

---

---

## 用于SAM D10的安全UART自举程序

---

---

### 简介

许多现代嵌入式系统需要通过固件更新来修复错误或支持新功能。同时，知识产权保护也起着重要作用。单片机具有强大的固件保护机制；然而，在从外部源传输数据时，固件容易被截取。

解决此问题的一种方法是使用安全的自举程序，并仅向公众发布加密的固件映像。本应用笔记介绍了SAM D10器件的安全自举程序的设计和工作原理，并说明了加密算法。

#### 安全自举程序的特性

- 安全
- 长度较短（2 KB）
- 使用UART RX和TX引脚以及可选自举程序进入引脚
- 支持自更新
- 固件完整性验证

---

## 目录

---

简介.....	1
1. 硬件配置.....	3
2. 进入方法.....	4
3. 自举程序命令.....	5
4. 响应代码.....	7
5. 编程算法.....	8
6. 附录A: 安全步骤.....	9
7. 附录B: 与加密映像配合使用的PC实用程序 .....	11
Microchip网站.....	12
变更通知客户服务.....	12
客户支持.....	12
Microchip器件代码保护功能.....	12
法律声明.....	13
商标.....	13
DNV认证的质量管理体系.....	14
全球销售及服务网点.....	15

## 1. 硬件配置

自举程序所使用的UART引脚取决于器件类型，具体在下表中列出。

**表1-1. 硬件配置**

器件	UART TX	UART RX	进入
SAM D10	PA10	PA11	PA25

自举程序进入引脚低电平有效。该引脚的值在自举程序执行开始时进行采样。尽管内部上拉电阻在采样引脚前已使能，仍建议从外部上拉自举程序进入引脚以提高抗噪声能力。

安全自举程序所使用的UART设置为**115200 8, N, 1**。该自举程序支持UART波特率自动调节功能，可用于无法设置确切波特率值的主机。可在工作过程中的任一时刻启动自动调节。要执行自动调节，主机必须发送中断信号（至少11位低电平），后跟字符**0x55**。该请求将没有响应。

## 2. 进入方法

自举程序可通过多种方式调用。

1. 如果没有有效的固件，则自举程序将自动运行。如果第一个字不是**0xFFFFFFFF**，则认为固件有效。通常，该字包含一个初始堆栈指针值，因此除非器件被擦除，否则第一个字始终不是**0xFFFFFFFF**。
2. 如果自举程序执行开始时自举程序进入引脚的值为低电平，则自举程序将基于外部请求运行。
3. 如果SRAM中的前四个存储单元等于**0x78656C41**，则自举程序将基于应用程序（内部）请求运行。

外部复位的优先级高于任何其他进入方法。

应用程序可使用以下代码请求执行自举程序：

```
{
  uint32_t *ram = (uint32_t *)HSRAM_ADDR;
  __disable_irq();
  ram[0] = 0x78656c41;
  ram[1] = 0x78656c41;
  ram[2] = 0x78656c41;
  ram[3] = 0x78656c41;
  NVIC_SystemReset();
}
```

### 3. 自举程序命令

所有自举程序命令均采用相同的通用格式，如下表所示。

表3-1. 自举程序命令

命令ID	保护值	数据0	...	数据N
1字节	4字节	4字节	...	4字节

数据字的数量和含义因命令而异。所有数据字必须以小尾数法（LSB在前）格式发送。

保护值必须为常量值0x78656C41，这可以提供防止虚假命令的额外保护。

命令帧的所有字节的发送间隔不得超过100 ms。经过100 ms的空闲时间后，不完整的命令会被丢弃，自举程序将返回等待新的命令ID。该行为允许主机在同步丢失时重新同步。

自举程序可理解以下命令：

- Unlock (0xA0)
- Data (0xA1)
- Verify (0xA2)
- Reset (0xA3)

Unlock命令必须在第一个Data命令之前发出，它具有以下有效负载：

- 数据0——起始偏移
- 数据1——映像大小
- 数据2–数据5——临时值

起始偏移是与闪存起始处的偏移。要自行升级自举程序，该值必须设置为0。应用程序映像偏移取决于器件，有效值在下表中列出。映像偏移必须在擦除单元大小边界处对齐，该边界同样取决于器件。映像大小必须以擦除单元字节为增量。

表3-2. 应用程序映像偏移的有效值

器件	应用程序偏移（字节）	用户区域偏移（字节）	擦除单元大小（字节）
SAM D10	2048	1792	256

临时值是一个任意的16字节值，对于给定的密钥不能重复。该数字可以是递增计数器值，也可以是随机字节序列或两者的组合。使用随机数时，确保其源自良好熵源。有关使用此数字进行加密和验证的详细信息，请参见附录A。

数据命令用于发送映像数据，它具有以下有效负载：

- 数据0——起始偏移
- 数据1–数据N——映像数据（擦除单元大小字节）
- 数据N+1–数据N+5——映像MAC

起始偏移必须位于之前通过Unlock命令解锁的区域。如果尝试请求在解锁区域以外执行写操作，则将导致错误，提供的数据将被丢弃。

映像数据必须进行加密和验证。映像报文验证代码（Message Authentication Code, MAC）可确保数据通过验证且不会在传输过程中损坏。MAC还可确保数据属于当前存储单元和当前文件。有关生成该数据以及使用该数据进行验证和加密的详细信息，请参见附录A。

安全自举程序支持写入闪存和接收下一个数据块同时进行。第一个数据块的状态代码返回后，即可发送下一个数据块。

受该行为影响，最后一个数据块的状态代码将在该数据块写入闪存前发送。要确保该数据块写入，主机必须发送另一条命令并等待响应。因此，Verify或Reset命令必须在最后一个数据块之后发送。

用户区域位于自举程序的最后一个块中。主加密密钥存储在用户区域的前16个字节中，剩余字节可用于存储任意用户数据（序列号和附加安全信息等）。用户区域的更新与常规数据块类似，因此需要全面的安全处理。这意味着必须使用旧密钥来加密和验证新密钥。如果旧密钥丢失，则无法使用该自举程序恢复器件。

默认加密密钥为00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:0f。

Verify命令用于验证映像数据，Verify命令无有效载荷。传输期间的映像完整性通过MAC来确保，自举程序将在数据写入闪存后读回数据。Verify命令可在映像上传期间的任意时刻发出，它将返回验证状态的当前值。

Reset命令用于退出自举程序和运行应用程序，这在主机无法控制复位引脚时十分必要。不过，即使主机能够控制复位，该命令也十分有用，因为该命令允许主机向应用程序发送多达四个字的任意信息。它具有以下有效载荷：

- 数据0——任意值0
- 数据1——任意值1
- 数据2——任意值2
- 数据3——任意值3

所提供的任意值将传送到应用程序中SRAM的前四个存储单元。

提供的所有值均不得等于0x78656C41，因为这将请求执行自举程序。

## 4. 响应代码

自举程序将发送一个单字符响应代码来响应每条命令。只能在接收到前一条命令的响应代码后或在100 ms超时（没有响应）后发送后续命令。

以下是可能的响应代码：

- 正常（0x50）——成功接收和处理命令
- 错误（0x51）——处理命令期间出现错误
- 无效（0x52）——接收到无效命令
- 验证通过（0x53）——映像验证成功
- 验证失败（0x54）——映像验证失败

## 5. 编程算法

发出每条命令后，主机必须等待响应代码至少100 ms。如果在此期间未接收到响应代码，则会认为命令丢失，可再次重复命令。

主机控制器必须执行以下操作来更新固件：

1. 请求进入自举程序。
2. 等待（至少5 ms）自举程序启动。
3. 发出带所需映像参数的Unlock命令。
4. 发送带固件数据的Data命令。
5. 重复步骤4，直至整个映像完成传输。
6. 发出Verify命令并检查响应代码。
7. 如果响应代码验证失败，则从步骤3开始重复更新过程。
8. 发出Reset命令。



## 6. 附录A: 安全步骤

自举程序使用Spritz流加密。Spritz是著名的RC4加密的替代方法，但与RC4相比，它实现了一些重要的改进。除了修复RC4中的一些偏差和漏洞之外，Spritz还可用于实现加密哈希函数、确定性随机数生成器和加密算法（对加密数据进行验证）。Spritz对于低端嵌入式系统非常友好，因为它主要依靠8位值和表查找的基本算术运算。

Spritz被称为“海绵加密”，因为它基于海绵函数。一般来说，海绵算法可以输入任意大小的输入比特流，并产生任意大小的输出。在生成输出流期间的任何时刻，新数据都可能被“吸收”。该属性以各种方式加以应用，可以构建基本的安全基元。

实际上，Spritz输入和输出限制为8位块以便与字节流对齐。因此，Spritz可采用任意输入字节流，并根据内部状态产生输出字节流。

Spritz加密所有可能的函数均由一小部分以多种方式修改内部状态的基本函数构成。最有用的基本构件是：

- `InitializeState()` —— 将算法的状态复位为可知的状态
- `Absorb(M)` —— 吸收报文M（字节数组），并对内部状态进行“洗牌”
- `AbsorbStop()` —— 吸收特殊的STOP符号，该符号不是输入字母的一部分
- `Squeeze(n)` —— 返回所请求数量的伪随机字节

`AbsorbStop()` 是Spritz算法的一个非常独特的特征。此函数以通过吸收常规字母中的任何字符均无法实现的方式修改内部状态。

许多安全算法的一个共同部分是计算多个字节流连接后的哈希值。这些字节流可能表示一个加密密钥或一条报文。例如，连接的字节流具有可变长度，则两个有效的输入组合可能出现哈希碰撞。例如，`Hash(FearNot || Secured)` 的值与 `Hash(Fear || NotSecured)` 的值相同。

要解决这一问题，算法通常需要将密码填充到已知的固定长度。使用Spritz时，`AbsorbStop()` 可用作连接符号，因此即使不进行填充，也不会出现上述碰撞。

在使用自举程序时，所有输入均具有预定义的大小，因此不会使用`AbsorbStop()`，因为它是多余的。

自举程序中的安全功能是与加密的典型用法迥然不同的应用。许多攻击均基于观察大量的加密数据来成功利用安全方案可能存在的漏洞。自举程序很少会出现这种问题，因此无法在器件的整个使用过程中观察到少量加密映像以外的内容。这通常允许降低加密算法的要求，从而带来缩短代码长度和提高性能的优势。这种情况下会遵循最佳的安全实践，牺牲一些潜在的性能。

数据的安全和验证基于存储在用户区域前16个字节中的主密钥。

始终不直接使用主密钥，并从主密钥和给定会话或固件映像特定的其他信息中获取会话密钥是一种很好的安全措施。

以下示例给出了获取会话密钥的过程。

```
ObtainSessionKey(MasterKey, UnlockCommand)
  InitializeState();
  Absorb(MasterKey);
  Absorb(UnlockCommand);
  return Squeeze(16)
```

MasterKey是来自用户区域的16字节序列，UnlockCommand是解锁命令的完整有效载荷，本身不包括命令ID，但包括保护值。该有效载荷的长度为28字节（保护值 + 映像偏移 + 映像大小 + 临时值）。

所得到的会话密钥对于闪存中的特定映像和存储位置是惟一的。临时值用于消除会话密钥可能重复的情况，因为通常应用程序固件映像将具有相同的偏移和大致相同的大小。

会话密钥的长度为16字节，它用于初始化各个数据块的加密和验证状态。

要为Data命令生成命令有效载荷，必须先加密原始数据。对在擦除块大小边界处对齐的数据块执行加密程序。它还需要命令头（保护值和块偏移）来确保验证的数据不能写入不同的存储单元。

```
EncryptBlock(SessionKey, CommandHeader, Data)
  InitializeState();
  Absorb(SessionKey);
  Absorb('E');
  Absorb(CommandHeader);
  Absorb(Data);
  EncryptedData = Data + Squeeze(EraseUnitSize)
  return CommandHeader || EncryptedData
```

此处的+执行逐字节的算术加法运算，||执行连接操作。

在会话密钥之后，EncryptBlock()将吸收字母E（0x45）对应的单个字节。这是为了区分内部状态和验证操作。不重复使用相同的安全资料进行加密和验证是一种很好的安全实践。

在数据块加密之后，它需要进行验证，因为加密容易受到无法在解密阶段期间检测到的密文修改的影响。

验证算法将对从EncryptBlock()函数返回的加密数据块起作用，并且会使用16字节验证值扩展加密数据。

```
AuthenticateBlock(SessionKey, EncryptedData)
  InitializeState();
  Absorb(SessionKey);
  Absorb('A');
  Absorb(EncryptedData);
  return EncryptedData || Squeeze(16)
```

自举程序接受的Data命令的最终有效载荷将具有以下结构：

**CommandHeader** (8字节) || **EncryptedData** (擦除单元大小) || **AuthenticationValue** (16字节)。

## 7. 附录B：与加密映像配合使用的PC实用程序

自举程序随附了大量评估实用程序。此过程分为准备一个可通过开放通道自由分布的加密映像以及一个实际更新。

`encrypt.py`是一个加密实用程序。它具有以下语法：

选项：

```
-h, --help          显示此帮助消息并退出
-f FILE, --file=FILE  输入文件
-k KEY, --key=KEY     加密密钥（以“:”分隔的16字节）
-o OFFSET, --offset=OFFSET 目标偏移（默认值为0x800）
```

示例调用：

```
python encrypt.py -k 00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:0f -f
test_app_d10.bin
```

`encrypt.py`会将后缀`.enc`添加到输入文件名，以获得输出文件名。

每次调用将产生不同的文件内容，因为每次调用都产生随机的临时值。

这一实现过程在C语言中称为`encrypt.c`。它在语法和操作上与Python版本完全等效。此版本可用作使用自举程序并在运行时生成映像的嵌入式应用程序的参考。

`boot.py`是一个更新实用程序，它会获取加密映像并通过串行端口上传该映像。它具有以下语法：

选项：

```
-h, --help          显示此帮助消息并退出
-v, --verbose       使能详细输出
-t, --tune          自动调节UART波特率
-i PATH, --interface=PATH 通信接口
-f FILE, --file=FILE 要编程的二进制文件
--boot             使能对自举程序区域的写操作
```

示例调用：

```
python boot.py -v -i COM12 -t -f test_app_d10.bin.enc
```

如果加密映像的偏移小于自举程序的大小，则必须使用`--boot`选项。这是防止意外覆盖自举程序或用户区域的额外保护措施。

`key_update.py`是用于生成密钥更新文件的实用程序。生成的文件可供`boot.py`实用程序用来执行实际密钥更新。它具有以下语法：

选项：

```
-h, --help          显示此帮助消息并退出
-f FILE, --file=FILE 输出文件名
-k OLD_KEY, --key=OLD_KEY 旧加密密钥（以“:”分隔的16字节）
-n NEW_KEY, --new=NEW_KEY 新加密密钥（以“:”分隔的16字节）
```

示例调用（单行）：

```
key_update.py -k 0:1:2:3:4:5:6:7:8:9:0:1:2:3:4:5 -n aa:bb:cc:dd:ee:ff:
00:11:22:33:44:55:66:77:88:99 -f new_key.enc
```

---

## Microchip网站

---

Microchip网站 (<http://www.microchip.com/>) 为客户提供在线支持。客户可通过该网站方便地获取文件和信息。只要使用常用的互联网浏览器即可访问，网站提供以下信息：

- **产品支持**——数据手册和勘误表、应用笔记和示例程序、设计资源、用户指南以及硬件支持文档、最新的软件版本以及归档软件
- **一般技术支持**——常见问题（FAQ）、技术支持请求、在线讨论组以及Microchip顾问计划成员名单
- **Microchip业务**——产品选型和订购指南、最新Microchip新闻稿、研讨会和活动安排表、Microchip销售办事处、代理商以及工厂代表列表

---

## 变更通知客户服务

---

Microchip的变更通知客户服务有助于客户了解Microchip产品的最新信息。注册客户可在他们感兴趣的某个产品系列或开发工具发生变更、更新、发布新版本或勘误表时，收到电子邮件通知。

欲注册，请登录Microchip网站<http://www.microchip.com/>。在“支持”（Support）下，点击“变更通知客户”（Customer Change Notification）服务后按照注册说明完成注册。

---

## 客户支持

---

Microchip产品的用户可通过以下渠道获得帮助：

- 代理商或代表
- 当地销售办事处
- 应用工程师（FAE）
- 技术支持

客户应联系其代理商、代表或应用工程师（FAE）寻求支持。当地销售办事处也可为客户提供帮助。本文档后附有销售办事处的联系方式。

也可通过以下网站获得技术支持：<http://www.microchip.com/support>

---

## Microchip器件代码保护功能

---

请注意以下有关Microchip器件代码保护功能的要点：

- Microchip的产品均达到Microchip数据手册中所述的技术指标。
- Microchip确信：在正常使用的情况下，Microchip系列产品是当今市场上同类产品中最安全的产品之一。
- 目前，仍存在着恶意、甚至是非法破坏代码保护功能的行为。就我们所知，所有这些行为都不是以Microchip数据手册中规定的操作规范来使用Microchip产品的。这样做的人极可能侵犯了知识产权。
- Microchip愿意与关心代码完整性的客户合作。

- **Microchip**或任何其他半导体厂商均无法保证其代码的安全性。代码保护并不意味着我们保证产品是“牢不可破”的。

代码保护功能处于持续发展中。**Microchip**承诺将不断改进产品的代码保护功能。任何试图破坏**Microchip**代码保护功能的行为均可视为违反了《数字器件千年版权法案 (Digital Millennium Copyright Act)》。如果这种行为导致他人在未经授权的情况下，能访问您的软件或其他受版权保护的成果，您有权依据该法案提起诉讼，从而制止这种行为。

## 法律声明

本出版物中所述的器件应用信息及其他类似内容仅为为您提供便利，它们可能由更新之信息所替代。确保应用符合技术规范，是您自身应负的责任。**Microchip**对这些信息不作任何明示或暗示、书面或口头、法定或其他形式的声明或担保，包括但不限于针对其使用情况、质量、性能、适销性或特定用途的适用性的声明或担保。

**Microchip**对因这些信息及使用这些信息而引起的后果不承担任何责任。如果将**Microchip**器件用于生命维持和/或生命安全应用，一切风险由买方自负。买方同意在由此引发任何一切伤害、索赔、诉讼或费用时，会维护和保障**Microchip**免于承担法律责任，并加以赔偿。除非另外声明，否则在**Microchip**知识产权保护下，不得暗或以其他方式转让任何许可证。

## 商标

AVR、AVR徽标、AVR Freaks、BitCloud、chipKIT、chipKIT徽标、CryptoMemory、CryptoRF、dsPIC、FlashFlex、flexPWR、Heldo、JukeBlox、KeeLoq、Kleer、LANCheck、LINK MD、maXStylus、maXTouch、MediaLB、megaAVR、MOST、MOST徽标、MPLAB、OptoLyzer、PIC、picoPower、PICSTART、PIC32徽标、Prochip Designer、QTouch、SAM-BA、SpyNIC、SST、SST徽标、SuperFlash、tinyAVR、UNI/O及XMEGA均为**Microchip Technology Inc.**在美国和其他国家或地区的注册商标。

ClockWorks、The Embedded Control Solutions Company、EtherSynch、Hyper Speed Control、HyperLight Load、IntelliMOS、mTouch、Precision Edge和Quiet-Wire均为**Microchip Technology Inc.**在美国的注册商标。

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、BodyCom、CodeGuard、CryptoAuthentication、CryptoAutomotive、CryptoCompanion、CryptoController、dsPICDEM、dsPICDEM.net、Dynamic Average Matching、DAM、ECAN、EtherGREEN、In-Circuit Serial Programming、ICSP、INICnet、Inter-Chip Connectivity、JitterBlocker、KleerNet、KleerNet徽标、memBrain、Mindi、MiWi、motorBench、MPASM、MPF、MPLAB Certified徽标、MPLIB、MPLINK、MultiTRAK、NetDetach、Omniscient Code Generation、PICDEM、PICDEM.net、PICkit、PICtail、PowerSmart、PureSilicon、QMatrix、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和ZENA均为**Microchip Technology Inc.**在美国和其他国家或地区的商标。

SQTP为**Microchip Technology Inc.**在美国的服务标记。

Silicon Storage Technology为**Microchip Technology Inc.**在除美国外的国家或地区的注册商标。

GestIC是**Microchip Technology Inc.**的子公司**Microchip Technology Germany II GmbH & Co. KG**在除美国外的国家或地区的注册商标。

在此提及的所有其他商标均为各持有公司所有。

© 2018, Microchip Technology Incorporated版权所有。

ISBN: 978-1-5224-3144-2

## DNV认证的质量管理体系

---

### ISO/TS 16949

Microchip位于美国亚利桑那州Chandler和Tempe与位于俄勒冈州Gresham的全球总部、设计和晶圆生产厂及位于美国加利福尼亚州和印度的设计中心均通过了ISO/TS-16949:2009认证。Microchip的PIC<sup>®</sup> MCU和dsPIC<sup>®</sup> DSC、KEELOQ<sup>®</sup>跳码器件、串行EEPROM、单片机外设、非易失性存储器和模拟产品严格遵守公司的质量体系流程。此外，Microchip在开发系统的设计和生产方面的质量体系也已通过了ISO 9001:2000认证。

## 全球销售及及服务网点

### 美洲

公司总部 **Corporate Office**  
2355 West Chandler Blvd.  
Chandler, AZ 85224-6199  
Tel: 1-480-792-7200  
Fax: 1-480-792-7277

技术支持:  
<http://www.microchip.com/support>

网址: [www.microchip.com](http://www.microchip.com)

**亚特兰大 Atlanta**  
Duluth, GA  
Tel: 1-678-957-9614  
Fax: 1-678-957-1455

**奥斯汀 Austin, TX**  
Tel: 1-512-257-3370

**波士顿 Boston**  
Westborough, MA  
Tel: 1-774-760-0087  
Fax: 1-774-760-0088

**芝加哥 Chicago**  
Itasca, IL  
Tel: 1-630-285-0071  
Fax: 1-630-285-0075

**达拉斯 Dallas**  
Addison, TX  
Tel: 1-972-818-7423  
Fax: 1-972-818-2924

**底特律 Detroit**  
Novi, MI  
Tel: 1-248-848-4000

**休斯敦 Houston, TX**  
Tel: 1-281-894-5983

**印第安纳波利斯 Indianapolis**  
Noblesville, IN  
Tel: 1-317-773-8323  
Fax: 1-317-773-5453  
Tel: 1-317-536-2380

**洛杉矶 Los Angeles**  
Mission Viejo, CA  
Tel: 1-949-462-9523  
Fax: 1-949-462-9608  
Tel: 1-951-273-7800

**罗利 Raleigh, NC**  
Tel: 1-919-844-7510

**纽约 New York, NY**  
Tel: 1-631-435-6000

**圣何塞 San Jose, CA**  
Tel: 1-408-735-9110  
Tel: 1-408-436-4270

**加拿大多伦多 Toronto**  
Tel: 1-905-695-1980  
Fax: 1-905-695-2078

### 亚太地区

中国 - 北京  
Tel: 86-10-8569-7000

中国 - 成都  
Tel: 86-28-8665-5511

中国 - 重庆  
Tel: 86-23-8980-9588

中国 - 东莞  
Tel: 86-769-8702-9880

中国 - 广州  
Tel: 86-20-8755-8029

中国 - 杭州  
Tel: 86-571-8792-8115

中国 - 南京  
Tel: 86-25-8473-2460

中国 - 青岛  
Tel: 86-532-8502-7355

中国 - 上海  
Tel: 86-21-3326-8000

中国 - 沈阳  
Tel: 86-24-2334-2829

中国 - 深圳  
Tel: 86-755-8864-2200

中国 - 苏州  
Tel: 86-186-6233-1526

中国 - 武汉  
Tel: 86-27-5980-5300

中国 - 西安  
Tel: 86-29-8833-7252

中国 - 厦门  
Tel: 86-592-238-8138

中国 - 香港特别行政区  
Tel: 852-2943-5100

中国 - 珠海  
Tel: 86-756-321-0040

台湾地区 - 高雄  
Tel: 886-7-213-7830

台湾地区 - 台北  
Tel: 886-2-2508-8600

台湾地区 - 新竹  
Tel: 886-3-577-8366

### 亚太地区

澳大利亚 **Australia - Sydney**  
Tel: 61-2-9868-6733

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

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

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

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

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

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

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

马来西亚  
**Malaysia - Kuala Lumpur**  
Tel: 60-3-7651-7906

马来西亚 **Malaysia - Penang**  
Tel: 60-4-227-8870

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

新加坡 **Singapore**  
Tel: 65-6334-8870

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

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

### 欧洲

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

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

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

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

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

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

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

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

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

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

以色列 **Israel - Ra'anana**  
Tel: 972-9-744-7705

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

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

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

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

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

罗马尼亚  
**Romania - Bucharest**  
Tel: 40-21-407-87-50

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

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

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

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