MOD8ID 用户使用手册

物联网设备安全加密芯片

文档历史发放及记录

序号	变更（+/-）说明	作者	版本号	日期	批准
1	创建文档		V1.2	2020-03-18	
2	增加编带说明		V1.3	2021-10-9	
3	增加地址说明		V1.4	2022-03-03	
4	增加上电说明		V1.5	2022-03-04	

阅读声明

深圳模微半导体有限公司（以下简称模微半导体）保有在不事先通知而修改这份文档的权利。模微半导体认为提供的信息是准确可信的。尽管这样，模微半导体对文档中可能出现的错误不承担任何责任。在购买前请联系模微半导体获取该产品说明的最新版本。未经模微半导体授权，任何单位及个人不得以任何方式或理由对本手册进行使用、复制、修改、抄录、传播等。

目录

一、概述

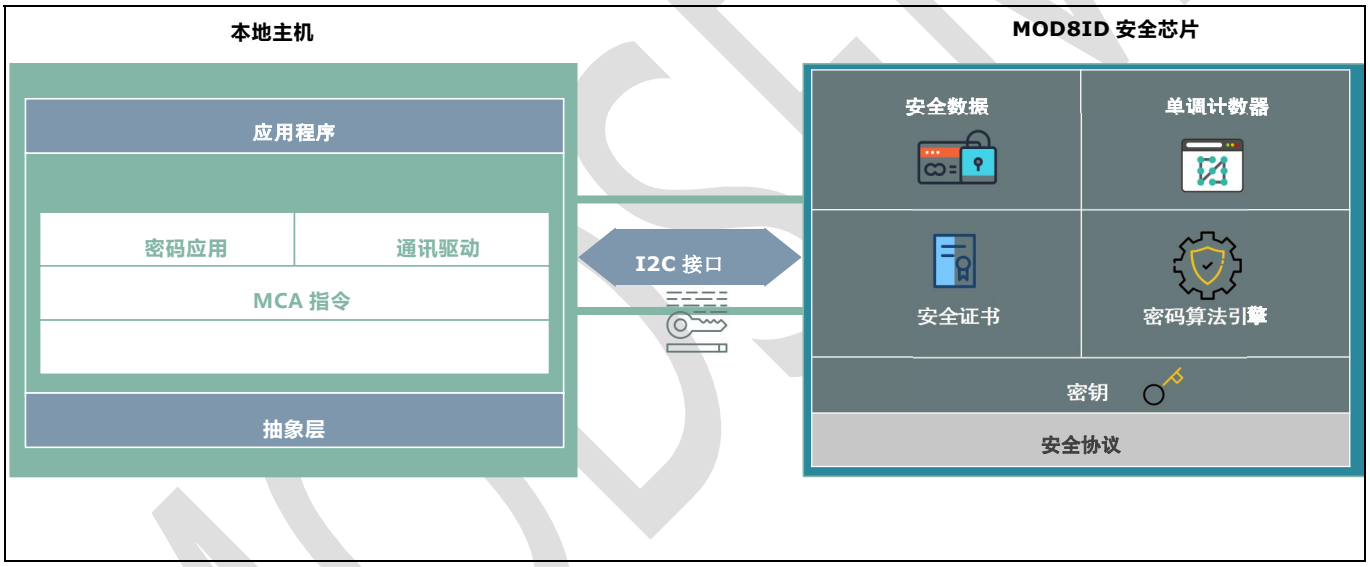
MOD8ID 是一款具有高安全性的金融级加密芯片，支持 IIC 协议，支持单线协议，它内置 PKE 公钥算法协处理器和 AES，HASH 加密算法引擎，可快速的为各类数字设备提供高安全属性，包括用于智能家居的物联网（IoT）节点，车载，工控设备，电子耗材，医疗，移动和其他电子设备应用。MOD8ID 内置 ECDSA/RSA/SM2 等验证功能，以提供高安全的非对称身份验证。基于超安全的算法引擎和安全防护设计，MOD8ID 安全加密芯片可为数字设备提供机密性，数据完整性和身份验证三大安全属性。MOD8ID 系列加密芯片支持低功耗应用，可定制封装，可快速集成，并高度兼容的适配各类应用场景。

二、关键特性

- 高性能加密算法引擎
  - RSA-支持 1024/2048
  - ECC-支持 P-256/P-192
  - 支持 SM2/SM4 国密算法
  - SHA1/256
  - AES128/256
- 存储加密加扰防护
- 防御各种侵入式与非侵入式攻击
- 支持密钥与证书安全存储
- 支持安全启动与双向认证

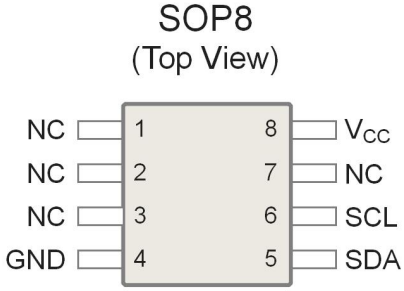
- 具备金属防护层和胶粘逻传感器层，探测到外部攻击后，内部数据不可逆自毁
- 总线和内存加密 ，时钟加扰
- 典型功耗：1.6mA
- 支持 I2C 通信接口
- 高兼容性，快速低成本集成。

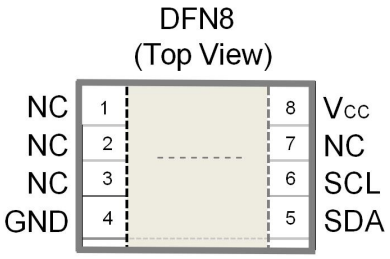
三、系统框图



MOD8ID 系统框图

四、引脚分配





PIN	功能
GND	地
SDA	串行数据
SCL	串行时钟输入
VCC	供电电源
NC	无连接

五、电气特性

6.1. 关键特性

参数	Min	Type	Max	单位
工作温度	-40	--	85	℃
工作电压	1.62	--	3.3	V
ESD(HBM)	-	-	4000	V

6.2. DC 特性

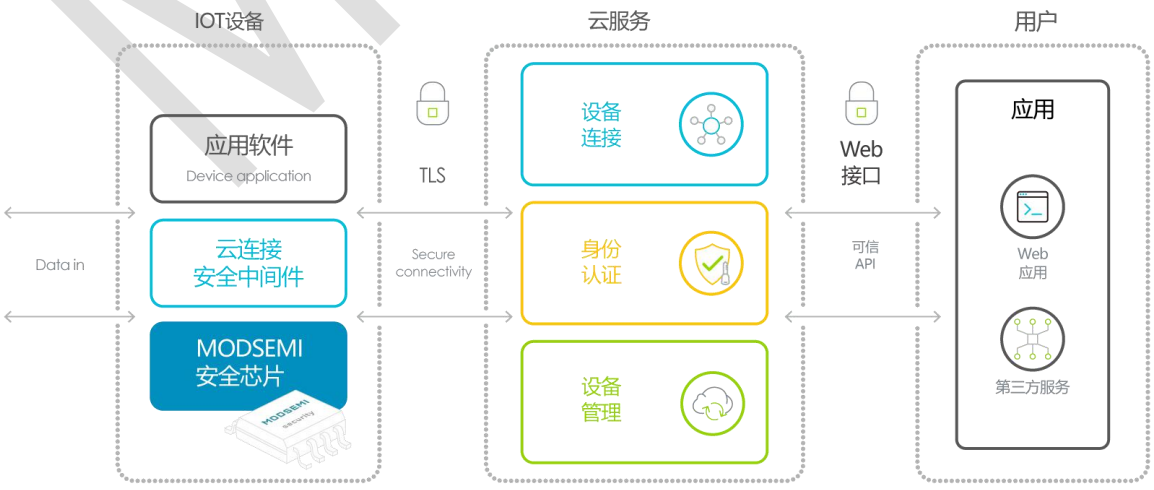
参数	条件	VCC	Min	Type	Max	单位
VIH	输入高压，所有标准输入和双向端口	3.3V	2.0	-	-	V
		1.8V	1.2	-	-	V
VIL	输入低电压，所有标准输入和双向端口	3.3V	-	-	0.8	V
		1.8V	-	-	0.6	V
VOH	输出高压，所有标准输入和双向端口	3.3V	VCC-0.4	-	-	V
		1.8V	VCC-0.4	-	-	V

VOL	输出低电压，所有标准输入和双向端口	3.3V	-	-	0.4	V
		1.8V	-	-	0.4	V
IIL	IO pad force -0.2V @VDDIO=3.6V，IIL= -120~-70uA					
IIH	IO pad force 3.8V @VDDIO=3.6V， IIH = 8uA~16uA					
Icc	在 I/O 传输或执行非 ECC/SM2 命令期间等待 I/O。与时钟分频器值无关。	3.3V	-	1.6	-	mA

六、使用指南

6.1. 概述

MOD8ID 芯片是具有高安全性的金融级加密芯片，基于 PKI 认证体系，通过提供硬件级 API 实现物联网高安全应用。MOD8ID 标准方案提供安全认证和关键数据存储，用户通过 I2C 通信调用 MOD8ID 的 API，完成出厂初始化，安全认证，关键数据存储，安全启动等功能。MOD8ID 作为板级核心信任根对板级进行唯一性认证，关键数据和私钥数据存储在安全芯片中，MOD8ID 易于集成到电子设备当中，本节详细描述 MOD8ID 的使用与集成。



6.2. 硬件集成示意图

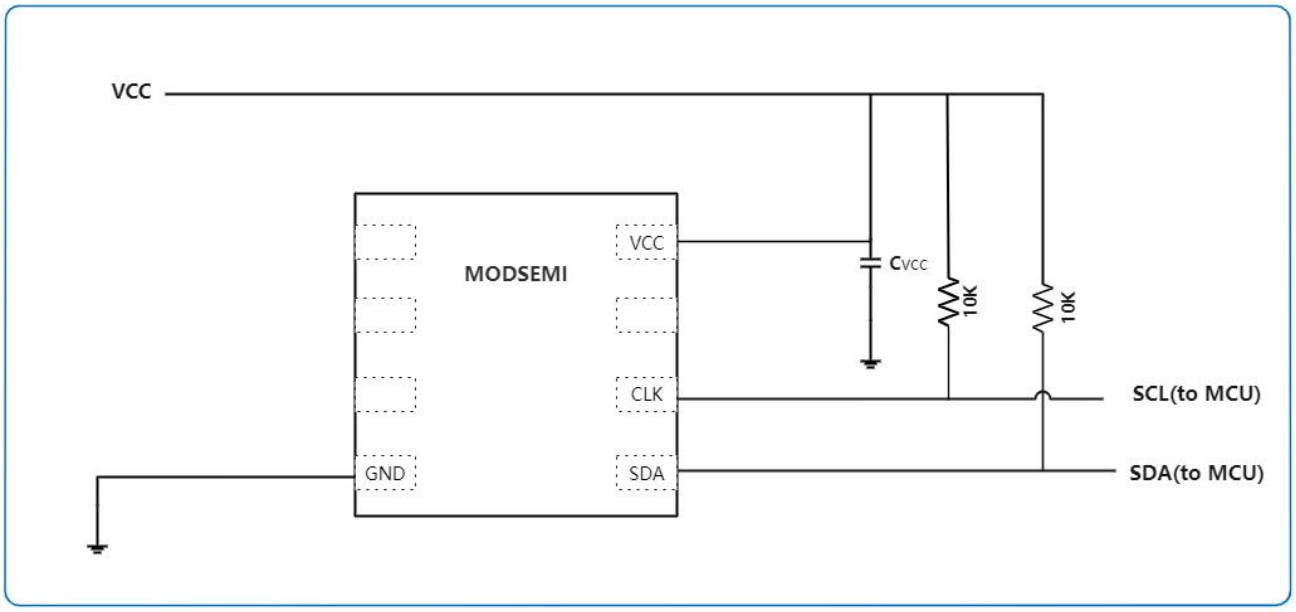


图 1 系统集成示意图

NOTE：上拉电阻的值取决于实际应用电路和实际 I2C SCL 频率。

6.3. I2C 接口时序

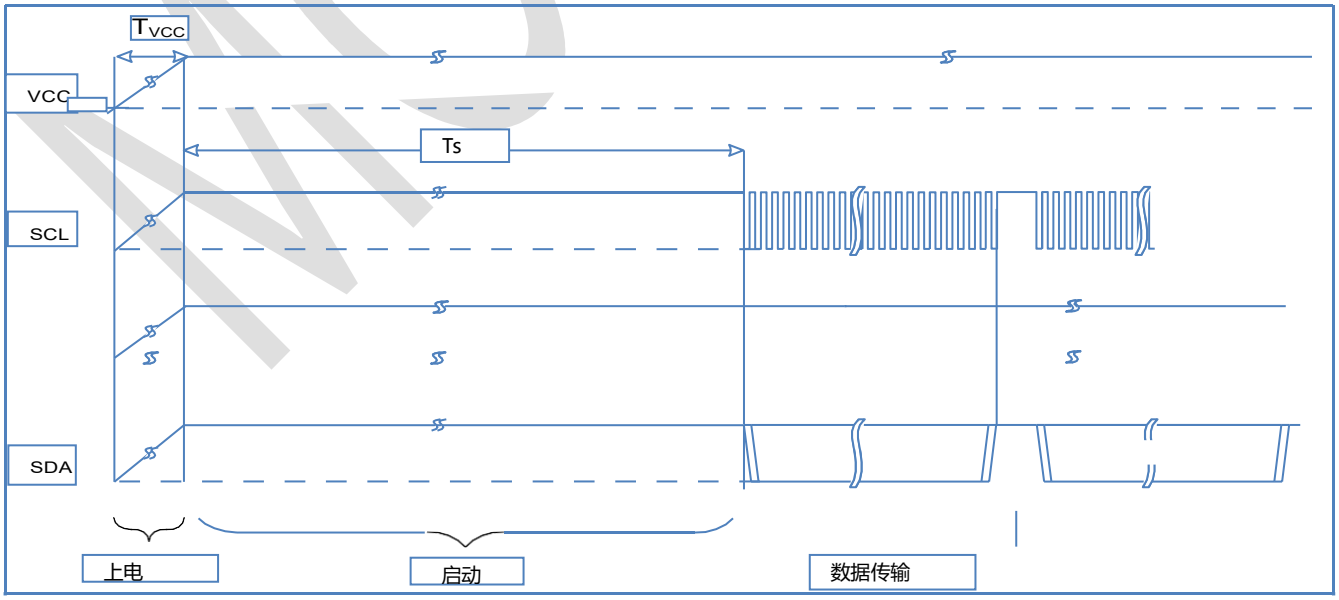


图 2 I2C 接口时序

参数	符号	值			单位	备注或测试条件
		Min	TYPE	MAX		
上电启动时间	Ts	25			mS	
VCC上电时间	Tvcc	0.1		1	mS	

表 1 启动时间参考

6.4. 系统集成

6.4.1. 集成步骤

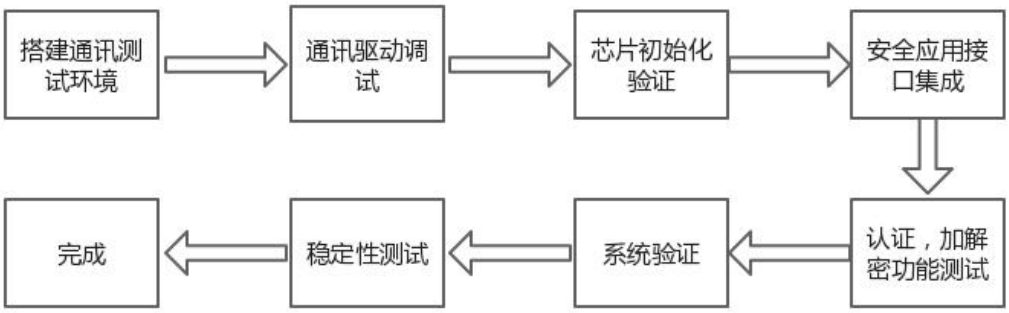


图 3 集成步骤图

6.4.2. 环境搭建

按照 1.2 节连接示意图连接 MOD8ID 安全芯片与主控，也可以使用 MODSEMI 官方提供的评估套件进行前期应用评估。

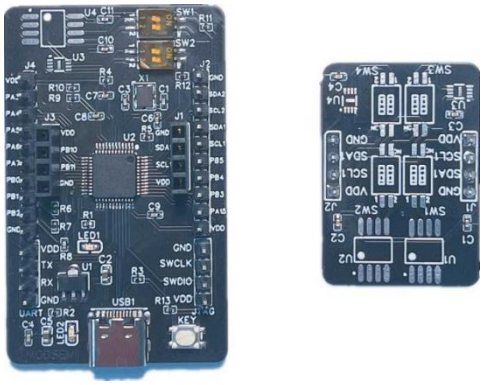


图 4 MODSEMI MOD8ID 评估套件

6.4.3. 通讯调试

MOD8ID 支持 I2C 标准模式（100Kbps），快速模式（400Kbps）和高速模式（1Mbps）。

6.4.4. 芯片初始化

MOD8ID 在出厂前已经支持基于对称算法与非对称算法的安全协议，安全应用使用前需要通过指令接口进行初始化，用于产生非对称认证、对称认证、读写加密用到的相关密钥与权限。

6.4.5. 地址编码

ReadData 和 WriteData 命令在 Param2 中需要一个 16 位的地址，该地址用于指定要访问的存储器位置。其中配置区大小为 128 字节；数据区可用于存储密钥或应用数据，大小为 1208 字节。

6.4.5.1. 配置区地址编码(Param2)

对于配置区，一次可访问 4 或 32 个字节。

地址格式：

字节1	字节0

未使用	未使用	块	偏移量
Addr[15:8]	Addr[7:5]	Addr[4:3]	Addr[2:0]

配置区地址：

块（Addr[4:3]）	偏移量（Addr[2:0]）							
	000	001	010	011	100	101	110	111
00	[0:3]	[4:7]	[8:11]	[12:15]	[16:19]	[20:23]	[24:27]	[28:31]
01	[32:35]	[36:39]	[40:43]	[44:47]	[48:51]	[52:55]	[56:59]	[60:63]
10	[64:67]	[68:71]	[72:75]	[76:79]	[80:83]	[84:87]	[88:91]	[92:95]
11	[96:99]	[100:103]	[104:107]	[108:111]	[112:115]	[116:119]	[120:123]	[124:127]

6.4.5.2. 数据区地址编码(Param2)

数据区总共有 16 个槽，槽的大小各不相同。每个槽的配置分别控制一个槽是否允许读取或写入。

地址格式：

区段	字节1		字节0		
	未使用	块	未使用	槽	偏移量
密钥槽（0~7）	Addr[15:9]	Addr[8]	Addr[7]	Addr[6:3]	Addr[2:0]
密钥槽（8）	Addr[15:12]	Addr[11:8]	Addr[7]	Addr[6:3]	Addr[2:0]
密钥槽（9~15）	Addr[15:10]	Addr[9:8]	Addr[7]	Addr[6:3]	Addr[2:0]

数据区地址：

槽	块	块偏移量（Addr[2:0]）							
		000	001	010	011	100	101	110	111
0~7	00	[0:3]	[4:7]	[8:11]	[12:15]	[16:19]	[20:23]	[24:27]	[28:31]
	01	[32:35]	无效	无效	无效	无效	无效	无效	无效
8	0000	[0:3]	[4:7]	[8:11]	[12:15]	[16:19]	[20:23]	[24:27]	[28:31]
	0001	[32:35]	[36:39]	[40:43]	[44:47]	[48:51]	[52:55]	[56:59]	[60:63]
	…	…	…	…	…	…	…	…	…
	1100	[384:387]	[388:391]	[392:395]	[396:399]	[400:403]	[404:407]	[408:411]	[412:415]

9~15	00	[0:3]	[4:7]	[8:11]	[12:15]	[16:19]	[20:23]	[24:27]	[28:31]
	01	[32:35]	[36:39]	[40:43]	[44:47]	[48:51]	[52:55]	[56:59]	[60:63]
	10	[64:67]	[68:71]	无效	无效	无效	无效	无效	无效

6.4.6. 应用指令

MOD8ID 通过应用指令接口提供全面的密码算法协议和密钥管理，通过应用指令，用户可根据不同的应用场景进行调用和组合。

命令名称	指令码	描述
AES	0x51	AES ECB模式加密或解密
ECDH	0x43	利用已有的私钥和输入的公钥计算共享密钥
GenEccKey	0x40	生成ECC私钥或通过私钥生成ECC公钥
Lock	0x17	锁定配置区或数据区
Nonce	0x16	生成一串一次性使用的数字供后续命令使用
Random	0x1B	生成随机数
ReadData	0x02	读取数据
WriteData	0x12	写入数据
SecureBoot	0x80	安全启动
SHA	0x47	计算SHA-256摘要
ECDSASign	0x41	ECC签名
ECDSAVerify	0x45	ECC验签
SM4	0x71	SM4 模式加密或解密

6.4.6.1. AES

功能说明

AES 命令使用指定密钥槽或 Tempkey 中的密钥对输入的数据进行 ECB 模式加密或解密。单组密钥长度为 16 字节，可以将多组密钥存在一个指定的槽内，每 16 字节为一组，单个密钥槽中最多可存 4 组密钥。

命令报文

编码	长度	值（HEX）
Opcode	1	51
P1	1	00：使用第一组密钥对明文进行加密 40：使用第二组密钥对明文进行加密 80：使用第三组密钥对明文进行加密 C0：使用第四组密钥对明文进行加密 01：使用第一组密钥对密文进行解密 41：使用第二组密钥对密文进行解密 81：使用第三组密钥对密文进行解密 C1：使用第四组密钥对密文进行解密
P2	2	0000~000F：密钥所在的槽 FFFF：使用TempKey
Data	16	明文（加密）或密文（解密）

响应报文

名称	长度	值（HEX）
Response	1 or 16	操作失败，则返回一个字节错误码 操作成功，则返回16字节密文（加密）或明文（解密）

6.4.6.2. ECDH

功能说明

ECDH 命令用于生成 ECC 共享密钥。可使用密钥槽中或 TempKey 中的 ECC 私钥，TempKey 中的 ECC 私钥须先使用 GenEccKey 命令生成。

命令报文

编码	长度	值（HEX）
Opcode	1	43
P1	1	05：使用TempKey中的私钥计算，共享密钥存在P2指定的密钥槽中 08：使用P2指定的密钥槽中的私钥计算，共享密钥存在TempKey中 09：使用TempKey中的私钥计算，共享密钥存在TempKey中 0C：使用P2指定的密钥槽中的私钥计算，以明文方式返回32字节共享密钥 0D：使用TempKey中的私钥计算，以明文方式返回32字节共享密钥 0E：使用P2指定的密钥槽中的私钥计算，以密文方式返回32字节共享密钥 0F：使用TempKey中的私钥计算，以密文方式返回32字节共享密钥
P2	2	0000~000F：密钥所在的槽
Data	64	用于计算的公钥

响应报文

名称	长度	值（HEX）
Response	1 or 32	操作失败，则返回一个字节错误码 操作成功，则返回32字节共享密钥

6.4.6.3. GenEccKey

功能说明

GenEccKey 命令用于生成 ECC 私钥或通过私钥生成 ECC 公钥。

命令报文

编码	长度	值（HEX）
Opcode	1	40
P1	1	00：使用存在P2指定的密钥槽中私钥生成公钥，返回公钥 04：生成ECC密钥对，私钥存在P2指定的密钥槽，返回公钥
P2	2	0000~000F：密钥槽
Data	0	

响应报文

名称	长度	值（HEX）
Response	1 or 64	操作失败，则返回一个字节错误码 操作成功，则返回64字节ECC公钥

6.4.6.4. Lock

功能说明

Lock 命令用于锁定配置区或数据区，防止被修改，锁定操作不可逆。

命令报文

编码	长度	值（HEX）
Opcode	1	17

P1	1	00：锁定配置区 01：锁定数据区
P2	2	0000
Data	0	

响应报文

名称	长度	值（HEX）
Response	1	操作失败，则返回一个字节错误码 操作成功，则返回00

6.4.6.5. Nonce

功能说明

Nonce 命令用于导入主机生成的随机数或其它数据供后续命令使用。

命令报文

编码	长度	值（HEX）
Opcode	1	16
P1	1	03：将32字节Data存入TempKey 23：将64字节Data存入TempKey
P2	2	0000
Data	32 or 64	Nonce数据

响应报文

名称	长度	值（HEX）
Response	1	操作失败，则返回一个字节错误码 操作成功，则返回00

6.4.6.6. Random

功能说明

Random 命令用于生成一组 32 字节的随机数。

命令报文

编码	长度	值（HEX）
Opcode	1	1B
P1	1	00
P2	2	0000
Data	0	

响应报文

名称	长度	值（HEX）
Response	32	随机数

6.4.6.7. ReadData

功能说明

ReadData 命令用于从配置区或数据区读取数据。

命令报文

编码	长度	值（HEX）
Opcode	1	02
P1	1	00：从配置区读4字节数据 80：从配置区读32字节数据 02：从数据区读4字节数据 82：从数据区读32字节数据
P2	2	参见：6.45 地址参数表
Data	0	

响应报文

名称	长度	值（HEX）
Response	4 or 32	读取到的数据

6.4.6.8. WriteData

功能说明

WriteData 命令用于将数据写入配置区或数据区。

命令报文

编码	长度	值（HEX）
Opcode	1	12
P1	1	00：配置区4字节写 80：配置区32字节写 02：数据区4字节写 82：数据区32字节写
P2	2	参见 ：6.45 地址参数表
Data	4 or 32	

响应报文

名称	长度	值（HEX）
Response	1	操作失败，则返回一个字节错误码 操作成功，则返回00

6.4.6.9. SecureBoot

功能说明

SecureBoot 命令用于对主机传入的代码摘要和签名数据进行验签。由 Config.SecureBoot.pubKey 指定验签公钥。

命令报文

编码	长度	值（HEX）
Opcode	1	80

P1	1	05：使用提前配置好的公钥对主机传入的数据进行验签
P2	2	0000
Data	96	32字节代码摘要+64字节签名

响应报文

名称	长度	值（HEX）
Response	1	操作失败，则返回一个字节错误码 操作成功，则返回00

6.4.6.10. SHA

功能说明

SHA 命令用于 SHA-256 摘要计算。

命令报文

编码	长度	值（HEX）
Opcode	1	47
P1	1	00：创建一个 multi-part hash 操作 01：添加 message 块到 multi-part hash 操作中 C2：完成 message 的 hash计算
P2	2	0000~0040
Data	0~64	在更新和完成操作阶段最多可传入64个字节的消息

响应报文

名称	长度	值（HEX）
Response	1	操作失败，则返回一个字节错误码 操作成功，则返回32字节摘要

6.4.6.11. ECDSASign

功能说明

ECDSASign 命令用于 ECDSA 签名，需要先用 Nonce 命令将消息装入 TempKey 中。

命令报文

编码	长度	值（HEX）
Opcode	1	41
P1	1	80
P2	2	0000~000F：指示签名私钥密钥槽
Data	0	

响应报文

名称	长度	值（HEX）
Response	1	操作失败，则返回一个字节错误码 操作成功，则返回64字节签名

6.4.6.12. ECDSAVerify

功能说明

ECDSAVerify 命令用于 ECDSA 验签，需要先用 Nonce 命令将消息摘要装入 TempKey 中。

命令报文

编码	长度	值（HEX）
Opcode	1	45
P1	1	00
P2	2	0000~000F：指示验签公钥密钥槽
Data	64	签名

响应报文

名称	长度	值（HEX）
Response	1	操作失败，则返回一个字节错误码 操作成功，则返回00

6.4.6.13. SM4

功能说明

SM4 命令使用指定密钥槽或 Tempkey 中的密钥对输入的数据进行 SM4 加密或解密。单组密钥长度为 16 字节，可以将多组密钥存在一个指定的槽内，每 16 字节为一组，单个密钥槽中最多可存 4 组密钥。

命令报文

编码	长度	值（HEX）
Opcode	1	71
P1	1	00：使用第一组密钥对明文进行加密 40：使用第二组密钥对明文进行加密 80：使用第三组密钥对明文进行加密 C0：使用第四组密钥对明文进行加密 01：使用第一组密钥对密文进行解密 41：使用第二组密钥对密文进行解密 81：使用第三组密钥对密文进行解密 C1：使用第四组密钥对密文进行解密
P2	2	0000~000F：密钥所在的槽 FFFF：使用TempKey
Data	16	明文（加密）或密文（解密）

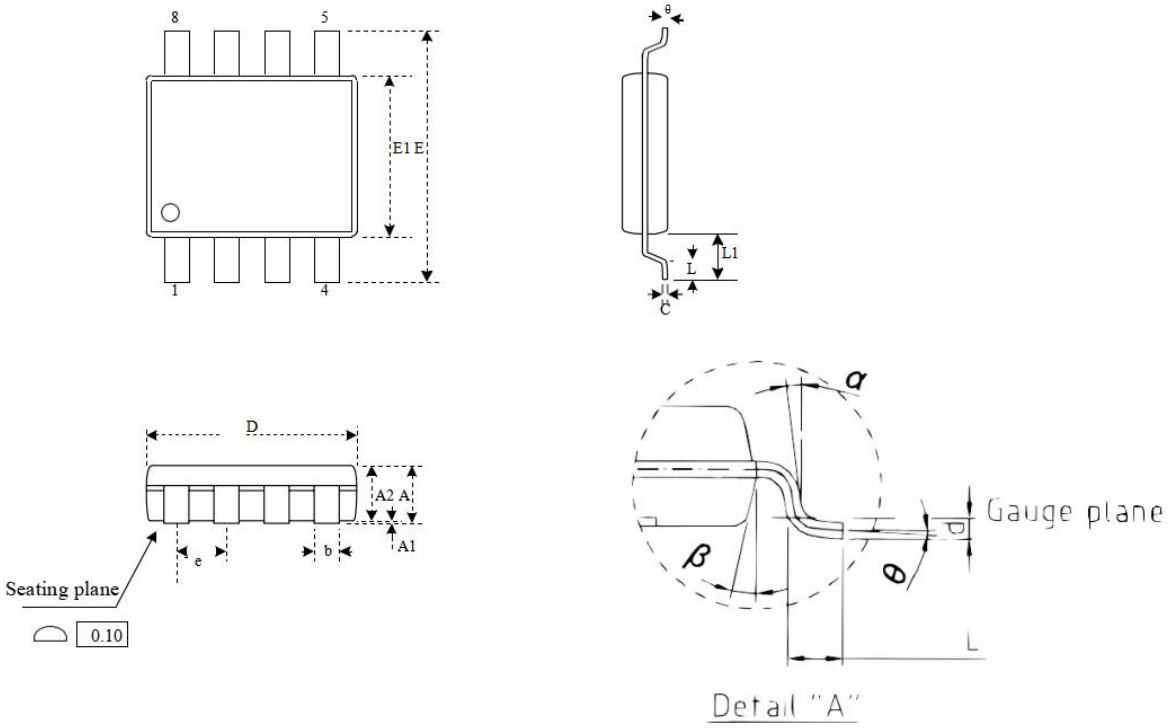
响应报文

名称	长度	值（HEX）
Response	1 or 16	操作失败，则返回一个字节错误码 操作成功，则返回16字节密文（加密）或明文（解密）

七、封装规格

7.1. SOP8

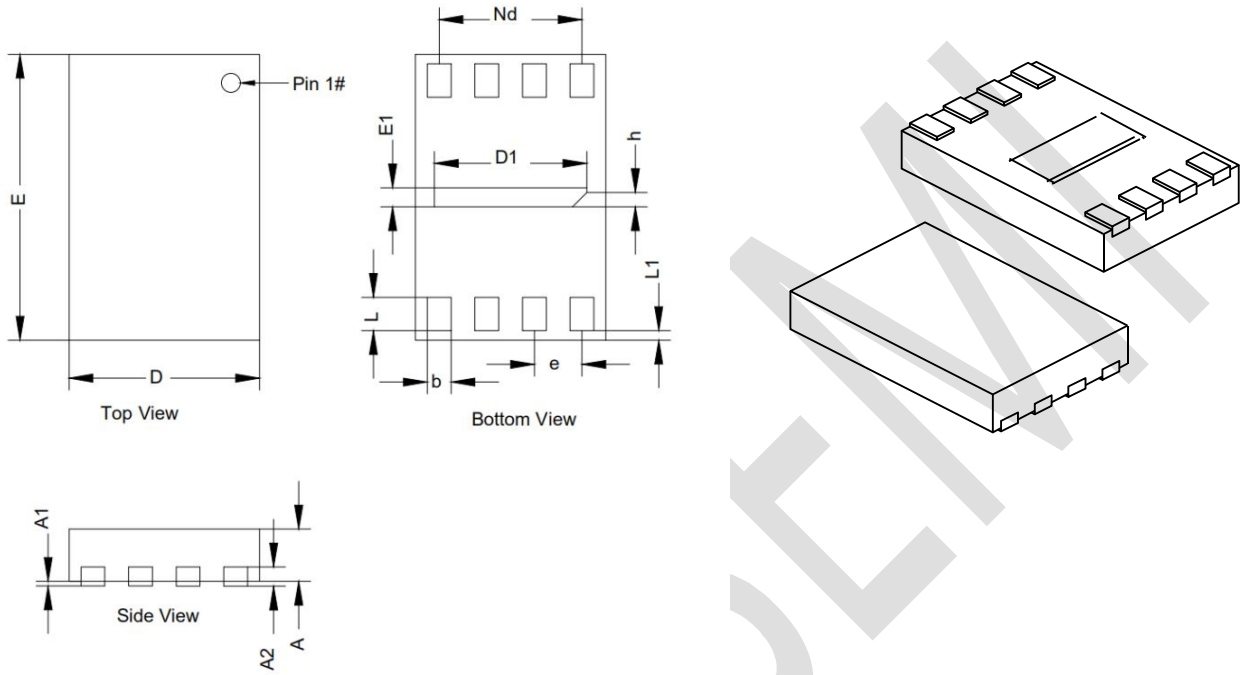
Narrow, 3.90 mm (.150 In.) Body [SOP8]



COMMON DIMENSIONS (UNITS OF MEASURE=MILLIMETERS)															
Symbol / **Unit**		**A**	**A1**	**A2**	**b**	**C**	**D**	**E**	**E1**	**e**	**L**	**L1**	**θ**	**α**	**β**
mm	**Min**	1.35	0.05	1.35	0.31	0.15	4.77	5.80	-	-	0.40	0.85	0°	6°	11°
	Nom	-	-	-	-	-	4.90	6.00	3.90	1.27	-	1.06	-	7°	12°
	Max	1.75	0.25	1.55	0.51	0.25	5.03	6.20	-	-	0.90	1.27	8°	8°	13°
Inch	**Min**	0.053	0.002	0.053	0.012	0.006	0.188	0.228	-	-	0.016	0.033	0°	6°	11°
	Nom	-	-	-	0.016	-	0.193	0.236	0.154	0.050	-	0.042	-	7°	12°
	Max	0.069	0.010	0.061	0.020	0.010	0.198	0.244	-	-	0.035	0.050	8°	8°	13°

7.2. DFN8

2x3mm body [DFN8]

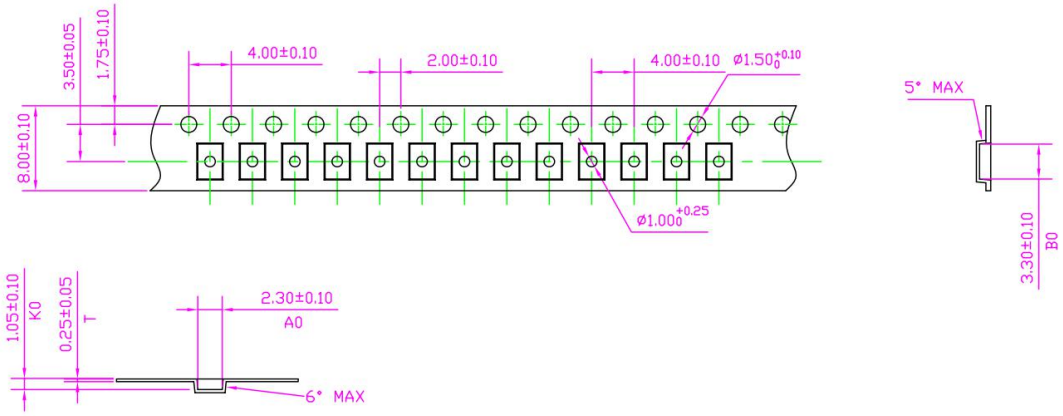


COMMON DIMENSIONS (UNITS OF MEASURE=MILLIMETERS)			
SYMBOL	MILLMETERS		
	MIN	NOM	MAX
A	0.50	0.55	0.60
A1	0.00	0.02	0.05
A2	0.152REF		
b	0.20	0.25	0.30
D	1.95	2.00	2.05
E	2.95	3.00	3.05
D1	1.50	1.60	1.70
E1	0.10	0.20	0.30
e	0.50BSC		
Nd	1.50BSC		
L	0.30	0.35	0.40
L1	0.05	0.10	0.15
h	0.10	0.15	0.20

7.3. 丝印对照表

圆点：1 号角位置
左上方：
第 1 字符：年份序号
第 2-3 个字符：生产周
第 4 个字符：批次号
第 5 个字符：封装厂
第 6 个字符：WAFER 版本
第 7 个字符：产品版本

7.4. 卷带尺寸（DFN8）



NOTE ：
1. 所有尺寸依国际EIA-481-3标准.
2. 任意10个棘轮孔的累积误差不超过 ±0.2mm.
3. 载带长度方向100mm距离的非平行度不可超过1mm.

2020年01月16日

单位 UNITS	mm	比例 SCALE	1/1	材质 MATERIAL		图号 DWG.NO.		图名 NAME	QFN-2*3

开发支持

- 定制与集成支持
- SDK

应用产品

- 智能家居设备
- IOT 节点设备
- 区块链设备
- 电子耗材