这是文档摘要。签署 NDA 后可获得完整文档。更多信息，请联系当地 Microchip 销售办事处。

ATECC608B

CryptoAuthentication™器件概要数据手册

特性

- 具有基于硬件的安全密钥存储的加密协处理器。
  - 受保护存储，最多可存储 16 个密钥、证书或数据
- 对非对称签名、验证、密钥协议的硬件支持：
  - ECDSA：FIPS186-3 椭圆曲线数字签名
  - ECDH：FIPS SP800-56A 椭圆曲线 Diffie-Hellman
  - NIST 标准 P256 椭圆曲线支持
- 对对称算法的硬件支持：
  - SHA-256 和 HMAC 哈希，包括片外上下文保存/恢复
  - AES-128：加密/解密，适用于 GCM 的 Galois 字段乘法
- 网络密钥管理支持：
  - 适用于 TLS 1.2 和 1.3 的交钥匙 PRF/HKDF 计算
  - SRAM 中的临时密钥生成和密钥协议
  - 密钥完全受保护的小报文加密
- 安全引导支持：
  - 完整的 ECDSA 代码签名验证，可选存储摘要/签名
  - 安全引导前可选择禁止通信密钥
  - 报文加密/身份验证，用以防止板上攻击
- 内部高质量 NIST SP 800-90A/B/C 随机数发生器（Random Number Generator，RNG）
- 两个高耐用性单调计数器
- 唯一的 72 位序列号
- 提供了两个接口选项：
  - 具有一个 GPIO 引脚的高速单线接口
  - 1 MHz 标准 I^2C 接口
- 1.8V 至 5.5V IO 电平，2.0V 至 5.5V 电源电压
- 提供两个温度范围：
  - 标准工业级温度范围：-40℃至+85℃
  - 扩展工业级温度范围：-40℃至+100℃
- <150 nA 的休眠电流
- 封装选项
  - 8 焊盘 UDFN、8 引脚 SOIC 和 3 引脚触点封装选项
  - 适用于符合条件的客户使用的卷带式管芯和 WLCSP 封装（请联系 Microchip 销售人员）

应用

- IoT 网络端点密钥管理和交换
- 小报文和 PII 数据加密
- 安全引导和受保护下载

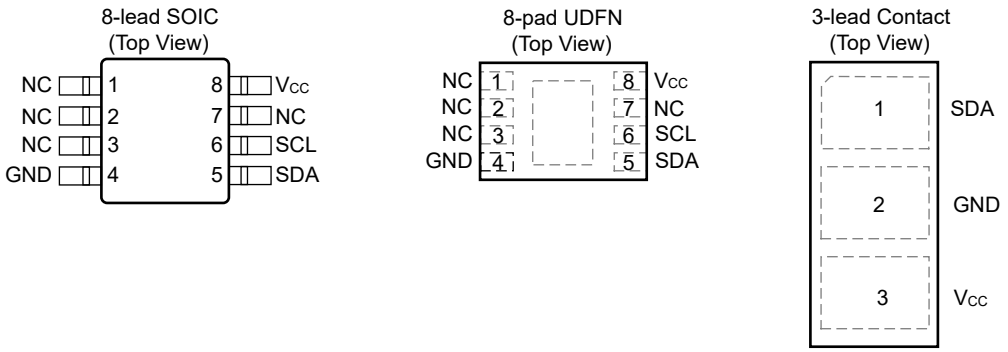
- 生态系统控制和防克隆

引脚配置和引脚排列

表 1. 引脚配置

引脚	I²C 功能接口	SWI 功能接口
NC	未连接	未连接
GND	地	地
SDA	串行数据	串行数据
SCL	串行时钟输入	GPIO
V_{CC}	电源	电源

图 1. 封装类型



注： 建议将 UDFN 背面焊盘连接至 GND。

目录

特性 1

应用 1

1. 简介 4
   - 1.1. 应用 4
   - 1.2. 器件特性 4
   - 1.3. 加密操作 5

引脚配置和引脚排列 2

2. 电气特性 6
   - 2.1. 绝对最大额定值 6
   - 2.2. 可靠性 6
   - 2.3. 交流参数：所有 I/O 接口 6
   - 2.4. 直流参数：所有 I/O 接口 9

3. 兼容性 12
   - 3.1. Microchip ATECC608A 12
   - 3.2. Microchip ATECC508A 12
   - 3.3. Microchip ATSHA204A 和 ATECC108A 13

4. 封装标识信息 14

5. 封装图 15
   - 5.1. 8 引脚 SOIC 15
   - 5.2. 8 焊盘 UDFN 18
   - 5.3. 3 引脚触点式 21

6. 版本历史 23

Microchip 网站 24

产品变更通知服务 24

客户支持 24

产品标识体系 25

Microchip 器件代码保护功能 26

法律声明 26

商标 26

质量管理体系 27

全球销售及服务网点 28

1. 简介

ATECC608B 是 Microchip 高安全性加密器件 CryptoAuthentication™系列的一员，该系列将一流的基于硬件的密钥存储与硬件加密加速器相结合，可实现各种身份验证和加密协议。

ATECC608B 提供比 ATECC608A 更高的安全性，同时还提供完整的向后兼容性。ATECC608A 的所有配置设置、命令、封装和功能在 ATECC608B 中仍旧可以使用，从而可以从 ATECC608A 轻松实现移植。对于新设计，建议客户直接从 ATECC608B 器件开始。对于正在升级且当前使用 ATECC508A 或 ATECC608A 的设计，建议将其移植到 ATECC608B。对于不打算升级的设计，建议客户检查其设计，看看是否能从 ATECC608B 的增强安全性中受益。有关将设计移植到 ATECC608B 的帮助信息，请参见移植参考资料部分。

有关与其他 Microchip CryptoAuthentication 产品兼容性的更多信息，请参见 3. 兼容性部分。

移植参考资料：

1. AN3539：提供有关从 ATECC508A 移植到 ATECC608B 的指导
2. AN2237：提供有关从 ATECC608A 移植到 ATECC608B 的指导

1.1 应用

ATECC608B 具有灵活的命令集，可在许多应用中使用，其中包括：

- **网络/物联网节点端点安全**
  可管理节点身份验证以及会话密钥创建和管理操作。支持多种协议的整个临时会话密钥生成流程，这些协议包括 TLS 1.2（及更早版本）和 TLS 1.3。
- **安全引导**
  可通过验证代码摘要并在成功时选择使能通信密钥来支持 MCU 主机。可通过多种配置提高性能。
- **小报文加密**
  可通过硬件 AES 引擎对小报文或数据（例如 PII 信息）进行加密和/或解密。可直接支持 AES-ECB 模式。可借助主机单片机实施其他模式。可通过其他 GFM 计算功能支持 AES-GCM。
- **为下载的软件生成密钥**
  支持为下载的映像生成本地保护的密钥。支持将一个映像广播到多个具有相同解密密钥的系统，或者为每个系统点对点下载唯一映像。
- **生态系统控制和防伪造**
  验证系统或组件是否为正版且来自铭牌上标示的 OEM。

1.2 器件特性

ATECC608B 包含一个 EEPROM 阵列，可用于存储最多 16 个密钥、证书、其他读/写、只读或机密数据、使用记录和安全配置。可以通过多种方式限制对存储器各个部分的访问，然后可以锁定配置以防止更改。

可通过标准 I^2C 接口访问器件，速度最高可达 1 Mbps。此接口符合标准串行 EEPROM I^2C 接口规范。该器件还支持单线接口（Single-Wire Interface，SWI），可以减少系统处理器所需的 GPIO 数量和/或减少连接器上的引脚数量。如果使能了单线接口，则其余引脚可用作 GPIO、经过身份验证的输出或篡改输入。

每个 ATECC608B 均附带一个确保唯一的 72 位序列号。主机系统或远程服务器可以借助器件支持的加密协议验证此序列号的签名，以证明序列号为正版，而非副本。序列号通常存储在标准串行 EEPROM 中；但是，由于这些内容很容易被复制，主机无法知晓此序列号是正版还是克隆。

ATECC608B 具有多种防御机制，专用于防止对器件本身实施物理攻击，或者对器件和系统之间传输的数据实施逻辑攻击。对使用或生成密钥的方式实施硬件限制，可进一步防御某些类型的攻击。

1.3 加密操作

ATECC608B 可采用椭圆曲线加密和 ECDSA 签名协议实施完整的非对称（公钥/私钥）加密签名解决方案。该器件可对 NIST 标准 P256 主曲线进行硬件加速，并支持从高质量私钥生成到 ECDSA 签名生成、ECDH 密钥协议和 ECDSA 公钥签名验证的完整密钥生命周期。

利用硬件加速器便可实现这种非对称加密操作，与标准单片机上运行的软件相比，其速度快十到上千倍，而不会出现标准单片机通常存在的密钥泄露高风险。

此外，ATECC608B 还可以在硬件中实施 AES-128、SHA256 以及多种 SHA 衍生品，例如 HMAC（SHA）、PRF（TLS 中的密钥派生功能）和 HKDF。为便于 GCM 加密/解密/身份认证，还支持 Galois 字段乘法（又名 Ghash）。

该器件可以安全存储多个私钥及其相关公钥和证书。签名验证命令可以使用任何存储的或外部的 ECC 公钥。可以将存储在器件中的公钥配置为需要通过证书链进行验证，以加快后续器件身份验证速度。

该器件支持在内部随机生成私钥，以确保器件外部永远不会知晓该私钥。生成与存储的私钥对应的公钥后始终会返回该公钥，也可以稍后计算该公钥。

ATECC608B 可通过内部随机数发生器生成高质量的随机数。这一复杂功能需要在运行时执行运行状况测试，用以确保从内部噪声源生成的值在使用时包含足够的熵。随机数发生器的设计符合 NIST 800-90A、800-90B 和 800-90C 文档中规定的要求。

这些随机数可用于任何用途，包括可用作器件加密协议的一部分。由于每个随机数基本上都可确保在该器件或任何其他器件生成的所有数字中是唯一的，因此在协议计算中使用该随机数可确保重放攻击（即重新发送先前成功的事务）始终会失败。

此外，ATECC608B 还支持基于哈希的质询/响应标准协议，以便在多种其他应用中使用。在最基本的实例中，系统将向器件发送一个质询，器件通过 MAC 命令将该质询与密钥组合在一起，然后将响应发送回系统。该器件会使用 SHA-256 加密哈希算法执行该组合，使总线上的观察者无法获取该密钥值。同时，接收方可以使用接收方系统上存储的一份密码副本执行相同计算来验证该响应是否正确。这一对称质询/响应机制可能存在多种形式。

2. 电气特性

2.1 绝对最大额定值

工作温度	-40°C 至+100°C
存储温度	-65°C 至+150°C
最大工作电压	6.0V
直流输出电流	5.0 mA
任何引脚上的电压	-0.5V 至（V_{CC} + 0.5V）
ESD 额定值：	
人体模型（**Human Body Model，HBM**）**ESD**	>4 kV
充电设备模型（**Charge Device Model，CDM**）**ESD**	>1 kV

注： 如果器件的工作条件超过上述“绝对最大额定值”，可能对器件造成永久性损坏。上述值仅代表本规范规定的极限工作条件，不代表器件在上述极限值或超出极限值的情况下仍可正常工作。器件长时间工作在绝对最大额定值条件下，其可靠性可能受到影响。

2.2 可靠性

ATECC608B 采用 Microchip 公司具有极高可靠性的 CMOS EEPROM 制造技术制作。

表 2-1. EEPROM 可靠性

参数	最小值	典型值	最大值	单位
+85°C 下的耐写入次数（每个字节）	400,000	—	—	写周期
数据保持时间（+55°C 时）	10	—	—	年
数据保持时间（+35°C 时）	30	50	—	年
耐读取次数	无限			读周期

2.3 交流参数：所有 I/O 接口

图 2-1. 交流时序图：所有接口

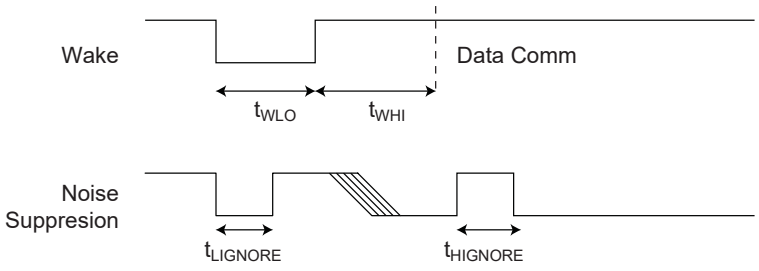


表 2-2. 交流参数：所有 I/O 接口

参数	符号	方向	最小值	典型值	最大值	单位	条件
上电延时（2）	t_{PU}	至加密器件	100	—	—	µs	t_{WLO} 启动前，V_{CC} > V_{CC} 最小值之间的最短时间。
唤醒低电平持续时间	t_{WLO}	至加密器件	60	—	—	µs	
唤醒至数据通信的高延时	t_{WHI}	至加密器件	1500	—	—	µs	除非实施轮询，否则 SDA 应在整个持续时间内保持稳定的高值。上电时不使能 SelfTest。
使能 SelfTest 时唤醒高延迟	t_{WHIST}	至加密器件	20	—	—	ms	除非实施轮询，否则 SDA 应在整个持续时间内保持稳定的高值。
处于工作模式时上桥臂毛刺滤波器	$t_{HIGNORE_A}$	至加密器件	45（1）	—	—	ns	无论处于工作模式时的状态如何，器件都将忽略小于此宽度值的脉冲。
处于工作模式时下桥臂毛刺滤波器	$t_{LIGNORE_A}$	至加密器件	45（1）	—	—	ns	无论处于工作模式时的状态如何，器件都将忽略小于此宽度值的脉冲。
处于休眠模式时下桥臂毛刺滤波器	$t_{LIGNORE_S}$	至加密器件	15（1）	—	—	µs	处于休眠模式时，器件将忽略小于此宽度值的脉冲。
看门狗超时	$t_{WATCHDOG}$	至加密器件	0.7	1.3	1.7	s	Config.ChipMode [2]为 0 时，从唤醒到器件被迫进入休眠模式的时间。

注：

1. 这些参数为特性值，但未经生产测试。
2. 如果在配置区域中使能了上电自检，则上电延时将显著延长。

2.3.1 交流参数：单线接口

图 2-2. 交流时序图：单线接口

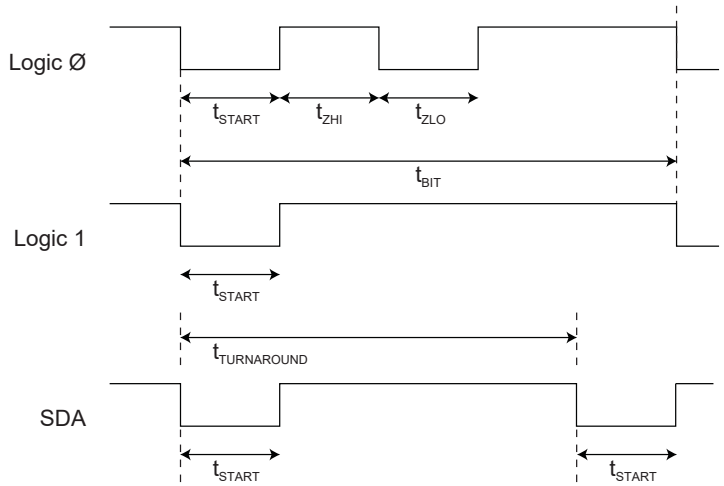


表 2-3. 交流参数：单线接口

除非另外说明，否则适用于以下条件：T_A = -40°C 至+100°C，V_{CC} = +2.0V 至+5.5V，C_L = 100 pF。

参数	符号	方向	最小值	典型值	最大值	单位	条件
启动脉冲持续时间	t_{START}	至加密器件	4.10	4.34	4.56	µs	—
		自加密器件	4.60	6	8.60	µs	—
零传输高脉冲	t_{ZHI}	至加密器件	4.10	4.34	4.56	µs	—
		自加密器件	4.60	6	8.60	µs	—
零传输低脉冲	t_{ZLO}	至加密器件	4.10	4.34	4.56	µs	—
		自加密器件	4.60	6	8.60	µs	—
位时间（1）	t_{BIT}	至加密器件	37	39	—	µs	如果位时间超过 $t_{TIMEOUT}$，ATECC608B 可能会进入休眠模式。
		自加密器件	41	54	78	µs	—
回转延迟	$t_{TURNAROUND}$	自加密器件	64	96	131	µs	ATECC608B 将在发送标志最后一位的启动脉冲初始下降沿之后经过此时间间隔后，启动第一个低电平跳变。
		至加密器件	93	—	—	µs	ATECC608B 发送某个组的最后一位之后，系统必须等待此间隔结束后，才能发送标志的第一位。该间隔从 ATECC608B 发送的最后一位的启动脉冲下降沿开始测量。
IO 超时	$t_{TIMEOUT}$	至加密器件	45	65	85	ms	如果总线处于非工作模式的时间超过此持续时间，则 ATECC608B 可能会转换为休眠模式。

注：

1. t_{START}、t_{ZLO}、t_{ZHI} 和 t_{BIT} 可与发送和接收均以 230.4 kBaud 速度运行的标准 UART 兼容。UART 必须设置为 7 个数据位（无奇偶校验）和一个停止位。

2.3.2 交流参数：I²C 接口

图 2-3. I²C 同步数据时序

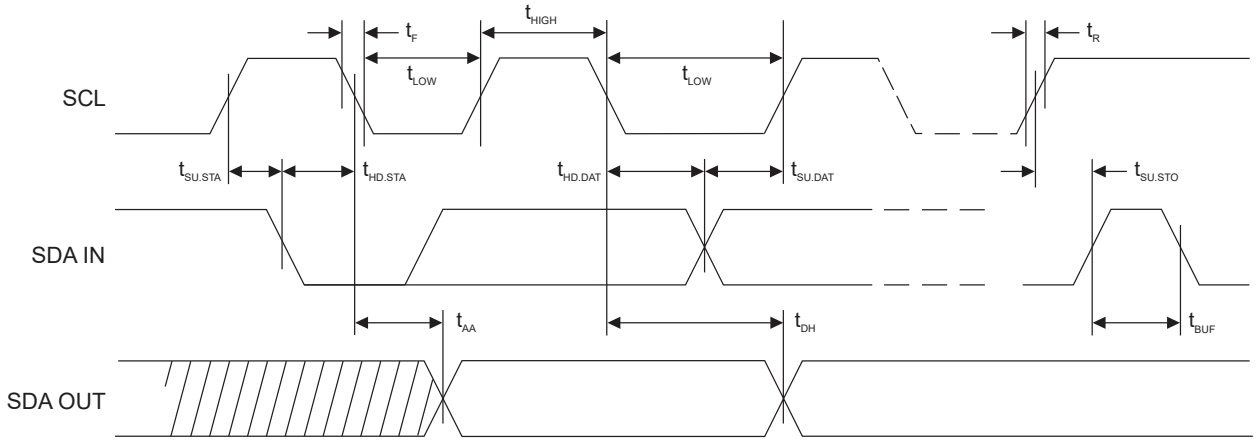


表 2-4. I²C 接口的交流特性（2）

除非另外说明，否则适用于以下建议工作范围：T_A = -40°C 至+100°C，V_{CC} = +2.0V 至+5.5V，C_L = 1 TTL 栅极和 100 pF。

参数	符号	最小值	最大值	单位
SCL 时钟频率	f_{SCL}	0	1	MHz

.....（续）

参数	符号	最小值	最大值	单位
SCL 高电平时间	t_{HIGH}	400	—	ns
SCL 低电平时间	t_{LOW}	400	—	ns
启动建立时间	$t_{SU.STA}$	250	—	ns
启动保持时间	$t_{HD.STA}$	250	—	ns
停止建立时间	$t_{SU.STO}$	250	—	ns
数据输入建立时间	$t_{SU.DAT}$	100	—	ns
数据输入保持时间	$t_{HD.DAT}$	0	—	ns
输入上升时间 [1]	t_R	—	300	ns
输入下降时间 [1]	t_F	—	100	ns
时钟低电平至数据输出有效	t_{AA}	50	550	ns
数据输出保持时间	t_{DH}	50	—	ns
SMBus 超时延时	$t_{TIMEOUT}$	25	75	ms
在开始新的传输前，总线必须保持空闲的时间 [1]	t_{BUF}	500	—	ns

注：

1. 数值基于特性，未经测试。
2. 交流测量条件：
   - R_L（连接 SDA 和 V_{CC}）：1.2 kΩ（V_{CC} = +2.0V 至+5.0V）
   - 输入脉冲电压：0.3V_{CC} 至 0.7V_{CC}
   - 输入上升时间和下降时间：≤ 50 ns
   - 输入和输出时序参考电压：0.5V_{CC}

2.4 直流参数：所有 I/O 接口

表 2-5. 所有 I/O 接口上的直流参数

参数	符号	最小值	典型值	最大值	单位	条件
环境工作温度	T_A	-40	—	+85	°C	标准工业级温度范围
		-40	—	+100	°C	扩展工业级温度范围
电源电压	V_{CC}	2.0	—	5.5	V	—
工作电源电流	I_{CC}	—	2	3	mA	在 I/O 传输或执行非 ECC 命令期间等待 I/O。与时钟分频比值无关。
		—	—	14	mA	在执行 ECC 命令期间。时钟分频比 = 0x0
		—	—	6	mA	在执行 ECC 命令期间。时钟分频比 = 0x5
		—	—	3	mA	在执行 ECC 命令期间。时钟分频比 = 0xD
空闲电源电流	I_{IDLE}	—	800	—	µA	当器件处于空闲模式时，V_{SDA} 和 V_{SCL} < 0.4V 或> V_{CC}-0.4

.....（续）

参数	符号	最小值	典型值	最大值	单位	条件
休眠电流	I_{SLEEP}	—	30	150	nA	当器件处于休眠模式时，$V_{CC} \leq 3.6V$，V_{SDA} 和 $V_{SCL} < 0.4V$ 或 $> V_{CC} - 0.4$，$T_A \leq +55°C$
		—	—	2	µA	当器件处于休眠模式时。 超出全 V_{CC} 和温度范围。
输出低电压	V_{OL}	—	—	0.4	V	当器件处于工作模式时，V_{CC} = 2.5 至 5.5V
输出低电流	I_{OL}	—	—	4	mA	当器件处于工作模式时，V_{CC} = 2.5 至 5.5V，V_{OL} = 0.4V
Theta JA	Θ_{JA}	—	166	—	°C/W	SOIC（SSH）
		—	173	—	°C/W	UDFN（MAH）
		—	146	—	°C/W	RBH

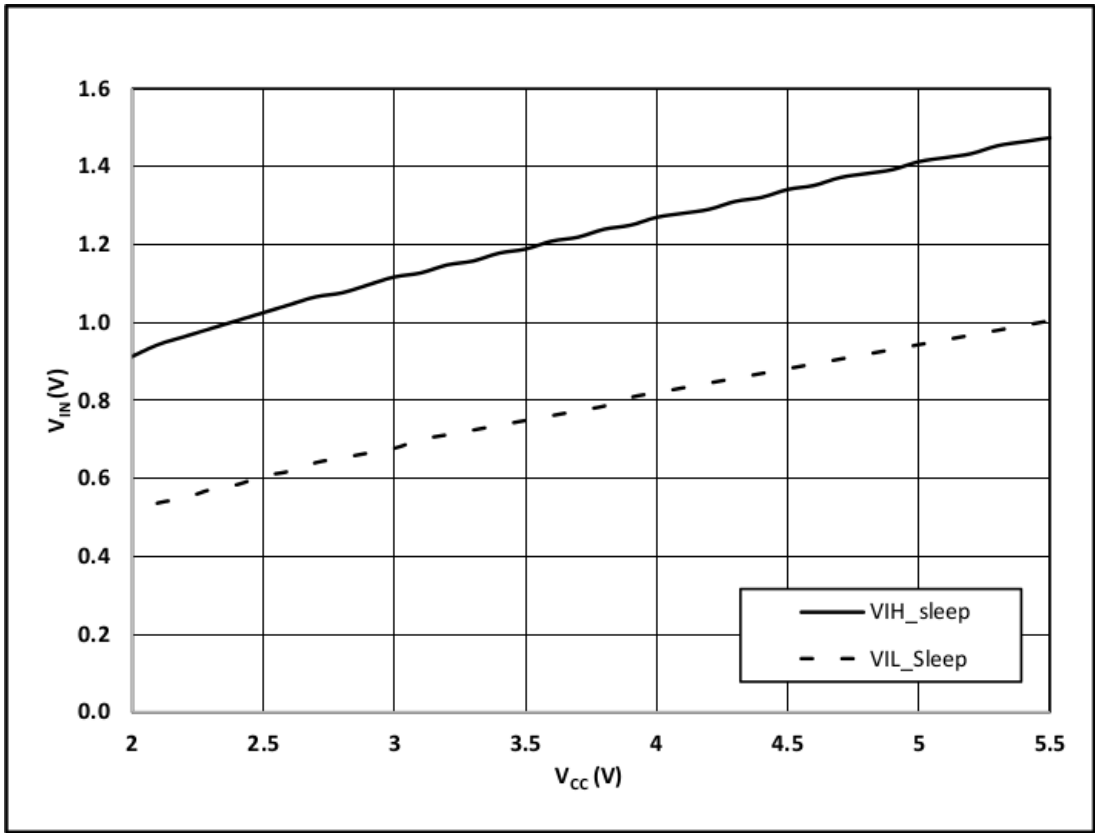
2.4.1 V_{IH} 和 V_{IL} 规格

器件的输入电平因器件模式和电压而异。在休眠或空闲模式下，输入电压阈值取决于 V_{CC} 电平，如图 2-4 所示。在休眠或空闲模式下，TTLenable 位不起作用。

表 2-6. 所有 I/O 接口上的 V_{IL} 和 V_{IH}（TTLenable = 0）

参数	符号	最小值	典型值	最大值	单位	条件
输入低电压	V_{IL}	-0.5	—	0.5	V	当器件处于工作模式且配置存储器中的 TTLenable 位为 0 时；否则参见上文。
输入高电压	V_{IH}	1.5	—	V_{CC} + 0.5	V	当器件处于工作模式且配置存储器中的 TTLenable 位为 0 时；否则参见上文。

图 2-4. 在休眠模式和空闲模式下的 V_{IH} 和 V_{IL}



3. 兼容性

3.1 Microchip ATECC608A

ATECC608B 旨在提供比 ATECC608A 更高的安全性配置，同时保持向后兼容性。下面将详细介绍器件更改和增强。配置位字段没有任何改变。为 ATECC608A 定义的配置与 ATECC608B 器件在功能上完全相同。

校正与增强

对 ATECC608B 器件中的以下项目进行了校正或增强：

- 现可提供两种温度范围：
  - 标准工业级温度范围：-40℃至+85℃
  - 扩展工业级温度范围：-40℃至+100℃
- 总线上存在多个器件时，将以较低的 I^2C 频率运行，不会再产生总线争用问题。
- 修改了 `Verify`、`SecureBoot`、`Lock` 和 `Read` 命令的命令时序。
- 新封装选项：仅符合条件的客户可使用 3 引脚触点封装和 WLCSP 封装。（有关 WLCSP 封装选项，请联系 Microchip 销售人员。）

3.2 Microchip ATECC508A

ATECC608B 的设计与 ATECC508A 器件完全兼容，但下文所列的功能除外。如果 ATECC608B 配置正确，则为 ATECC508A 编写的软件无需任何更改也可用于 ATECC608B，但同样下文所列的功能除外。

注： ATECC608B 配置区域中大多数元素的位置和数值均与 ATECC508A 完全相同。但是，可能需要更改 LastKeyUse 字段中存储的初始值，才能使其符合这些字节的新定义，如本文档中所示。该字段包含插槽 15 限制使用功能的初始计数，而在 ATECC608B 中可通过单调计数器使用此功能。

⚠ CAUTION ATECC608B 和 ATECC508A 的命令执行时间有所不同。如果已实施轮询，则这些差异不会产生问题。如果使用了固定时间，则必须根据需要进行评估和更新。

ATECC608B 与 ATECC508A 相比新增的功能

- 安全引导功能以及 IO 加密和身份验证
- `KDF` 命令，支持 PRF、HKDF 和 AES
- `AES` 命令，包括加密/解密
- 用于 AES 的 GCM AEAD 模式的 GFM 计算功能
- 更新了 NIST SP800-90 A/B/C 随机数发生器
- 灵活的 `SHA/HMAC` 命令，具有上下文保存/恢复功能
- 显著缩短了 `SHA` 命令执行时间
- 易失性密钥许可功能，用于阻止器件传输
- 传输密钥锁定功能，用于在交付期间保护已编程器件
- 计数器限制匹配功能
- 可在 SRAM 中临时生成密钥，ECDH 和 KDF 也支持该功能
- 可通过 MAC 验证 `Verify` 命令输出
- 对 ECDH 输出进行加密
- 增加了自检命令，可选择自动上电自检
- 用于内置 X.509 证书密钥验证的公钥未对齐

- 可选择在执行时间较长时降低功耗
- 数据（机密）区域锁定后可编程 I^2C 地址

ATECC608B 与 ATECC508A 相比取消的功能

- 删除了 HMAC 命令，替换为更强大的全新 SHA 命令
- 取消了 OTP 使用模式，现在变为只读模式
- 取消了暂停命令以及 UpdateExtra 中的相关选择器功能
- 取消了插槽 15 特有的限制使用功能，取而代之的是标准单调计数器限制使用功能
- SHA 命令在摘要计算期间不再使用 TempKey，并且在整个 SHA 操作过程中，TempKey 中的结果均保持不变。但是，仍然可以使用 TempKey 来初始化 HMAC_Start 的 SHA 或存储最终摘要。

3.3 Microchip ATSHA204A 和 ATECC108A

ATECC608B 通常与所有 ATSHA204/A 和 ATECC108/A 器件兼容。如果配置正确，则它可以在目前使用这些器件的大多数情形下使用。有关 ATSHA204A 和 ATECC108A 的兼容性限制的信息，请参见 ATECC508A 数据手册。

4. 封装标识信息

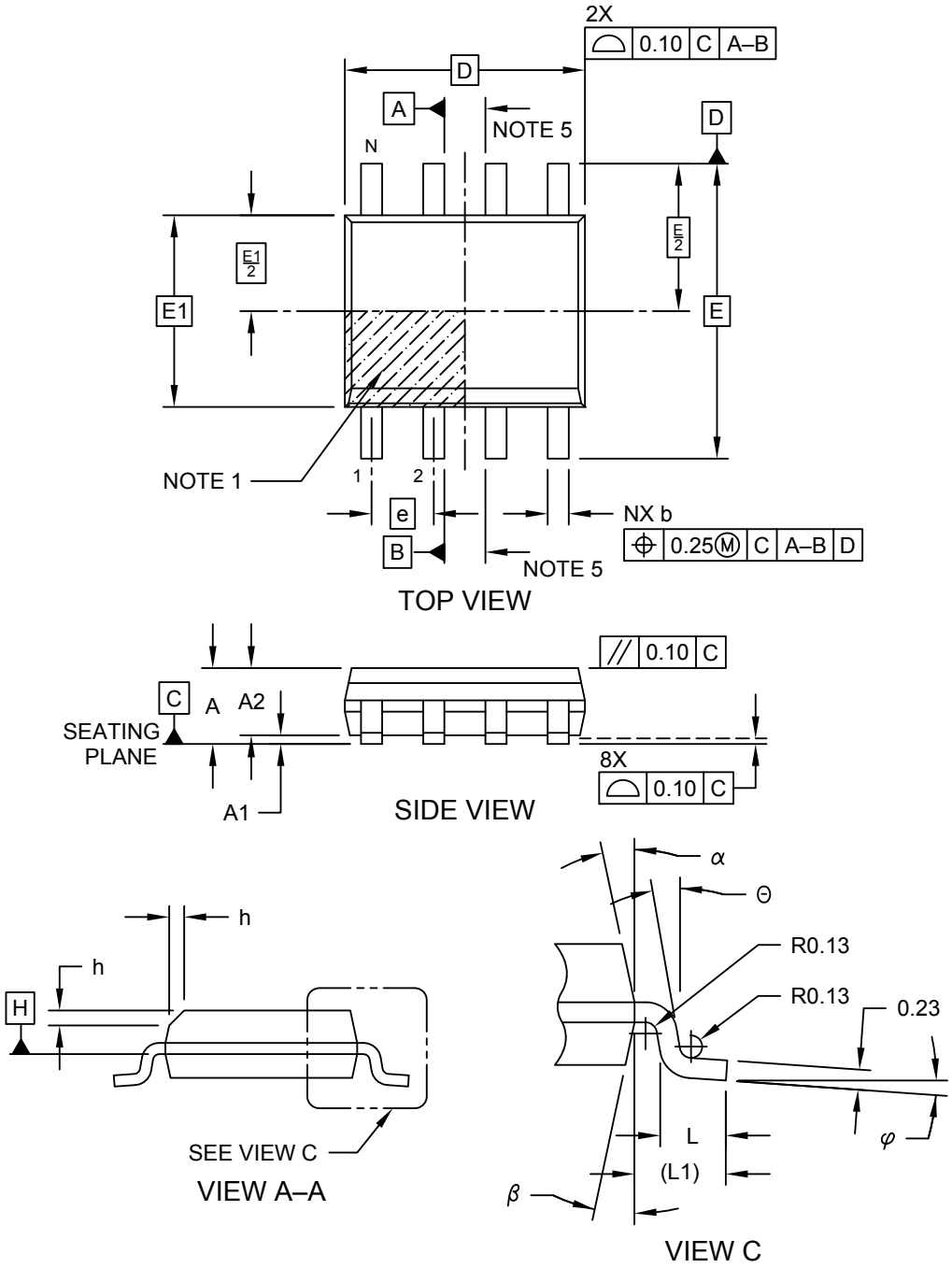
为保证 Microchip 的整体安全性，所有加密器件的部件标识有意进行了模糊处理。封装顶部的标识不会提供有关实际器件类型或器件制造商的任何信息。封装上的字母数字代码提供制造信息，并随封装批次的不同而异。不应在任何来料检验过程中使用此封装标识。

5. 封装图

5.1 8 引脚 SOIC

8-Lead Plastic Small Outline - Narrow, 3.90 mm (.150 In.) Body [SOIC]
Atmel Legacy Global Package Code SWB

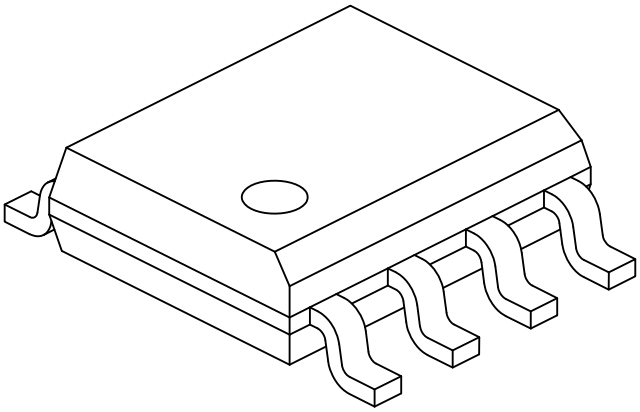
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing No. C04-057-SWB Rev E Sheet 1 of 2

8-Lead Plastic Small Outline - Narrow, 3.90 mm (.150 In.) Body [SOIC]
Atmel Legacy Global Package Code SWB

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		
Foot Angle	φ	0°	-	8°
Lead Thickness	c	0.17	-	0.25
Lead Width	b	0.31	-	0.51
Mold Draft Angle Top	α	5°	-	15°
Mold Draft Angle Bottom	β	5°	-	15°

Notes:

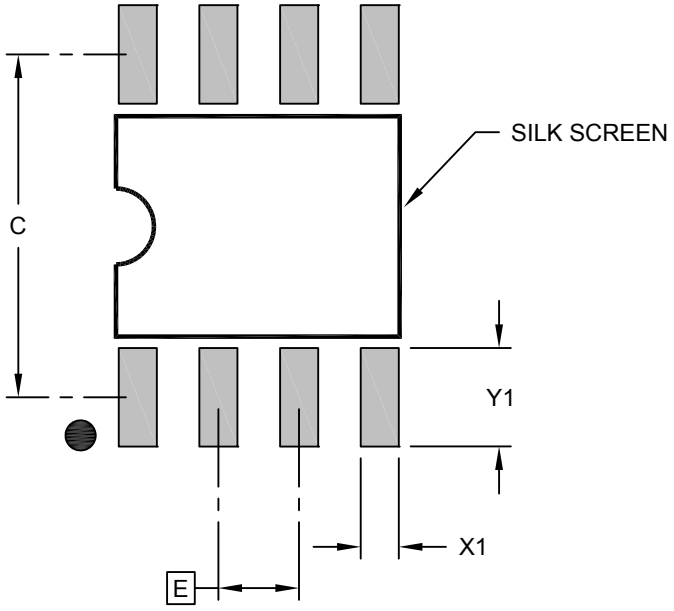
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. § Significant Characteristic
3. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.15mm per side.
4. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic 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-SWB Rev E Sheet 2 of 2

© 2017 Microchip Technology Inc.

8-Lead Plastic Small Outline - Narrow, 3.90 mm (.150 In.) Body [SOIC]
Atmel Legacy Global Package Code SWB

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:

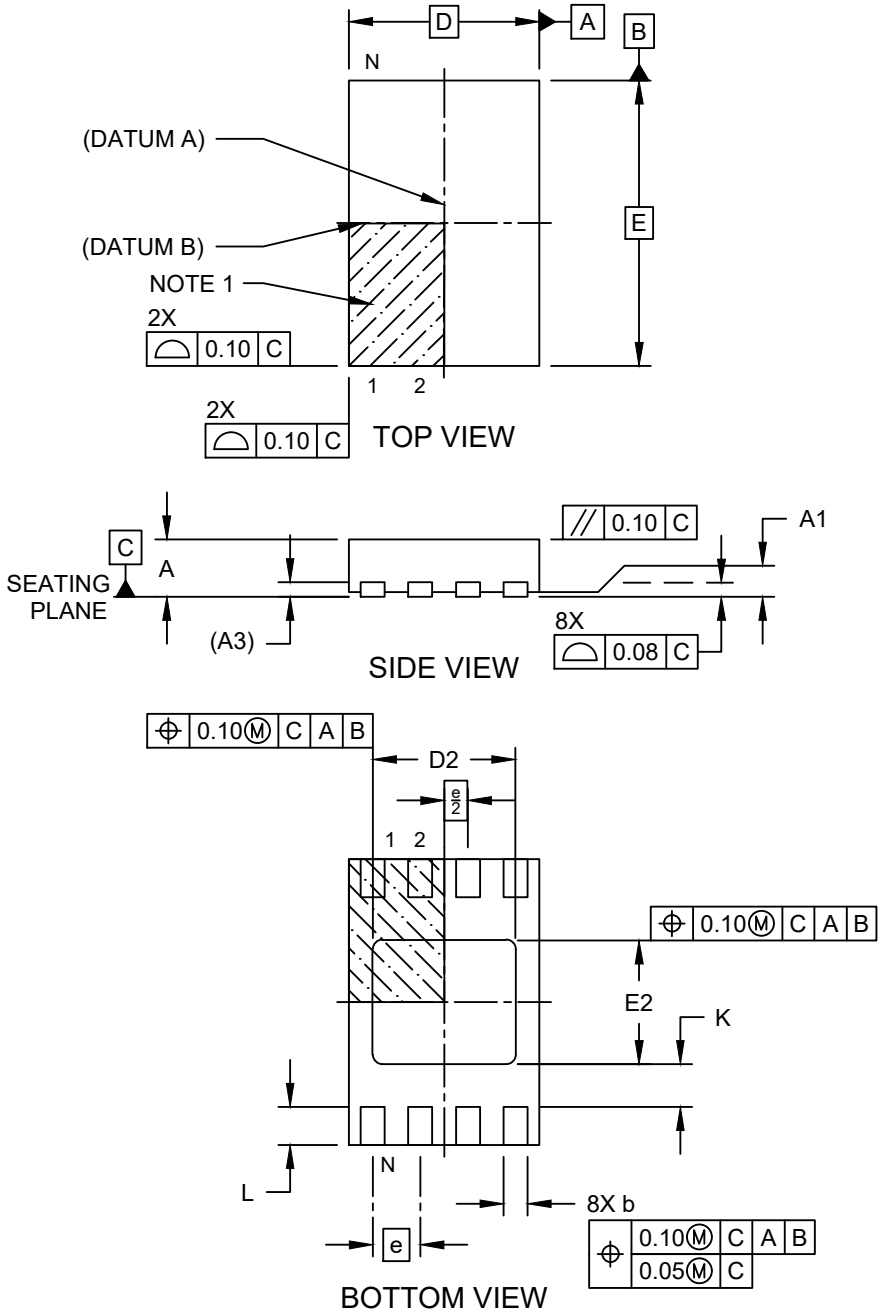
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-2057-SWB Rev E

5.2 8 焊盘 UDFN

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

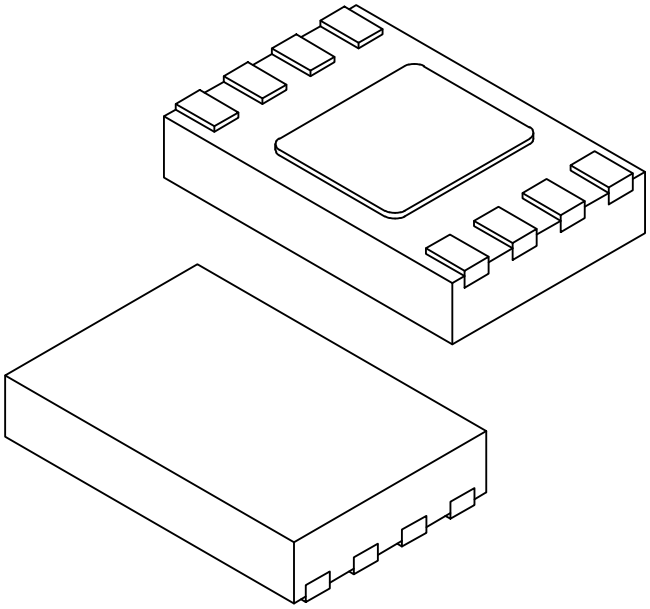
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing C04-21355-Q4B Rev B 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	0.35	0.40	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

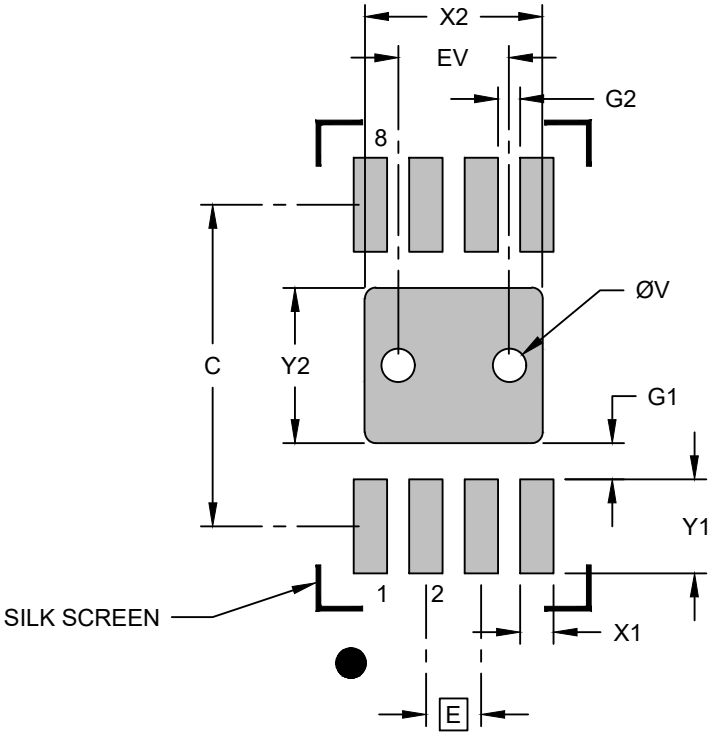
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

   REF: Reference Dimension, usually without tolerance, for information purposes only.

Microchip Technology Drawing C04-21355-Q4B Rev B 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:

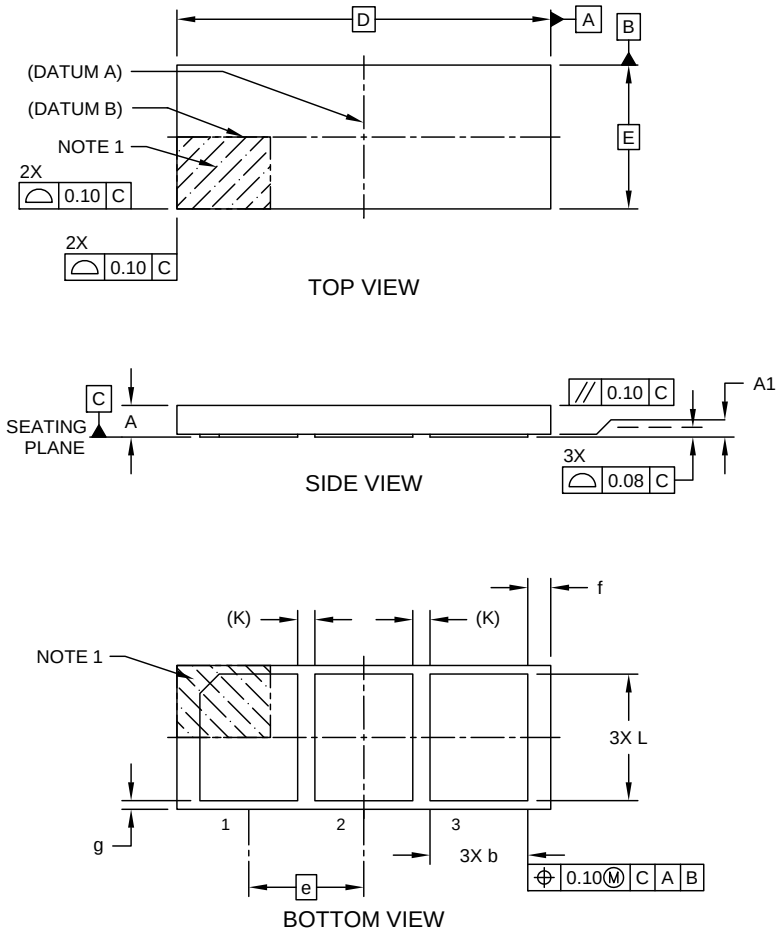
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
2. For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

Microchip Technology Drawing C04-23355-Q4B Rev B

5.3 3 引脚触点式

3-Lead Contact Package (LAB) - 6.54x2.5 mm Body [Contact]
Atmel Legacy Global Package Code RHB

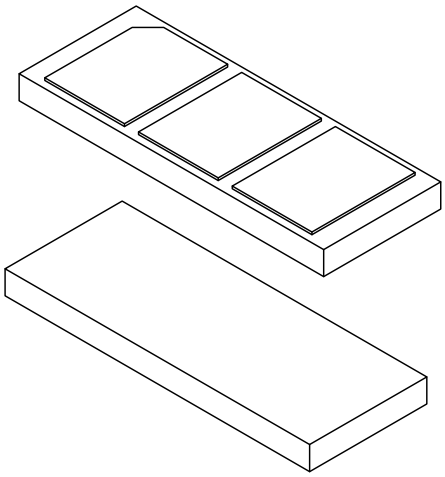
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing C04-21303 Rev A Sheet 1 of 2

3-Lead Contact Package (LAB) - 6.54x2.5 mm Body [Contact]
Atmel Legacy Global Package Code RHB

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	3		
Pitch	e	2.00 BSC		
Overall Height	A	0.45	0.50	0.55
Standoff	A1	0.00	0.02	0.05
Overall Length	D	6.50 BSC		
Overall Width	E	2.50 BSC		
Terminal Width	b	1.60	1.70	1.80
Terminal Length	L	2.10	2.20	2.30
Terminal-to-Terminal Spacing	K	0.30 REF		
Package Edge to Terminal Edge	f	0.30	0.40	0.50
Package Edge to Terminal Edge	g	0.05	0.15	0.25

Notes:

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. 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 C04-21303 Rev A Sheet 2 of 2

6. 版本历史

版本	日期	说明
A	2020 年 7 月	初始版本。基于 ATECC608A 摘要数据手册版本 B（DS40001977B_CN）

Microchip 网站

Microchip 网站（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 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 获得网上技术支持。

产品标识体系

欲订货或获取价格、交货等信息，请与我公司生产厂或各销售办事处联系。

PART NO.	-XX	X	XX	-X
Device	Package	Temp Range	I/O Type	Tape and Reel

器件：	ATECC608B：具有基于硬件的安全密钥存储的加密协处理器。	
封装选项（3）	SS	8 引脚（0.150 英寸宽体）塑封鸥翼小外形封装（JEDEC SOIC）
	MA	8 焊盘 2 x 3 x 0.6 mm 主体、耐热增强型塑封超薄双列扁平无引线封装（UDFN）
	RB	3RB、3 引脚主体 2 x 5 x 6.5 mm、2.0 mm 引脚间距触点封装（Sawn）
温度范围	H	标准工业级温度范围：-40 ℃至 85 ℃
	V	扩展工业级温度范围：-40 ℃至 100 ℃
I/O 类型	CZ	单线接口
	DA	I^2C 接口
卷带式选项	B	管式
	T	大卷带（尺寸随封装类型而异）
	S	小卷带（仅适用于 MA 封装类型）

器件订购代码

温度范围		说明
标准工业级	扩展工业级	
ATECC608B-SSHCZ-T	ATECC608B-SSVCZ-T	8 引脚（0.150 英寸宽体）塑封鸥翼小外形封装（JEDEC SOIC），单线，卷带式，每卷 4,000 片
ATECC608B-SSHCZ-B	ATECC608B-SSVCZ-B	8 引脚（0.150 英寸宽体）塑封鸥翼小外形封装（JEDEC SOIC），单线，管式，每管 100 片
ATECC608B-SSHDA-T	ATECC608B-SSVDA-T	8 引脚（0.150 英寸宽体）塑封鸥翼小外形封装（JEDEC SOIC），I^2C，卷带式，每卷 4,000 片
ATECC608B-SSHDA-B	ATECC608B-SSVDA-B	8 引脚（0.150 英寸宽体）塑封鸥翼小外形封装（JEDEC SOIC），I^2C，管式，每管 100 片
ATECC608B-MAHCZ-T	ATECC608B-MAVCZ-T	8 焊盘主体 2 x 3 x 0.6 mm、耐热增强型塑封超薄双列扁平无引线封装（UDFN），单线，卷带式，每卷 15,000 片
ATECC608B-MAHDA-T	ATECC608B-MAVDA-T	8 焊盘主体 2 x 3 x 0.6 mm、耐热增强型塑封超薄双列扁平无引线封装（UDFN），I^2C，卷带式，每卷 15,000 片
ATECC608B-MAHCZ-S	ATECC608B-MAVCZ-S	8 焊盘主体 2 x 3 x 0.6 mm、耐热增强型塑封超薄双列扁平无引线封装（UDFN），单线，卷带式，每卷 3,000 片
ATECC608B-MAHDA-S	ATECC608B-MAVDA-S	8 焊盘主体 2 x 3 x 0.6 mm、耐热增强型塑封超薄双列扁平无引线封装（UDFN），I^2C，卷带式，每卷 3,000 片
ATECC608B-RBHCZ-T	ATECC608B-RBVCZ-T	单线，卷带式，每卷 5,000 片，3 引脚触点封装
ATECC608B-RBHCZ-B	ATECC608B-RBVCZ-B	单线，管式，每管 56 片，3 引脚触点封装

注：

1. 卷带式标识符仅出现在产品目录的部件编号描述中。此标识符用于订购目的，不会印在器件封装上。有关是否提供卷带式封装选项，请向 Microchip 销售办事处咨询。
2. 另外还提供小型封装选项。有关是否提供小型封装，请访问 www.microchip.com/packaging，或者联系您当地的销售办事处。
3. 卷带式管芯和 WLCSP 封装仅供符合条件的客户使用。此表中未列出这些封装的订购代码。有关这些封装选项的更多信息，请联系 Microchip 销售人员。

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规范。
- Microchip 确信：在正常使用的情况下，Microchip 系列产品非常安全。
- 目前，仍存在着用恶意、甚至是非法的方法来试图破坏代码保护功能的行为。我们确信，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。这种试图破坏代码保护功能的行为极可能侵犯 Microchip 的知识产权。
- Microchip 愿与那些注重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。

© 2021，Microchip Technology Incorporated，美国印刷，版权所有。

ISBN：978-1-5224-7939-0

质量管理体系

有关 Microchip 的质量管理体系的信息，请访问 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： www.microchip.com/support 网址： 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：86-592-2388138 **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：45-4485-5910 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