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

TA101 CryptoAutomotive™ Summary Data Sheet

TA101

Description

The Microchip Technology Inc. Trust Anchor security device TA101 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 (FCE) – High-Speed Hardware Cryptographic Functions
  - AES-CMAC (128-bit) calculation and validation at SPI bus speed (up to 16 MHz)
  - SHA-256, HMAC-SHA256 at SPI bus speed (up to 16 MHz)
- Elliptic Curves Support: ECC
  - P-224 – Elliptic Curve Digital Signature Algorithm (ECDSA) sign, verify, KeyGen, Elliptic Curve Diffie–Hellman (ECDH) and Elliptic-Curve Burmester-Desmedt (ECBD)
  - P-256 – ECDSA sign, verify, KeyGen and ECDH
  - P-384 – ECDSA sign, verify, KeyGen and ECDH
  - P-521 – ECDSA sign, verify, KeyGen and ECDH
  - Ed25519 – EdDSA sign, verify and KeyGen
    - Supported Modes: Pure, CTX, PH
  - X25519 – KeyGen and ECDH
  - Secp256k1 (Bitcoin/Blockchain) – ECDSA sign, verify and KeyGen
  - 256-bit Brainpool – ECDSA sign, verify, KeyGen and ECDH
- RSA Support:
  - 1024-bit, 2048-bit, 3072-bit, 4096-bit RSA-OAEP encrypt/decrypt
  - 2048-bit, 3072-bit, 4096-bit RSA signature generation and verification
  - 2048-bit, 3072-bit, 4096-bit RSA key generation and key derivation
- Symmetric Cryptography and Algorithm Support
  - AES Key Generation (16- or 32-byte keys)
  - AES-ECB encryption/decryption (128-bit, 256-bit). Support for external API software implementation with host MCU of alternate ciphers CBC, CCM, Counter mode and others
  - AES-CMAC (128-bit, 256-bit) calculation and validation
  - Authenticated Encryption with Associated Data (AEAD) using AES-GCM (128-bit or 256-bit supporting single and split modes)
  - SHA-256, SHA-384, SHA-512 and HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512 digest calculation

- ECDH Key Management Capability with Integrated KDF in Counter Mode Using HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512
- Multiple Key Derivation Functions (KDF) are Supported
  - Includes PRF, HKDF, SP800-108 KDF and SHA-256 one-step KDF
  - TLS V1.2 – Full-session establishment support including PRF KDF in conjunction with host SW
  - TLS V1.3 – Full-session establishment support including HKDF in conjunction with host SW
  - Cryptographic support for HDCP V2.2 including two specific AES options for key management
- Certifications
  - NIST SP800-90 A/B/C Random Number Generator (RNG)
  - NIST compliance mode to allow FIPS 140-3 security rules to be enforced. Allows for formal NIST certification
  - Vulnerability Assessment Rating of JIL High
- 6k to 11k Bytes of Available User Memory (Varies with the Number of Stored Keys)
- Multiple I/O Options for Security Commands Include:
  - 1 MHz standard I^2C interface
  - 16 MHz SPI interface Modes 0 and 3
- Package Options:
  - 8-lead SOIC
  - 24-pad 4 mm x 4 mm VQFN
- Voltage Supply Range: 2.7V to 5.5V
- AEC-Q100 Automotive Qualified
- Automotive Grade 1 Temperature Range: -40°C to +125°C Ambient Operating Range

Use Cases

- Validation of Code Integrity via Full or Partial Secure Boot
- Secure Firmware Update
- CAN Message Authentication
- WPC 1.3 Qi High Power Transmitter Authentication
- High-Bandwidth Digital Content Protection (HDCP) Cryptographic Support
- Secure Network Authentication and Session Establishment using TLS
- Electric Vehicle (EV) Battery Authentication

Table of Contents

1. Pin Configuration

The TA101 device is available in three package configuration options based on the desired I/O interface. These include:

- SPI-only interface in 8-pin SOIC
- I^2C-only interface in 8-pin SOIC
- SPI and I^2C interfaces in 24-pin 4 mm x 4 mm VQFN with 0.5 mm pad pitch

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

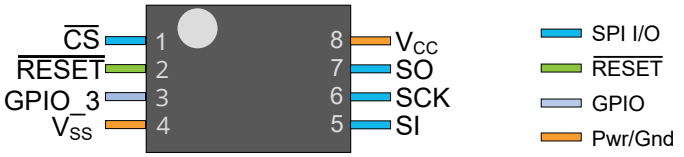
1.1 SOIC-8 Pinout with SPI Interface

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
$\overline{CS}$	1	Chip Select for SPI
$\overline{RESET}$	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



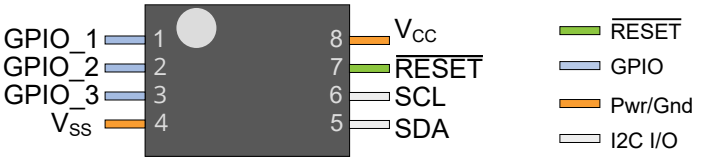
1.2 SOIC-8 Pinout with I^2C Interface

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

Table 1-2. 8-Pin SOIC I^2C 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
SDA	5	I^2C Data
SCL	6	I^2C Clock
$\overline{RESET}$	7	Reset Input, active low
V_{CC}	8	2.7V-5.5V Power Supply

Figure 1-2. Pinout



1.3 VQFN-24 Pinout with I²C and SPI Interface

In the 24-pin VQFN package, there is access to both the I²C and SPI bus pins. Both can be used simultaneously. However, any concurrent transactions must be to different blocks in the device.

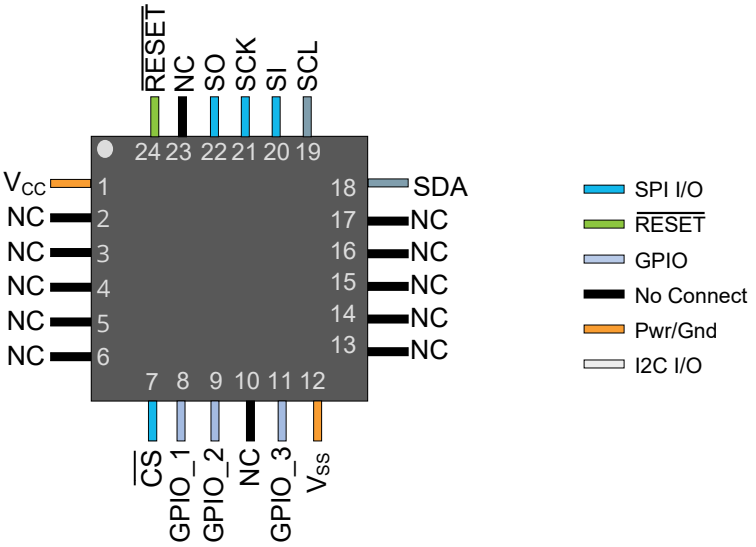
Pull-up resistors are required for proper operation of the I²C bus, sized according to the board configuration and bus speed required per the I²C specification.

Table 1-3. 24-Pin VQFN Pin Configuration

Pin Name	Pin Number	Function
V_{CC}	1	2.7V-5.5V Power Supply
NC	2, 3, 4, 5, 6, 10, 13, 14, 15, 16, 17, 23	Not Internally Connected
$\overline{CS}$	7	Chip Select for SPI
GPIO_1	8	General Purpose I/O pin
GPIO_2	9	General Purpose I/O pin
GPIO_3	11	General Purpose I/O pin
V_{SS}	12	Ground
SDA	18	I²C Data
SCL	19	I²C Clock
SI	20	SPI Serial Data Input
SCK	21	SPI Clock
SO	22	SPI Serial Data Output
$\overline{RESET}$	24	Reset Input, active low

Note: The exposed paddle is electrically isolated from the die. It is recommended that this be connected to GND.

Figure 1-3. Pinout



2. Overview

The TA101 security device interfaces with a host MCU to provide a hardened Root-of-Trust (RoT) with symmetric and asymmetric computation ability to facilitate multiple security-related capabilities within an automotive system. The algorithm summary tables referenced below highlight the individual cryptographic algorithms' support within the device. These algorithms allow the following functional capabilities within the product:

- Secure boot support: Validation of the host code image and host code signature validation. Support for both 128-bit and 256-bit security strength functions.
- X.509 certificate storage, parsing and validation, supporting both ECC and RSA
- Monotonic counters protected against tearing
- Elliptic curves support: ECC
  - P-224 – Elliptic Curve Digital Signature Algorithm (ECDSA) sign, verify, KeyGen, Elliptic Curve Diffie–Hellman (ECDH) and Elliptic-Curve Burmester-Desmedt (ECBD)
  - P-256 – ECDSA sign, verify, KeyGen and ECDH
  - P-384 – ECDSA sign, verify, KeyGen and ECDH
  - P-521 – ECDSA sign, verify, KeyGen and ECDH
  - Ed25519 – EdDSA sign, verify and KeyGen
  - X25519 – KeyGen and ECDH
  - Secp256k1 (Bitcoin/Blockchain) – ECDSA sign, verify and KeyGen
  - 256-bit Brainpool – ECDSA sign, verify, KeyGen and ECDH
- RSA Support:
  - 1024-bit, 2048-bit, 3072-bit, 4096-bit RSA-OAEP encrypt/decrypt
  - 2048-bit, 3072-bit, 4096-bit RSA signature generation and verification
  - 2048-bit, 3072-bit, 4096-bit RSA key generation and key derivation
- ECDH key management capability with integrated KDF in Counter mode using HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512
- Multiple Key Derivation Functions (KDF) are supported
  - Includes PRF, HKDF, SP800-108 KDF and SHA-256 one-step KDF
  - TLS V1.2 – Full-session establishment support including PRF KDF in conjunction with host SW
  - TLS V1.3 – Full-session establishment support including HKDF in conjunction with host SW
  - Cryptographic support for HDCP V2.2 including two specific AES options for key management
- Symmetric Cryptography and Algorithm Support
  - AES Key Generation (16 or 32 byte keys)
  - AES-ECB encryption/decryption (128-bit, 256-bit). Support for external API software implementation with host MCU of alternate ciphers CBC, CCM, Counter mode and others
  - AES-CMAC (128-bit, 256-bit) calculation and validation
  - Authenticated Encryption with Associated Data (AEAD) using AES-GCM (128-bit or 256-bit supporting single and split modes)
  - SHA-256, SHA-384, SHA-512 and HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512 digest calculation
- NIST SP800-90 Random Number Generator (RNG) – 256-bit security strength
- Approximately 6k to 11k bytes of available user memory (varies with the number of stored keys)

- I/O buffer with a maximum size of 1024 bytes
- Advanced Crypto Engine (ACE) for Execution of All Cryptography Commands
- Fast Crypto Engine (FCE) – High-speed hardware cryptographic functions
  - AES-CMAC (128-bit) calculation and validation at SPI bus speed (up to 16 MHz)
  - SHA-256, HMAC-SHA256 at SPI bus speed (up to 16 MHz)
- Multiple I/O options for security commands include:
  - 1 MHz Standard I^2C interface
  - 16 MHz SPI protocol, I/O type 0 and 3

The TA101 will be certified to the FIPS 140-3 certification scheme.

The TA101 was developed to achieve a vulnerability assessment rating of JIL High for the protection level of the private/secret keys in accordance with the vulnerability analysis scoring procedure defined in the specification: JIL-Application-of-Attack-Potential-to-Smartcards-and-Similar-Devices_v3-1.

3. Device Features

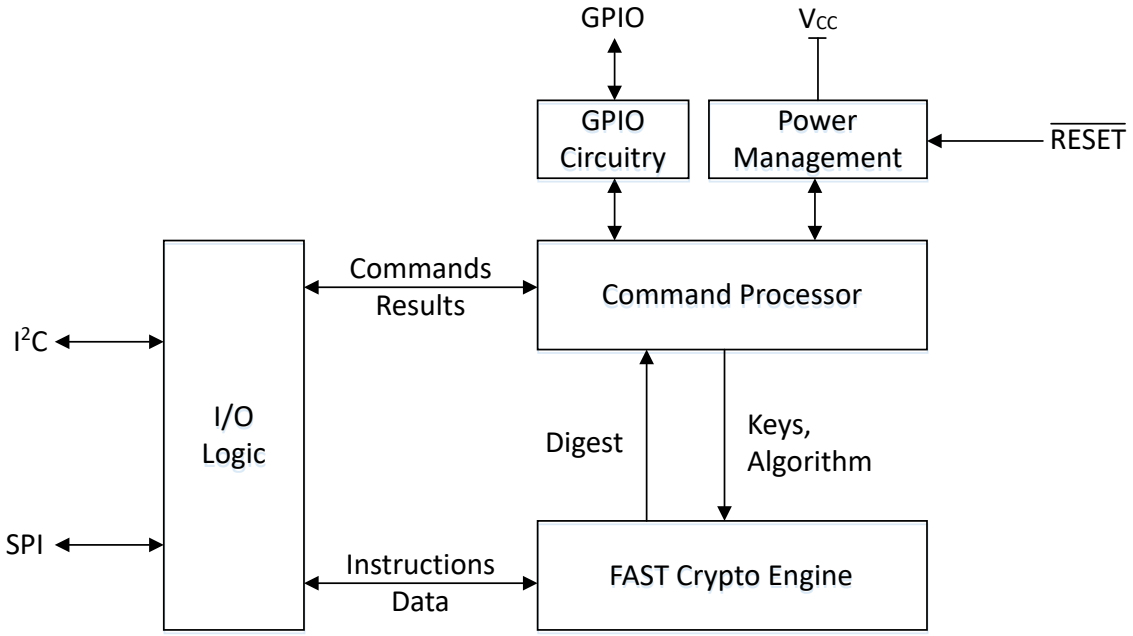
The TA101 device supports several broad features, including secure boot (host code authentication), MAC generation, secure key and certificate storage and management.

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 TA101 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 TA101 shows the major architectural features of the device.

Figure 3-1. TA101 Block Diagram



4. Nonvolatile Memory

The nonvolatile memory within the TA101 device is split into three pieces:

Configuration Memory:	The configuration memory is used to enable various features and functions for a given application. In general, this area is expected to be written prior to the placement of the TA101 device on the application board. When the configuration is complete, it is recommended that this area be locked to prevent further modification.
Shared Data Memory:	The shared data memory area can be used for storing keys, secrets, certificates and/or data. The TA101 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:	The dedicated data memory stores the 8-byte unique serial number of and software revision information associated with the device.

5. Security Features

The TA101 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. Cryptographic Algorithm Specifications

The following describes the controlling documents for the cryptographic algorithms implemented within the TA101 device.

1. The RNG function is comprised of an NRBG and a DRBG component combined according to the rules of NIST SP800-90C specified in the following documents:
   a. DRBG: NIST Special Publication 800-90Ar1
   b. NRBG: NIST Special Publication 800-90B
   c. RNG: NIST Special Publication 800-90C second draft
2. Cryptographic digests using SHA-256, SHA-384, SHA-512:
   a. NIST FIPS Publication 180-4 – Secure Hash Standard (SHS)
3. HMAC calculations are performed with key sizes varying from 16 to 128 bytes. The underlying algorithm is SHA-256, SHA-384 or SHA-512:
   a. NIST FIPS Publication 198-1 – The Keyed-Hash Message Authentication Code (HMAC)
4. Authorization session establishment uses the HMAC-SHA256 – The counter key derivation function (KDF HMAC-Counter) specified in the following documents:
   a. KDF HMAC-Counter according to specification:
      NIST Special Publication 800-108 – Recommendation for Key Derivation Using Pseudorandom Functions
   b. Support for SHA-256 one-step KDF composed of a single SHA-256 iteration used in other protocols, as specified in the following document:
      NIST Special Publication 800-56Cr2 – Recommendation for Key-Derivation Methods in Key Establishment Schemes
5. Support for the TLS 1.2 KDF (PRF), as specified in:
   a. IETF RFC5246 – The Transport Layer Security (TLS) Protocol Version 1.2
   b. NIST Special Publication 800-135 – Recommendation for Existing Application-Specific Key Derivation Functions
6. Support for the TLS 1.3 KDF (HKDF), as specified in:
   a. IETF RFC5869 – HMAC-Based Extract-and-Expand Key Derivation Function (HKDF)
   b. IETF RFC8446 – The TLS Protocol Version 1.3
7. Symmetric encryption/decryption AES-128 and AES-256 implemented according to:
   a. ECB: NIST FIPS Publication 197 – Advanced Encryption Standard (AES)
8. The AES-CMAC algorithm is implemented according to:
   a. NIST Special Publication 800-38B – Recommendation for Block Cipher Modes of Operation: *The CMAC Mode for Authentication*
9. AES encryption/decryption for authorization sessions uses the GCM AEAD mode according to:
   a. NIST Special Publication 800-38D – Recommendation for Block Cipher Modes of Operation: *Galois/Counter Mode (GCM) and GMAC*
10. RSA key generation and signatures are generated and/or verified using the RSASSA-PKCS1-V1_5 scheme according to the specified PKCS#1 procedures. The supported key sizes are 2048, 3072 and 4096. The exponent is fixed at `0x10001`, except for the 3072-bit verify, which optionally supports e = 3 (support of the HDCP protocol).
    a. IETF RFC8017 – PKCS #1 RSA Cryptography Specifications Version 2.2
    b. NIST FIPS Publication 186-5 – Digital Signature Standard (DSS)

11. RSA key generation and signatures are generated and/or verified using the RSASSA-PSS schemes according to the specified PKCS#1 procedures. The supported key sizes are 2048, 3072 and 4096.
    a. IETF RFC8017 – PKCS #1 RSA Cryptography Specifications Version 2.2
    b. NIST FIPS Publication 186-5 – DSS
12. RSA (RSAES-OAEP) encryption and decryption with an exponent of `0x10001` are supported using the specified RSAES_OAEP PKCS#1 V2.2 scheme. The supported key sizes are 1024, 2048, 3072 and 4096.
    a. IETF RFC8017 – PKCS #1 RSA Cryptography Specifications Version 2.2
13. Elliptic Curve ECDSA key generation and signatures using the NIST curves P-224, P-256, P-384 and P-521 are generated/verified according to the following specifications. Keys for all curves can be generated using the internal RNG.
    a. ANSI X9.62-2005, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*: www.ansi.org/
    b. NIST FIPS Publication 186-5 – DSS
14. ECDH key agreement. All ECDH public and private keys are treated as ephemeral keys with the corresponding key validation. Ephemeral Unified C (2e, 0s, ECC CDH) scheme (56Ar3 6.1.2.2).
    a. P-224, P-256, P-384 and P-521 curves are supported according to this specification: NIST Special Publication 800-56Ar3 – Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography
15. Edwards Curve Support:
    Ed25519/EdDSA key generation and signatures (128-bit security strength) are generated/verified according to the following document.
    a. Ed25519/EdDSA is supported according to this specification: IETF RFC8032 – Edwards-Curve Digital Signature Algorithm (EdDSA)

    ECDH X25519 key generation and key agreement (128-bit security strength) are supported according to the following document.
    a. X25519/ECDH is supported according to this specification: IETF RFC7748 Elliptic Curves for Security, Section 5 and 6
16. Elliptic curve computations for the 256-bit Brainpool (ECC-256_R1) curve are supported according to the following document. Sign, verify, key generation and ECDH key agreement are all supported. The device does not support Brainpool curves for X.509 certificate parsing.
    a. IETF RFC7027 Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)
17. ECDSA sign, verify and key generation operations are supported for the secp256k1 (Bitcoin) curve, often used in block chain applications. ECDH is **not** supported for this curve. It is specified in document:
    a. SECG SEC 2: Recommended Elliptic Curve Domain Parameters v2.0
18. The TA101 device can execute the Burmester-Desmedt protocol variation of ECDH (**ECBD**) described at Eurocrypt '94. Contact Microchip for more technical details. A version of that paper is available here:
    a. "A Secure and Scalable Group Key Exchange System"
19. The TA101 device is designed to support the HDCP cryptographic protocols, as specified in:
    a. "High-Bandwidth Digital Content Protection System, Interface Independent Adaptation, Rev. 2.2"
20. Qi Standard Point Expansion based upon the compression protocols specified in document:
    a. https://tools.ietf.org/id/draft-jivsov-ecc-compact-00.xml – *Compact representation of an elliptic curve point*

21. Contact Microchip for CAVP certification status of the appropriate cryptographic algorithms.

7. Electrical Characteristics

7.1 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]	-0.5V to V_{CC} + 0.5V
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 where 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.

7.2 DC Characteristics

Table 7-1. 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
Theta JA	—	Θ_{JA}	—	73	—	℃/W	8-Pin SOIC
				41.3			24-pad VQFN

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 7-2. DC Characteristics – SPI Interface, $\overline{RESET}$ 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 7-3. DC Characteristics of SDA and SCL Pins for I^2C 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 V_{CC} > 3.6V to 5.5V	V_{OL}	0	—	0.4	V	B
	I_{OL} = 14 mA 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}.

7.3 AC Characteristics

7.3.1 All Interfaces

Table 7-4. 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	6.0	ms	A
Power-up Time from V_{CC} < 2.7V	$t_{PU.POWERON}$[1]	—	4	6.0	ms	A
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 $\overline{RESET}$ 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 TA101	$t_{WAKE\_GPIO\_LOW}$	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 clean-up 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

7.3.2 I²C Interface Timing

Table 7-5. AC Characteristics of I²C Interface

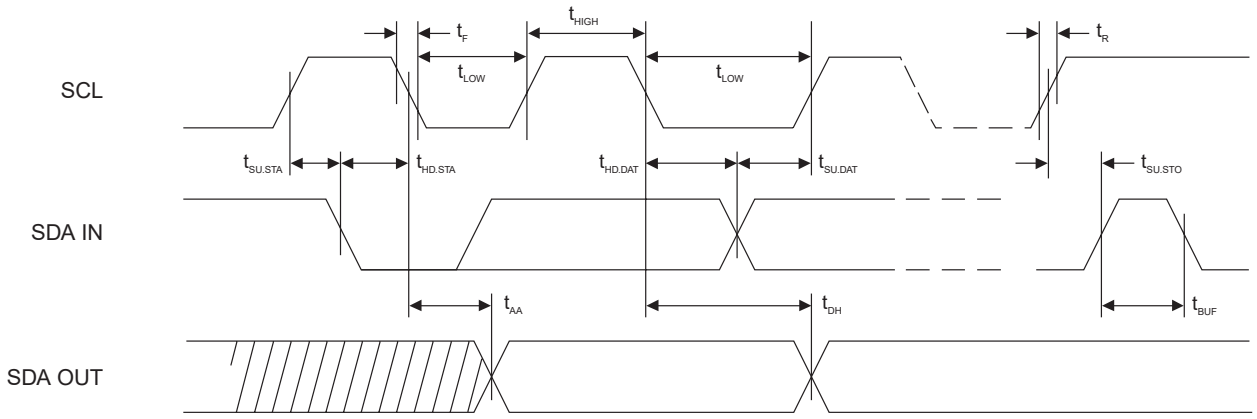
Applicable over the recommended operating range from T_A = -40°C to +125°C, V_{CC} = +2.7V to +5.5V.

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
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 I²C 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 7-1. I^2C Synchronous Data Timing



7.3.3 SPI Interface Timing

Table 7-6. 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
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 7-2. SPI Mode 0 Synchronous Data Timing

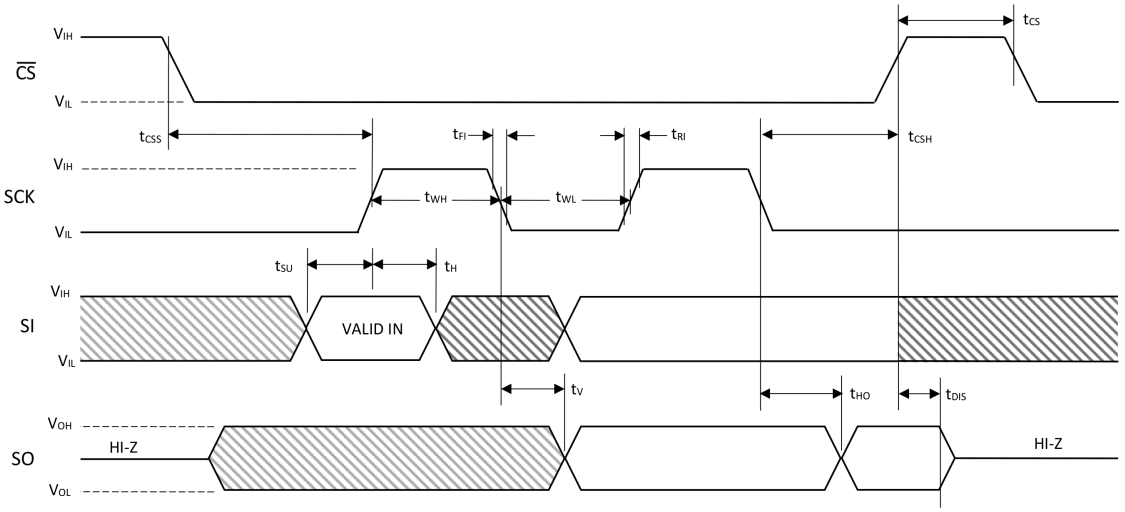
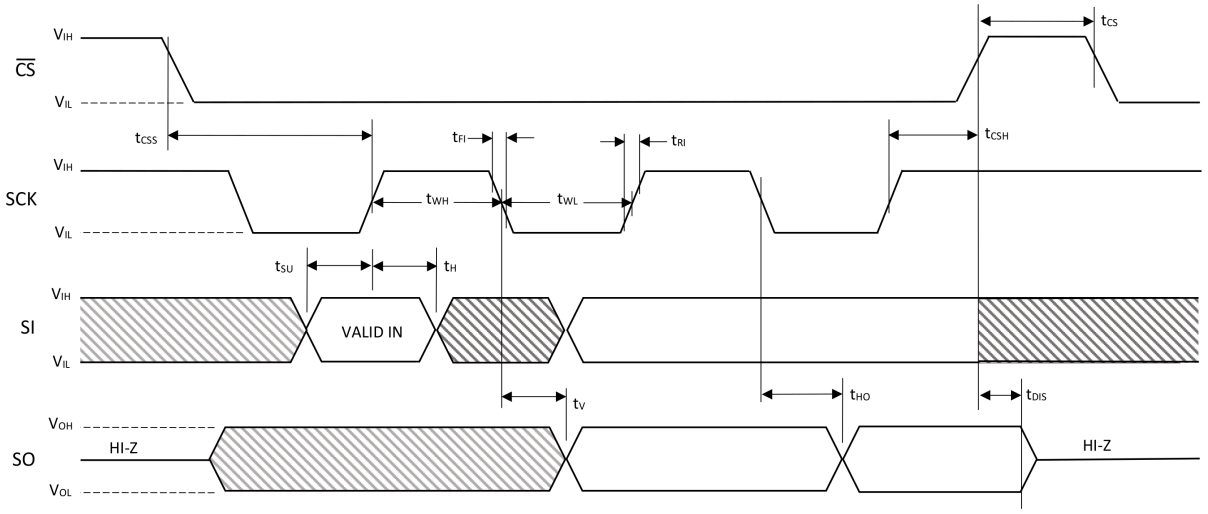


Figure 7-3. SPI Mode 3 Synchronous Data Timing



8. Package Marking Information

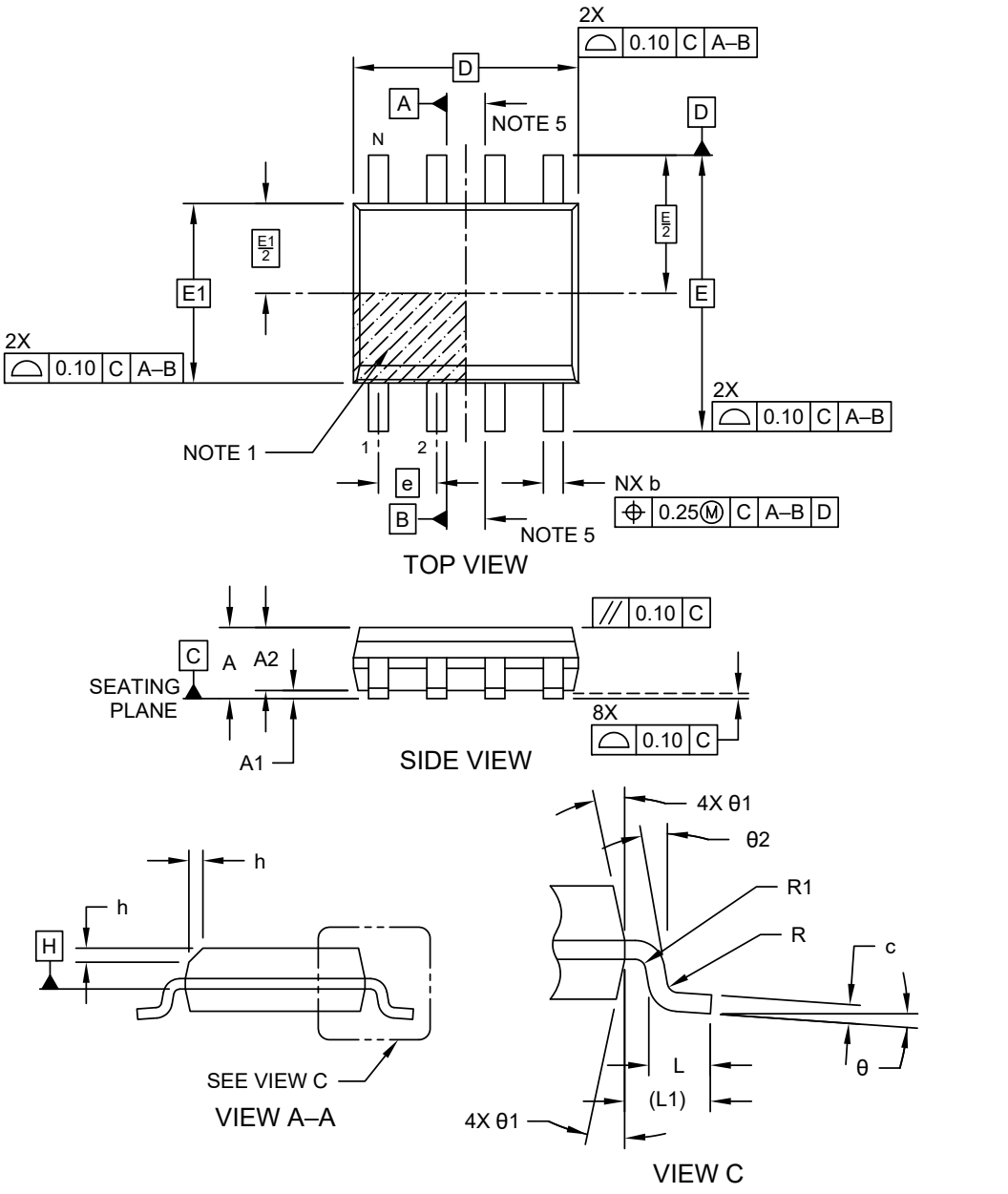
As part of Microchip's overall security features, the part marking for all crypto devices is intentionally vague. The marking on the top of the package does not provide any information as to the actual device type or the manufacturer of the device. The alphanumeric code on the package provides manufacturing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

9. Package Drawings

9.1 8-Lead SOIC

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

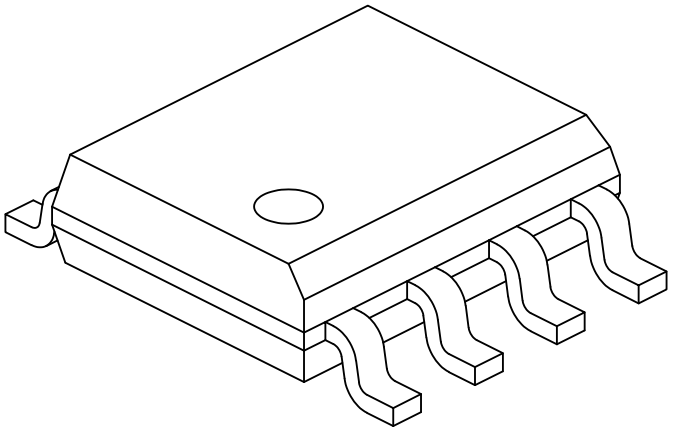
Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



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

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

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



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

Notes:

1. 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

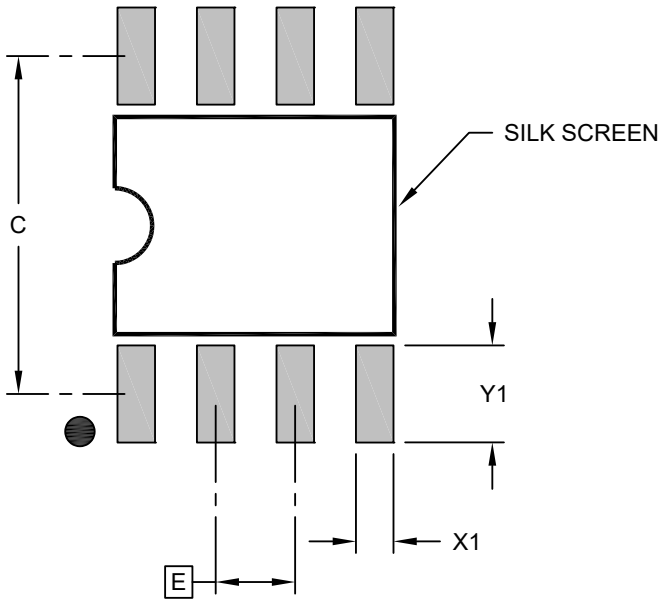
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

   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 K Sheet 2 of 2

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

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



RECOMMENDED LAND PATTERN

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

Notes:

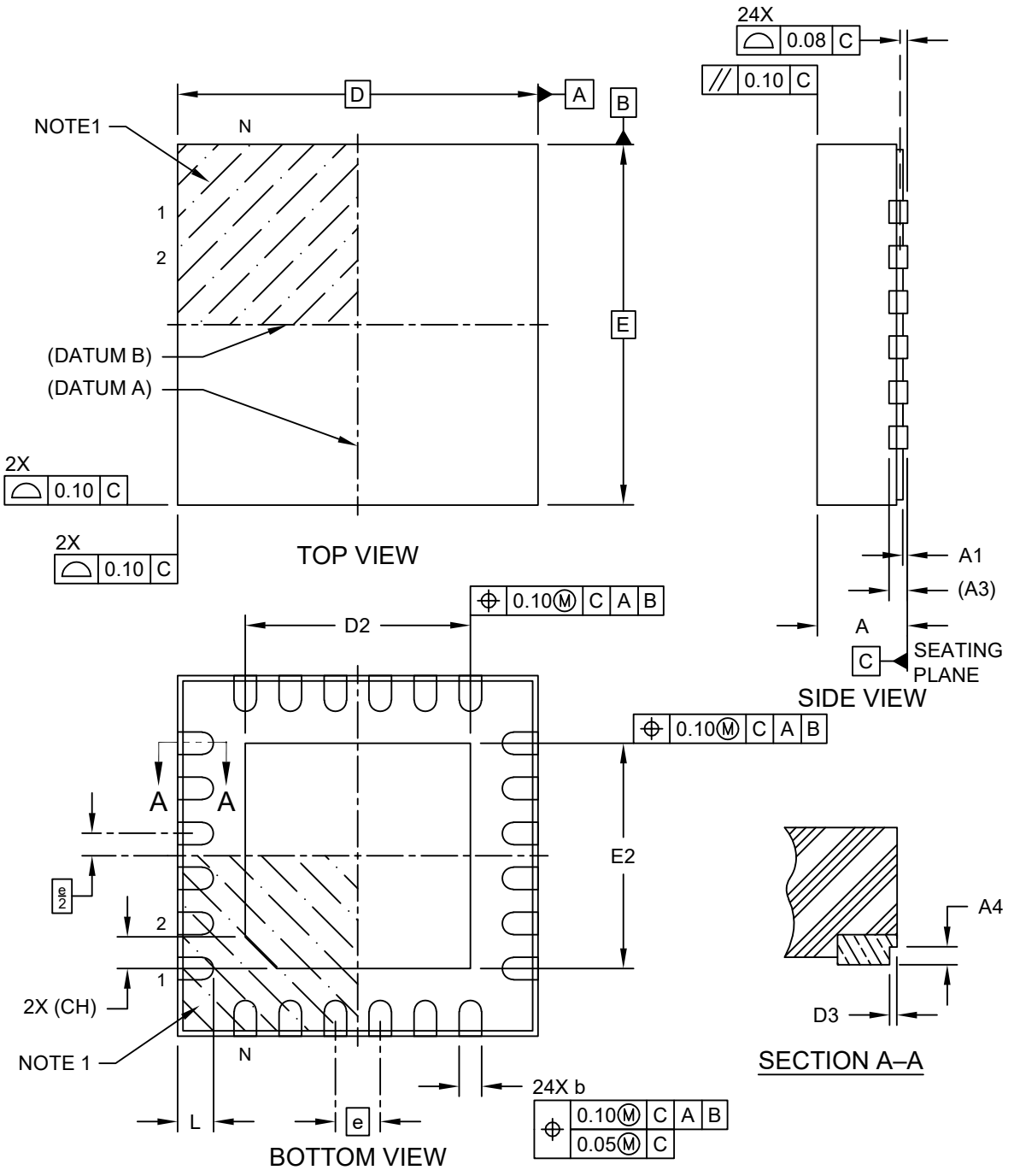
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-2057-OA Rev K

9.2 24-Pad VQFN

24-Lead Very Thin Plastic Quad Flat, No Lead Package (UFB) - 4x4x1.0 mm Body [VQFN] With 2.50 mm Exposed Pad and Stepped Wettable Flanks

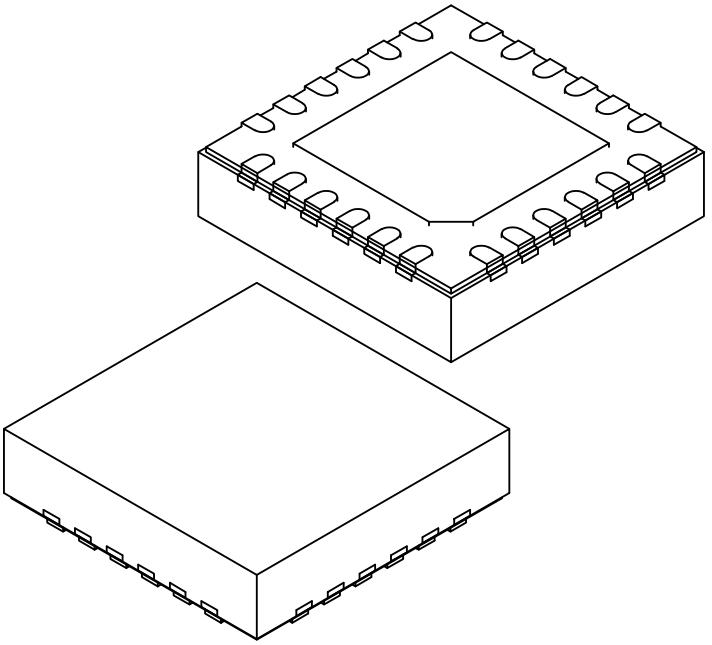
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing C04-21549 Rev A Sheet 1 of 2

24-Lead Very Thin Plastic Quad Flat, No Lead Package (UFB) - 4x4x1.0 mm Body [VQFN] With 2.50 mm Exposed Pad and Stepped Wettable 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		24	
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		4.00 BSC	
Exposed Pad Length	D2	2.40	2.50	2.60
Overall Width	E		4.00 BSC	
Exposed Pad Width	E2	2.40	2.50	2.60
Exposed Pad Index Chamfer	CH		0.35 REF	
Terminal Width	b	0.20	0.25	0.30
Terminal Length	L	0.30	0.40	0.50
Wettable Flank Step Cut Length	D3	-	-	0.085
Wettable Flank Step Cut Height	A4	0.10	-	0.19

Notes:

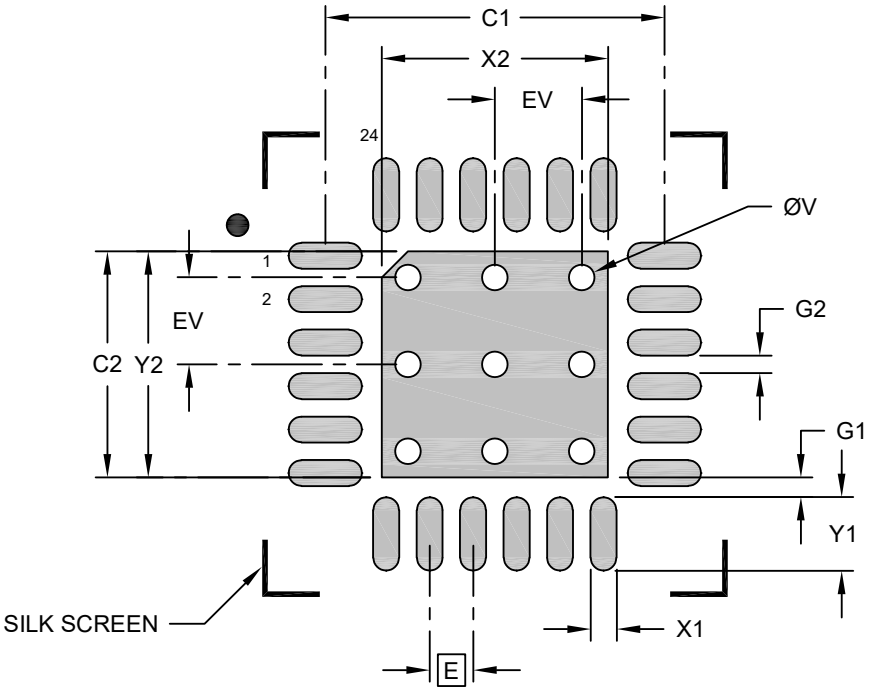
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M

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

Microchip Technology Drawing C04-21549 Rev A Sheet 2 of 2

24-Lead Very Thin Plastic Quad Flat, No Lead Package (UFB) - 4x4x1.0 mm Body [VQFN] With 2.50 mm Exposed Pad and Stepped Wettable 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			2.60
Center Pad Length	Y2			2.60
Contact Pad Spacing	C1		3.90	
Contact Pad Spacing	C2		3.90	
Contact Pad Width (X24)	X1			0.30
Contact Pad Length (X24)	Y1			0.85
Contact Pad to Center Pad (X24)	G1	0.23		
Contact Pad to Contact Pad (X20)	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 C04-23549 Rev A

10. Revision History

Revision A (November 2023)
Original release of the document

Microchip Information

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:	TA101	
I/O Type	Blank	24-PAD VQFN SPI and I²C Interfaces
	Blank	8-PIN SOIC SPI Interface Only
	T	8-PIN SOIC I²C Interface Only
Temperature Range:	Y	-40℃ to +125℃
IC Revision(2)	xxx	Contact Microchip for Information
Package Option	C2X	8-Pin SOIC
	UFB	24-Pad VQFN
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 I²C Pull-Up	Package	Delivery	Personalization
TA101T-Y250C2X01-00T-VAO	I²C	No	SOIC-8	Tape and Reel	Standard Configuration
TA101T-Y250C2X01-00B-VAO	I²C	No	SOIC-8	Bulk	Standard Configuration
TA101-Y250C2X01-00T-VAO	SPI	—	SOIC-8	Tape and Reel	Standard Configuration
TA101-Y250C2X01-PDT-VAO	SPI	—	SOIC-8	Tape and Reel	SPI Pull-ups Disabled
TA101-Y250C2X01-00B-VAO	SPI	—	SOIC-8	Bulk	Standard Configuration
TA101-Y250C2X01-PDB-VAO	SPI	—	SOIC-8	Bulk	SPI Pull-ups Disabled
TA101-Y250UFB01-00T-VAO	I²C, SPI	No	VQFN-24	Tape and Reel	Standard Configuration
TA101-Y250UFB01-00B-VAO	I²C, SPI	No	VQFN-24	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, 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, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet-Wire, SmartFusion, SyncWorld, TimeCesium, TimeHub, TimePictra, TimeProvider, 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, Clockstudio, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, EyeOpen, GridTime, IdealBridge, IGaT, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, IntelliMOS, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, MarginLink, maxCrypto, maxView, memBrain, Mindi,

ISBN: 978-1-6683-3453-9

Quality Management System

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

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office	**Australia - Sydney**	**India - Bangalore**	**Austria - Wels**
2355 West Chandler Blvd.	Tel: 61-2-9868-6733	Tel: 91-80-3090-4444	Tel: 43-7242-2244-39
Chandler, AZ 85224-6199	**China - Beijing**	**India - New Delhi**	Fax: 43-7242-2244-393
Tel: 480-792-7200	Tel: 86-10-8569-7000	Tel: 91-11-4160-8631	**Denmark - Copenhagen**
Fax: 480-792-7277	**China - Chengdu**	**India - Pune**	Tel: 45-4485-5910
Technical Support:	Tel: 86-28-8665-5511	Tel: 91-20-4121-0141	Fax: 45-4485-2829
www.microchip.com/support	**China - Chongqing**	**Japan - Osaka**	**Finland - Espoo**
Web Address:	Tel: 86-23-8980-9588	Tel: 81-6-6152-7160	Tel: 358-9-4520-820
www.microchip.com	**China - Dongguan**	**Japan - Tokyo**	**France - Paris**
Atlanta	Tel: 86-769-8702-9880	Tel: 81-3-6880- 3770	Tel: 33-1-69-53-63-20
Duluth, GA	**China - Guangzhou**	**Korea - Daegu**	Fax: 33-1-69-30-90-79
Tel: 678-957-9614	Tel: 86-20-8755-8029	Tel: 82-53-744-4301	**Germany - Garching**
Fax: 678-957-1455	**China - Hangzhou**	**Korea - Seoul**	Tel: 49-8931-9700
Austin, TX	Tel: 86-571-8792-8115	Tel: 82-2-554-7200	**Germany - Haan**
Tel: 512-257-3370	**China - Hong Kong SAR**	**Malaysia - Kuala Lumpur**	Tel: 49-2129-3766400
Boston	Tel: 852-2943-5100	Tel: 60-3-7651-7906	**Germany - Heilbronn**
Westborough, MA	**China - Nanjing**	**Malaysia - Penang**	Tel: 49-7131-72400
Tel: 774-760-0087	Tel: 86-25-8473-2460	Tel: 60-4-227-8870	**Germany - Karlsruhe**
Fax: 774-760-0088	**China - Qingdao**	**Philippines - Manila**	Tel: 49-721-625370
Chicago	Tel: 86-532-8502-7355	Tel: 63-2-634-9065	**Germany - Munich**
Itasca, IL	**China - Shanghai**	**Singapore**	Tel: 49-89-627-144-0
Tel: 630-285-0071	Tel: 86-21-3326-8000	Tel: 65-6334-8870	Fax: 49-89-627-144-44
Fax: 630-285-0075	**China - Shenyang**	**Taiwan - Hsin Chu**	**Germany - Rosenheim**
Dallas	Tel: 86-24-2334-2829	Tel: 886-3-577-8366	Tel: 49-8031-354-560
Addison, TX	**China - Shenzhen**	**Taiwan - Kaohsiung**	**Israel - Ra'anana**
Tel: 972-818-7423	Tel: 86-755-8864-2200	Tel: 886-7-213-7830	Tel: 972-9-744-7705
Fax: 972-818-2924	**China - Suzhou**	**Taiwan - Taipei**	**Italy - Milan**
Detroit	Tel: 86-186-6233-1526	Tel: 886-2-2508-8600	Tel: 39-0331-742611
Novi, MI	**China - Wuhan**	**Thailand - Bangkok**	Fax: 39-0331-466781
Tel: 248-848-4000	Tel: 86-27-5980-5300	Tel: 66-2-694-1351	**Italy - Padova**
Houston, TX	**China - Xian**	**Vietnam - Ho Chi Minh**	Tel: 39-049-7625286
Tel: 281-894-5983	Tel: 86-29-8833-7252	Tel: 84-28-5448-2100	**Netherlands - Drunen**
Indianapolis	**China - Xiamen**		Tel: 31-416-690399
Noblesville, IN	Tel: 86-592-2388138		Fax: 31-416-690340
Tel: 317-773-8323	**China - Zhuhai**		**Norway - Trondheim**
Fax: 317-773-5453	Tel: 86-756-3210040		Tel: 47-72884388
Tel: 317-536-2380			**Poland - Warsaw**
Los Angeles			Tel: 48-22-3325737
Mission Viejo, CA			**Romania - Bucharest**
Tel: 949-462-9523			Tel: 40-21-407-87-50
Fax: 949-462-9608			**Spain - Madrid**
Tel: 951-273-7800			Tel: 34-91-708-08-90
Raleigh, NC			Fax: 34-91-708-08-91
Tel: 919-844-7510			**Sweden - Gothenberg**
New York, NY			Tel: 46-31-704-60-40
Tel: 631-435-6000			**Sweden - Stockholm**
San Jose, CA			Tel: 46-8-5090-4654
Tel: 408-735-9110			**UK - Wokingham**
Tel: 408-436-4270			Tel: 44-118-921-5800
Canada - Toronto			Fax: 44-118-921-5820
Tel: 905-695-1980			
Fax: 905-695-2078			