max. | Units |
|---|---|---|---|---|
| SCK Clock Frequency | $f_{SCK}$ | — | 16 | MHz |
| SCK High Time | $t_{WH}$ | 20 | — | ns |
| SCK Low Time | $t_{WL}$ | 25 | — | ns |
| $\overline{CS}$ High Time | $t_{CS}$ | 100 | — | ns |
| $\overline{CS}$ Setup Time | $t_{CSS}$ | 100 | — | ns |
| $\overline{CS}$ Hold Time | $t_{CSH}$ | 100 | — | ns |
| Data in Setup Time | $t_{SU}$ | 5 | — | ns |
| Data in Hold Time | $t_H$ | 5 | — | ns |
| Input Rise Time[1, 2] | $t_{RI}$ | — | 2 | µs |

© 2020-2021 Microchip Technology Inc.
and its subsidiaries

...........continued

| Parameters | Symbol | Min. | Max. | Units |
|---|---|---|---|---|
| Input Fall Time[1, 2] | $t_{FI}$ | — | 2 | µs |
| Output Valid | $t_V$ | — | 25 | ns |
| Output Hold Time | $t_{HO}$ | 0 | — | ns |
| Output Disable Time | $t_{DIS}$ | — | 25 | ns |

**Notes:**

1. Values are based on characterization and are not production tested.
2. System designers must ensure that all AC parametrics are met, which will typically require rise and fall times faster than these values for most clock rates. Ramp rates slower than this may result in improper operation.

**Figure 6-2. SPI Mode 0 Synchronous Data Timing**

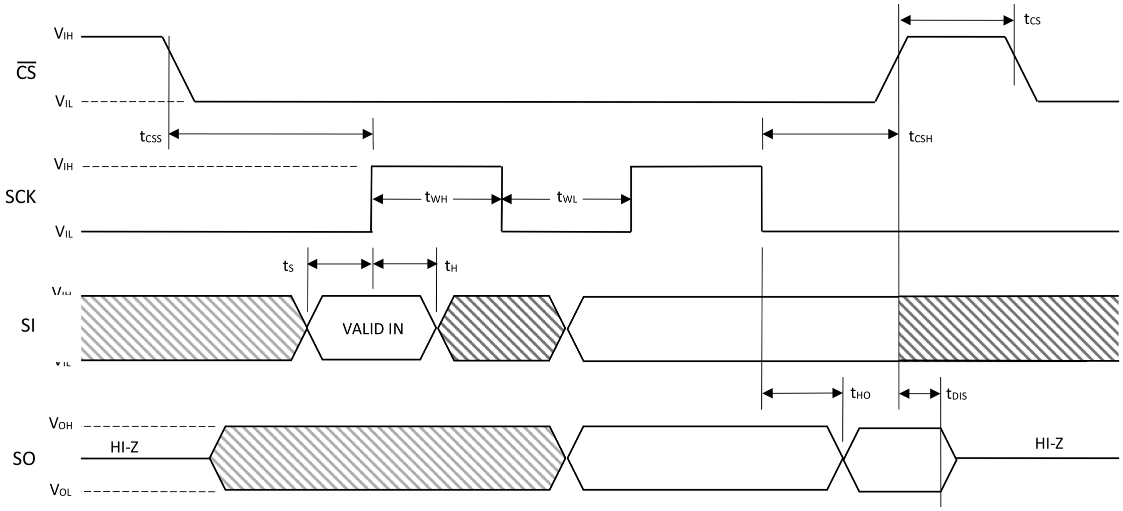
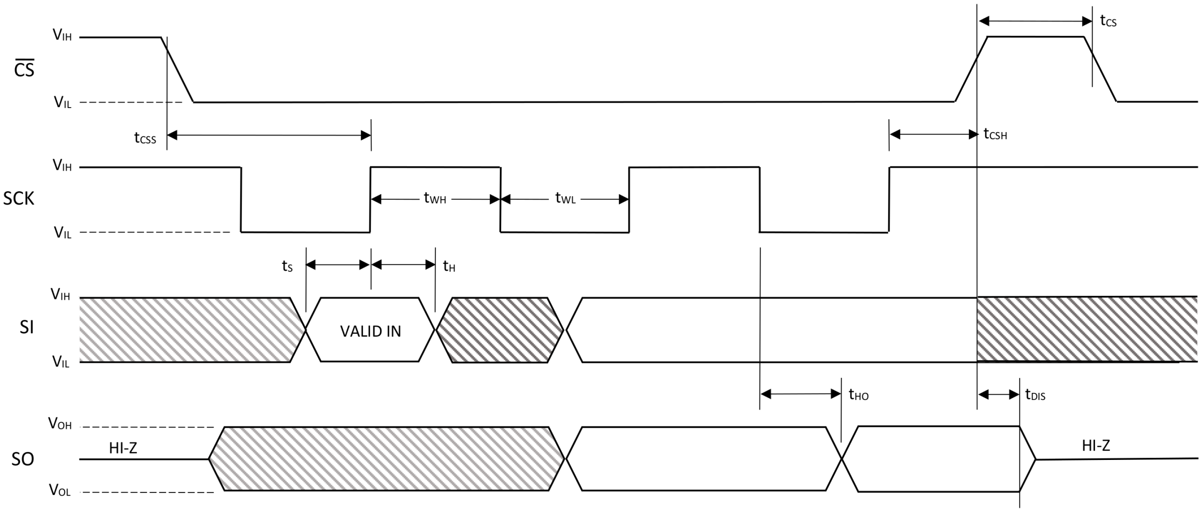


**Figure 6-3. SPI Mode 3 Synchronous Data Timing**



© 2020-2021 Microchip Technology Inc.
and its subsidiaries

# 7. Package Marking Information

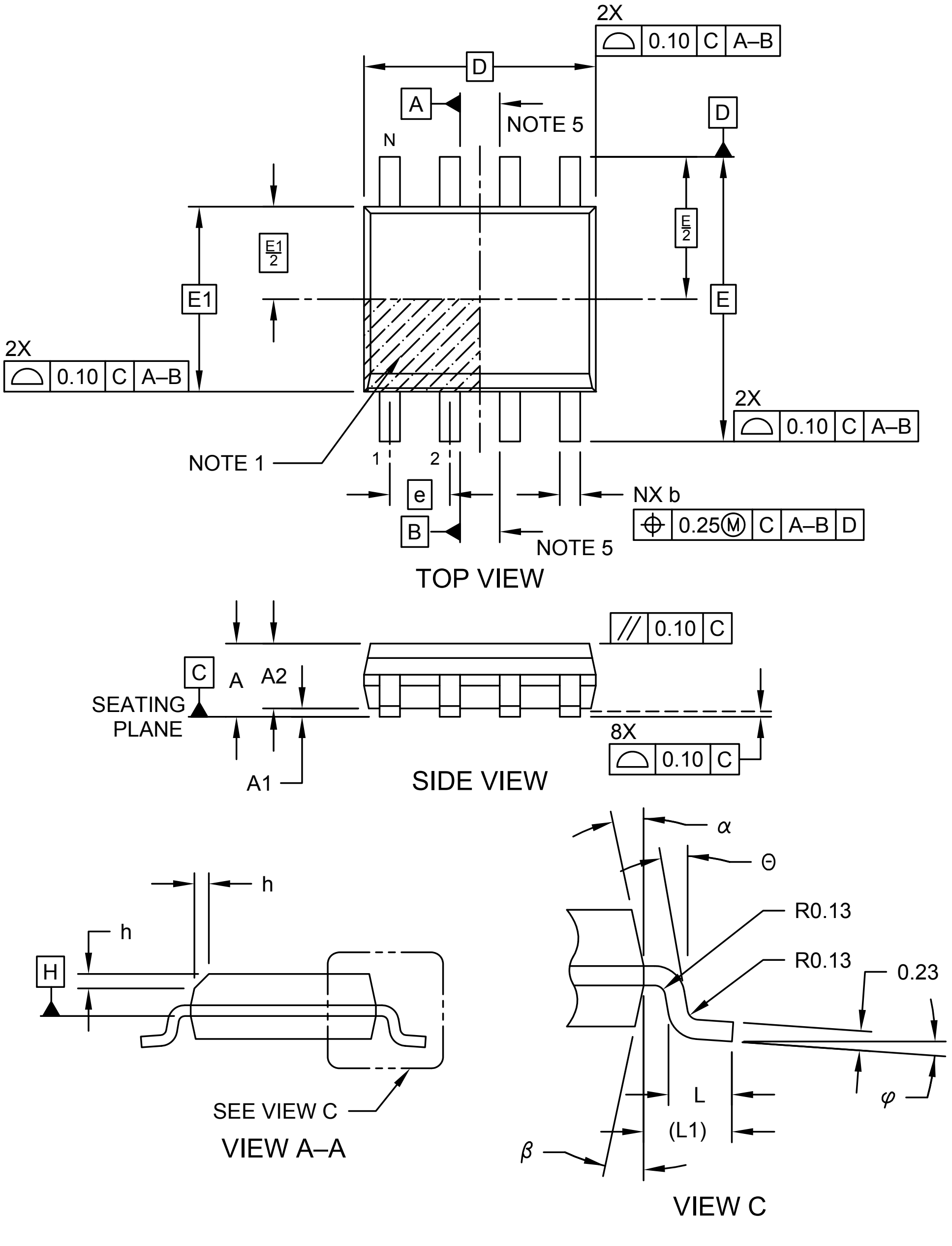
As part of Microchip's overall security features, the part marking for all crypto devices is intentionally vague. The marking on the top of the package does not provide any information as to the actual device type or the manufacturer of the device. The alphanumeric code on the package provides manufacturing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

# 8. Package Drawings

## 8.1 8-Lead SOIC

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

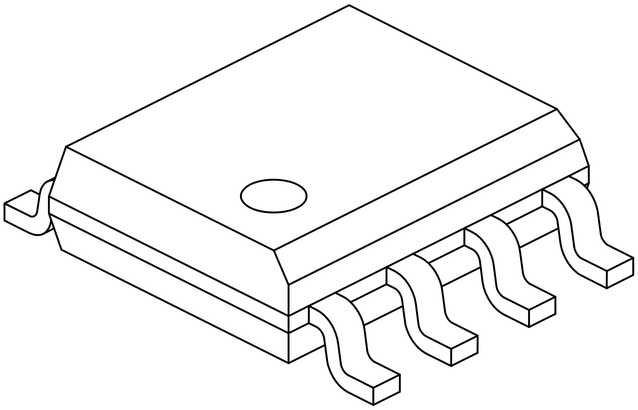
**Note:** For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing No. C04-057-OA Rev F Sheet 1 of 2

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

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



| Units | | MILLIMETERS | | |
|---|---|---|---|---|
| Dimension Limits | | MIN | NOM | MAX |
| Number of Pins | N | 8 | | |
| Pitch | e | 1.27 BSC | | |
| Overall Height | A | - | - | 1.75 |
| Molded Package Thickness | A2 | 1.25 | - | - |
| Standoff § | A1 | 0.10 | - | 0.25 |
| Overall Width | E | 6.00 BSC | | |
| Molded Package Width | E1 | 3.90 BSC | | |
| Overall Length | D | 4.90 BSC | | |
| Chamfer (Optional) | h | 0.25 | - | 0.50 |
| Foot Length | L | 0.40 | - | 1.27 |
| Footprint | L1 | 1.04 REF | | |
| Foot Angle | $\varphi$ | 0° | - | 8° |
| Lead Thickness | c | 0.17 | - | 0.25 |
| Lead Width | b | 0.31 | - | 0.51 |
| Mold Draft Angle Top | $\alpha$ | 5° | - | 15° |
| Mold Draft Angle Bottom | $\beta$ | 5° | - | 15° |

Notes:

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

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

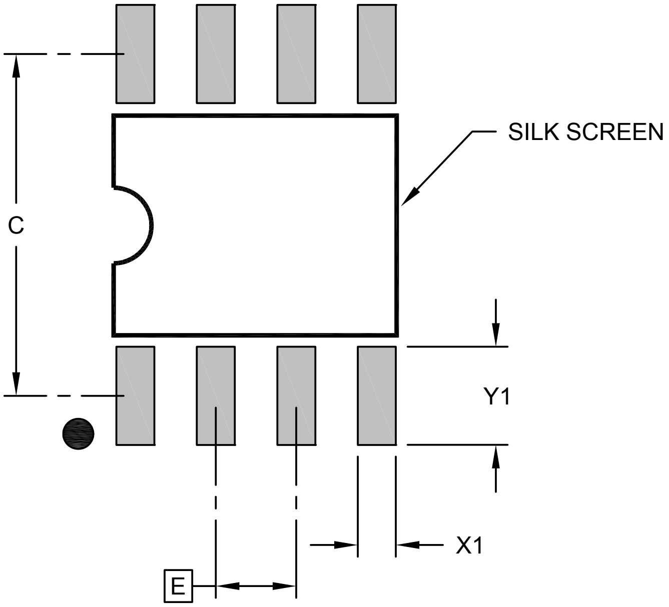
   REF: Reference Dimension, usually without tolerance, for information purposes only.
5. Datums A & B to be determined at Datum H.

Microchip Technology Drawing No. C04-057-OA Rev F Sheet 2 of 2

© 2020-2021 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.

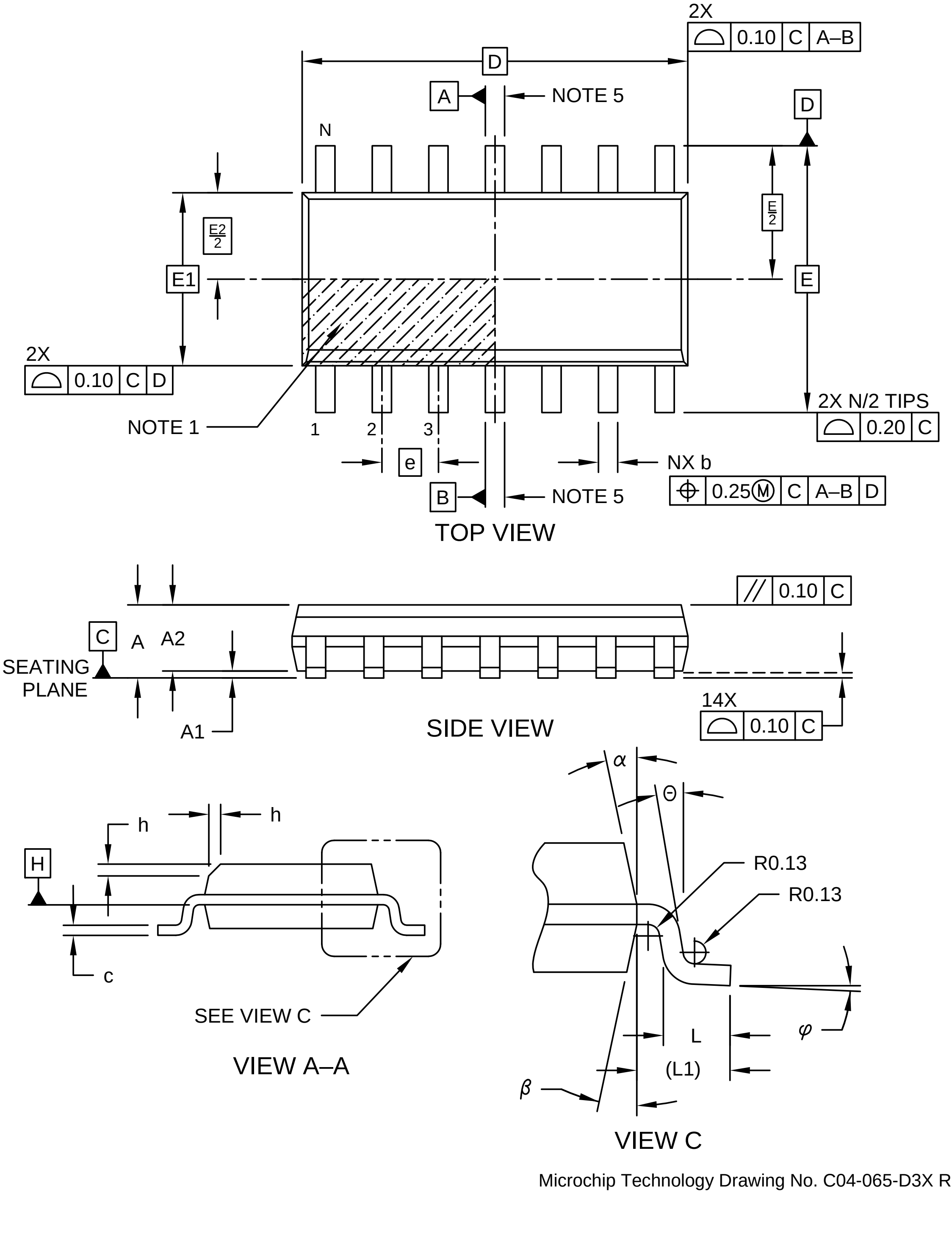
Microchip Technology Drawing C04-2057-OA Rev F

© 2020-2021 Microchip Technology Inc.
and its subsidiaries

## 8.2 14-Lead SOIC

### 14-Lead Plastic Small Outline (D3X, UEB, M5B, UEB) - Narrow, 3.90 mm Body [SOIC] Atmel Legacy Global Package Code SVQ

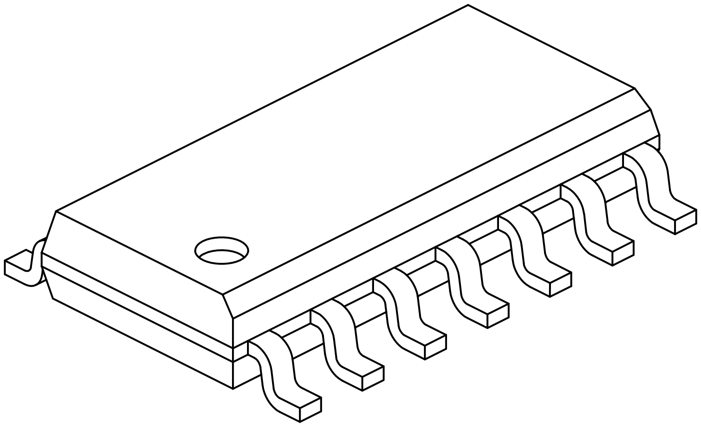
| **Note:** | For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging |
|---|---|



Microchip Technology Drawing No. C04-065-D3X Rev D

## 14-Lead Plastic Small Outline (D3X, UEB, M5B, UEB) - Narrow, 3.90 mm Body [SOIC] Atmel Legacy Global Package Code SVQ

**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 | 14 | | |
| 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 | 8.65 BSC | | |
| Chamfer (Optional) | h | 0.25 | - | 0.50 |
| Foot Length | L | 0.40 | - | 1.27 |
| Footprint | L1 | 1.04 REF | | |
| Lead Angle | Θ | 0° | - | - |
| Foot Angle | $\varphi$ | 0° | - | 8° |
| Lead Thickness | c | 0.10 | - | 0.25 |
| Lead Width | b | 0.31 | - | 0.51 |
| Mold Draft Angle Top | $\alpha$ | 5° | - | 15° |
| Mold Draft Angle Bottom | $\beta$ | 5° | - | 15° |

Notes:

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. § Significant Characteristic
3. Dimension D does not include mold flash, protrusions or gate burrs, which shall not exceed 0.15 mm per end. Dimension E1 does not include interlead flash or protrusion, which shall not exceed 0.25 mm per side.
4. Dimensioning and tolerancing per ASME Y14.5M

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

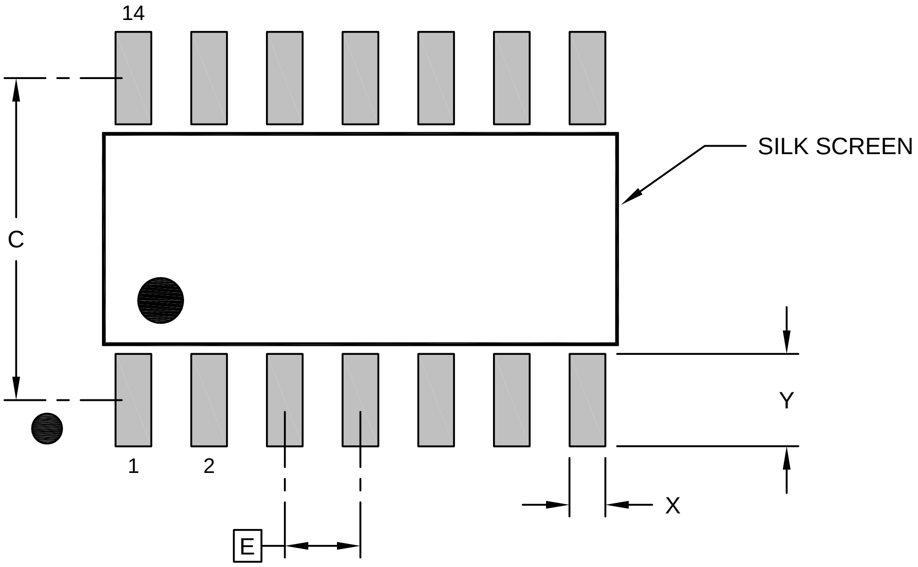
   REF: Reference Dimension, usually without tolerance, for information purposes only.
5. Datums A & B to be determined at Datum H.

Microchip Technology Drawing No. C04-065-D3X Rev D Sheet 2 of 2

© 2020-2021 Microchip Technology Inc.
and its subsidiaries

## 14-Lead Plastic Small Outline (D3X, UEB, M5B, UEB) - Narrow, 3.90 mm Body [SOIC] Atmel Legacy Global Package Code SVQ

**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 (X14) | X | | | 0.60 |
| Contact Pad Length (X14) | Y | | | 1.55 |

Notes:

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

Microchip Technology Drawing No. C04-2065-D3X Rev D

© 2020-2021 Microchip Technology Inc.
and its subsidiaries

# 9. Revision History

**Revision C (Dec 2021)**

- Removed References to 24-VQFN Package. Not an option for B5 Silicon.
- Added Type of testing column to Table 6-4
- Added Figure 6-3 for SPI Mode 3 Timing information.

**Revision B (Feb 2021)**

- Updated Feature List to include RSA signature generation and verification capabilities
- Correction to Table 6-2 RPU Max value
- Update to Product Identification System

**Revision A (Nov 2020)**
Original release of the document

## The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **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 (FAQs), technical support requests, online discussion groups, Microchip design partner 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

## Product Change Notification Service

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

To register, go to www.microchip.com/pcn and follow the registration instructions.

## Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: 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 | I/O Type | - | Temperature Range | IC Revision | Package Option | Firmware Revision | - | OTS | Shipping Format | - | Product Identifier |
|---|---|---|---|---|---|---|---|---|---|---|---|
| xxxxx | y | - | t | xxx | ppp | ff | - | cc | s | - | VAO |

| Device: | TA100 | |
|---|---|---|
| I/O Type | Blank | 14-Pin SOIC SPI and $I^2C$ Interfaces |
| | Blank | 8-PIN SOIC SPI Interface Only |
| | T | 8-PIN SOIC $I^2C$ Interface Only |
| Temperature Range: | Y | -40℃ to +125℃ |
| IC Revision[2] | xxx | Contact Microchip for Information |
| Package Option | C2X | 8-Pin SOIC |
| | D3X | 14-Pin SOIC |
| Firmware Revision | 01 | Firmware Release 01 |
| | 02 | Firmware Release 02 |
| OTS or Customer Code | 00 | Standard Configuration |
| | PD | SPI Pull-ups Disabled |
| Shipping Options | T | Tape and Reel[1] |
| | B | Bulk Units |
| Product Identifier | VAO | Generic Automotive Product |

Examples:

| Customer Ordering Code | I/O Interfaces | Internal $I^2C$ Pull-up | Package | Delivery | Personalization |
|---|---|---|---|---|---|
| TA100T-Y230C2X01-00T-VAO | $I^2C$ | No | SOIC-8 | Tape and Reel | Standard Configuration |
| TA100T-Y230C2X01-00B-VAO | $I^2C$ | No | SOIC-8 | Bulk | Standard Configuration |
| TA100-Y230C2X01-00T-VAO | SPI | — | SOIC-8 | Tape and Reel | Standard Configuration |
| TA100-Y230C2X01-PDT-VAO | SPI | — | SOIC-8 | Tape and Reel | SPI Pull-ups Disabled |
| TA100-Y230C2X01-00B-VAO | SPI | — | SOIC-8 | Bulk | Standard Configuration |
| TA100-Y230C2X01-PDB-VAO | SPI | — | SOIC-8 | Bulk | SPI Pull-ups Disabled |
| TA100-Y230D3X01-00T-VAO | $I^2C$, SPI | No | SOIC-14 | Tape and Reel | Standard Configuration |
| TA100-Y230D3X01-00B-VAO | $I^2C$, SPI | No | SOIC-14 | Bulk | Standard Configuration |

**Notes:**

1. Tape and Reel identifier only appears in the catalog part number description. This identifier is used for ordering purposes and is not printed on the device package. Check with your Microchip Sales Office for package availability with the Tape and Reel option.
2. IC Revision code indicates the base silicon revision and ROM code revision.

## 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 product is 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.

## 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.

## Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AnyRate, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, CryptoMemory, CryptoRF, dsPIC, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, IntelliMOS, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet- Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, TrueTime, WinPath, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, Augmented Switching, BlueSky, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController,

dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, GridTime, IdealBridge, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, NVM Express, NVMe, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, TSHARC, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, Symmcom, and Trusted Time are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2020-2021, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.

ISBN: 978-1-5224-8955-9

## Quality Management System

For information regarding Microchip’s Quality Management Systems, please visit www.microchip.com/quality.

# Worldwide Sales and Service

## AMERICAS

**Corporate Office**
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
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

## ASIA/PACIFIC

**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

## ASIA/PACIFIC

**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

## EUROPE

**Austria - Wels**
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

**Denmark - Copenhagen**
Tel: 45-4485-5910
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: 49-7131-72400

**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