DT100104

ATECC608A可信开发板用户指南

简介

ATECC608A可信开发板是一款附加板，可用于 CryptoAuth可信平台和其他包含 MikroElektronika mikroBUS™连接器的 Microchip 开发平台。该开发板可与任何具有主机 mikroBUS 连接的电路板相连。该开发板为需要插座基板执行初始开发和测试的示例设备提供了替代方案。

ATECC608A可信开发板包含 ATECC608A-TNGTLS（Trust&GO）、ATECC608A-TFLXTLS（TrustFLEX）和 ATECC608A-MAHDA（TrustCUSTOM）安全元件。用户可根据应用需求，从这些器件中选择任何一款器件来开发解决方案。本用户指南简要介绍可在该开发板上实现的连接和开关设置。

图 1.正面

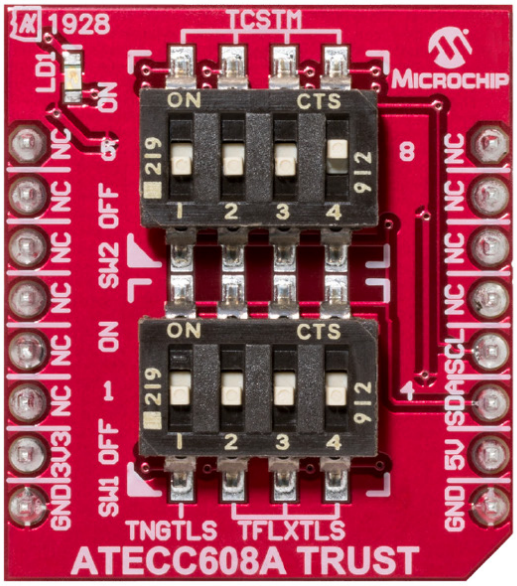
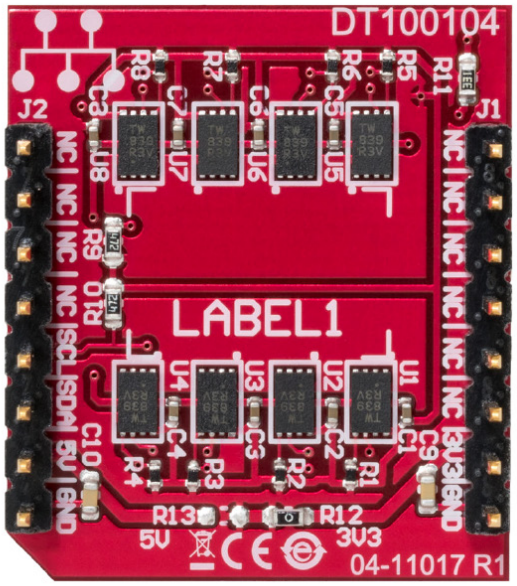


图 2.反面



目录

简介 1

1. 硬件说明 3
   1.1 原理图与关键特性 3
   1.2 器件选择 3
   1.3 硬件文档 4

2. 连接开发板 6
   2.1 CryptoAuth可信平台连接 6
   2.2 Xplained Pro 连接 7

3. 文档版本历史 9

Microchip 网站 10

产品变更通知服务 10

客户支持 10

Microchip 器件代码保护功能 10

法律声明 10

商标 11

质量管理体系 11

全球销售及服务网点 12

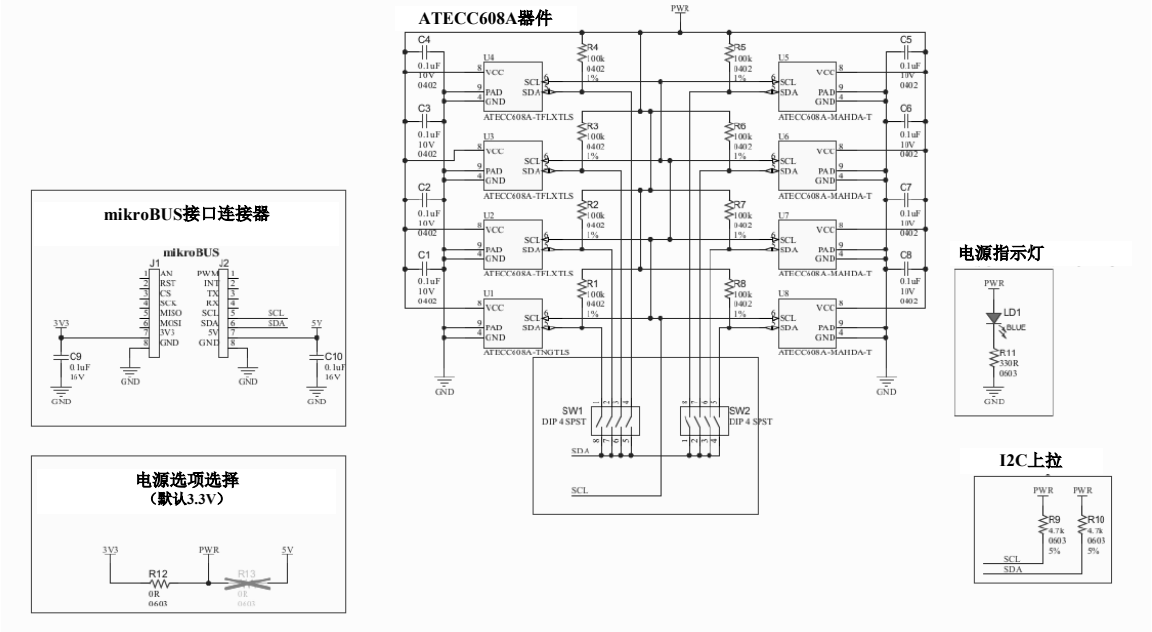
1. 硬件说明

1.1 原理图与关键特性

- 一个 ATECC608A-TNGTLS Trust&GO 器件（U1）
- 三个 ATECC608A-TFLXTLS 原型 TrustFLEX 器件（U2、U3 和 U4）
- 四个 ATECC608A-MAHDA TrustCUSTOM 器件（U5、U6、U7 和 U8）
- 两个用于器件选择的 4 位置 SPST DIP 开关（SW1 和 SW2）
- 一个 mikroBUS 连接器（J1 和 J2）
- 板载 4.7k I^2C 上拉电阻（R9 和 R10）
- 板载 LED 电源指示灯（LD1）
- 零欧姆电阻跳线，用于选择 3.3V 或 5V 电源（通过 R12 默认使能 3.3V）

  注：如需使能 5V 电源，请移除 R12 并在 R11 中焊接一个零欧姆电阻。

图 1-1.ATECC608A可信开发板原理图



1.2 器件选择

器件硬件选择

每个安全元件都有一个开关连接，用户可通过开关连接选择给定的器件。将 DIP 开关滑动至 ON（开启）状态以使能器件选择。进行器件选择，然后通过 DIP 开关即可连接相应的 SDA 线。所有八个器件的 SCL 信号连接在一起。每个器件的 SDA 线上都有一个大数值上拉电阻，使得器件在未选择时处于低电流状态。请注意，电路板顶部显示的开关编号*（不是开关上的数字）*与电路板背面的器件标识符 U＃相对应。

图 1-2.器件选择

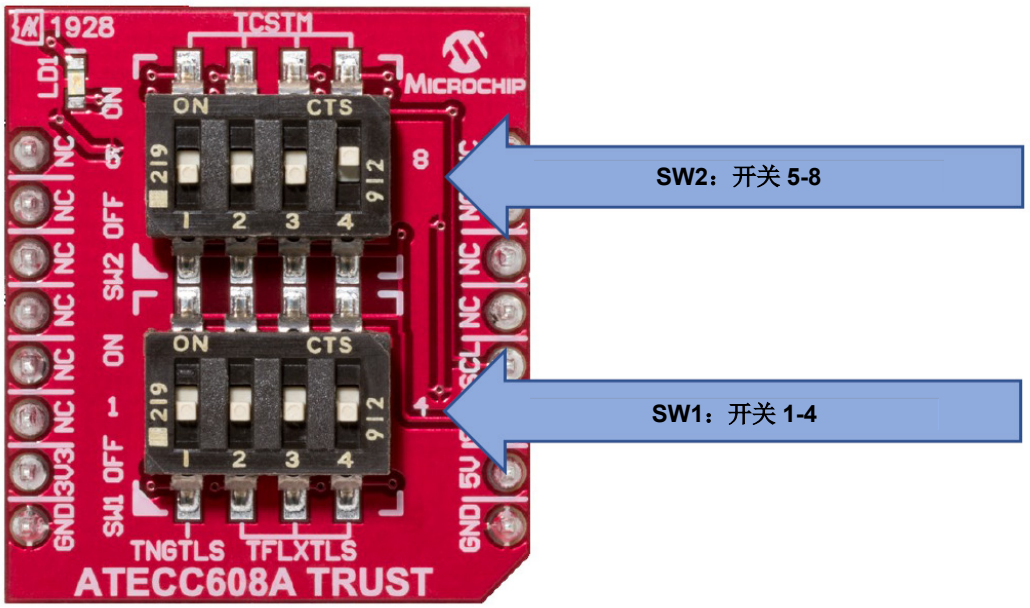


表 1-1.器件选择开关

开关#	DIP 开关	安全元件	可信元件类型
SW1	1	ATECC608A-TNGTLS	Trust&GO
	2，3，4	ATECC608A-TFLXTLS	TrustFLEX
SW2	5，6，7，8	ATECC608A-MAHDA	TrustCUSTOM

器件软件选择

一旦选择了特定器件，就必须使用特定的 I^2C 地址来寻址给定的器件类型。虽然每个器件最初编程时都有一个默认的 I^2C 地址，但可以覆盖该地址。更多信息请参见特定器件的数据手册。

表 1-2.默认 I^2C 地址

器件	默认 7 位 I^2C 地址	8 位已编程 I^2C 地址值[(1)]
ATECC608A-TNGTLS	0x35	0x6A
ATECC608A-TFLXTLS	0x36	0x6C
ATECC608A-MAHDA	0x60	0xC0

注：

1. 这是编程到 ATECC608A 器件中的 I2C_Address 字节值。

请注意，如果多个器件具有不同的 I^2C 地址，则可以使能多个器件。如果选择了具有相同地址的多个器件，则会由于 I^2C 总线冲突而发生故障。

1.3 硬件文档

该工具包的其他文档可在 Microchip 网站的 ATECC608A可信（DT100104）开发工具包中找到。

包括：

1. 电路板设计文档，包括原理图/3D 视图。
2. Gerber 文件。
3. ATECC608A 可信开发板用户指南。

2. 连接开发板

选择 ATECC608A可信开发板外形尺寸的原因是 Microchip 已经在主机板上大量采用了 mikroBUS 连接器。Microchip的许多开发平台将支持一个或多个 mikroBus 接口。包括：

- Microchip Explorer 16/32 开发板
- MPLAB® Xpress 评估板
- 汽车联网开发板
- PIC® Curiosity 板
- PIC Curiosity Nano 板
- AVR® Curiosity Nano 板

2.1 CryptoAuth可信平台连接

ATECC608A可 信 开发板通过 mikroBUS 连接器提供 I^2C 连接，使其能够连接至 可信平台上的 mikroBUS 主机连接器，或具有 mikroBUS 连接器的任何 PIC/AVR/SAM MCU 主机开发板。

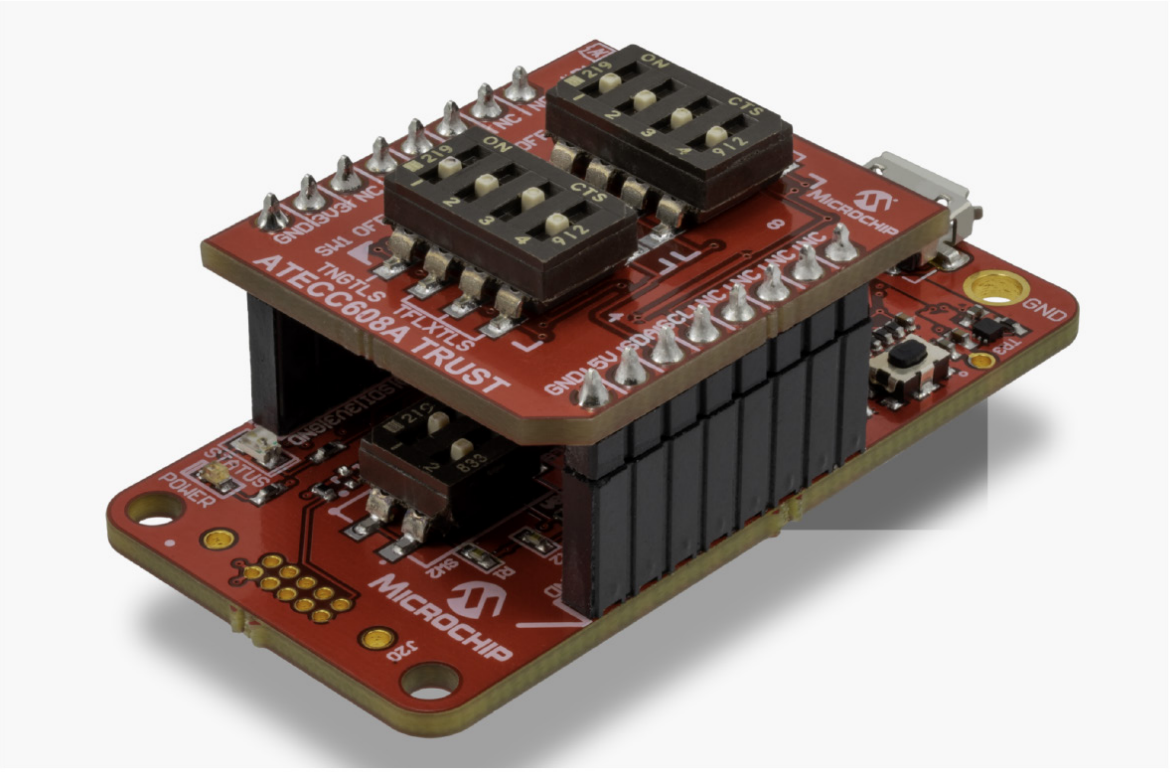
将 ATECC608A 可信开发板连接到 CryptoAuth可信平台

1. 通过设置 CryptoAuth可信平台上的开关，可使能 mikroBUS 连接器和禁用板载器件。此设置以粗体加斜体突出显示如下：

开关设置		使能对象	
SW2_1	**SW2_2**	**mikroBUS™连接器**	**板上器件**
开启	开启	是	是
关闭	开启	否	是
开启	***关闭***	***是***	***否***
关闭	关闭	否	否

2. 两块板的连接如图 2-1 所示。

图 2-1. ATECC608A可信连接至 CryptoAuth可信平台开发板



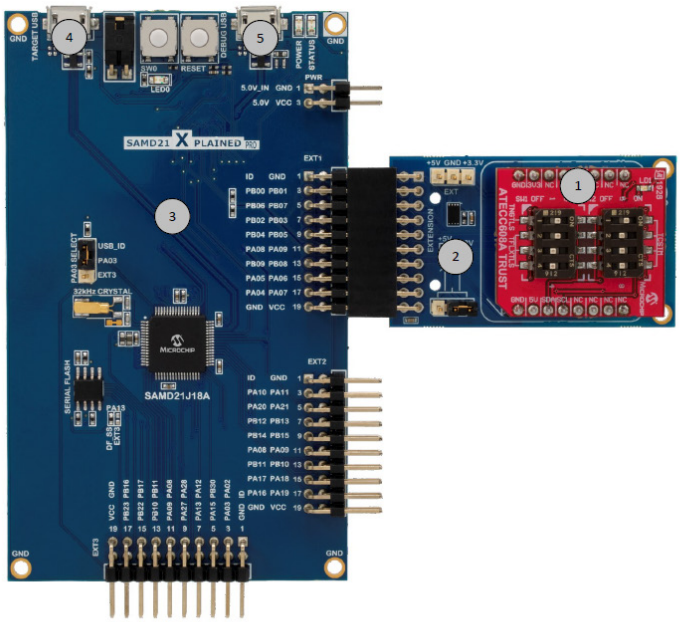
注意：ATECC608A可信开发板上的斜角切口必须与丝印上 mikroBUS 连接器附近的斜线对齐。

3. 选择想要通过 ATECC608A可信开发板上所示的 DIP 开关与主机相连的器件。开关 3 开启，所有其他开关均关闭。这将选择一个 ATECC608A-TFLXTLS 器件。
4. 在开发软件的主机系统上的 CryptoAuth可信平台之间连接一根 USB 线缆。
5. 为给定的应用或正在开发的用例调用软件工具。

2.2 Xplained Pro 连接

某些 Microchip 开发板仅支持 Xplained Pro 扩展接头。通过使用适配器板，仍可以使用 ATECC608A可信开发板。图 2-2 显示了 ATECC608A可信开发板、ATMBUSADAPTER-XPRO 和 ATSAMD21-XPRO 开发板的完整组装。

图 2-2. 与 Xplained Pro 开发平台的连接



1. ATECC608A可信开发板
2. ATMBUSADAPTER-XPRO
3. ATSAMD21-XPRO 开发板
4. 目标 USB 端口
5. 调试 USB 端口

如何将 ATECC608A可信开发板连接至 Xplained Pro 主机板

1. 将 ATMBUSADAPTER 连接到 ATECC608A可信开发板（如图 2-2 所示）。
2. 将 ATMBUSADAPTER 和 ATECC608A可信开发板的组合连接至主机板上的 XPRO 扩展接头之一。图 2-2 中使用了 EXT1。
3. 设置 ATECC608A可信开发板上的一个或多个开关，以使能需要连接的器件。
   注：开关设置（如图所示）可以使能 ATECC608A-TNGTLS、ATECC608A-TFLXTLS 和 ATECC608A-MAHDA TrustCUSTOM 中的每一个器件。这是合法的，因为所有选定器件的 I^2C 地址都是唯一的。通常，只会选择一个器件。
4. 将 USB 电缆连接到目标 USB 端口和调试 USB 端口以及主机系统。
5. 为应用调用适当的软件开发工具。

3. 文档版本历史

版本 A（2019 年 9 月）

- 本文档的初始版本

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。我们的网站提供以下内容：

- **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设计合作伙伴计划成员名单
- **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

产品变更通知服务

Microchip 的产品变更通知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，请访问 http://www.microchip.com/pcn，然后按照注册说明进行操作。

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（ESE）
- 技术支持

客户应联系其代理商、代表或 ESE 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www.microchip.com/support网站获得技术支持。

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

提供本文档的中文版本仅为了便于理解。请勿忽视文档中包含的英文部分，因为其中提供了有关 Microchip 产品性能和使用情况的有用信息。Microchip Technology Inc.及其分公司和相关公司、各级主管与员工及事务代理机构对译文中可能存在的任何差错不承担任何责任。建议参考 Microchip Technology Inc.的英文原版文档。

本出版物中提供的信息仅仅是为方便您使用 Microchip 产品或使用这些产品来进行设计。本出版物中所述的器件应用信息及其他类似内容仅为您提供便利，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 按原样 提供这些信息。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，包括但不限于针对非侵权性、适销性和特定用途的适用性的暗示担保，或针对其使用情况、质量或性能的担保。

在任何情况下，对于因这些信息或使用这些信息而产生的任何间接的、特殊的、惩罚性的、偶然的或间接的损失、损害或任何类型的开销，MICROCHIP 概不承担任何责任，即使 MICROCHIP 已被告知可能发生损害或损害可以预见。在法律允许的最大范围内，对于因这些信息或使用这些信息而产生的所有索赔，MICROCHIP 在任何情况下所承担的全部责任均不超出您为获得这些信息向 MICROCHIP 直接支付的金额（如有）。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损害、索赔、诉讼或费用时，会维护和保障 Microchip 免于承担法律责任。除非另外声明，在 Microchip 知识产权保护下，不得暗中或以其他方式转让任何许可证。

商标

Microchip 的名称和徽标组合、Microchip 徽标、Adaptec、AnyRate、AVR、AVR 徽标、AVR Freaks、BesTime、BitCloud、chipKIT、chipKIT 徽标、CryptoMemory、CryptoRF、dsPIC、FlashFlex、flexPWR、HELDO、IGLOO、JukeBlox、KeeLoq、Kleer、LANCheck、LinkMD、maXStylus、maXTouch、MediaLB、megaAVR、Microsemi、Microsemi 徽标、MOST、MOST 徽标、MPLAB、OptoLyzer、PackeTime、PIC、picoPower、PICSTART、PIC32 徽标、PolarFire、Prochip Designer、QTouch、SAM-BA、SenGenuity、SpyNIC、SST、SST 徽标、SuperFlash、Symmetricom、SyncServer、Tachyon、TempTrackr、TimeSource、tinyAVR、UNI/O、Vectron 和 XMEGA 均为 Microchip Technology Incorporated 在美国和其他国家或地区的注册商标。

APT、ClockWorks、The Embedded Control Solutions Company、EtherSynch、FlashTec、Hyper Speed Control、HyperLight Load、IntelliMOS、Libero、motorBench、mTouch、Powermite 3、Precision Edge、ProASIC、ProASIC Plus、ProASIC Plus 徽标、Quiet-Wire、SmartFusion、SyncWorld、Temux、TimeCesium、TimeHub、TimePictra、TimeProvider、Vite、WinPath 和 ZL 均为 Microchip Technology Incorporated 在美国的注册商标。

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、BlueSky、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、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 Incorporated 在美国和其他国家或地区的商标。

SQTP 是 Microchip Technology Incorporated 在美国的服务标记。

Adaptec 徽标、Frequency on Demand、Silicon Storage Technology 和 Symmcom 为 Microchip Technology Inc.在其他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。

© 2020，Microchip Technology Inc. 版权所有。

ISBN：978-1-5224-7316-9

质量管理体系

有关 Microchip 质量管理体系的信息，请访问 http://www.microchip.com/quality。

全球销售及服务网点

美洲	亚太地区	亚太地区	欧洲
公司总部 2355 West Chandler Blvd. Chandler, AZ 85224-6199 电话：480-792-7200 传真：480-792-7277 技术支持： http://www.microchip.com/support 网址： http://www.microchip.com **亚特兰大** 德卢斯，佐治亚州 电话：678-957-9614 传真：678-957-1455 **奥斯汀，德克萨斯州** 电话：512-257-3370 **波士顿** 韦斯特伯鲁，马萨诸塞州 电话：774-760-0087 传真：774-760-0088 **芝加哥** 艾塔斯卡，伊利诺伊州 电话：630-285-0071 传真：630-285-0075 **达拉斯** 阿迪森，德克萨斯州 电话：972-818-7423 传真：972-818-2924 **底特律** 诺维，密歇根州 电话：248-848-4000 **休斯敦，德克萨斯州** 电话：281-894-5983 **印第安纳波利斯** 诺布尔斯维尔，印第安纳州 电话：317-773-8323 传真：317-773-5453 电话：317-536-2380 **洛杉矶** 米慎维荷，加利福尼亚州 电话：949-462-9523 传真：949-462-9608 电话：951-273-7800 **罗利，北卡罗来纳州** 电话：919-844-7510 **纽约，纽约州** 电话：631-435-6000 **圣何塞，加利福尼亚州** 电话：408-735-9110 电话：408-436-4270 **加拿大 - 多伦多** 电话：905-695-1980 传真：905-695-2078	**澳大利亚 - 悉尼** 电话：61-2-9868-6733 **中国 - 北京** 电话：86-10-8569-7000 **中国 - 成都** 电话：86-28-8665-5511 **中国 - 重庆** 电话：86-23-8980-9588 **中国 - 东莞** 电话：86-769-8702-9880 **中国 - 广州** 电话：86-20-8755-8029 **中国 - 杭州** 电话：86-571-8792-8115 **中国 - 香港特别行政区** 电话：852-2943-5100 **中国 - 南京** 电话：86-25-8473-2460 **中国 - 青岛** 电话：86-532-8502-7355 **中国 - 上海** 电话：86-21-3326-8000 **中国 - 沈阳** 电话：86-24-2334-2829 **中国 - 深圳** 电话：86-755-8864-2200 **中国 - 苏州** 电话：86-186-6233-1526 **中国 - 武汉** 电话：86-27-5980-5300 **中国 - 西安** 电话：86-29-8833-7252 **中国 - 厦门** 电话：86-592-2388138 **中国 - 珠海** 电话：86-756-3210040	**印度 - 班加罗尔** 电话：91-80-3090-4444 **印度 - 新德里** 电话：91-11-4160-8631 **印度 - 浦那** 电话：91-20-4121-0141 **日本 - 大阪** 电话：81-6-6152-7160 **日本 - 东京** 电话：81-3-6880-3770 **韩国 - 大邱** 电话：82-53-744-4301 **韩国 - 首尔** 电话：82-2-554-7200 **马来西亚 - 吉隆坡** 电话：60-3-7651-7906 **马来西亚 - 槟榔屿** 电话：60-4-227-8870 **菲律宾 - 马尼拉** 电话：63-2-634-9065 **新加坡** 电话：65-6334-8870 **台湾地区 -新竹** 电话：886-3-577-8366 **台湾地区 -高雄** 电话：886-7-213-7830 **台湾地区 -台北** 电话：886-2-2508-8600 **泰国 - 曼谷** 电话：66-2-694-1351 **越南 - 胡志明市** 电话：84-28-5448-2100	**奥地利 - 韦尔斯** 电话：43-7242-2244-39 传真：43-7242-2244-393 **丹麦 - 哥本哈根** 电话：45-4450-2828 传真：45-4485-2829 **芬兰 - 埃斯波** 电话：358-9-4520-820 **法国 - 巴黎** 电话：33-1-69-53-63-20 传真：33-1-69-30-90-79 **德国 - 加兴** 电话：49-8931-9700 **德国 - 哈恩** 电话：49-2129-3766400 **德国 - 海尔布隆** 电话：49-7131-72400 **德国 - 卡尔斯鲁厄** 电话：49-721-625370 **德国 - 慕尼黑** 电话：49-89-627-144-0 传真：49-89-627-144-44 **德国 - 罗森海姆** 电话：49-8031-354-560 **以色列 - 若那那市** 电话：972-9-744-7705 **意大利 - 米兰** 电话：39-0331-742611 传真：39-0331-466781 **意大利 - 帕多瓦** 电话：39-049-7625286 **荷兰 - 德卢内市** 电话：31-416-690399 传真：31-416-690340 **挪威 - 特隆赫姆** 电话：47-72884388 **波兰 - 华沙** 电话：48-22-3325737 **罗马尼亚 - 布加勒斯特** 电话：40-21-407-87-50 **西班牙 - 马德里** 电话：34-91-708-08-90 传真：34-91-708-08-91 **瑞典 - 哥德堡** 电话：46-31-704-60-40 **瑞典 - 斯德哥尔摩** 电话：46-8-5090-4654 **英国 - 沃金厄姆** 电话：44-118-921-5800 传真：44-118-921-5820