
CryptoAuth可信平台用户指南

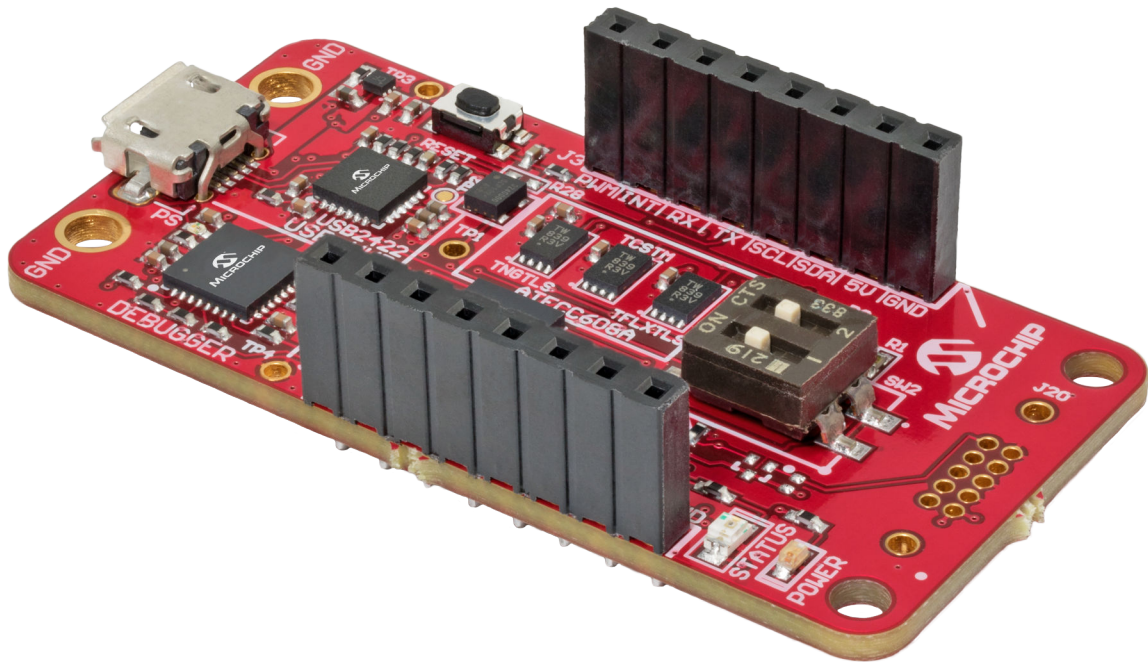
简介

Microchip CryptoAuth 可信平台是 CryptoAuthentication™ 评估工具包的最新成员。通过预置备的 ATECC608A Trust&GO、预配置的 TrustFLEX 以及完全可定制的 TrustCUSTOM 产品，该工具包可用于探索和开发物联网领域解决方案。

Trust&GO 和 TrustFLEX 产品旨在简便地为物联网云解决方案添加硬件安全功能。将该工具包与 Microchip 开发工具和经配置的系统搭配使用，就能帮助项目量较小的客户轻松地在其应用中实施安全身份验证。

本用户指南简要介绍与 CryptoAuth 可信平台开发工具包相关的连接、元件和功能。

图 1. CryptoAuth 可信平台



目录

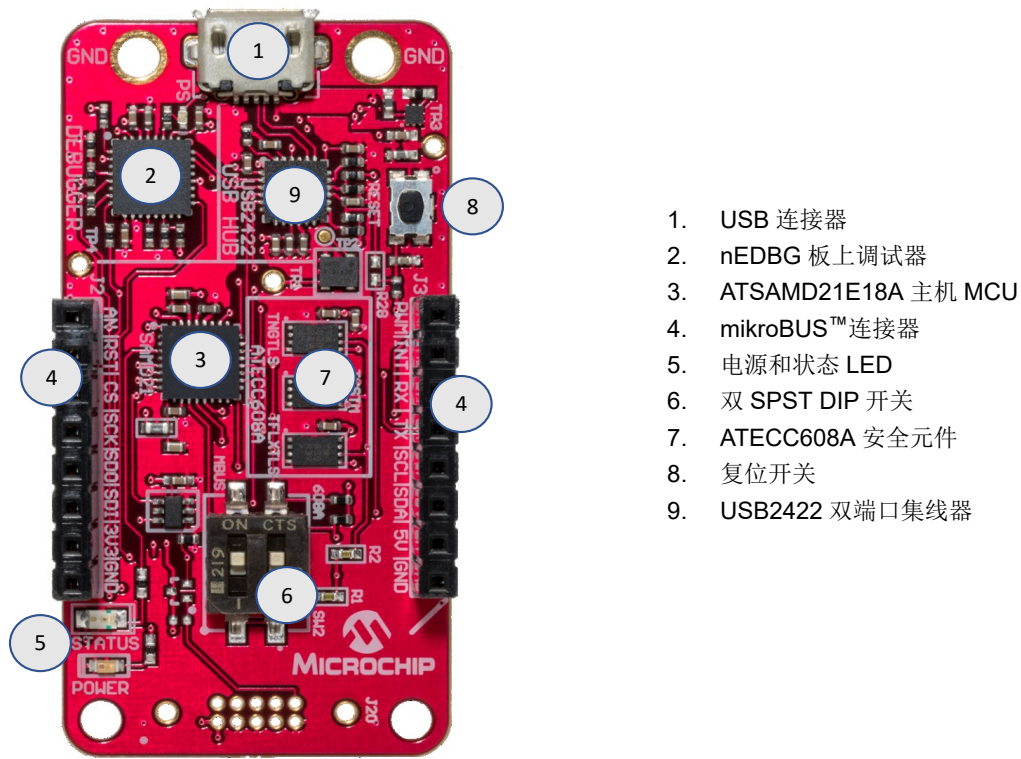
简介.....	1
1. 硬件概述.....	3
1.1. 工具包订购代码和组件.....	3
1.2. 功能说明.....	4
1.3. 硬件文档.....	5
2. mikroBUS™和 Click 附加板.....	6
3. 软件要求.....	7
3.1. 软件应用开发.....	7
3.2. 固件升级.....	7
4. 文档版本历史.....	9
Microchip 网站.....	10
产品变更通知服务.....	10
客户支持.....	10
Microchip 器件代码保护功能.....	10
法律声明.....	10
商标.....	11
质量管理体系.....	11
全球销售及服务网点.....	12

1. 硬件概述

CryptoAuth 可信平台由配置为主 MCU 的 Microchip SAM D21 单片机组成。出厂时就通过 Microchip 安全产品部 (Secure Products Group, SPG) 工具包协议进行了预编程。该协议用于通过 USB HID 接口在 CryptoAuthentication 器件和主机 MCU 之间进行通信。安全元件和主机 MCU 之间的数据传输由状态 LED 指示。

可信平台包含三个安全元件：ATECC608A-TNGTLS (Trust&GO)、ATECC608A-TFLXTLS 原型 (TrustFLEX) 和 ATECC608A-MAHDA (TrustCUSTOM)。每个安全元件都有一个不同的 I²C 地址，以使其能够与主机 MCU 进行通信，从而消除了线路争用的问题。

图 1-1. CryptoAuth 可信平台电路板元件



1. USB 连接器
2. nEDBG 板上调试器
3. ATSAM D21E18A 主机 MCU
4. mikroBUS™ 连接器
5. 电源和状态 LED
6. 双 SPST DIP 开关
7. ATECC608A 安全元件
8. 复位开关
9. USB2422 双端口集线器

1.1 工具包订购代码和组件

订购信息

工具包名称: [CryptoAuth 可信平台开发工具包](#)

订购代码: DM320118

供货情况: 该工具包可从 Microchip 直销网站和多家代理商处购买。

CryptoAuth 可信平台工具包的内容和要求

CryptoAuth 可信平台工具包包含:

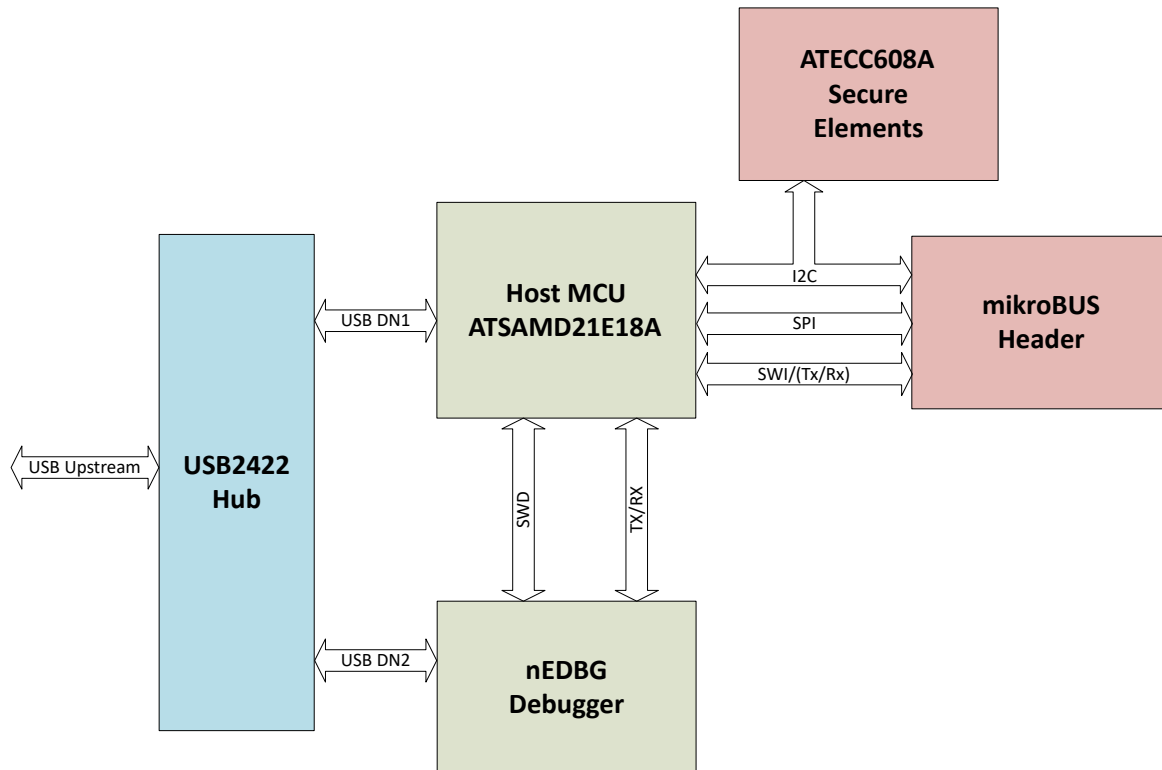
- CryptoAuth 可信平台电路板

要操作该板，需要 micro USB 电缆（未包括）。

1.2 功能说明

图 1-2 中的框图说明了 CryptoAuth 可信平台的主要连接。有关更多详细信息，请参见本文档的 1.3 硬件文档章节中引用的电路板原理图。

图 1-2 框图



主要板上元件

- **ATSAMD21:** Microchip SAM D21 是基于 ARM® Cortex M0+ 的单片机。MCU 通过 I²C 连接到三个安全元件。mikroBUS 连接器通过 I²C、SPI、UART、GPIO 和模拟连接方式连接到单片机。这样就可以将 CryptoAuth 可信平台与各类 MikroElektronika Click boards™ 配合使用。
- **安全元件:** 可信平台由三个基于 ATECC608A 的 IC 组成，如下表所示。有关更多详细信息，请参见与每个器件相关的特定数据手册。

器件	默认 7 位 I ² C 地址	8 位已编程 I ² C 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。

- **mikroBUS 连接器：**mikroBUS 连接器是所有 MikroElektronika 板的预定义连接器。这使用户可以将各类 Click 传感器和附加板连接到可信平台。可信平台通过 SPI、I²C、UART、GPIO 和模拟连接方式连接到主机单片机。
- **DIP 开关：**该开关用于在板上 ATECC608A 可信平台器件和 mikroBUS 连接器之间进行选择。开关会断开 I²C 接口的 SDA 线，以防止在两个 I²C 地址相同的情况下发生冲突。如果所有 I²C 地址在连接到该板上的所有器件上都是唯一的，则可以使能这两个开关。

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	无	是
开启	关闭	是	无
关闭	关闭	无	无

- **nEDBG 调试器：**调试器用于对主机 MCU 进行编程和烧写。还可以通过调试器接口从主机 MCU 读回调试信息。当插入系统并使用 MPLAB® X IDE 打开时，将显示 nEDBG 调试器，其序列号为 MCHP3311xxxxxxxxxxxxxx。
- **USB 集线器：**Microchip USB2422 是一款双端口 USB 集线器。集线器将在上游端口和下游器件之间传递数据。下游器件是调试器和主机 MCU。

1.3 硬件文档

该工具包的其他文档可在 Microchip 网站的 [DM320118](#) 中找到。

包括：

1. 电路板设计文档，包括原理图和 3D 视图
2. Gerber 文件
3. CryptoAuth 可信平台（DM320118）用户指南
4. 可信平台设计套件工具

2. mikroBUS™ 和 Click 附加板

mikroBUS 连接器的外形已经成为实际的行业标准附加板基准。CryptoAuth 可信平台板具有单个 mikroBUS 主机连接器。此功能可以极大地扩展该板在开发和原型设计新应用时的实用性。除非另有说明，否则表 2-1 中列出的所有板均由 MikroElektronika 开发。

表 2-1. mikroBUS 附加板

板名称	支持的器件	制造商	说明
ATECC608A DT100104 ⁽¹⁾	ATECC608A-TNGTLS ATECC608A-TFLXTLS ATECC608A-MAHDA	Microchip	ATECC608A Trust 板提供用于进行开发的其他示例设备。该板是使用插座板的替代方案。可以使用板上 DIP 开关分别选择每个器件。
Secure UDFN click	所有 Microchip CryptoAuthentication™ 器件	MikroElektronika	Secure UDFN Click boards™ 是 8 引脚 UDFN 插座解决方案，用于配置和置备 CryptoAuthentication™ 器件。这些器件可用于安装到早期的原型或生产板上。
Secure SOIC click	所有 Microchip CryptoAuthentication 器 件	MikroElektronika	Secure SOIC click 板是 8 引脚 SOIC 插座解决方案，用于配置和置备 CryptoAuthentication 器件。这些器件可用于安装到早期的原型或生产板上。
WiFi 7 click	ATWINC1510	MikroElektronika	使用 ATWINC510 的 Wi-Fi® 模块。该板支持 IEEE® 802.11 b/g/n 协议和通过 SPI 接口进行通信。
Secure 4 click	ATECC608A	MikroElektronika	配备带 I²C 接口的通用 ATECC608A 安全元件。该器件与 CryptoAuth 可信平台板上安装的 ATECC608A TrustCustom 器件相同。
Secure click	ATECC508A	MikroElektronika	配备带 I²C 接口的通用 ATECC508A 安全元件。
Secure 3 click	ATSHA204A	MikroElektronika	配备带 I²C 接口的通用 ATSHA204A 安全元件。该器件配备采用基于硬件的对称安全密钥存储的密码协处理器。
Secure 6 click	ATSHA204A	MikroElektronika	配备带 SWI 接口的通用 ATSHA204A 安全元件。该器件配备采用基于硬件的对称安全密钥存储的密码协处理器。
Secure 2 Click	ATAES132A	MikroElektronika	配备带 I²C 接口的通用 ATAES132A 安全元件。ATAES132A 是一个 32K 串行 EEPROM，可以配置为安全存储器件。
mikroBUS Shuttle	Click 扩展板	MikroElektronika	mikroBUS Shuttle 是一种微型附加板，可用于将 mikroBUS 扩展到多个 mikroBUS 连接器。
Shuttle Click	Click 扩展板	MikroElektronika	Shuttle Click 是一种插座扩展板，可以井然有序地堆叠多达四个 Click 板。

注：

1. 由 Microchip 制造。

3. 软件要求

CryptoAuth 可信平台可通过多种方式使用。包括：

1. 作为开发工具，与用例工具的 **Microchip** 可信平台设计套件配合使用。
2. 作为 **Microchip** 预定义应用的开发和演示平台。
3. 作为开发自己应用的开发平台，使用 **Microchip** 基于 Python 或者 C 的工具。

CryptoAuth 可信平台支持多种软件工具。

3.1 软件应用开发

以下工具适用于开发或修改应用。

可信平台设计套件

用例工具的 **Microchip 可信平台设计套件** 基于 Jupyter Notebook 和 Python 程序，帮助开发人员快速定义和开发面向可信平台产品的应用。

Microchip 可信平台设计套件能够实现与板上 ATECC608A CryptoAuthentication 器件或通过 mikroBUS 连接器连接的 CryptoAuthentication 器件进行互操作。该工具易于从可用的器件选项中进行选择，并生成设备所需的必要配置文件。该工具还可用于使用 **CryptoAuth** 可信平台开发应用。

MPLAB®X IDE

MPLAB X 是在 Windows®、macOS®和 Linux®环境中工作的集成开发环境（Integrated Development Environment, IDE）。该工具可用于使用板上 SAM D21 单片机开发新的嵌入式应用。该工具将自动使用板上 nEDBG 调试器对 SAM D21 单片机进行编程。调试器还可用于通过 COM 端口将调试信息从主机单片机传回终端窗口。

Atmel Studio 7

Atmel Studio 7 是在 Windows®环境中工作的集成开发环境（IDE）。该工具可用于使用板上 SAM D21 单片机开发新的嵌入式应用。该工具将自动使用板上 nEDBG 调试器对 SAM D21 单片机进行编程。调试器还可用于通过 COM 端口将调试信息从主机单片机传回终端窗口。

CryptoAuthLib

CryptoAuthLib 旨在让使用 **Microchip** CryptoAuthentication 器件变得简单直接。CryptoAuthLib 设计了硬件抽象层（Hardware Abstraction Layer, HAL），使其易于扩展到其他单片机。同时提供该库的 C 和 Python 版本。该库的 Python 版本由 **Microchip** 维护，可通过 Python Package Index 网站（pypi.org）获取。最新版本的 CryptoAuthLib 可以在 **Microchip** 的 GitHub 网站上找到。

- [CryptoAuthLib-Python](#)
- [CryptoAuthLib-GitHub](#)

3.2 固件升级

带来新功能或增强功能的 **CryptoAuth** 可信平台新固件将会定期提供。此外，**Microchip** 开发的特定应用程序也可用于该开发板。固件的最新版本和有关其他应用程序的信息可在 **DM320118** 产品页面上找到。

现有两种 **Microchip** 工具可用于升级 **CryptoAuth** 可信平台开发工具包的固件。使用这两种工具可通过标准方式完成固件升级，在此不再赘述。这两个选项都使用 nEDBG 板上调试器。这些选项是：

- **MPLAB X IPE**（集成编程环境）——该工具作为 **MPLAB X IDE** 下载的一部分提供。
- **Atmel Studio 7**——集成设计环境。



注： 建议升级到最新的工具版本。该工具的旧版本可能无法识别 nEDBG 调试器或特定的工具包信息。

4. 文档版本历史

版本 A（2019 年 9 月）

- 本用户指南的初始版本。

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**——常见问题解答 (FAQ)、技术支持请求、在线讨论组以及 Microchip 设计伙伴计划成员名单
- **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 <http://www.microchip.com/support> 获得网上技术支持。

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。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 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、PackerTime、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 及 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 为 Microchip Technology Incorporated 在美国的服务标记。

Adaptec 徽标、Frequency on Demand、Silicon Storage Technology 和 Symmcom 均为 Microchip Technology Inc. 在除美国外的国家或地区的注册商标。

GestIC 为 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 Incorporated 版权所有。

ISBN: 978-1-5224-5770-1

质量管理体系

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

全球销售及服务中心

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 休斯顿, 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: 86-592-238-8138 中国 - 珠海 电话: 86-756-321-0040	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 - 檳榔嶼 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: 45-4485-5910 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: 47-7288-4388 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

02/28/20