爱特梅尔ATSHA204

爱特梅尔CryptoAuthentication

数据表

特点

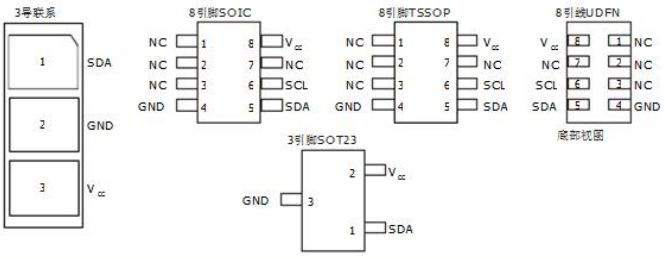
- 安全的身份验证和验证设备
- 为主机和客户端操作的综合能力
- 优越的SHA-256哈希算法，HMAC选项
- 最佳的类中， 256位密钥长度;存储多达16个按键
- 保证唯一的72位序列号
- 内部，高品质的随机数发生器（ RNG ）
- 4.5 - Kbit的EEPROM，用于密钥和数据
- 512 OTP （一次性可编程）位固定信息
- 多个I / O选项
  - 高速，单线接口
  - 1MHz的我2接口
- 2.0V - 5.5V电源电压范围
- 1.8V - 5.5V通信
- <150nA休眠电流
- 扩展的，多层次的硬件安全
- 8引脚SOIC， 8引脚TSSOP封装， 3引脚SOT23封装， 8盘UDFN ，并3引脚封装联系

应用

- 对于配件，子卡和消耗品防克隆保护
- 安全启动验证，软件反盗版
- 网络和计算机的访问控制
- 加密下载密钥交换
- 用于控制网络身份验证/加密通信

图1 。 销刀豆网络gurations

引脚名称	功能
SDA	串行数据
SCL	串行时钟输入
GND	地
Vcc	电源



介绍

以下各节介绍Atmel公司的特性和功能 ®ATSHA204认证装置。

应用

该ATSHA204是爱特梅尔CryptoAuthentication ™系列的高安全性的硬件认证设备中的一员。它具有灵活的指令集，允许使用对许多应用，其中包括以下内容：

- **防伪**
  验证一个可拆卸，可更换，或耗材的客户是真实的。例如客户可以是打印机墨盒，电子子卡，或其他零配件。它也可以被用于验证软件/固件模块或存储器的存储元件。
- **保护固件或媒体**
  验证存储在闪存中的代码在系统启动，以防止未经授权的修改（即安全启动），加密下载的媒体文件，并且唯一的加密代码图象是关于仅一个单一的系统可用。
- **会话密钥交换**
  可靠且容易地用一个加密/解密引擎在系统中交换数据流的加密密钥的使用微处理器来管理这些事情的保密通信信道或加密的下载。
- **安全的数据存储**
  通过在标准的微处理器加密加速器存储秘密密钥使用。它也可以被用于存储小量所必需的结构，标定，电子钱包值，消耗数据，或其它机密数据。透过加密/身份验证的可编程保护读取和写入操作。
- **用户密码检查**
  验证用户输入的密码，而不让期望值出名，地图简单的密码复杂的，并且安全地交换密码的值与远程系统。

1.2 设备特点

该ATSHA204包括可用于电可擦除可编程只读存储器（EEPROM）阵列存储密钥，杂读/写，只读，或秘密数据，消费记录和安全配置。访问到的存储器中的各个部分可以被限制在以各种方式和配置，然后锁定，以防止修改。参见第2.1节“ EEPROM组织”，为在EEPROM组织的更多细节。

该ATSHA204设有专门设计，以防止该装置上的物理攻击的防御机制各种各样本身或在设备和系统之间传输的数据的逻辑攻击（参见第3.4节“安全功能”，为更多详细信息）。在其中键使用或产生的方式，在3.3节中描述的硬件限制，“核心价值”提供对某些款式的攻击进一步防御。

对设备的访问是通过一个标准的I²C接口速度高达1Mbit /秒（见本接口第6节的详细信息）。它与标准的串行EEPROM I²C接口规格。该设备还支持一个单线接口可以降低系统处理器上所需的GPIO的数量和/或减少引脚的连接器上的数量。该单线接口进行更详细的第5节中描述的，“单线接口”。

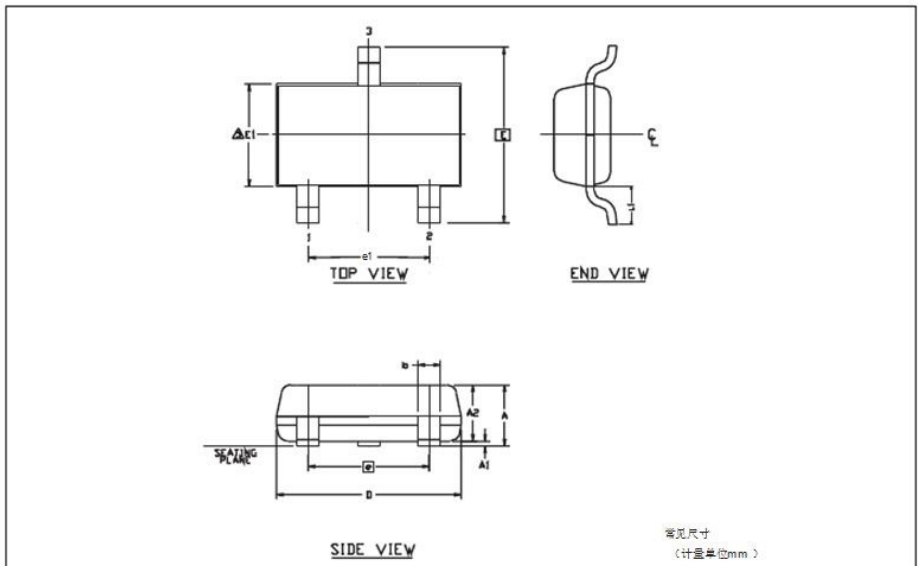
使用任我 ²C或单线接口，多ATSHA204设备可以共享同一条总线，从而节省处理器GPIO用法与多个客户端系统，比如不同颜色的墨水盒或多个零部件。参见第4.2节“共享在接口方面，“和第8.10节，”暂停命令，“就在这个实现方式的更多细节。

每个ATSHA204附带了一个保证唯一的72位序列号。使用由所支持的加密协议装置中，一台主机系统或远程服务器可以证明的序列号是两个真实的和不拷贝。序列号是常存储在一个标准的串行EEPROM，但这些可以很容易地被复制，并且没有办法让主机知道如果串行数字是真实的还是克隆。

爱特梅尔ATSHA204可以生成高质量的随机数，并聘请他们为任何目的，包括为部分该装置的加密协议。因为每个256位的随机数被保证是从以往的所有数值独特在这个或任何其他设备产生的，将其纳入协议计算保证了重放攻击（重新发送

封装图纸

3引脚SOT23



SIDE VIEW

常见尺寸
（计量单位mm ）

（计量单位mm ）

符号	民	喃	最大	记
A	0.89	-	1.12	
A1	0.01	-	0.10	
A2	0.88	-	1.02	
D	2.80	2.90	3.04	1,2
E	2.10	-	2.64	
E1	1.20	1.30	1.40	1,2
L1	0.54 REF			
e1	1.90 BSC			
b	0.30	-	0.50	3

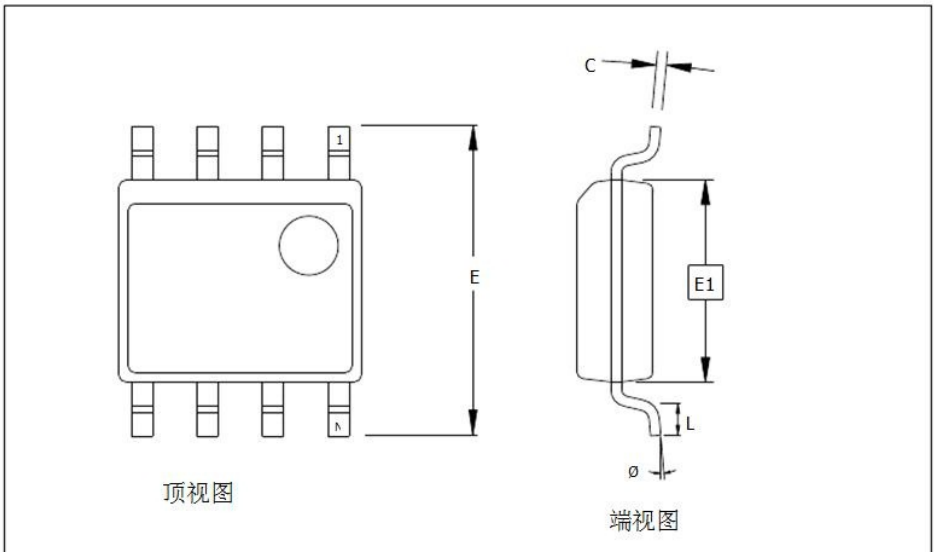
1.尺寸D不包括毛边，突出或毛刺。模具闪光灯。
突出或毛刺不得超过每月底0.25毫米。尺寸E1不
不包括引脚间的薄膜或凸出。间的薄膜或突起不得
超过每边0.25毫米。
2.封装的顶部可以比包底小。尺寸D和E1
表塑料体的最外 极限独家模具的确定
闪光灯，拙杆毛刺，门毛刺和引脚间。但包括任何不匹配
塑料体的顶部和底部之间。
3.这些尺寸适用于引线0.08毫米和之间的平坦部
0.15毫米从导管尖端。

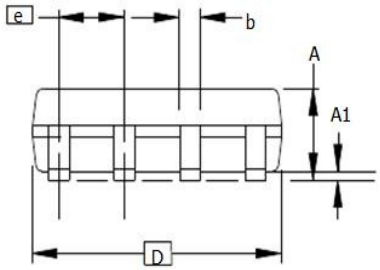
此图仅供一般信息。请参阅
JEDEC绘图TO- 236 ，变化AB额外
信息。

11/5/08

封装图纸联系方式: packagedrawings@atmel.com	标题 3TS1， 3导联， 1.30毫米体，塑料薄 紧缩小型封装（ SOT收缩）	GPC TBG	图号. 3TS1	启示录 A

8引脚SOIC





SIDE VIEW

注：本图仅供一般信息。
请参考JEDEC绘图MS- 012，变化AA
进行适当的尺寸，公差，基准等。

常见尺寸
（计量单位mm）

符号	最小值	喃	最大	记
A	1.35	–	1.75	
A1	0.10	–	0.25	
b	0.31	–	0.51	
C	0.17	–	0.25	
D	4.80	–	5.05	
E1	3.81	–	3.99	
E	5.79	–	6.20	
e	1.27 BSC			
L	0.40	–	1.27	
Ø	0°	–	8°	

6/22/11

	标题	GPC	图号。	启示录
封装图纸联系方式： packagedrawings@atmel.com	8S1， 8引脚（ 0.150 "宽体） ，塑料鸥翼小外形（ JEDEC SOIC ）	SWB	8S1	G