# Differences Between the ATECC608A and ATECC508A CryptoAuthentication™ Devices

*Author: Karthikeyan Logaswamy*
*Microchip Technology Inc.*

## INTRODUCTION

The ATECC608A is a new member of the Microchip CryptoAuthentication™ family of high-security cryptographic devices, which combine world class hardware-based key storage and hardware cryptographic accelerators to implement various authentication and encryption protocols.

## APPLICATIONS

Compared to the ATECC508A, the ATECC608A provides additional features that allow easy integration into resource constrained systems, reduction in operation time, and a decreased number of transactions between the host and the device. The new features include the Secure Boot and the Session key for Transport Layer Security (TLS) (1.1, 1.2, 1.3). They provide a secure IO Protection key for the secure transfer of keys between the host and the device.

The ATECC608A has a flexible command set that allows its use in many applications, including the following:

- Network/Internet of Things (IoT) Node Endpoint Security – it manages node identity authentication and Session key creation and management. It supports the entire ephemeral Session key generation flow for multiple protocols including TLS 1.2 (and earlier) and TLS 1.3.
- Secure Boot – it supports the microcontroller (MCU) host by validating code digests and optionally enabling communication keys on success. For enhanced performance, various configurations are available.
- Small Message Encryption – hardware Advanced Encryption Standard (AES) engine to encrypt and/ or decrypt small messages or data such as Personally Identifiable Information (PII). The device supports the AES-ECB mode directly, other AES modes are supported with help from the host. Additional Galois Field Multiply (GFM) calculation functions support Advanced Encryption Standard/ Galois Counter Mode (AES-GCM).
- Key Generation for Software Download – it supports local protected key generation for downloaded images. Both broadcasts of one image to many systems, each with the same decryption key, and point-to-point download of unique images per system are supported.
- Ecosystem Control and Anti-Counterfeiting – it validates the authenticity of a system or component.

The ATECC608A is designed to be compatible with the ATECC508A devices, with some limited exceptions. If the ATECC608A is properly configured, the software written for the ATECC508A should work with the ATECC608A. For more information, see **Section “Migration from the ATECC508A to the ATECC608A”**. This application note lists the features, commands and configuration differences between the ATECC608A and the ATECC508A. It provides high-level details about the differences. For detailed information on the commands and configurations, see the ATECC608A Data Sheet.

## REFERENCES

- ATECC608A Product Details
- ATECC508A Product Details

## FEATURES

The following section describes the various new features available for the ATECC608A, compared to the ATECC508A. It also describes updated features and features that are removed from this device.

### New Features

#### SECURE BOOT

The ATECC608A provides a mechanism to support secure boot operations in a connected MCU/MPU (microprocessor). This can help to identify situations in which fraudulent code has been installed on the host. On power-up, the boot code within the host MCU sends the code digest and/or signature to the ATECC608A. If the signature validates the digest using the public key stored in the ATECC608A or the digest is compared to the stored digest, a message is returned to the MCU host. It also enables a reduction in the execution time of the boot process with its different methods and thus provides the secure boot speed optimization. To avoid the Man-in-the-Middle (MITM) attack, the ATECC608A returns the optional Message Authentication Code (MAC) value to the MCU host, where the MCU host verifies the returned MAC.

#### KEY DERIVATION FUNCTION

The ATECC608A supports the Key Derivation Function (KDF), which derives the KDF key from the Premaster Secret key. The final derived KDF key is mainly used in TLS transactions. The ATECC608A supports three key derivation functions: Pseudo Random Function (PRF), AES, and HMAC-Based Extract-and-Expand KDF (HKDF). The PRF is used in TLS version 1.2 and HKDF is planned to be used in TLS version 1.3.

#### AES

The ATECC608A supports a Hardware 128-bit AES engine to encrypt and/or decrypt small messages or data packets. It supports an Electronic Code Block (ECB) mode and GFM calculation for AES-GCM.

#### SELF-TEST

The ATECC608A provides a mechanism to test the internal cryptographic engines. It supports the self validation testing of the Symmetric HASH Algorithm (SHA), AES, Random Number Generator (RNG), Elliptic Curve Diffie-Hellman (ECDH), Elliptic Curve Digital Signature Algorithm (ECDSA) verify and ECDSA sign functions. Self-Test can be run on device power-up or wake-up or on the Self-Test command from the host.

#### IO PROTECTION KEY

The ATECC608A provides a method to protect the I/O transmissions between this device and the host MCU for ECDH, KDF, Verify, and Secure Boot commands. The IO Protection key is a randomly generated secret key stored in the slot and is shared between the host MCU and the device.

For example, the Premaster key generated from ECDH or the generated KDF key are encrypted by the IO Protection key. The encrypted key is sent to the host, and the host decrypts this with the IO Protection key. In the secure boot process and the signature verification process, a MAC is generated using the IO Protection key, it is sent to the host and provides additional authentication to the host.

#### PERSISTENT LATCH

The Persistent Latch is a single bit of volatile memory used to indicate to the device that an associated key has been enabled for use with cryptographic functions. It can retain its state as long as the $V_{CC}$ remains above 2V. It is always set to zero on power-up and may be manipulated using the operations. When the key in slot is linked to the persistent latch, a persistent latch state activates/deactivates the key in the slot. There are four ways to control the persistent latch: Volatile key usage, secure boot, authorization output and intrusion detection. When one of the above methods is run successfully, the persistent latch will be set, thus enabling the key in the designated slot.

#### VOLATILE KEY USAGE PERMISSION

The Volatile key is used to control the state of the persistent latch. The Volatile key must be the secret that is shared between the MCU and the device. The cryptographic operation is performed between the host and the device with the Volatile key. If successful, the persistent latch can be set, thus enabling the keys in the slot that are attached to the persistent latch.

#### PROGRAMMABLE I$^2$C ADDRESS

The ATECC608A provides the flexibility to change the I$^2$C address after the configuration zone has been locked. It can only be changed once. This feature helps to update the device address dynamically even when the device is deployed in the field.

#### COUNTER MATCH

The counter match function provides a mechanism of altering the limit to which the first monotonic counter (Counter 0) can be incremented. The key usage can be connected to the counter to prevent its use when Counter 0 reaches the limit value of the counter match slot. The counter match value in the slot can be changed any number of times and, for each change, Counter 0 gets linked to the new limit.

### TRANSPORT/USE LOCK

The general purpose usage of the device is prohibited until the device is cryptographically enabled. The cryptographic operation is performed with the stored key in the slot and the known key is provided by the host. Once the operation is successful, the ATECC608A can be used normally.

### POWER REDUCTION

The ATECC608A provides an option for reducing power consumption. The power consumption is reduced at the cost of the execution time. It helps when the device is used for low power applications. See **Section "Configuration Zone Updates"**.

### ADDITIONAL BUFFERS FOR IMPROVED OPERATION

The ATECC608A provides new SRAM buffers: Message Digest Buffer, Alternate Key Buffer, and SHA Context Buffer. The Message Digest Buffer and Alternate Key Buffer can be used when TempKey register holds other information. It also reduces the transaction between the device and host, and the device can execute different commands directly from the buffers.

The ATECC608A supports multiple instances for the SHA calculation with SHA context. The SHA buffer helps the host to perform read and write operations on SHA context, which enables the host to execute multiple instances of SHA calculations.

## Updated Features

The TempKey buffer size is increased by 32 bytes, thus providing more storage and easy operation for other commands like AES, KDF, etc.

The ATECC608A includes an enhanced high-quality cryptographic random number generator implemented using a combination of non-deterministic noise (entropy) source (NRBG), and seeding a deterministic algorithm (DRBG) implemented according to the National Institute of Standards and Technology (NIST) standards. The NRBG is used in the instantiation and each time an RNG number is required.

## Unsupported Features

The EEPROM One Time Programmable (OTP) Consumption mode has been eliminated from the ATECC608A. After the device configuration zone is locked, no change to the OTP zone is allowed. Only reading of the OTP zone data is allowed.

Limited key use or LastkeyUse functionality for Key 15 has been eliminated. Slot 15 of the ATECC608A has the same functionalities as other slots and cannot be used for the limited key usage.

The functionality to select the device from multiple devices sharing the same medium, when operating in Single-Wire Interface (SWI) mode using the selector byte, has been removed.

## COMMANDS

The following section provides details regarding various new commands available for the ATECC608A. It also mentions updated commands and commands that have been removed from this device.

### New Commands

#### SECURE BOOT

The Secure Boot command verifies the user application code during booting. This command supports three modes:

- Full mode. The signature and digest are passed to the ATECC608A. The public key in the slot verifies the sent signature and digest. The response may be a Boolean or MAC, depending on the Secure Boot command.
- Full Store mode. In Full Store mode, the digest or signature is stored in the slot. If the digest is stored in the slot, it is sent to the device for verification. If the signature is stored in the slot, the digest is transmitted to the device, which verifies it with the stored signature and public key.
- Full Copy mode. This mode is run when the secure boot code updates the user application. Both the digest and signature are sent to the device, which verifies them with the stored public key. Once the command is executed successfully, either the digest or signature is copied to the slot, which depends on the secure boot settings in the configuration zone.

In a scenario where wire(s) protection is needed, the command has the option to inform the device that encrypted digest is sent to the device. In this case, the digest is encrypted using the IO Protection key and TempKey. The return value from the device is either the validating MAC or the status code based on the selection of digest encryption. When the encrypted digest is sent, the MAC is returned from the device. The host also calculates the MAC using the IO Protection key, nonce, digest and verifies the returned MAC. If the mode is Full Store Signature, then the signature is also included for calculating the MAC and the host verifies the returned MAC. The command has the option to prohibit the secure boot function until the next power cycle.

#### SELF-TEST

The Self-Test command is used for testing cryptographic engines like AES, SHA, ECDH, ECDSA Verify, Sign, and RNG. This command has different modes that help in testing the individual cryptographic engines separately or they can be combined. The return status from the device gives the individual cryptographic engine test results.

#### AES

The AES command supports a 128-bit Advanced Encryption Standard - Electronic Code Book (AES-ECB) encryption, AES-ECB decryption and calculates the GFM of the input data. An operation for encryption and decryption is performed for 16 bytes at a time.

This command supports the selection of a 16 byte AES key, which can be taken from any of the below sources:

- TempKey – feature to select one of the 16 bytes as key from TempKey
- Slot – feature to select one of the 16 bytes as key from the slot

The return value from the device is the encrypted/decrypted data, GFM data or error code.

#### KDF

The KDF command is used to generate the KDF key from the Premaster Secret key and the input data.

The command supports three modes for creating the KDF key:

- AES – this mode selects the source of the 16 bytes key location
- PRF – this mode selects the length of the source key, Authenticated Encryption with Associated Data (AEAD). It also selects the length of the target key to be generated.
- HKDF – this mode provides the flexibility to select the source location input data and the zero key. There is an IV Special Function in HKDF that compares the strings of the input data with the predefined string in the configuration zone and generates the KDF key once it matches.

The command selects the source location of the source key and can select the target KDF key location. This additional feature provides more security without the KDF key being returned to the device. The source and target key location can be the EEPROM slot, TempKey or Alternate Key Buffer. The command also provides the option to send the KDF key in plain or encrypted to the host. The host decrypts the encrypted KDF key using the IO Protection key and nonce.

Depending on the mode, the return value from the command is either the plain/encrypted KDF key or return status code. If the encrypted KDF key is returned, then a random nonce is also returned for decrypting the KDF key in the host.

## Updated Commands

### ECDH

The ECDH command can additionally select the source private key location and target Premaster Secret key location. The two possible sources for the private key location are the TempKey and EEPROM key slot. The target Premaster key location can have any of the following locations: output buffer, EEPROM or TempKey.

When the Encrypted mode is selected by the ECDH command, the output premaster secret is encrypted using the IO Protection key.

### GENKEY

The GENKEY command now supports a new private key generation to TempKey and the resulting private key is used only by the ECDH command. When the private key is stored in TempKey, it frees the slot for other uses. The generated private key is used for the Premaster Secret key generation.

### INFO

The INFO command is updated to set and reset the state of the persistent latch. This command helps to read the current state of the persistent latch.

### NONCE

The Nonce command allows for the input data to be stored in any of the following buffers: TempKey buffer, Message Digest Buffer or the Alternate Key Buffer. The Nonce command also allows up to 64 bytes to be passed into the TempKey or Message Digest Buffer, when in PassThrough mode.

### SHA

The SHA command supports write and read context switching. This allows for multiple SHA digests to be calculated concurrently. The SHA mode is updated to support variable length data compared to earlier fixed 64-byte data. The output of the command is directed to any of the following locations: output buffer and TempKey, or output buffer and Message Digest Buffer or output buffer only.

### SIGN

In addition to signing the message in TempKey, the Sign command provides the message in Message Digest Buffer for signing the data, freeing the TempKey for other operations.

### VERIFY

In addition to verifying the message in TempKey, the Verify command provides the message in Message Digest Buffer for verifying the data, freeing the TempKey for other operations. It has an additional mode to send the MAC from device to host, where the MAC is calculated from the IO Protection key.

## Unsupported Commands

### PAUSE

For the ATECC508A, the Pause command is useful when using multiple devices on the SWI Interface. This allows the ATECC508A to select only the device that matches the selector byte to do the further communication and all other devices in the same shared medium enter the Idle mode. The Selector Byte functionality has been removed from the ATECC608A.

### HMAC

While the HMAC command no longer exists for the ATECC608A, the HMAC calculation can still be performed. The ATECC608A provides the feature for calculating the HMAC value using the SHA command. In both ATECC608A and ATECC508A, the resulting HMAC value from using the SHA command always matches. However, the ATECC608A HMAC value calculated using the SHA command does not match the HMAC value from using the HMAC command in the ATECC508A.

## CONFIGURATION ZONE UPDATES

Table 1 lists the new fields added in the ATECC608A configuration zone. It also mentions the differences between the two devices.

### TABLE 1: CONFIGURATION ZONE UPDATES

| Byte | ATECC608A | ATECC508A |
|---|---|---|
| 13 | AES_Enable – this byte enables/disables the AES functionalities for both AES and KDF commands. | Reserved for future use |
| 18 | CountMatch – this byte enables/disables the CountMatch function and selects the slot to be used as the Counter Match key. | OTP mode – used to set Read Only or Consumption mode to the OTP zone |
| 19 | ChipMode – bits 3-7 in the ChipMode byte are used to define the Power/Timing mode of the device. Three possible modes are allowed. The lower power is achieved by changing the internal clock divider at the expense of slower execution times.<br>Bit 0 is used to indicate if the I$^2$C address can be changed after the configuration zone has been locked.<br>The new byte helps to reduce the power consumption of the device by its three modes. It also selects the source I$^2$C address, either from the I$^2$C_Address or the UserExtraAdd byte. | Chip mode |
| 68 | UseLock – this new byte controls the transport lock functionality. It enables/disables the transport lock function and the slot to be used as the transport key. | LastKeyUse (16 bytes) – this field controls the KeyID 15 limited-use functionality |
| 69 | VolatileKey Permission – this new byte enables/disables the Volatile key functionality and selects the Volatile key slot for Volatile key functionalities. | |
| 70-71 | SecureBoot – this new byte configures the secure boot functionalities:<br>• selection of one of the Secure Boot modes<br>• whether to set the persistent latch on successfully Secure Boot command execution<br>• the slot to be used for digest/signature<br>• the slot to be used for public key<br>• the random number generator to be used for Secure Boot command | |
| 72 | kdflvLoc – index within the KDF(HKDF) input string, where the two bytes stored below (KdflvStr) should be found | |
| 73 | KdflvStr – two-byte KDF IV string that must be found in the KDF message for the KDF(HKDF) Special IV mode | |
| 85 | UserExtraAdd – if non-zero, it is the I$^2$C address to which this device will respond on the bus | Selector byte – it selects which device will remain in Active mode after the execution of the Pause command |
| 90 | ChipOptions<br>The new byte provides the following features:<br>• whether to run the Self-Test automatically on power-on or wake-up<br>• enables/disables the IO Protection key<br>• enables/disables the KDF AES function<br>• sets the ECDH and KDF protection functionality<br>• the slot to be used for the IO Protection key | Reserved for future use |
| 96-127 | KeyConfig – in KeyType, two new types (AES, SHA) and the function to enable the key based on the state of the persistent latch are added. | KeyConfig |

## MIGRATION FROM THE ATECC508A TO THE ATECC608A

The ATECC608A supports additional features compared to the ATECC508A. The migration from ATECC508A to ATECC608A is very simple and provides the same functionality in ATECC608A with few exceptions discussed in the previous sections. To allow the ATECC608A to operate similarly to the ATECC508A, the configuration zone changes shown in Table 2 must be made. Note that this configuration does not take advantage of the new features or commands associated with the ATECC608A. Also, some functionalities of the ATECC508A are not supported by the ATECC608A (OTP Consumption mode, LastkeyUse of Slot15 and Pause command).

TABLE 2: ATECC508A TO ATECC608A MIGRATION

| Byte | ATECC608A | ATECC508A |
|---|---|---|
| 18 | CountMatch – 0x00 | OTP mode<br>0xAA – Read Only mode<br>0x55 – Consumption mode<br>All other values are reserved |
| 19 | ChipMode – bits 3-7 of the byte should be zero | |
| 68 | UseLock – 0x00 | LastKeyUse – generally initialized to 0xFF |
| 69 | VolatileKey Permission – 0x00 | |
| 70-71 | SecureBoot – 0x0000 | |
| 72 | kdflvLoc – 0x00 | |
| 73 | KdfIvStr – 0x00 | |
| 85 | UserExtraAdd – 0x00 | Selector byte – any value depending on the device configured for Pause command |
| 90 | ChipOptions – 0x00 | Reserved for future use<br>0x00 |

NOTES:

**Note the following details of the code protection feature on Microchip devices:**

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Information contained in this publication regarding device applications and the like 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. 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 ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE**.** Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

*Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.*

**QUALITY MANAGEMENT SYSTEM**
**CERTIFIED BY DNV**
**═ ISO/TS 16949 ═**

**Trademarks**

The Microchip name and logo, the Microchip logo, AnyRate, AVR, AVR logo, AVR Freaks, BeaconThings, BitCloud, chipKIT, chipKIT logo, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Heldo, JukeBlox, KEELOQ, KEELOQ logo, Kleer, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, RightTouch, SAM-BA, SpyNIC, SST, SST Logo, SuperFlash, tinyAVR, UNI/O, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

ClockWorks, The Embedded Control Solutions Company, EtherSynch, Hyper Speed Control, HyperLight Load, IntelliMOS, mTouch, Precision Edge, and Quiet-Wire 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, BodyCom, CodeGuard, CryptoAuthentication, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, EtherGREEN, In-Circuit Serial Programming, ICSP, Inter-Chip Connectivity, JitterBlocker, KleerNet, KleerNet logo, Mindi, MiWi, motorBench, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PureSilicon, QMatrix, RightTouch logo, REAL ICE, Ripple Blocker, SAM-ICE, Serial Quad I/O, SMART-I.S., SQI, SuperSwitcher, SuperSwitcher II, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

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

Silicon Storage Technology is a registered trademark of Microchip Technology Inc. in other countries.

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

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

ISBN: 978-1-5224-2391-1

# Worldwide Sales and Service

## AMERICAS

**Corporate Office**
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
http://www.microchip.com/support
Web Address:
www.microchip.com

**Atlanta**
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

**Austin, TX**
Tel: 512-257-3370

**Boston**
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

**Chicago**
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

**Dallas**
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

**Detroit**
Novi, MI
Tel: 248-848-4000

**Houston, TX**
Tel: 281-894-5983

**Indianapolis**
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453
Tel: 317-536-2380

**Los Angeles**
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608
Tel: 951-273-7800

**Raleigh, NC**
Tel: 919-844-7510

**New York, NY**
Tel: 631-435-6000

**San Jose, CA**
Tel: 408-735-9110
Tel: 408-436-4270

**Canada - Toronto**
Tel: 905-695-1980
Fax: 905-695-2078

## ASIA/PACIFIC

**Australia - Sydney**
Tel: 61-2-9868-6733

**China - Beijing**
Tel: 86-10-8569-7000

**China - Chengdu**
Tel: 86-28-8665-5511

**China - Chongqing**
Tel: 86-23-8980-9588

**China - Dongguan**
Tel: 86-769-8702-9880

**China - Guangzhou**
Tel: 86-20-8755-8029

**China - Hangzhou**
Tel: 86-571-8792-8115

**China - Hong Kong SAR**
Tel: 852-2943-5100

**China - Nanjing**
Tel: 86-25-8473-2460

**China - Qingdao**
Tel: 86-532-8502-7355

**China - Shanghai**
Tel: 86-21-3326-8000

**China - Shenyang**
Tel: 86-24-2334-2829

**China - Shenzhen**
Tel: 86-755-8864-2200

**China - Suzhou**
Tel: 86-186-6233-1526

**China - Wuhan**
Tel: 86-27-5980-5300

**China - Xian**
Tel: 86-29-8833-7252

**China - Xiamen**
Tel: 86-592-2388138

**China - Zhuhai**
Tel: 86-756-3210040

## ASIA/PACIFIC

**India - Bangalore**
Tel: 91-80-3090-4444

**India - New Delhi**
Tel: 91-11-4160-8631

**India - Pune**
Tel: 91-20-4121-0141

**Japan - Osaka**
Tel: 81-6-6152-7160

**Japan - Tokyo**
Tel: 81-3-6880- 3770

**Korea - Daegu**
Tel: 82-53-744-4301

**Korea - Seoul**
Tel: 82-2-554-7200

**Malaysia - Kuala Lumpur**
Tel: 60-3-7651-7906

**Malaysia - Penang**
Tel: 60-4-227-8870

**Philippines - Manila**
Tel: 63-2-634-9065

**Singapore**
Tel: 65-6334-8870

**Taiwan - Hsin Chu**
Tel: 886-3-577-8366

**Taiwan - Kaohsiung**
Tel: 886-7-213-7830

**Taiwan - Taipei**
Tel: 886-2-2508-8600

**Thailand - Bangkok**
Tel: 66-2-694-1351

**Vietnam - Ho Chi Minh**
Tel: 84-28-5448-2100

## EUROPE

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

**Denmark - Copenhagen**
Tel: 45-4450-2828
Fax: 45-4485-2829

**Finland - Espoo**
Tel: 358-9-4520-820

**France - Paris**
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

**Germany - Garching**
Tel: 49-8931-9700

**Germany - Haan**
Tel: 49-2129-3766400

**Germany - Heilbronn**
Tel: 49-7131-67-3636

**Germany - Karlsruhe**
Tel: 49-721-625370

**Germany - Munich**
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

**Germany - Rosenheim**
Tel: 49-8031-354-560

**Israel - Ra’anana**
Tel: 972-9-744-7705

**Italy - Milan**
Tel: 39-0331-742611
Fax: 39-0331-466781

**Italy - Padova**
Tel: 39-049-7625286

**Netherlands - Drunen**
Tel: 31-416-690399
Fax: 31-416-690340

**Norway - Trondheim**
Tel: 47-7289-7561

**Poland - Warsaw**
Tel: 48-22-3325737

**Romania - Bucharest**
Tel: 40-21-407-87-50

**Spain - Madrid**
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

**Sweden - Gothenberg**
Tel: 46-31-704-60-40

**Sweden - Stockholm**
Tel: 46-8-5090-4654

**UK - Wokingham**
Tel: 44-118-921-5800
Fax: 44-118-921-5820