RNG90 CryptoAuthentication Data Sheet

RNG90

Introduction

Random numbers are a primary building block in cryptography. The overall security strength of a system is primarily dictated by the strength of the random numbers generated. The generated random numbers are used in a wide variety of cryptography use cases, including key generation, random challenges, initialization vectors, passwords, digital signatures, nonce generation, etc.

Generation of a true random number is a difficult process. Independent evaluation of randomness ensures that a given device targeted to generate random numbers is providing the expected randomness. For this reason, Microchip developed the RNG90 per NIST specifications and certified the device working with a NIST-certified laboratory. The RNG90 generates a 256-bit random number that has a security strength of 128 bits each time the `Random` command is executed.

The RNG90 is a member of the Microchip Technology Inc. CryptoAuthentication™ product family. The device is targeted for those systems where a secure random number generator is required. The device is ready-to-use and does not require any customization. The device implements an industry standard I^2C interface. Software support is provided via Microchip's CryptoAuthentication Library (CAL), which can be easily adapted through a Hardware Abstraction Layer (HAL) to work with the majority of microcontrollers and microprocessors.

Features

- Internal High-Quality NIST SP 800-90A/B/C Random Number Generator (RNG)
- FIPS Compliant Health Tests and Self-Tests for Entropy
- Designed for FIPS140-3 NIST CMVP Entropy Source Validation (ESV) Compliance
- Unique 72-Bit Serial Number
- 400 kHz Fast-Mode I^2C Interface
- 130 nA Nominal Sleep Current
- V_{CC} Operating Range: 1.65 to 5.5V
- Extended Industrial Temperature Range: -40℃ to +105℃
- ESD >4 kV Human Body Model (HBM)
- Extensive Security Measures:
  - Active shield to protect against invasive attacks
  - Low and high-supply voltage tampers
  - Low and high-temperature tampers
- Packaging Options:
  - 2 x 3 mm 8-Pad UDFN
  - 8-Lead SOIC

Applications

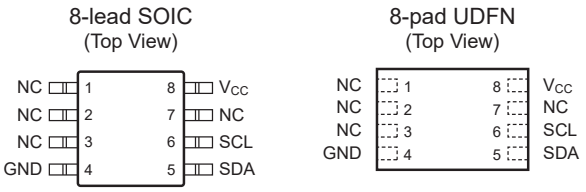
- Cryptographic Operations
- Password Generation
- Gaming Systems
- Crypto Currency
- Scientific Applications
- Aerospace and Defense applications

Pin Configuration and Pinouts

Table 1. Pin Configuration

Package = 8-Lead SOIC or 8-Pad UDFN		
Pin #	Function	Pin Name
1-3,7	No Connect	NC
4	Ground	GND
5	Serial I/O	SDA
6	Serial Clock	SCL
8	Supply	V_{CC}

Figure 1. Pinouts(1)



Note:

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

Table of Contents

1. Overview

The RNG90 can be used for a wide variety of applications that require random numbers. Cryptographic operations that require random numbers, such as the generation of keys, nonces, random challenges, signature generation, etc., can all benefit by using this device.

Through use of the industry standard I^2C interface and the wide power supply range, the device can typically be implemented without hardware changes to a system. The device is acceptable for applications over commercial, industrial and extended industrial temperature ranges.

Attention: For applications that require a higher temperature range or additional features, contact Microchip Sales to determine availability.

1.1 Cryptographic Operation

RNG90 can generate high-quality random numbers using its internal physical random number generator. This sophisticated function includes runtime health testing designed to ensure that the values generated from the internal noise source contain sufficient entropy at the time of use. The random number generator is designed to meet the requirements documented in the NIST SP800-90A, SP800-90B and SP800-90C documents.

These random numbers can be employed for any purpose, including usage as part of cryptographic protocols and algorithms used by the system. Because each random number is assured to be essentially unique from all numbers ever generated on this or any other device, their inclusion in the protocol calculation ensures that replay attacks (i.e., re-transmitting a previously successful transaction) will always fail.

1.2 Terminology

The following is a set of terms or nomenclatures used throughout this document.

Table 1-1. Document Terms

Term	Meaning
DRBG	Deterministic Random Bit Generator. Generates a random number based on an unknown seed. The output is pseudo-random. The output of the DRBG is an input to the RNG.
Entropy	A measure of randomness collected by a system or device. This value is generated by the NRBG and is an input source to the RNG.
mode[b]	Indicates bit b of the parameter mode.
LSB/MSB	Least Significant Byte/Most Significant Byte
LSb/MSb	Least Significant bit/Most Significant bit
NIST	The United States National Institute of Standards. NIST Defines the standards the RNG90 adheres to when generating random numbers.
NRBG	Non-Deterministic Random Bit Generator. Also known as a true random bit generator.
RNG	Random Number Generator

2. Security Features

2.1 Physical Security

The RNG90 incorporates a number of physical security features designed to protect the operation of the RNG.

Among many others, these security measures include:

- Active Shield Circuitry
- Glitch Protection
- Voltage and Temperature Tamper Detection

2.2 Random Number Generator (RNG)

RNG90 includes a high-quality cryptographic random number generator implemented using a physical non-deterministic noise source (NRBG producing an entropy bit stream) seeding a deterministic algorithm (DRBG) implemented according to the following NIST standards. Entropy bits from the NRBG are used both in the instantiation and each time an RNG number is required.

The NRBG output is evaluated using the methods in NIST SP 800-90B. A Hash_DRBG is designed using the SHA256 variant specified within NIST SP 800-90A. The combination of the two create the final random number generator and follow the methods specified in NIST SP 800-90C.

- NIST SP800-90A: Certified as part of the NIST Cryptographic Algorithm Validation Program (CAVP) certification process (Hash DRBG CAVP Certification)
- NIST SP 800-90B: Will be certified as part of the NIST Entropy Source Validation (ESV) certification process
- NIST SP 800-90C: Is currently a draft specification with implementation recommendations and does not have a specific certification procedure

Remember: As of the initial date of this document, both SP800-90A and SP800-90B were released, but SP800-90C in still in draft stage.

When a random number is requested, the following two conditions are met prior to use of the random number:

- Health testing is applied to the output of the noise source per SP 800-90B to ensure the entropy of the bit stream meets expectations at the current time and under the current environmental conditions.
- If insufficient entropy was collected from the noise source, the DRBG function will be delayed for sufficient time to accumulate the required entropy.

If the internal health testing fails when running the `Random` command, a failure code of `0x08` will be returned. After the command completes, the internal failure latch will be cleared. When the next `Random` command is run, the health test will be run again and if it succeeds on this subsequent command, the command will execute normally.

If the health test failed prior to executing the `Random` command, the health test failure state and error flag can be cleared by running the RNG mode of the `SelfTest` command. It can also be cleared by going through a sleep->wake cycle or a power-down->power-up cycle. Health test failure code (0x07) is not the same as a self-test failure (0x08). Self-Test checks the health of the DRBG function in addition to the health testing.

For customers intending to include RNG90 in FIPS-certified systems, proper device firmware integrity tests are run on initial power-up and wake events in addition to the assurance that DRBG and NRBG self-test and health-tests completed successfully prior to execution of the `Random` command.

3. I/O Interfaces

The I²C interface uses the SDA and SCL pins to transfer commands, data and status to and from the RNG90 device. Data flow is controlled by the host controller.

Interface Terminology

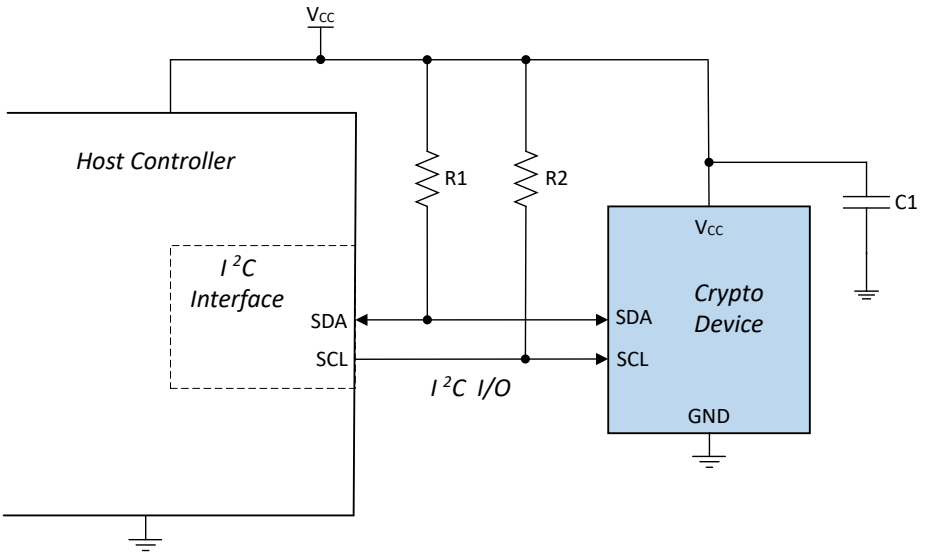
Host:	The host MCU that generates the command and controls the data flow on the bus to one or more client devices.
Client:	The RNG90 device always operates as a client device on the I²C and cannot take control of the bus.
Device Address:	7-bit address used to address a client device. This is part of the first byte sent to a client device for each write or read transaction.
Open-Drain:	The RNG90 device has an open-drain output buffer where the bus is actively pulled low by the output buffer but is passively pulled high by an external pull-up resistor.

Remember: The original I²C standard uses the terminology “Master” and “Slave”. Version 7 of the standard now uses the terms "Controller" and "Target". The equivalent Microchip terminology used in this document is “Host” and “Client”, respectively.

3.1 General I/O Information

RNG90 operates as a client device and utilizes an I²C serial interface to communicate with a host controller. The host device controls all read and write operations to the client device(s) on the serial bus and operates with a bit rate up to 400 kbps.

Figure 3-1. Application Diagram for Using I²C Interface



3.1.1 Byte and Bit Ordering

CryptoAuthentication devices use a common ordering scheme for bytes and also for the way numbers and arrays are represented in this data sheet:

- Data bits are transferred to and from the RNG90 MSb first on the bus.

- All multi-byte aggregate elements are treated as arrays of bytes and are processed in the order received or transmitted with index #0 first.
- 16-bit (2-byte) integers, typically Param2, appear on the bus LSB first.

In this document, the MSb or nibble of a byte or 16-bit word appear towards the left-hand side of the page.

3.2 I²C Interface

The RNG90 follows the standard and has a fixed I²C Address of 0x40.

The SDA pin is normally pulled high with an external pull-up resistor because the RNG90 includes only an open-drain driver on its output pin. The host system may use either an open-drain or totem pole driver. In the latter case, the driver must be tri-stated when the RNG90 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 external resistor.

The serial interface is comprised of just 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 is always latched into RNG90 on the rising edge of SCL and always output from the device on the falling edge of SCL. Both the 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 Most Significant bit (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 Acknowledge (ACK) or a No-Acknowledge (NACK) response bit during a ninth clock 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 changes 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.

3.2.1 I/O Conditions

The device responds to the following I/O conditions:

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

RNG90 will only exit low-power mode if the device address sent by system microprocessor contains a client address that matches the address stored in the I²C_Address byte. The RNG90 will NACK the device address but ignore all subsequent bytes until t_{PU} has expired.

Device is Awake

When the device is awake, it honors the conditions listed in 3.2.2. I2C Bus Transactions.

3.2.2 I²C Bus Transactions

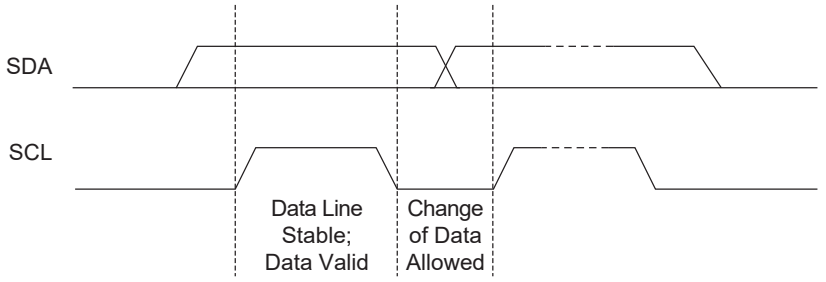
Types of data transmitted over the I²C bus:

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

3.2.2.1 Data Input and Output Frames

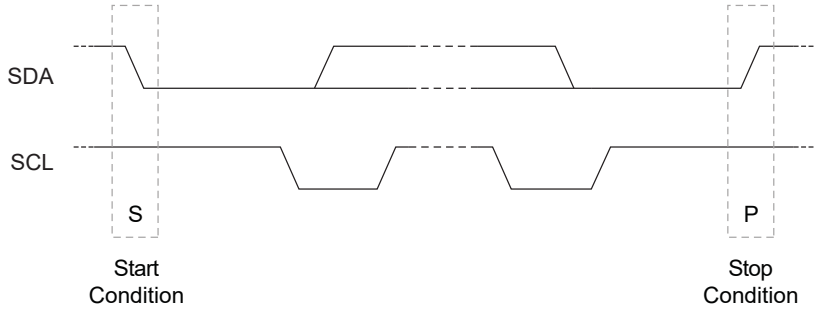
- **DATA Zero**: If SDA is low and stable while SCL goes from low to high to low, a zero bit is transferred on the bus. SDA can change while SCL is low.
- **DATA One**: If SDA is high and stable while SCL goes from low to high to low, a one bit is transferred on the bus. SDA can change while SCL is low.

Figure 3-2. Data Bit Transfer on the I^2C Interface



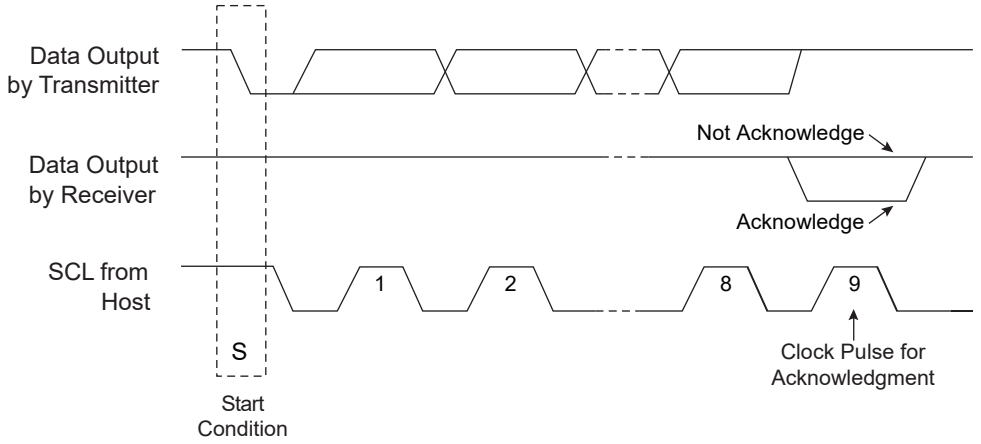
- **Start Condition**: A high-to-low transition of SDA with SCL high is a Start condition that must precede all commands.
- **Stop Condition**: A low-to-high transition of SDA with SCL high is a Stop condition. After this condition is received by the device, the current I/O transaction ends. On input, 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 3-3. Start and Stop Conditions on the I^2C 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 3-4. NACK and ACK Conditions on the I²C Interface



The RNG90 device can share a common system I²C interface bus provided all devices on that bus have a unique I²C address.

3.2.3 I²C Synchronization

It is possible for the system to lose synchronization with the I/O port on the RNG90, perhaps due to a system reset, I/O noise or other conditions. Under this circumstance, the RNG90 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
   - Another Start bit condition
   - A Stop bit condition

   A read sequence can now be issued, and, if synchronization is properly completed, the RNG90 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 RNG90 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 I²C 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.

3.3 Address Counter

Writes to and/or reads from the RNG90 I/O buffer over the I/O interface are treated as if the device were a FIFO.

The first byte transmitted to the device is treated as the size byte. Any attempt to send more than this number of bytes or any attempts to write beyond the end of the I/O buffer will cause the RNG90 to NACK those bytes.

Data may be read from the device under the following three conditions:

- On power-up, the single byte `0x11` can be read inside a 4-byte group.
- If a complete block is received by the device but there are any errors in parsing or executing the command, a single byte of error code is available (also inside a 4-byte group).
- Upon completion of a command execution, results are available to be read.

Any attempt to read beyond the end of the valid output buffer returns `0xFF` to the system and the read address counter does not wrap around to the beginning of the buffer.

There may be situations where the system needs to re-read the output buffer, for example, when the CRC check reveals an error. In this case, the host must send a 2-byte sequence to the RNG90, consisting of the correct device address and a word address of `0x00` (Reset, per 3.4.1. Word Address Values), followed by a Stop condition. This causes the address counter to be reset to zero and permits the data to be re-written (or re-read) to (or from) the device.

The RNG90 supports write and read operations split into multiple packets if need be. If a split write operation is interrupted by a read operation, the RNG90 will NACK the valid read device address and abort the split write operation. If a split read operation is interrupted by a write operation (RNG90 received length byte of the packet), the RNG90 will abort the previous split read operation and reset the Read Address Counter. It is important to know when the write/read address counter gets reset.

Write Address Buffer Counter Reset conditions:

- Power-up or wake from sleep
- Upon receiving valid Read Device Address
- Upon receiving the number of bytes indicated by the Count byte
- Upon receiving valid Write Device Address with Word Address value of `0x00`

Read Address Buffer Counter Reset conditions:

- Power-up or wake from sleep
- Upon receiving valid Write Device Address with Word Address value of `0x00`

3.4 I/O Transmission to the RNG90

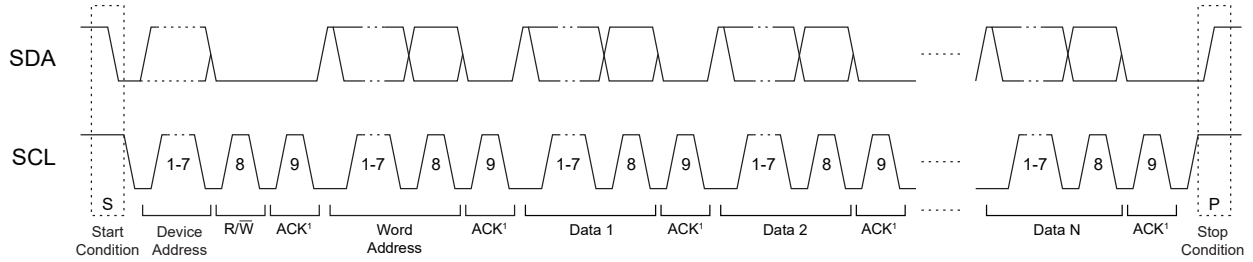
The transmission of data from the system to the RNG90 is summarized in the table below. This transmission sequence is valid for I^2C communications. The order of transmission is as follows:

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

Table 3-1. Transmission to the RNG90

Name	I/O Name	Description
Device Address	Device Address	This byte selects a particular device on the I/O interface. RNG90 is selected if bits 1 through 7 of this byte match the 7-bit I^2C address 0x40. 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 3.4.1. 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 3-5. Normal I²C Transmission to the RNG90



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.

The system must send a Stop condition after the last command byte to ensure that the RNG90 will start the computation of the command. Failure to send a Stop condition may eventually result in a loss of synchronization.

3.4.1 Word Address Values

During an I/O write packet, the RNG90 interprets the second byte sent as the word address, which indicates the packet function as it is described in the table below:

Table 3-2. 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 RNG90 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 RNG90.

3.4.2 Sleep Sequence

Upon completion of the use of the RNG90 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.

3.4.3 Command Completion Polling

After a complete command is sent to the RNG90, 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. 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.

Related Links

3.5. I/O Transmission from the RNG90

3.5 I/O Transmission from the RNG90

When the RNG90 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.

Table 3-3. I/O Transmission from the RNG90

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 RNG90 will be selected if bits 1 through 7 of this byte match the 7-bit I^2C address 0x40. 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 RNG90 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 RNG90 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/W == R)]` is sent to the device, the RNG90 will NACK the device address to indicate that no data are available to be read.

4. Electrical Characteristics

4.1 Absolute Maximum Ratings

Operating Temperature	-40°C to +105°C
Storage Temperature	-65°C to +150°C
Maximum Operating Voltage	6.0V
DC Output Low Current	20 mA
Voltage on any Pin -0.5V to (V_{CC} + 0.5V)	-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.

4.2 AC Parameters

4.2.1 AC Parameters: All I/O Interfaces

Table 4-1. AC Parameters: All I/O Interfaces
Unless otherwise indicated, these values are applicable over the specified operating range from T_A = -40℃ to +105℃, V_{CC} =+1.65V to +5.5V.

Parameter	Sym.	Direction		Min.	Typ.	Max.	Units	Conditions
Power-up Delay	t_{PU}(1)	To RNG90	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	
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.

4.2.2 AC Parameters: I²C Interface

Figure 4-1. I²C Synchronous Data Timing

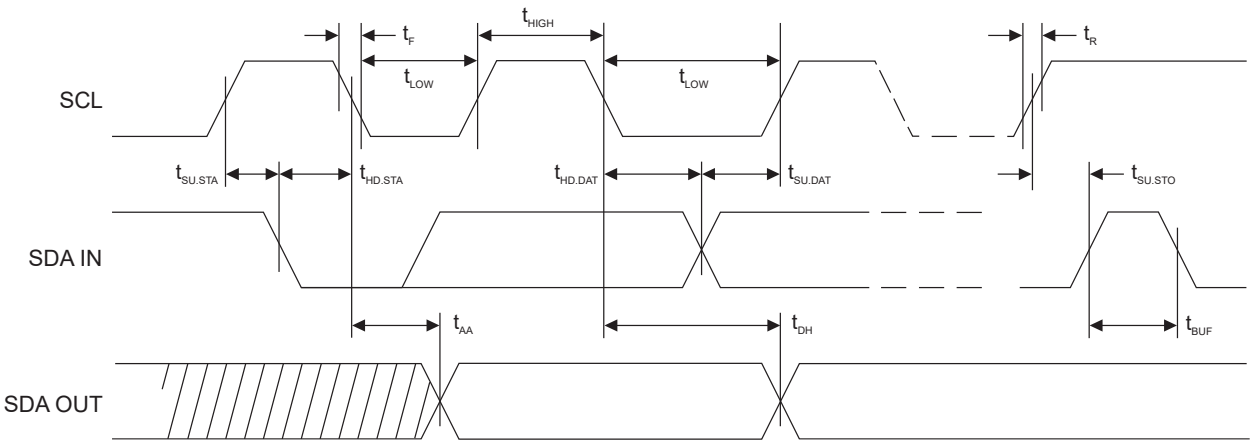


Table 4-2. AC Characteristics of I²C Interface
Unless otherwise indicated, these values are applicable over the specified operating range from T_A = -40℃ to +105℃, V_{CC} = +1.65V to +5.5V, C_L = 1 TTL Gate and 100 pF.

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

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}
   - 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.

4.3 DC Parameters: All I/O Interfaces

Table 4-3. DC Parameters
Unless otherwise specified, applicable over recommended operating range from T_A = -40℃ to +105℃, V_{CC} = +1.65V to +5.5V

Parameter	Sym.	Min.	Typ.	Max.	Units	Conditions
Supply Voltage	V_{CC}	1.65	—	5.5	V	—
V_{CC} Ramp Rate(2)	V_{RISE}	—	—	0.1	V/µs	—
Ambient Operating Temperature	T_A	-40	—	+105	°C	—
Output Low Voltage	V_{OL}	—	—	0.4	V	When device is in Active mode, V_{CC} = 1.65V to 3.6V for Output low current = 4.0 mA
Input Low Threshold	V_{IL1}	-0.5	—	0.3*V_{CC}	V	Device is Active
Input High Threshold	V_{IH1}	0.7*V_{CC}	—	V_{CC}+0.5	V	Device is Active
Sleep Current(1)	I_{SLEEP}	—	130	325(2)	nA	When device is in Sleep mode, VCC ≤ 3.6V, I/O's at either GND or V_{CC} TA ≤ +55℃
		—	130	500	nA	When device is in Sleep mode. V_{CC} 1.65 to 3.6 and -40℃ to 105℃ temperature range.
		—	130	1000	nA	When device is in Sleep mode. Over full V_{CC} and -40℃ to 105℃ temperature range.
Current Consumption in I/O Mode	$I_{I/O}$	—	60	250	µA	Waiting for I/O
Current Consumption in Computation Mode.	$I_{COMPUTE}$	—	—	0.75	mA	During Command Execution
Theta JA	Θ_{JA}	—	166	—	°C/W	8-PIN SOIC
		—	173	—	°C/W	8-Pad UDFN

Notes:

1. 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.
2. This condition is characterized but not production tested.

5. General Command Information

5.1 I/O Groups

Commands are sent to the device using the I^2C interface. The structure of the command is constructed as shown in the table below.

Table 5-1. I/O Groups

Byte	Name	Meaning
0	Count	Number of bytes to be transferred to (or from) the device in the group, including Count byte, Packet bytes and Checksum bytes. The Count byte must always have a value of (N+1), where N is equal to the number of bytes in the packet plus the two Checksum bytes. For a group with one Count byte, 50 Packet bytes and two Checksum bytes, the Count byte must be set to 53. The maximum group size (and value of count) is 87 bytes and the minimum size group is 4 bytes. Values outside this range will cause the device to return an I/O error.
1 to (N-2)	Packet	Command, parameters and data or response. See 5.2. Command Packets for more details.
N-1, N	Checksum	CRC-16 verification of the Count and Packet bytes. The CRC polynomial is `0x8005`. The initial register value will be '0', and, after the last bit of the Count and Packet is transmitted, the internal CRC register will have a value that matches the Checksum bytes in the block. The first CRC byte transmitted (N-1) is the LSB of the CRC value, so the last byte of the group is the MSB of the CRC.

For the RNG90, the count value in the input group must be consistent with the size requirements that are specified in the command parameters. If the count value is less than 4 or greater than 87, the RNG90 will NACK the Count byte and all the subsequent bytes in the packet. If the count value is in between the range (4-87) but still inconsistent with the command opcode and/or parameters within the packet, the RNG90 will respond with a Parse error code.

5.2 Command Packets

The command packet is broken down as shown in the table below:

Table 5-2. Command Packets

Byte	Name	Meaning
0	Opcode	The command code
1	Param1	The first parameter; always present
2-3	Param2	The second parameter; always present
4+	Data	Optional remaining input data

After the RNG90 receives all the bytes in a group, the device transitions to the busy state and attempts to execute the command. Neither status nor results can be read from the device when it is busy. During this time, the I/O interface of the device ignores all SDA transitions regardless of the I/O interface selected. The command execution delays are listed in 5.6. Command Summary and Execution Times.

If insufficient bytes are sent to the RNG90, it continues to wait for the remaining bytes until a Start/Stop condition is received by the device.

Related Links

5.6.1. Command Summary

5.3 Status/Error Codes

The device does not have a dedicated status register, so the output FIFO is shared among status, error and command results. All outputs from the device are returned to the system as complete groups, which are formatted identically to input groups:

- Count
- Packet
- Two-byte CRC

After the device receives the first byte of an input command group, the system cannot read anything from the device until the system sends all the bytes to the device.

After wake and after execution of a command, there will be error, status or result bytes in the device's output register that can be retrieved by the system. When the length of that group is four bytes, the codes returned are detailed in Table 5-3. The details of what errors are supported by which commands is shown below. Some commands return more than four bytes when they execute successfully. The resulting packet description is listed in the 5.2. Command Packets.

No particular precedence is enforced among the errors if more than one occurs.

Table 5-3. Status/Error Codes in Four byte Groups

State Description	Error/Status	Description
Successful Command Execution	0x00	Command executed successfully.
Parse Error	0x03	Command was properly received but the length, command opcode or parameters are illegal. Parameters input to the command must be corrected before it is re-attempted.
Self Test Error	0x07	There was a self test error and the chip is in failure mode waiting for the failure to be cleared.
Health Test Error	0x08	There was a random number generator health test error and the chip will fail subsequent commands requiring a random number until it is cleared.
Execution Error	0x0F	Command was properly received but could not be executed by the device in its current state. Changes in the device state or the value of the command bits must be made before it is re-attempted.
After Wake, Prior to First Command	0x11	Indication that RNG90 received a proper Wake condition.
CRC or Other Communications Error	0xFF	Command was not properly received by RNG90 and must be re-transmitted by the I/O driver in the system. No attempt was made to parse or execute the command.

Table 5-4. Error Codes by Command

Error Code	Code Value	Command List			
		Info	Random	Read	SelfTest
Success	0x00	(3)	(1)	(1)	✔
Parse	0x03	✔	✔	✔	✔
SelfTest(7)	0x07	—	✔	(5)	(6)
HealthTest	0x08	—	✔	—	(4)
Execution Fail	0x0F	✔	✔	✔	✔
Successful Wake(2)	0x11	—	—	—	—
Bad CRC , Communication Fail	0xFF	✔	✔	✔	✔

Notes:

1. Success is indicated by an actual output value not by the `0x00` success code.
2. Successful Wake code occurs when the device is first addressed after the device comes out of Sleep mode.
3. Success on the `Info` command is indicated by an actual output value not by the `0x00` success code. Value may differ depending on the mode of operation.
4. Health Tests error can be returned in RNG mode if there is not enough entropy in the generated value.
5. When in Self-Test Failure state, the `Read` command can be used to read the device serial number without error.
6. A Self-Test failure that occurs during a `SelfTest` command is reported as a byte value that indicates which test fails. It does not show a Self-Test failure.
7. The current state of the failure register can be read by calling the `SelfTest` command with a mode parameter of 0x00.

5.4 Checksum

As a way to ensure the integrity of the data being sent to the RNG90 device and received from the device, a Cyclic Redundancy Check (CRC) is included in each command transaction.

For data being sent to the RNG90 device, all bytes starting with the byte count value to the last data byte of the command are included as part of the CRC calculation. The device address and command type are not included. The host device must attach the CRC to the command packet with LSB of the CRC being the first byte. The CRC is sent with the command and is, then, recalculated and compared by the RNG90 device. A CRC error will be flagged if the values do not match and returned in the command response.

For data being read out of the RNG90 device, a CRC will be calculated over the entire packet and attached at the end. This includes data that are intentionally read from the device or from a command response being read back. It is recommended that the host check the incoming data bytes and calculate a CRC value and compare it to the CRC that was read. How the host handles a CRC error is left up to the host but the result must be considered invalid.

CRC Calculation and Example

The RNG90 device uses the 16-bit CRC polynomial `0X8005`. This corresponds to the polynomial $x^{16} + x^{15} + x^2 + x^0$. Data are sent in LSB first. The initial value of the polynomial is `0x0000`. The CRC value is entered or returned as LSB, MSB.

CRC Calculation Examples

Example #1: `Info` Command

Data (Hex): `07 30 01 00 00`

CRC (Hex): `00 D7`

Example #2: Random Data

Data (Hex): `4D 49 43 52 4F 43 48 49 50 54 45 43 48 4E 4F 4C 4F 47 59`

CRC (Hex): `E3 FE`

5.5 Watchdog Timer

The RNG90 WDT is implemented as a fail safe to prevent some condition that indefinitely hangs up the device. The WDT will start to run upon the RNG90 successfully receiving a command. When the action initiated by the command is complete, the WDT will be automatically stopped and reset. If for some reason the command continues to run, the WDT will run for t_{WDT}, then reset the device. The WDT minimum delay is significantly longer than any command execution times.

5.6 Command Summary and Execution Times

5.6.1 Command Summary

The following commands are implemented by the RNG90:

Table 5-5. Commands, Opcodes and Command Descriptions

Command	Opcode	Description
`Info`	`0x30`	Return device state information.
`Random`	`0x16`	Generate a 32-byte random number.
`Read`	`0x02`	Read the unique serial number of the device.
`SelfTest`	`0x77`	Test the RNG.

5.6.2 Command Execution Times

During execution of a properly received command, the device will be busy. The interval the device will be busy varies depending on the command parameters, device state, the environmental conditions and other factors.

The following table shows representative typical and maximum execution times for the command assuming no error conditions, typical mode setting and chip state. Some modes may be faster, while others may be slower. In a typical polling configuration for the I^2C, it is recommended for the host software to wait for the typical interval, then start polling to determine the actual command completion. In most but not all cases, failing commands will return relatively quickly.

Table 5-6. Command Execution Times (ms)

Command	Condition	Typ.	Max.
`Info`	Param 1 = `0x00` (Revision)	0.28	0.40
`Random` (First Execution)	Param 1 = `0x00`	57.0	72.0
`Random` (Subsequent Executions)	Param 1 = `0x00`	20.2	25.3
`Read`	Param 1 = `0x01` (Config 16 bytes)	0.4	0.6
`SelfTest`	Param 1 = `0x01` (DRBG-SelfTest)	25.3	31.8
	Param 1 = `0x20` (SHA256-SelfTest)	11.4	14.5
	Param 1 = `0x00` (Status)	0.27	0.4

Note:

1. First execution of the `Random` command will include the execution time of the self-tests. Subsequent execution times will not.

6. Detailed Command Descriptions

6.1 `Info` Command

The `Info` command is used to access the silicon revision information.

Revision Mode

Table 6-1. Revision Mode Input

OpCode	Param 1	Param 2
0x30	0x00	0x00 0x00

Table 6-2. Revision Mode Output Response

Byte 0	Byte 1	Byte 2	Byte 3
RFU	Device_ID Byte	Silicon ID	Silicon Rev
0x00	0xD0	0x20	0x10

Related Links

5.3. Status/Error Codes

6.2 `Random` Command

The `Random` command is used to generate and output a 32-byte random number for use by the system. Upon initial execution of this command after a sleep->wake cycle or power-down->power-up cycle, both the SHA256 and DRBG self tests will automatically run. The 20 bytes of data can be any value, including all zeros. This parameter must be present but does not impact the value generated by the RNG. A parse error will occur if this data is not included as part of the command.

Table 6-3. Random Number Generation

OpCode	Param 1	Param 2	Data
0x16	0x00	0x0000	20 bytes of data

Table 6-4. Output Response

Response	Width (Bytes)	Description
Success	32	32-byte Random Number
Fail	1	Error Code

Related Links

2.2. Random Number Generator (RNG)
6.4. SelfTest Command
5.3. Status/Error Codes

6.3 `Read` Command

The `Read` command reads back 16-bytes of data. The data includes the unique serial number associated with the device.

Table 6-5. Read Commands

Memory Read	OpCode	Param 1	Param 2	Data[0:15]
Device Serial Number	0x02	0x01	0x0000	• [0:8] Device Serial Number • Other bytes can be ignored

Table 6-6. Output Parameter

Response	Size (Bytes)	Notes
Success	16	The contents of the specified Memory location
Fail	1	Error Code

Related Links

5.3. Status/Error Codes

6.4 `SelfTest` Command

The `SelfTest` command performs on-demand testing of the RNG by executing the RNG self tests. The resulting output of the command will indicate which of the self-tests passed or failed and also indicates if a test has yet to be run. When the `SelfTest` command is run with the mode parameter set to '0', a status of whether a test was run and if it passed is reported. After an initial Sleep->Wake or Power-Down->Power-up cycle, the initial state will be `0x12`.

Upon initial execution of the Random command, after a Sleep->Wake or Power-Down->Power-up cycle, the self tests will automatically run. Note that this will result in the initial execution time of the `Random` command being longer than subsequent executions.

Tip: If a consistent execution time is desirable, it is recommended that the `SelfTest` command be run prior to the execution of the `Random` command for the first time.

The `SelfTest` command can be run any time after the initial start-up procedure completes. Upon successful completion of a test, the appropriate self-test run bits and self-test pass/fail bits will be set. If all tests pass, the Status byte will report `0x00`. If a SelfTest test fails, one of the PASS/FAIL bits will be set. Additional runs of either the `SelfTest` command or the `Random` command is required to clear the fail condition.

Table 6-7. SelfTest Command Input

Command Mode	OpCode	Param 1	Param 2
Read SelfTest Status	0x77	0x00	0x0000
Run DRBG SelfTest	0x77	0x01	0x0000
Run SHA256 SelfTest	0x77	0x20	0x0000
Run DRBG and SHA256 SelfTest	0x77	0x21	0x0000

Table 6-8. SelfTest Output Response

Response Type	Width (Bytes)	Description
Success	1	0x00 = Self Tests were successfully Run and Passed
SelfTest Fail	1	0x01(2) = DRBG Self Test failed 0x20(2) = SHA256 Self Test failed 0x21 = DRBG and SHA256 Self test failed
SelfTest Not Run	1	0x02(1) = DRBG Self Test not run 0x10(1) = SHA256 Self Test not run 0x12(1)= Neither Self Test ran
Fail	1	Error Code

Notes:

1. This condition will occur when the SelfTest Status mode runs after an initial Power-down->Power-up or Sleep->Wake cycle occurrs.
2. This failure can occur after either a failed `SelfTest` command or after the `Random` command automatically executes the RNG SelfTest.

Related Links

2.2. Random Number Generator (RNG)
6.2. Random Command
5.3. Status/Error Codes

7. Package Marking Information

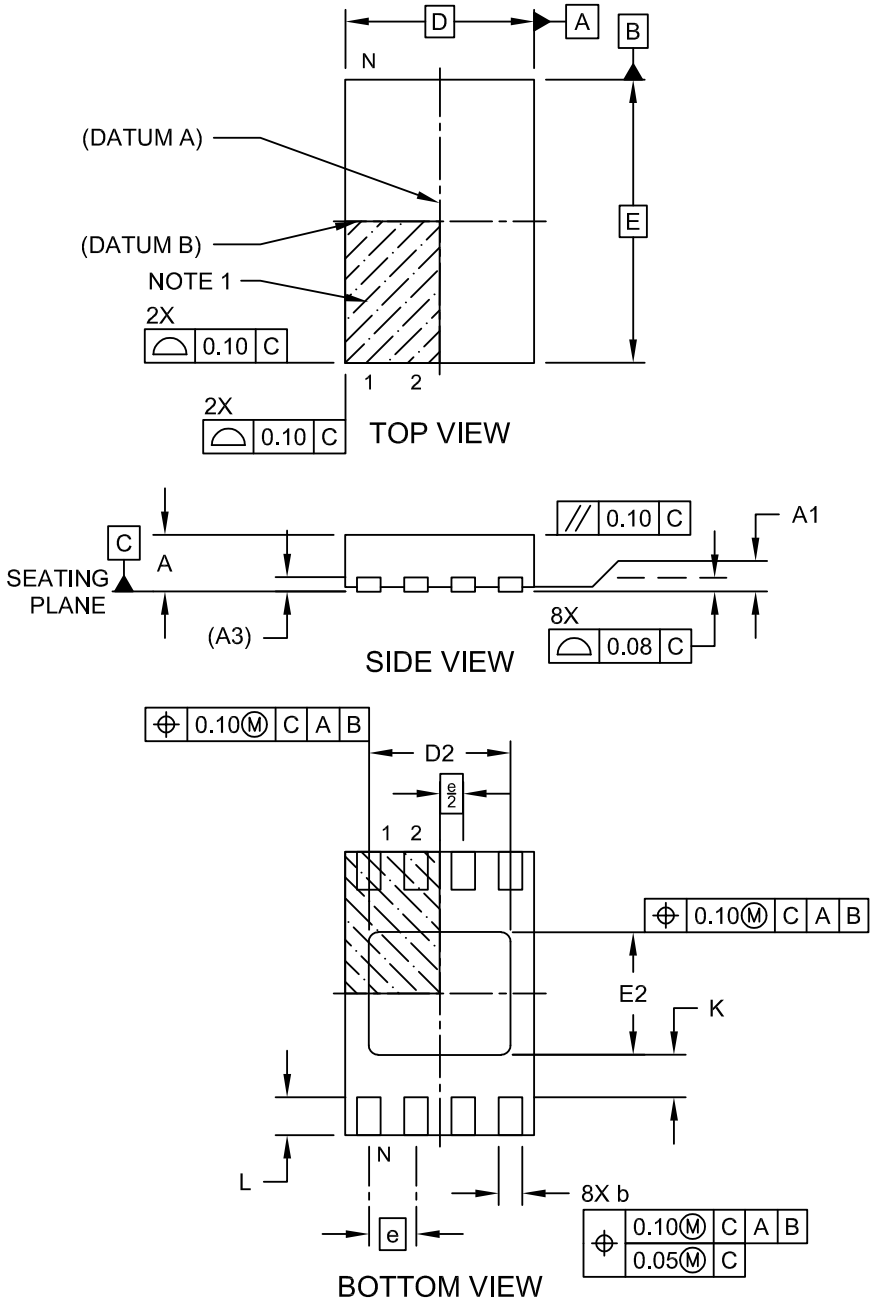
As part of Microchip's overall security features, the part marking for all crypto devices is intentionally vague. The marking on the top of the package does not provide any information as to the actual device type or the manufacturer of the device. The alphanumeric code on the package provides manufacturing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

8. Package Drawings

8.1 8-Pad UDFN

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

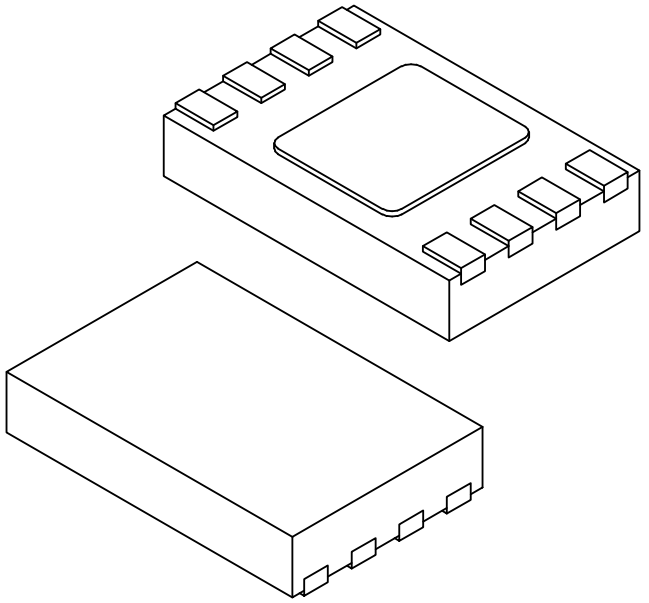
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing C04-21355-Q4B Rev C Sheet 1 of 2

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

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



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Terminals	N		8	
Pitch	e		0.50 BSC	
Overall Height	A	0.50	0.55	0.60
Standoff	A1	0.00	0.02	0.05
Terminal Thickness	A3		0.152 REF	
Overall Length	D		2.00 BSC	
Exposed Pad Length	D2	1.40	1.50	1.60
Overall Width	E		3.00 BSC	
Exposed Pad Width	E2	1.20	1.30	1.40
Terminal Width	b	0.18	0.25	0.30
Terminal Length	L	0.25	0.35	0.45
Terminal-to-Exposed-Pad	K	0.20	-	-

Notes:

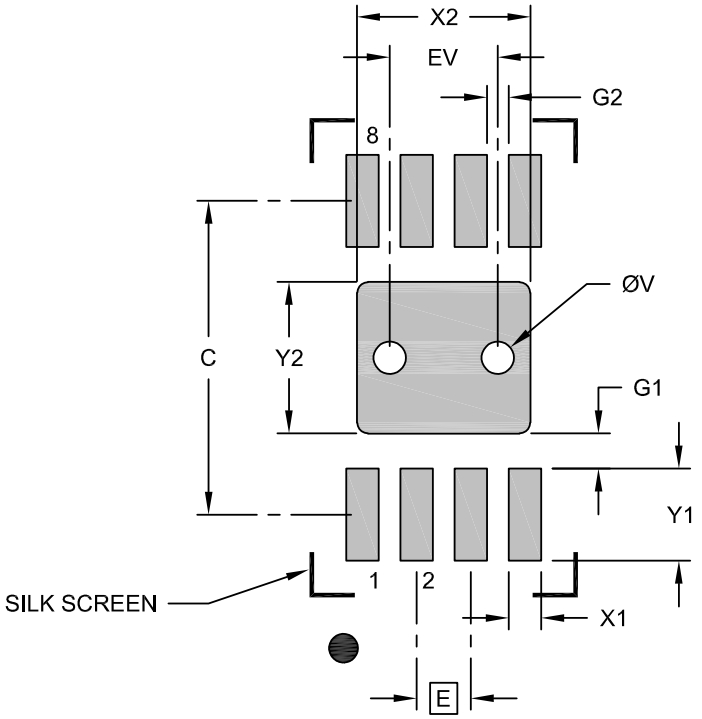
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M

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

Microchip Technology Drawing C04-21355-Q4B Rev C Sheet 2 of 2

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

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



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		0.50 BSC	
Optional Center Pad Width	X2			1.60
Optional Center Pad Length	Y2			1.40
Contact Pad Spacing	C		2.90	
Contact Pad Width (X8)	X1			0.30
Contact Pad Length (X8)	Y1			0.85
Contact Pad to Center Pad (X8)	G1	0.33		
Contact Pad to Contact Pad (X6)	G2	0.20		
Thermal Via Diameter	V		0.30	
Thermal Via Pitch	EV		1.00	

Notes:

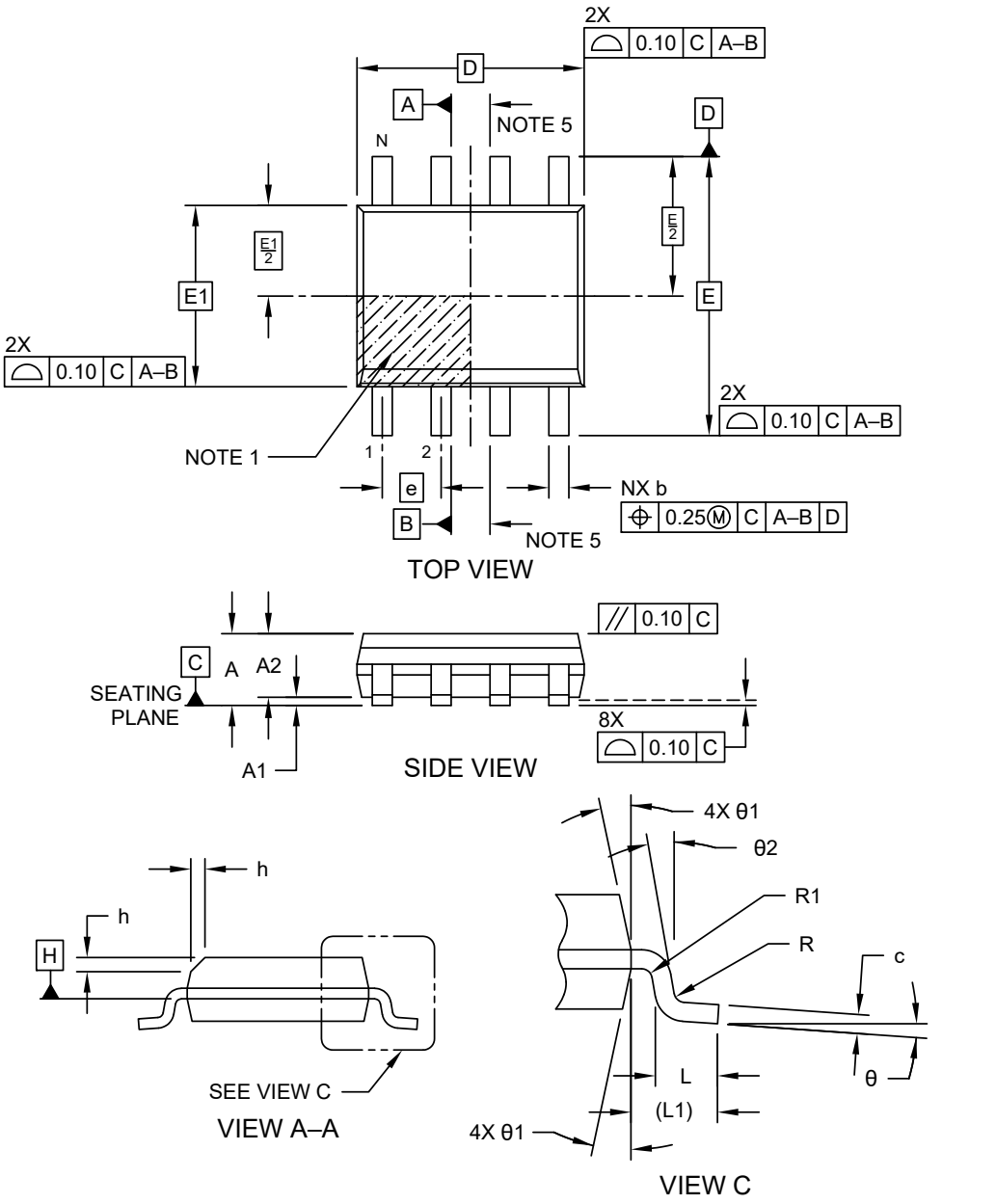
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
2. For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

Microchip Technology Drawing C04-23355-Q4B Rev C

8.2 8-Lead SOIC

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

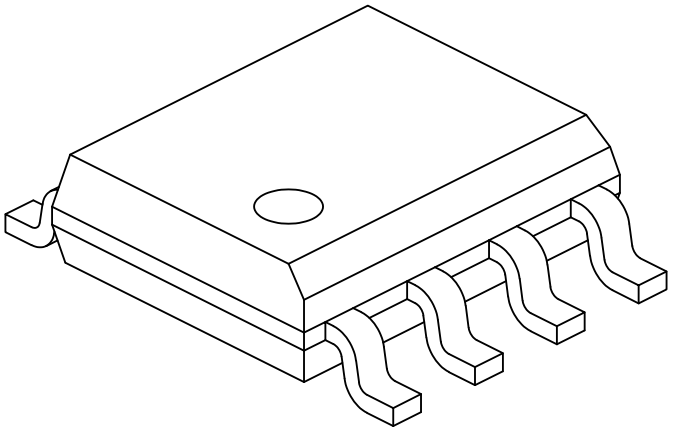
Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing No. C04-057-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

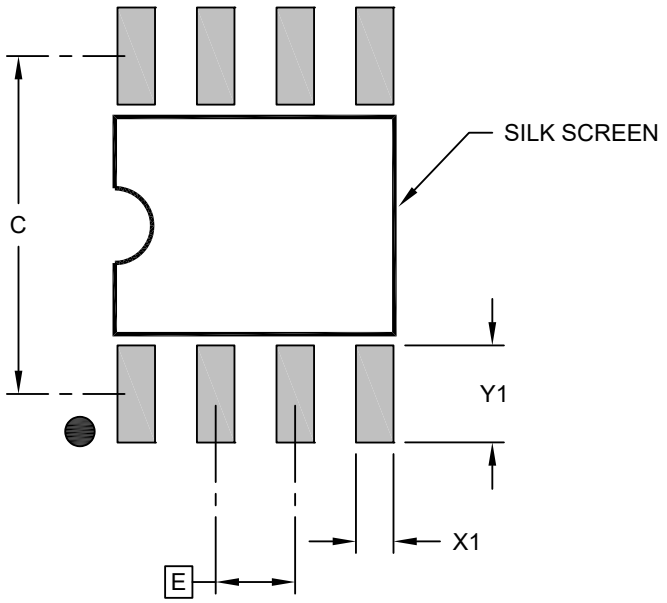
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

   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. Revision History

Revision A (May 2023)

- Initial data sheet release

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.	-XXX	XX	-X
Device	Package	I/O Type	Tape and Reel

Device:	RNG90: NIST Certified Random Number Generator	
Package Options	SS	8-Lead (0.150” Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC)
	MA	8-Pad 2 x 3 x 0.6 mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat NoLead Package (UDFN)
Temperature Grade	V	Extended Industrial Temperature Range. -40℃ to 105℃
I/O Type	DA	I^2C Interface
Tape and Reel Options	T	Large Reel (Size varies by package type)

- RNG90-SSVDA-T: 8-Lead (0.150” Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC), I^2C, Tape and Reel, 3,300 per Reel, With extended Industrial Temperature Range
- RNG90-MAVDA-T: 8-Pad 2 x 3 x 0.6 mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat NoLead Package (UDFN), IC, Tape and Reel, 5,000 per Reel With extended Industrial Temperature Range

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. Small form-factor packaging options may be available. Please check www.microchip.com/packaging for small-form factor package availability, or contact your local Sales Office.

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,

ISBN: 978-1-6683-2412-7

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			