ECC608-TMNGTLS CryptoAuthentication™数据手册

简介

ECC608-TMNGTLS 是 ATECC608 的 Trust Manager 预配置型号。ECC608-TMNGTLS 器件将与由 Kudelski IoT 提供支持的 keySTREAM™软件即服务（Software-as-a-Service，SaaS）结合使用。该器件预先配置了一组加密密钥，用于连接到 keySTREAM SaaS。当包含 ECC608-TMNGTLS 的 IoT 设备被部署到市场中时，将连接到 keySTREAM SaaS，以便在“现场”为设备配置其自定义 PKI，从而将 IoT 设备的所有权移交给预期所有者。该解决方案真正实现了零接触，因为无需物理干预机密信息交换。加密密钥现在可以进行远程动态管理，同时在安全身份验证 IC 的物理边界内受到保护。该解决方案可确保在 IoT 设备被部署后遵循与密钥管理相关的产品生命周期管理安全实践。

本数据手册提供了 ECC608-TMNGTLS 器件的槽和密钥配置信息。该信息定义了每个数据区域槽的访问策略。本文档中提供了有限的命令和 I/O 工作信息。此外，还设有专门的章节介绍了可帮助开发用户应用程序的 Microchip 软硬件工具。指导用例可在 Microchip 的 Trust Platform Design Suite（TPDS）中使用。所需的机密信息和私钥通过 keySTREAM SaaS 在现场配置。

特性

- 完全指定的配置区
- 具有可一次性更改 I^2C 地址的 I^2C 接口
- JIL 高评级——经验证符合 JIL Application of Attack Potential to Smartcards and Similar Devices（版本 3.1）
- 通过内部高质量 NIST SP 800-90A/B/C 真随机数生成器（True Random Number Generator，TRNG）NIST CMVP ESV 认证
- 与 Kudelski keySTREAM SaaS 配合使用的预定义槽访问策略：
  - ECC P-256 器件标识密钥
  - ECC P-256 认证私钥
  - 客户指定标识信息
- 用于现场配置的槽：
  - 器件和签名人压缩证书槽
- 1.8V 至 5.5V I/O 电压，2.0V 至 5.5V 电源电压
- 标准工业级温度范围：-40°C 至+85°C
- 30 nA 的标称休眠电流
- 提供 8 焊盘 UDFN 和 8 引脚 SOIC 封装，原型器件固定提供一卷 10 件样片，生产订单的最小订购量（Minimum-Order-Quantity，MOQ）为 2k 件

用例

- 安全 IoT TLS 1.2 和 1.3 连接，包括自定义根 CA 设置及相关 PKI
- 动态证书管理，包括轮换、撤销和更新
- 安全引导
- 端到端数据保护

- 私钥轮换，确保安全敏捷性

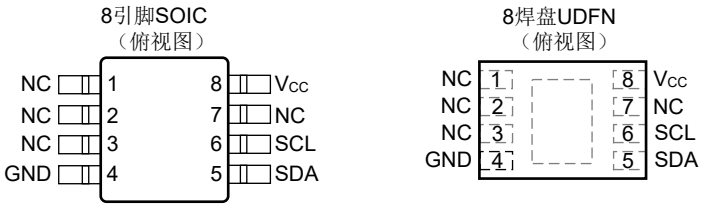
目录

1. 引脚配置和引脚分配

表 1-1. 引脚配置

引脚	功能
NC	无连接
GND	地
SDA	I^2C 串行数据
SCL	I^2C 串行时钟输入
V_{CC}	电源

图 1-1. UDFN 和 SOIC 引脚分配



注：建议将 UDFN 背面的焊盘连接至 GND。

相关信息

10.2. 8 焊盘 UDFN
10.3. 8 引脚 SOIC

2. Trust Manager 体验

ECC608-TMNGTLS 安全身份验证 IC 专注于将 IoT 产品的硬件安全性打造成为一种自助式体验，同时在项目的整个生命周期内保持高级别的安全性。

keySTREAM SaaS 可提供什么

keySTREAM SaaS 服务提供必要的 HSM 基础架构来设置根 CA 及相关 PKI，并在现场将其随 TLS 加密密钥、数据和证书一起配置到 ECC608-TMNGTLS 的安全边界中。这些加密凭证现在可以在整个产品生命周期内得到主动管理。该解决方案可以实现：

- 证书管理，以确保对任何云平台执行安全身份验证。证书更新或轮换，以确保在证书到期时不会断开 IoT 产品的连接。最终的结果是降低器件管理成本和复杂度。
- 与基础架构无关的 SaaS（IaaS）与开箱即用的 AWS®和 Microsoft Azure®配合使用。
- 在 keySTREAM HSM 中以经济高效的方式托管加密密钥，并提供相关的访问和维护。

keySTREAM SaaS 产品提供了节省空间的嵌入式库（keySTREAM Trusted Agent KTA），能够适应从存储器受限的 MCU 到 MPU 的各类产品。因此，不需要在存储器方面花费大量成本即可在各种不同复杂度的器件上实现安全性。这些工具与电信级云托管平台相结合，旨在满足 IoT 产品的广泛需求。

Trust Manager 流程

上手使用 ECC608-TMNGTLS 相对来说非常简单。

1. 注册 Kudelski IoT 帐户即可访问 keySTREAM 安全管理服务。提供与您的公司和项目相关的惟一信息，以确保您的产品具有无法克隆的惟一标识。根据 keySTREAM SaaS 中的自动索赔流程，请务必记录在 Microchip 订购系统中使用的购买者的电子邮件地址。
2. 订购 ECC608-TMNGTLS 器件。Microchip 提供 10 件装样片，旨在降低器件评估的入门成本。这些器件都是现成的，购买前不需要任何手动配置。keySTREAM SaaS 能够验证具体器件是否已由 Microchip 配置为 keySTREAM SaaS 远程管理。
3. 使用 keySTREAM SaaS 创建自定义根 CA 及相关 PKI。
4. 使用 keySTREAM SaaS 服务领取通过 MicrochipDirect 购买的器件。之后，在嵌入式系统连接到 Kudelski keySTREAM SaaS 时进行现场配置。keySTREAM SaaS 服务可用于在托管和管理的 HSM 中创建自定义 PKI、输入惟一的客户信息、创建证书，以及创建用于安全通信的 I/O 保护密钥。
5. 在现场部署产品。
6. 使用现场管理功能轮换密钥，以及/或者更新或轮换证书。

3. EEPROM 存储器和数据区域访问策略

EEPROM 存储器共有 1400 字节，分为以下几个区域：

表 3-1. ECC608-TMNGTLS EEPROM 区域

区域	说明	命名法
配置	128 字节（1024 位）EEPROM 区域，包含： • 器件配置 • 槽访问策略信息 • 计数器值 • 器件序列号 • 锁定信息 LockConfig 字节已设置。无法向该区域直接写入任何内容。始终可读取该区域。	Config[a:b] = 配置区域某个字段内的字节范围
数据	1208 字节（9.7 Kb）区域，分为 16 个通用只读或读/写存储器槽。配置区域字节定义的访问策略信息决定了每个槽的访问方式。ECC608-TMNGTLS 器件中每个数据槽的访问策略均已设置，并且配置区域定义的槽访问策略完全生效。	Slot[YY] = 存储在数据区域的 Slot YY 中的全部内容
一次性编程（One-Time-Programmable，OTP）	64 字节（512 位）区域，分为两个块，每个块 32 字节。对于 ECC608-TMNGTLS，该区域预装了一个预定义值。该区域无法修改，但可以随时读取。有关更多信息，请参见 3.3. ECC608-TMNGTLS EEPROM 一次性编程（OTP）区域。	OTP[bb] = OTP 区域内的一个字节，而 OTP[aa:bb] 表示一个字节范围

表 3-2. 文档术语

本文档中讨论的术语具有以下含义：

术语	含义
块	特定存储区域的单个 256 位（32 字节）区域。工业标准 SHA-256 文档还使用术语“块”来表示报文输入的 512 位片段。在本文档内，仅当描述哈希输入报文时使用此约定。
KeyID	KeyID 相当于指定为保存密钥值的槽的编号。Key1（有时称为 key[1]）存储在 Slot[1]中，依此类推。当全部 16 个槽均可保存密钥时，配置为允许明文读取的槽通常不会被加密命令用作私钥或机密信息密钥。
mode[b]	表示参数模式的 bit（b）。
SRAM	包含输入和输出缓冲区以及内部状态存储单元。用户无法直接访问该存储器。
字	从块读取或写入块的单个 4 字节数据字。字是数据访问的最小单位。
LSB/MSB	最低有效字节/最高有效字节。
LSb/MSb	最低有效位/最高有效位。

相关信息

3.1. ECC608-TMNGTLS 配置区域

3.2. 数据区域和访问策略

3.3. ECC608-TMNGTLS EEPROM 一次性编程（OTP）区域

3.1 ECC608-TMNGTLS 配置区域

ECC608-TMNGTLS 配置是固定的，客户无法进行修改。有关如何配置器件的信息显示在下方或槽信息中。通过 keySTREAM SaaS 在现场配置密钥。

器件配置信息

- 每个器件的序列号都是惟一的，存储在 Byte[0:3, 8:12]中。Byte[0:1]为 0x01 0x23，Byte[8]为 0x01。所有其他字节都是惟一的。
- 默认的 7 位 I^2C 地址为 0x38。用于写操作和读操作的 I^2C 8 位地址字节分别为 0x70 和 0x71。可使用 `UpdateExtra` 命令改写 I^2C 地址。

> **重要：**ECC608-TMNGTLS 的默认 I^2C 地址与标准 ECC608 器件的不同。

- 除安全引导公钥（Slot 15）、安全引导摘要（Slot 13）和 I/O 保护（Slot 7）之外的所有数据槽均由 Kudelski 管理。
- 使能 AES128 操作。
- ChipMode 功能
  - 时钟分频器设置为最大执行时间速度。
  - 看门狗定时器（Watchdog Timer，WDT）的最大超时设置为 1.3s。
  - I/O 电压设置为固定参考电压；因此，主机处理器可以在低于 ECC608-TMNGTLS 器件电压的电压下工作。
  - 使能备用 I^2C 地址设置。
- 安全引导功能
  - 使能 FullStore 摘要模式。
  - 安全引导 ECC P-256 公钥存储在 Slot 15 中，并在制造时装载。
  - 安全引导摘要存储在 Slot 13 中。
  - 不需要但建议使用随机 Nonce。
  - 禁止安全引导持久锁存器。
  - 用于对命令的输出进行加密的 I/O 保护密钥。
- 芯片选项功能
  - 存储在 Slot 7 中的密钥可用作 I/O 保护密钥。
  - KDF 函数的输出将采用明文形式，但可基于 `KDF` 命令的模式进行加密。
  - 使能 KDF AES 模式。
  - ECDH 主机密信息的输出将采用明文形式，但可基于 `ECDH` 命令的模式进行加密。
  - 无论何时因运行状况测试失败而导致命令失败后，运行状况测试失败位都会清零。如果失败征兆是暂时的，则在第二次运行时，命令将会通过。
  - 禁止上电自检。如果需要，必须明确运行自检。
  - 无论何时因运行状况测试失败而导致命令失败后，运行状况测试失败位都会清零。如果失败征兆是暂时的，则在第二次运行时，命令将会通过。
- 单调计数器可供系统使用，并且未关联到任何密钥。
- 配置区域永久锁定，禁止更新配置。

相关信息

3.2.3. ECC608-TMNGTLS 槽配置汇总

3.2 数据区域和访问策略

以下各节介绍了与每个槽关联的详细访问策略信息。实际访问策略信息存储在 EEPROM 配置区域的槽和密钥配置段中。每个数据区域槽都具有与其关联的 2 个槽配置字节和 2 个密钥配置字节。这 4 个字节一起为每个槽创建访问策略。存储在槽中的数据的实际类型由该槽的访问策略确定。

3.2.1 数据区域数据类型

以下各节提供了有关可以存储在 ECC608-TMNGTLS 数据槽中的各个数据类型的详细信息。

3.2.1.1 私钥

ECC P-256 私钥是 ECC608-TMNGTLS 的 ECC 安全性的基本构件。这些密钥是私密的，并且对于每个器件都是惟一的，无法读取。ECC 私钥由安全元件的 TRNG 随机生成，并安全地保存在配置为 ECC 私钥的槽中。

主私钥

这是主身份验证密钥，存储在 Slot 0 中。每个器件都有自己惟一的私钥。只要 Slot 0 未锁定即可修改密钥。

由以下两种主椭圆曲线函数生成该密钥：

- 用于身份验证的 ECDSA 签名
- 用于密钥协议的 ECDH。如果需要对 ECDH 输出进行加密，则需要先设置 I/O 保护密钥。有关设置的详细信息，请参见 3.2.1.7. I/O 保护密钥。

该私钥是生成相应公钥和 X.509 证书的基础。

辅助私钥

Slot 1 和 Slot 3 中存储可供附加服务使用的附加私钥；这些密钥保留供 Kudelski 工具使用。

由以下主椭圆曲线函数生成此类密钥：

- 用于身份验证的 ECDSA 签名。
- 用于密钥协议的 ECDH。如果需要对 ECDH 输出进行加密，则需要先设置 I/O 保护密钥。有关设置的详细信息，请参见 3.2.1.7. I/O 保护密钥。
- GenKey，用于使用在内部生成的新随机私钥覆盖槽。

这些其他密钥可以用内部生成的新私钥覆盖（GenKey 命令模式 = 0x04），以使能密钥删除、密钥轮换和远程配置。这些密钥也是槽可锁定的（KeyConfig.Lockable 位设置为零），这意味着 Lock 命令可用于 SlotLock 模式，以使当前密钥成为永久密钥，并防止 GenKey 命令更改该密钥。更改密钥时，需要通过密钥认证来确保向另一个系统提供的器件的新公钥实际上来自相关器件。

密钥认证

Slot 1 中的私钥配置为仅内部签名密钥，这意味着，它只能签名由 GenKey 或 GenDig 命令在内部生成的报文，并且不能用于签名任意外部报文。通过此功能，可将内部签名密钥用于向任何已知（并信任）内部签名公钥的系统证明器件中的密钥及其配置/状态。

3.2.1.2 公钥

公钥与 ECC 私钥相关联。每个 ECC 私钥将具有自己的惟一公钥。与器件上存储的私钥相关的公钥可使用 GenKey 命令检索。与芯片外存储的 ECC 私钥相关的公钥可存储在器件中为公钥配置的槽中。

对于 ECC608-TMNGTLS，公钥已存储在 Slot 11、Slot 14 和 Slot 15 中。

3.2.1.3 证书存储

ECC608-TMNGTLS 存储围绕安全保存密钥进行。由于 X.509 证书的大小通常比单个 ECC608-TMNGTLS 器件槽大，因此使用压缩格式。该技术更应被称为部分证书，因为它在器件上存储动态证书信息，并施加了一些限制。动态信息是可以随器件更改的证书内容（例如，公钥和有效日期等）。固件应具有证书定义与

完整 X.509 证书的模板，证书中包含静态信息（对于所有证书均相同的数据）以及有关如何利用压缩证书中的动态信息重新编译完整证书的说明。

以下应用笔记记录了压缩证书格式：《压缩证书定义》（DS20006367A_CN）。

CryptoAuthLib 库还包含用于处理压缩证书的 API。

器件证书

器件证书包含与实际最终器件关联的信息。对于 ECC608-TMNGTLS，压缩器件证书存储在 Slot 10 中。

签名人证书

签名人证书包含与用于签名器件证书的签名人证书颁发机构相关的信息。对于 ECC608-TMNGTLS，压缩签名人证书存储在 Slot 12 中。此外，还需要添加签名人公钥来重新编译完整的签名人证书。

签名人公钥

签名人公钥用于验证签名人和与签名人压缩证书关联的信息。对于 ECC608-TMNGTLS，签名人公钥存储在 Slot 11 中。

下表列出了与 ECC608-TMNGTLS 中的证书关联的所有槽：

槽	说明
0	主私钥。在模式 = 0x00 时，可使用 GenKey 命令随时生成公钥。
10	器件证书。以压缩格式存储在此处。
11	签名人公钥。
12	签名人证书。以压缩格式存储。

对于 ECC608-TMNGTLS，这些槽只要未锁定就可以进行改写。

相关信息

3.1. ECC608-TMNGTLS 配置区域

3.2.4. 详细的 ECC608-TMNGTLS 槽访问策略

5.5.3. 证书存储

3.2.1.4 安全引导

为 ECC608-TMNGTLS 使能 SecureBoot 命令。这样，系统便可在执行完全引导之前通过自举程序加密验证其固件。该功能还可用于在全新固件映像被装载之前对其进行验证。

安全引导功能需要在使用之前构建 ECC P-256 固件签名密钥。私钥将由固件开发人员持有，用以对固件映像进行签名。公钥将被写入安全引导公钥槽，并且该槽将在合同制造商工厂制造期间被锁定以设为永久。

要实现安全引导，需要多个数据槽。

安全引导摘要

安全引导摘要是通过固件应用程序代码计算的 32 字节 SHA-256 摘要。每次更新固件时，都需要更新该摘要。对于 ECC608-TMNGTLS，摘要存储在 Slot 13 中。

安全引导公钥

安全引导公钥用于执行验证功能来验证安全引导摘要和签名。安全引导公钥存储在 Slot 15 中。

I/O 保护密钥

I/O 保护密钥存储在 Slot 7 中，可用于保护 SecureBoot 命令输出。

相关信息

3.1. ECC608-TMNGTLS 配置区域

3.2.4. 详细的 ECC608-TMNGTLS 槽访问策略

6.2.3. SecureBoot 命令

3.2.1.5 机密信息密钥

Slot 5 可用于存储 32 字节的机密信息密钥。该密钥可与 ECC608-TMNGTLS 的对称密钥命令（GenDig、MAC、CheckMac、KDF、SHA/HMAC 和 AES）一起使用。

必须使用存储在 Slot 6 中的加密密钥以加密写入的方式写入该密钥。

3.2.1.6 AES 密钥存储

ECDH 和 KDF 等命令输出对称密钥。上述命令还可将这些密钥保存到一个槽中以实现安全存储并用作 AES 密钥。AES 密钥存储槽已设置为这些密钥的目标槽。在数据 Slot 9 中，可以存储 1 到 4 个 16 字节的 AES128 密钥。

3.2.1.7 I/O 保护密钥

Verify、ECDH、SecureBoot 和 KDF 命令还可选择使用 I/O 保护功能来加密某些参数并（通过 MAC）验证一些响应。这有助于防止物理 I^2C 总线上出现中间人攻击。在安全引导期间，I/O 保护密钥也可用于防止重放攻击。但是，为了能够使用该功能，MCU 和 ECC608-TMNGTLS 需要事先生成并保存惟一的 I/O 保护密钥，实际上是将 MCU 和 ECC608-TMNGTLS 器件彼此配对。必须在客户生产厂内进行配对过程。

I/O 保护密钥生成：

1. MCU 使用随机命令来生成一个随机的 32 字节 I/O 保护密钥。
2. MCU 将 I/O 保护密钥保存在其内部闪存中。
3. MCU 将 I/O 保护密钥写入 I/O 保护密钥槽中。
4. MCU 槽锁定该槽以使 I/O 保护密钥具有永久性。

作为配对检查，MCU 可以使用 MAC 命令向 I/O 保护密钥发出质询，并验证闪存中存储的 I/O 保护密钥是否与 ECC608-TMNGTLS 中的密钥匹配。

3.2.1.8 通用数据存储

如果未实现安全引导且 Slot 15 不包含安全引导公钥，则该槽可用于存储通用数据。该槽可用于存储允许公开访问的任何数据，并且始终可采用明文形式读取和写入。

3.2.2 槽配置术语

以下部分提供了一组用于讨论配置选项的术语。

术语	说明
AES 密钥	槽可用作 AES 命令的密钥源。ECC608-TMNGTLS 的 AES 密钥为 128 位长。
始终写入	可以使用 Write 命令以明文方式写入槽。
明文读取	槽视为公共（非机密）的，可以使用 Read 命令以明文方式读取其内容。
ECDH	椭圆曲线 Diffie Hellman。私钥可与 ECDH 命令一起使用。
外部签名	私钥可用于对外部（任意）报文进行签名。
内部签名	私钥可用于对 GenKey 或 GenDig 命令生成的内部报文进行签名。用于证明器件的内部密钥和配置。
可锁定	槽可以在将来的某个时间锁定。锁定后，槽内容将无法更改（仅供读取/使用）。
不允许读取	槽被视为机密，无法使用 Read 命令读取其内容。私钥和对称机密信息必须始终配置为“不可读取”。
不允许写入	无法使用 Write 命令更改槽。
永久	私钥是永久的/不可更改。它是出厂配置期间在内部生成的。
可更新	私钥稍后可由内部生成的新随机私钥覆盖。其初始值是出厂配置期间在内部生成的。

3.2.3 ECC608-TMNGTLS 槽配置汇总

ECC608-TMNGTLS 具有 16 个槽，均作为 Trust Manager 解决方案的一部分配置为特定用途。这些槽分为几种类型，在下表中的“槽类型”一列指定。这些槽类型的定义如下：

- K = 仅供 Kudelski 使用的 keySTREAM SaaS 槽
- P = 通过 keySTREAM SaaS 配置的应用槽。该信息供客户应用使用，但受 keySTREAM SaaS 控制。
- C = 客户配置槽。该信息仅对客户已知，并在客户的生产线中更新。
- A = 应用特定配置槽。该槽在运行时配置。
- R = 保留。在创建本数据手册时尚未使用，但可能用于未来的应用。

槽	槽类型	密钥名称	说明
0	P	器件标识密钥	用于对存储在 Slot 10 中的器件压缩证书进行签名的主私钥。
1	K	认证密钥	供 Kudelski 用于证明器件真实性的私钥。只有 Kudelski 知道相应的公钥。
2	K	印章标识 ID	存储在该槽中的惟一配置文件用户 ID（User ID，UID）。
3	K	非对称密钥	由 Kudelski 管理和保留
4	K	对称密钥	由 Kudelski 管理和保留
5	R	用于现场配置的对称密钥	用于保存客户对称密钥的槽。该槽只能通过 keySTREAM™ SaaS 更新。该槽设置为加密写入，WriteKey 位于 Slot 6 中。
6	R	加密写入密钥	用于 Slot 5 和 Slot 14 的加密 WriteKey（在 Micorchip 工厂中配置）。父密钥仅对 Kudelski 已知。存储的密钥多样化。
7	C	IO 保护密钥	用于保存客户 I/O 保护密钥的槽。该槽由客户在其生产线中更新。
8	K	keySTREAM SaaS 引导流程数据	用于多个 keySTREAM SaaS 操作的 Kudelski 特定数据。
9	A	AES128 密钥	可更新的客户 AES128 密钥。
10	P	器件压缩证书	压缩的器件证书。
11	P	签名人公钥	与 Kudelski 签名人关联的公钥。
12	P	签名人压缩证书	Kudelski 压缩签名人证书。
13	P	安全引导摘要	用于保存安全引导摘要（存储摘要模式）的槽。只能使用安全引导命令在内部更新。
14	R	用于现场配置的公钥。	用于保存客户特定公钥的槽。该槽只能通过 keySTREAM SaaS 更新。该槽设置为加密写入，WriteKey 位于 Slot 6 中。
15	P	安全引导公钥或 C-Data	用于保存客户安全引导公钥的槽。该槽需在客户的生产线中配置。

相关信息

3.2.4. 详细的 ECC608-TMNGTLS 槽访问策略

3.2.4 详细的 ECC608-TMNGTLS 槽访问策略

每个数据槽的 ECC608-TMNGTLS 槽访问策略均已经过完全配置。每个槽都有指定用途。在大多数情况下，需要使用所有槽来确保给定用例安全正常地运行。这些槽分为 K 槽和 C 槽，K 槽主要供 Kudelski 用作 keySTREAM SaaS 操作环境的一部分，C 槽供客户用作特定用途。

槽锁定选项

槽锁定选项针对各个槽调用，将属于以下两种类型之一。

槽可锁定 槽锁定选项置 1 的槽允许最终用户在初始制造阶段之后的将来某个时候锁定槽。这可以用来在 Microchip 之外的最终制造步骤中或由最终用户设置密钥或数据。可使用 `Lock` 命令锁定槽。槽一旦锁定，就无法再对其中的数据进行修改。

永久锁定 永久锁定的槽在离开 Microchip 制造厂后将无法更新。在配置这些器件之前，必须将正确的数据或密钥提供给 Microchip。

详细的槽配置

下表更加详细地说明了器件上各个已配置槽的槽配置和密钥配置设置。“已使能功能的说明”一列提供密钥和槽配置的相关信息。具体的密钥类型显示在密钥名称后面的（）中。关于密钥类型说明，可参见 3.2.3. ECC608-TMNGTLS 槽配置汇总。

表 3-3. Slot 0：器件标识密钥（P）

槽	配置值	已使能功能的说明
0	密钥：	• 包含 P256 NIST ECC 私钥。 • 可以生成私钥。 • 可以根据私钥生成公钥。 • 运行命令之前需要随机 Nonce。 • 槽可以单独锁定。
	槽：	• 槽是机密的。 • 可用于对外部报文进行签名。 • 可用于通过 ECDH 命令生成会话密钥。

表 3-4. Slot 1：认证密钥（K）

槽	配置值	已使能功能的说明
1	密钥：	• 包含 P256 NIST ECC 私钥。 • 密钥在配置时写入。 • 永远无法生成相应的公钥。
	槽：	• 槽是机密的。 • 可以对通过 GenDig 或 GenKey 命令在内部生成的报文进行签名。

表 3-5. Slot 2：印章标识 ID（K）

槽	配置值	已使能功能的说明
2	密钥：	• 包含用于标识用户的数据，并将包含器件配置文件 UID。 • 槽可以单独锁定。
	槽：	• 始终允许明文读取。 • 始终允许明文写入。

表 3-6. Slot 3：非对称密钥（K）

注：该槽仅供 Kudelski IoT 使用

槽	配置值	已使能功能的说明
3	密钥：	• 包含 P256 NIST ECC 私钥。 • 始终可以生成相应的公钥。 • 需要随机 Nonce。 • 槽可以单独锁定。
	槽：	• GenKey 可用于在锁定之前在该槽中生成新的 ECC 私钥。 • 槽是机密的。 • 可对外部报文进行签名。 • 可用于通过 ECDH 命令生成会话密钥。

表 3-7. Slot 4：对称密钥（K）

注：该槽仅供 Kudelski IoT 使用

槽	配置值	已使能功能的说明
4	密钥：	• 槽将包含 AES 会话密钥。 • 槽使用存储在 Slot 3 中的密钥保存 ECDH 命令的输出。 • 槽不可单独锁定。
	槽：	• 槽是机密的，无法读取。 • 槽可以直接写入。

表 3-8. Slot 5：用于现场配置的对称密钥（R）

槽	配置值	已使能功能的说明
5	密钥：	• 包含 AES 密钥。 • 始终需要随机 Nonce。
	槽：	• 内容是机密的，永远无法读取。 • 可以使用 Slot 6 中的密钥将加密数据写入该槽。 • 加密写入需要 MAC。

表 3-9. Slot 6：加密写入密钥（R）

槽	配置值	已使能功能的说明
6	密钥：	• 包含用于加密数据的密钥。 • 使用该密钥时，需要随机 Nonce。 • 该槽永久锁定。
	槽：	• 不允许读取该槽。 • 始终不允许写入该槽。

表 3-10. Slot 7：IO 保护密钥（C）

槽	配置值	已使能功能的说明
7	密钥：	• 包含用于加密 I/O 数据的密钥。 • 使用该密钥之前需要随机 Nonce。 • 槽可以单独锁定。
	槽：	• 该槽无法读取。 • 允许对该槽进行明文写入。

⚠ CAUTION 通常，必须使 Slot 7 中存储的 I/O 保护密钥保持“槽可锁定”状态。在大多数情况下，I/O 保护密钥对于每个器件通常都是惟一的。如果对于某些用例，所有器件的 I/O 保护密钥均相同，则可以选择永久锁定选项。

表 3-11. Slot 8：keySTREAM™ SaaS 引导流程数据（K）

槽	配置值	已使能功能的说明
8	密钥：	• 保留供 Kudelski 用于为客户提供引导流程的数据槽。 • 槽可锁定。
	槽：	• 允许对该槽进行明文读取。 • 在该槽未锁定时允许对其进行明文写入。

表 3-12. Slot 9：AES 密钥（A）

槽	配置值	已使能功能的说明
9	密钥：	• 槽最多可存储 4 个 AES 128 位对称密钥。
	槽：	• 槽是机密的，无法读取密钥。 • 允许对该槽进行明文写入。

表 3-13. Slot 10：器件压缩证书（P）

槽	配置值	已使能功能的说明
10	密钥：	• 槽定义为存储其他数据。 • 槽可以单独锁定。
	槽：	• 数据始终可采用明文形式读取。 • 数据可采用明文形式写入（除非槽已锁定）。

表 3-14. Slot 11：签名人公钥（P）

槽	配置值	已使能功能的说明
11	密钥：	• 该槽中存储与签名人证书相关的 P256 NIST ECC 公钥。 • 槽可以锁定。
	槽：	• 数据始终可采用明文形式读取。 • 数据可采用明文形式写入（除非槽已锁定）。

表 3-15. Slot 12：签名人压缩证书（P）

槽	配置值	已使能功能的说明
12	密钥：	• 槽定义为存储其他数据。 • 槽可以单独锁定。
	槽：	• 数据始终可采用明文形式读取。 • 数据可采用明文形式写入（除非槽已锁定）。

表 3-16. Slot 13：安全引导摘要（P）

槽	配置值	已使能功能的说明
13	密钥：	• 槽定义为保存安全引导摘要。 • 槽不可单独锁定。
	槽：	• 无法从该槽读取数据。 • 无法直接向该槽写入数据。可以使用安全引导命令来存储摘要。

表 3-17. Slot 14：用于现场编程的公钥（R）

槽	配置值	已使能功能的说明
14	密钥：	• 用于现场编程的 P256 NIST ECC 客户公钥。 • 槽在配置时解锁。
	槽：	• 数据始终可采用明文形式读取。 • 可以使用 Slot 6 中的密钥通过加密写入的方式将数据写入槽。 • 加密写入必须包含 MAC。

表 3-18. Slot 15：安全引导公钥或 C-Data（P）

槽	配置值	已使能功能的说明
15	密钥：	• 用于通过 `Verify` 命令验证安全引导操作的 P256 NIST ECC 客户公钥。 • 槽可以单独锁定。
	槽：	• 数据始终可采用明文形式读取。 • 数据可采用明文形式写入（除非槽已锁定）。

相关信息

3.2.1. 数据区域数据类型

以下各节提供了有关可以存储在 ECC608-TMNGTLS 数据槽中的各个数据类型的详细信息。

3.3 ECC608-TMNGTLS EEPROM 一次性编程（OTP）区域

64 字节（512 位）的 OTP 区域是 EEPROM 阵列的一部分，用于只读存储。它分为 2 个块，每个块 32 字节。对于 ECC608-TMNGTLS，OTP 区域出厂时已预先锁定，其中包含以下数据：

```
02 25 70 13 37 B9 CF F0 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

写入 OTP 区域的数据字节值始终可通过 4 字节或 32 字节读取方式进行读取，但始终不可进行修改。

NOTICE OTP 区域中的字节可能会随时间变化。建议不要在任何加密计算中使用这些值。

4. 静态 RAM（SRAM）存储器

此器件还包括用于存储输入命令或输出结果、Nonce、中间计算值、临时密钥和 SHA 上下文等内容的 SRAM 阵列。SRAM 的内容始终不能直接读取；仅供安全元件在内部使用。每当器件进入休眠模式或断电时，此存储器的全部内容便无效。

SRAM 阵列包含以下缓冲区：

TempKey

TempKey 是 SRAM 阵列中的主存储寄存器，可用于存储由不同命令生成的各种中间值。TempKey 的长度为 64 字节，分为高半部分和低半部分。此寄存器的内容始终不能从器件读取（尽管器件本身可以在内部读取和使用内容）。

报文摘要缓冲区

报文摘要缓冲区是一个 64 字节寄存器，在需要通过 TempKey 寄存器来保留其他信息时，用于将输入报文摘要传送到 Verify 和 Sign 命令。SHA 命令可将摘要直接写入该寄存器，以简化外部主机编程。

备用密钥缓冲区

备用密钥缓冲区是一个 32 字节寄存器，在需要通过 TempKey 寄存器来保留其他信息时，供 KDF 命令用于存储密钥。可通过 Nonce 命令对其写入固定输入值，或通过 KDF 命令对其写入机密信息值。

SHA 上下文缓冲区

SHA 上下文缓冲区允许中断摘要的生成以执行其他功能或生成其他摘要。SHA 命令使用标准三阶段流程：初始化、更新和完成。在许多情况下，更新阶段会多次运行。内部 SRAM 存储器用于存储这些阶段之间的中间状态（也称为 SHA 上下文）。

5. 一般命令信息

以下各节介绍了有关基本 I/O 事务、命令结构、错误代码、存储器寻址以及 ECC608-TMNGTLS 中使用的密钥和签名格式的一般信息。

5.1 I/O 事务

ECC608-TMNGTLS 使用 I²C 协议与主机单片机通信。在采用以下方式构建的事务中，安全命令将发送到器件，并从器件接收响应：

表 5-1. I/O 事务格式

字节	名称	含义
0	计数	要传入（或传出）器件的组中的字节数，其中包括计数字节、数据包字节和校验和字节。因此，计数字节的值必须始终为（N + 1），其中 N 等于数据包中的字节数加上 2 个校验和字节。对于具有 1 个计数字节、50 个数据包字节和 2 个校验和字节的组，必须将计数字节设置为 53。最大的组（与计数值）为 155 个字节，最小的组为 4 个字节。如果值超出此范围，将导致器件返回 I/O 错误。
1 至（N-2）	数据包	命令、参数和数据或响应。有关一般命令数据包的信息，请参见 5.2. 命令数据包；有关每个命令的具体参数，请参见 6. 器件命令。
N-1 和 N	校验和	计数字节和数据包字节的 CRC-16 验证。CRC 多项式为 0x8005。在开始 CRC 计算之前，将 CRC 寄存器初始化为零。在计数和数据包的最后一位发送后，内部 CRC 寄存器的值必须与块中的校验和字节相匹配。发送的第一个 CRC 字节（N-1）是 CRC 值的 LSB，因此此组的最后一个字节是 CRC 的 MSB。

ECC608-TMNGTLS 的设计应使输入组中的计数值与命令参数中指定的大小要求一致。如果计数值与数据包内的命令操作码和/或参数不一致，则 ECC608-TMNGTLS 将根据具体命令以不同的方式响应。响应可能包含错误指示，也可能默默忽略一些输入字节。

5.2 命令数据包

表 5-2 对命令数据包进行了分解：

表 5-2. 命令数据包

字节	名称	含义
0	操作码	命令代码。请参见 6. 器件命令。
1	Param1	第 1 个参数，始终存在。
2-3	Param2	第 2 个参数，始终存在。
0-155	数据	可选的剩余输入数据。

在 ECC608-TMNGTLS 接收到组中的所有字节之后，器件将转换到繁忙状态并尝试执行命令。当器件繁忙时，无法从其中读取状态和结果。在此期间，器件的 I/O 接口会忽略 I²C SDA 输入信号的所有转换。

5.3 状态/错误代码

器件没有专用的状态寄存器，因此状态、错误和命令结果共用输出 FIFO。器件的所有输出都将以完整组的形式返回到系统，这些组的格式与输入组相同：

- 计数
- 数据包
- 2 字节 CRC

器件接收到输入命令组的第 1 个字节后，系统将无法读取器件中的任何内容，直到系统将所有字节发送给器件。

在唤醒和执行命令后，器件的输出寄存器中会有错误、状态或结果字节，可通过系统获取。当此组的长度是 4 个字节时，返回的代码详见表 5-3。有些命令执行成功时会返回超过 4 个字节。得到的数据包说明在 6. 器件命令中列出。

CRC 错误始终在任何其他类型的错误之前返回。它们表明发生了某种 I/O 错误，并且此命令可重新发送给器件。如果还发生了多个其他错误，则这些错误没有特定的优先顺序。

表 5-3. 4 字节组中的状态/错误代码

状态说明	错误/状态	说明
命令执行成功	0x00	命令执行成功。
CheckMac 或 Verify 不匹配	0x01	CheckMac 或 Verify 命令已正确发送到器件，但输入响应与预期值不匹配。
解析错误	0x03	命令已正确接收，但长度、命令操作码或参数非法，而与 ECC608-TMNGTLS 的状态（易失性存储器和/或 EEPROM 配置）无关。命令位的值必须在重新尝试之前进行更改。
ECC 故障	0x05	ECC 处理期间发生计算错误，导致结果无效。重试命令可能会使执行成功。
自检错误	0x07	发生自检错误，芯片处于故障模式，等待清除故障。
运行状况测试错误	0x08	发生随机数发生器运行状况测试错误，并且在清除该错误之前，芯片无法执行需要随机数的后续命令。
执行错误	0x0F	命令已正确接收，但无法由器件在当前状态下执行。器件状态或命令位的值必须在重新尝试之前进行更改。
在唤醒之后、第 1 条命令之前	0x11	指示 ECC608-TMNGTLS 已收到适当的 Wake 令牌。
看门狗即将超时	0xEE	在 WDT 超时之前没有足够的时间执行给定的命令。系统必须通过进入空闲或休眠模式来复位 WDT。
CRC 或其他通信错误	0xFF	命令未由 ECC608-TMNGTLS 正确接收，必须由系统中的 I/O 驱动器重新发送。未尝试解析或执行命令。

5.4 地址编码

以下各小节提供了有关如何寻址 ECC608-TMNGTLS 器件的各个存储区域的详细信息。

5.4.1 配置区域寻址

对于配置区域，可一次性访问 4 或 32 个字节。无法访问单个字节。配置区域地址为 2 字节（16 位值）。配置区域寻址仅使用地址字的低 5 位。对于 ECC608-TMNGTLS 器件，这些地址只能与 Read 命令一起使用。

表 5-4. 地址格式

Byte 1：Addr[15:8]	Byte 0：Addr[7:0]		
未使用	未使用	块	失调电压
Addr[15:8]	Addr[7:5]	Addr[4:3]	Addr[2:0]

表 5-5. 配置区域地址

块号（Addr[4:3]）	偏移值（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]

5.4.2 OTP 区域寻址

对于 OTP 区域，可一次性访问 4 或 32 个字节。该区域总共有 64 个字节。无法访问单个字节。OTP 区域地址为 2 字节（16 位值）。仅低四位用于寻址。

对于 ECC608-TMNGTLS 器件，这些地址只能与 Read 命令一起使用。

表 5-6. 地址格式

Byte 1：Addr[15:8]	Byte 0：Addr[7:0]		
未使用	未使用	块	偏移量
Addr[15:8]	Addr[7:4]	Addr[3]	Addr[2:0]

表 5-7. OTP 区域字节地址

块号（Addr[3]）	块偏移值（Addr[2:0]）							
	000	001	010	011	100	101	110	111
0	[0:3]	[4:7]	[8:11]	[12:15]	[16:19]	[20:23]	[24:27]	[28:31]
1	[32:35]	[36:39]	[40:43]	[44:47]	[48:51]	[52:55]	[56:59]	[60:63]

5.4.3 数据区域寻址

与配置区域和 OTP 区域相比，对数据区域的读/写访问要复杂得多。数据区域有 16 个槽，槽的大小各不相同。每个槽的访问策略分别控制一个槽是否允许读取或写入。

对于 ECC608-TMNGTLS：

- 数据 Slot 2、Slot 4、Slot 7-12 和 Slot 15 配置为采用明文形式写入。
- 数据 Slot 5 和 Slot 14 可采用密文形式写入。
- 数据 Slot 2、Slot 8、Slot 10-12 和 Slot 14-15 可采用明文形式读取。
- 任何未指定的槽均无法读写。

表 5-8. 基于数据槽大小的地址格式

数据区域	Byte 1：Addr[15:8]		Byte 0：Addr[7:0]		
	未使用	块	未使用	槽	偏移量
数据 Slot[7:0]	Addr[15:9]	Addr[8]	Addr[7]	Addr[6:3]	Addr[2:0]
数据 Slot[8]	Addr[15:12]	Addr[11:8]	Addr[7]	Addr[6:3]	Addr[2:0]
数据 Slot[15:9]	Addr[15:10]	Addr[9:8]	Addr[7]	Addr[6:3]	Addr[2:0]

数据 Slot[7:0]

要完全访问这些槽之一，需要进行两次 32 字节访问或 9 次 4 字节访问。

表 5-9. 数据区域寻址 Slot 0-7

槽号（Addr[6:3]）	块号（Addr[8]）	块偏移值（Addr[2:0]）							
		000	001	010	011	100	101	110	111
0x0 至 0x7	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

数据 Slot[8]

要完全访问此槽，需要进行 13 次 32 字节访问或 104 次 4 字节访问，或结合使用这两种方法。

表 5-10. 数据区域寻址 Slot 8

槽号（Addr[6:3]）	块号（Addr[8]）	块偏移值（Addr[2:0]）							
		000	001	010	011	100	101	110	111
0x8	0x0	[0:3]	[4:7]	[8:11]	[12:15]	[16:19]	[20:23]	[24:27]	[28:31]
	0x1	[32:35]	[36:39]	[40:43]	[44:47]	[48:51]	[52:55]	[56:59]	[60:63]
	...	...	...	...	...	...	...	...	...
	0xC	[384:387]	[388:391]	[392:395]	[396:399]	[400:403]	[404:407]	[408:411]	[412:415]

数据 Slot[15:9]

要完全访问这些槽，需要进行 3 次 32 字节访问或 18 次 4 字节访问，或结合使用这两种方法。

表 5-11. 数据区域寻址 Slot 9-15

槽号（Addr[6:3]）	块号（Addr[8]）	块偏移值（Addr[2:0]）							
		000	001	010	011	100	101	110	111
0x9 至 0xF	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

5.5 密钥、签名和证书的格式

以下各节提供了有关 ECC 密钥、签名和压缩证书的详细格式信息。

5.5.1 ECC 密钥格式

公钥和私钥的格式取决于命令和密钥的长度。通常，最高有效字节（MSB）首先出现在总线上的存储器最低地址处。在本节剩余部分中，左侧的字节为 MSB。Microchip 建议将所有填充字节设置为 0 以保持一致性。

- ECC 私钥对用户来说仅仅为 `PrivWrite` 命令的输入参数。此参数的长度始终为 36 个字节，前 4 个字节（32 位）全部为填充位。
  ECC 公钥作为几个命令的输入或输出参数出现，也可以存储在 EEPROM 中。其组成方式为：总线上或存储器中的 X 值在前，后跟 Y 值。它们的格式有所不同，具体取决于如下所述的情况：
- **公钥是 `GenKey` 命令的输出或 `Verify` 命令的输入：**
  先是 32 个 X 字节，随后是 32 个 Y 字节。（36 个字节）没有填充字节。
- **`Write` 命令：**
  公钥可使用 `Write` 命令直接写入 EEPROM，其长度始终为 72 字节，格式如下：4 个填充字节，32 个 X 字节，4 个填充字节，32 个 Y 字节。
- **`GenKey` 命令：**
  SHA 报文： 可通过 `GenKey` 命令对公钥进行哈希运算并将其置于 TempKey 中。SHA 报文包含与密钥大小无关的各个字节。其后依次为 25 个填充字节，32 个 X 字节，32 个 Y 字节。
- **`Verify` 命令：**
  SHA 报文： 当用于验证存储的公钥时，`Verify` 命令需要通过存储器中存储的密钥的 SHA-256 摘要创建的输入签名。 此类内部 SHA 计算始终通过 72 个字节来执行，这些字节在 EEPROM 中的存储格式为 4 个填充字节、32 个 X 字节、4 个填充字节，随后是 32 个 Y 字节。

当公钥配置为通过 `Verify` 命令验证时，存储器中第一个字节的高 4 位供器件在内部用来保存验证状态。它们始终由 `Write` 命令设置为无效状态（`0xA`），之后可通过 `Verify` 命令设置为有效状态（`0x5`）。

下面将介绍 I/O 协议的最低层。在 I/O 协议层之上，完全相同的字节传入和传出器件以实现命令。后续章节将对错误代码进行说明。

5.5.1.1 公钥格式

ECC608-TMNGTLS 支持两种格式的 P-256 椭圆曲线公钥。以下示例详细说明了这两种格式。

对于以下示例，我们将使用示例公钥，其中 X 和 Y 整数以固定宽度的大尾数无符号整数表示：

```
X：b2be345ad7899383a9aab4fb968b1c7835cb2cd42c7e97c26f85df8e201f3be8
Y：a82983f0a11d6ff31d66ce9932466f0f2cca21ef96bec9ce235b3d87b0f8fa9e
```

命令公钥格式

任何返回公钥（GenKey）或接受公钥作为参数的命令（Verify 和 ECDH）都会将公钥格式化为 X 和 Y 大尾数无符号整数连在一起的形式，因而总共 64 个字节。

例如：

```
b2be345ad7899383a9aab4fb968b1c7835cb2cd42c7e97c26f85df8e201f3be8
a82983f0a11d6ff31d66ce9932466f0f2cca21ef96bec9ce235b3d87b0f8fa9e
```

存储的公钥格式

将公钥存储在槽中以便与 Verify 命令搭配使用时，X 和 Y 整数将分别被填充为两个 36 个字节并连在一起，因而总共为 72 个字节。

例如：

```
00000000b2be345ad7899383a9aab4fb968b1c7835cb2cd42c7e97c26f85df8e201f3be8
00000000a82983f0a11d6ff31d66ce9932466f0f2cca21ef96bec9ce235b3d87b0f8fa9e
```

注：仅 Slot 8-15 便足以保存公钥。

存储的经验证公钥格式

经验证和未经验证的公钥格式与存储的公钥格式相同，但 LSB 的高四位除外。如果密钥经验证，则最低有效半字节将为 0x5，如果未经验证则为 0xA。这些值可在验证或未验证模式下通过 Verify 命令进行更改。写入的密钥最初为未验证状态。

生效公钥示例：

```
50000000b2be345ad7899383a9aab4fb968b1c7835cb2cd42c7e97c26f85df8e201f3be8
00000000a82983f0a11d6ff31d66ce9932466f0f2cca21ef96bec9ce235b3d87b0f8fa9e
```

失效公钥示例：

```
A0000000b2be345ad7899383a9aab4fb968b1c7835cb2cd42c7e97c26f85df8e201f3be8
00000000a82983f0a11d6ff31d66ce9932466f0f2cca21ef96bec9ce235b3d87b0f8fa9e
```

注：仅 Slot 8-15 便足以保存公钥。

5.5.2 签名格式

无论是由 Sign 命令生成并输出的 ECDSA 签名还是输入到 Verify 命令的 ECDSA 签名，长度始终为 64 字节。签名分为 R 和 S 两个组成部分。这两者的长度均为 32 字节，并且在总线上 R 始终出现在 S 之前。签名的每个部分在总线上都先显示 MSB，这意味着签名的 MSB 位于最低存储单元中。

R/S 签名示例

任何返回签名（Sign）或接受签名作为参数的命令（Verify）都会将签名格式化为 R 和 S 大尾数无符号整数连在一起的形式，因而总共 64 个字节。

例如：

```
R: 7337887F8C39DF79FD8BF88DDFBFB9DB15D7B1AD68196AE3FB0CE5BFA2842DF3
S:  72868A43A42831E950E1DA9F73B29F5C0ED8A96B2889E3CBBE8E61EA6C67F673
```

5.5.3 证书存储

器件内的完整 X.509 证书所需的存储空间较大，可能会很快占满多个 EEPROM 存储器槽。根据实际应用的不同，这些槽也并非一定适合用来存储证书。为了应对这些存储限制，Microchip 定义了一种编码方式，以便能够基于少量信息重建完整的 X.509 证书。

主机系统实际上将负责重建完整的 X.509 证书，但是如何执行将由存储在编码证书中的数据决定。对于给定系统，所有器件共用的数据可轻松存储在主机系统中。其他数据可根据已存储在器件中的数据轻松进行计算或提取。 表 5-12 指示 X.509 证书中存储的数据类型，以及如何对其进行编码以便能够存储到单个 72 字节槽中。

表 5-12. 证书存储

X.509 证书		编码证书		
X.509 元素	大小（字节）	编码证书元素	器件证书（位）	签名人证书（位）
序列号	8-20	序列号来源	4	4
颁发日期	13	压缩格式	19	19
有效期	13	有效年数	5	5
签名人 ID[2]	4	用于对证书（器件证书）进行签名的特定签名人的 ID 或签名人本身（签名人证书）的 ID	16	16
颁发机构密钥标识符	20	颁发机构公钥的 SHA1 哈希	0	0
主题密钥标识符	20	主题公钥的 SHA1 哈希	0	0
签名 R	32	存储在器件中	256	256
签名 S	32	存储在器件中	256	256
公钥 X[1]	32	根据私钥计算或存储在器件中 [1]	0	256
公钥 Y[1]	32	根据私钥计算或存储在器件中 [1]	0	256
N/A	0	证书格式	4	4
N/A	0	模板 ID	4	4
N/A	0	链 ID	4	4
N/A	0	保留/用户自定义	8	8
总数	（206-218 字节）	—	576 位（72 字节）	1088 位（136 字节）

注：

1. 对于器件证书，可以根据私钥重新生成器件公钥。对于签名人证书，公钥通常存储在单独的槽中。
2. 对于器件证书，将存储用于对证书进行签名的签名人的 ID。对于签名人证书，将存储签名人的实际 ID，以便设备能够识别。

Slot 8 总共包含 416 个字节。根据证书中存储的序列号的大小，可能会也可能不会存储两个完整的证书。通常，在已创建信任链的器件中，器件证书、签名人证书和签名人公钥必须存储在器件中。

有关更多信息，请参见《压缩证书定义》（DS20006367A_CN）应用笔记。

6. 器件命令

以下部分详细介绍了 ECC608-TMNGTLS 中允许的基于命令模式细分的所有命令。这些命令分为以下三类：

1. **常规器件命令**
   此类命令分为两类：
   - 常规器件访问命令，用于将数据发送到器件或检索数据，但通常不执行任何加密功能。
   - 常规加密命令，可由器件或系统使用，但通常不会用于特定数据槽。
2. **非对称加密命令**
   这些命令执行非对称加密操作，例如密钥生成、报文签名和报文验证（使用 ECC 公钥或私钥）。这些命令仅限用于 ECC 数据区域槽。
3. **对称加密命令**
   这些命令执行对称加密功能，例如生成摘要或 MAC、密钥派生或 AES 加密和解密。

所有命令的输入参数

除非另有说明，否则输入参数表中的多字节输入参数以大尾数值的形式（MSB 在前）显示。请注意，ECC608-TMNGTLS 器件实际上希望数据以小尾数形式（LSB 在前）发送。

表 6-1. 命令、说明和命令类别

命令	说明	命令类别
AES	执行 AES-ECB 加密或解密功能。计算 Galois 域乘法。	对称加密命令
CheckMac	验证在另一个 CryptoAuthentication™器件上计算的 MAC。	对称加密命令
Counter	读取或递增单调计数器之一。	常规器件命令
ECDH	使用存储的私钥和输入公钥生成 ECDH 预主机密信息。	非对称加密命令
GenDig	通过随机或输入种子和存储的值生成数据摘要。	对称加密命令
GenKey	生成 ECC 公钥。也可以生成 ECC 私钥。	非对称加密命令
Info	返回器件状态信息。	常规器件命令
KDF	实现 PRF 或 HKDF 密钥派生函数	对称加密命令
Lock	防止进一步修改器件的某个区域或槽。	常规器件命令
MAC	使用 SHA-256 计算密钥和其他内部数据的摘要（响应）。	对称加密命令
Nonce	生成一个 32 字节的随机数和一个内部存储的临时值。	常规器件命令
Random	生成一个随机数。	常规器件命令
Read	从器件读取 4 个或 32 个字节，可以使用或不使用身份验证和加密。	常规器件命令
SecureBoot	上电时验证代码签名或代码摘要。	非对称加密命令
SelfTest	测试各种内部加密计算元素。	常规器件命令
Sign	ECDSA 签名计算。	非对称加密命令
SHA	计算系统通用的 SHA-256 或 HMAC 摘要。	常规器件命令
UpdateExtra	配置区域锁定后，更新配置区域内的 Byte 84 或 85。	常规器件命令
Verify	ECDSA 验证计算。	非对称加密命令
Write	向器件写入 4 个或 32 个字节，可以使用或不使用身份验证和加密。	常规器件命令

相关信息

6.1. 常规器件命令
6.2. 非对称加密命令
6.3. 对称加密命令

6.1 常规器件命令

下表总结了常规器件命令：

表 6-2. 常规器件命令

命令名称	说明
Counter	递增并读取单调计数器
Info	用于从器件中读取版本和状态信息
Lock	用于锁定器件中的各个可锁定槽
Nonce	用于为器件生成或传递仅使用一次的数字
Random	用于生成供系统使用的 32 字节随机数
Read	用于读取器件的各个区域
SelfTest	测试各种内部加密计算元素
SHA	计算系统通用的 SHA-256 或 HMAC 摘要
UpdateExtra	配置区域锁定后，更新配置区域内的 Byte 84 或 85
Write	用于向器件写入 4 个或 32 个字节，可以使用或不使用身份验证和加密

6.1.1 Counter 命令

Counter 命令在配置区域内读取器件上 2 个单调计数器之一的二进制计数值。此计数器可达到的最大值为 2,097,151。尝试计数超出此值将导致错误代码。此计数器的设计可确保即使计数操作期间电源中断，也始终不会丢失计数。在某些电力损失的情况下，计数器可能会以超过 1 的值递增。

对于 ECC608-TMNGTLS，计数器未关联到任何密钥，但仍可供系统使用。每个计数均设置为其默认值，并且可以计数到最大值。

6.1.2 Info 命令

Info 命令用于读取器件的状态。该信息对于确定错误或使用各种命令很有用。

6.1.3 Lock 命令

对于 ECC608-TMNGTLS，配置区域已锁定，并且数据区域的访问策略已设置。但是，仍然可以通过使用其他命令来更新几个数据槽。如有需要，可以使用 Lock 命令的槽锁定模式将其中一些槽永久锁定，以避免未来的更新。

6.1.4 Nonce 命令

Nonce 命令通过将随机数（可在内部或外部生成）与来自系统的输入值相组合来生成 Nonce（使用一次的数字），以供后续命令使用。得到的 Nonce 在内部存储在三个可能的缓冲区中：TempKey 缓冲区、报文摘要缓冲区和备用密钥缓冲区。如有必要，可将值直接传递给器件，而不生成 Nonce。

6.1.5 Random 命令

Random 命令生成一个随机数，以供系统使用。随机数通过内部 NIST 800-90 A/B/C 随机数发生器生成。该命令始终在总线上输出 32 字节数字。该数字不能存储在任何数据槽或 SRAM 单元中。

6.1.6 Read 命令

Read 命令可用于访问 ECC608-TMNGTLS 器件的任何 EEPROM 区域。基于为每个槽设置的访问策略，数据区域访问将受到限制。如果设置了特定的访问策略，则只能在数据区域槽上进行加密读取。

6.1.7 SelfTest 命令

SelfTest 命令对 ECC608-TMNGTLS 芯片中的一个或多个加密引擎执行测试。将根据输入模式参数测试部分或全部算法。

对于 ECC608-TMNGTLS 器件，SelfTest 命令已被禁止，以避免在上电或唤醒事件后自动运行。但是，如有需要，可以通过系统执行该命令。无需运行该测试。

如果任何自检失败，则无论是在上电和唤醒时自动调用还是通过此命令调用，芯片都将进入故障状态，芯片操作将受限。存储的故障状态始终在唤醒或掉电再上电后清除。

6.1.8 SHA 命令

SHA 命令用于计算主机系统通用的 SHA-256 或 HMAC/SHA 摘要。SHA 计算在内部 ECC608-TMNGTLS 存储器中未被任何其他命令读取和写入的特殊部分（上下文缓冲区）中执行。任意命令都可以穿插在 SHA 命令各个阶段之间，而不会产生问题。上电和唤醒时会使该 SHA 上下文失效。在大多数情况下，如果执行 SHA 命令时发生错误，上下文将保持不变。

6.1.9 UpdateExtra 命令

UpdateExtra 命令用于更新 UpdateExtra 和 UpdateExtraAdd 字节（分别为配置区域中的 Byte 84 和 85）。这些字节只能通过此命令进行更新。这些字节是可一次性更新的字节，只能在当前值为 0x00 时更新。如果值不为 0x00，则尝试更新此字节将导致错误。

对于 ECC608-TMNGTLS 器件，UpdateExtraAdd 字节（Byte 85）已配置为备用 I^2C 地址。

6.1.10 Write 命令

对于 ECC608-TMNGTLS，配置区域和 OTP 区域为锁定状态，无法更新这些区域。根据每个槽的访问策略，数据区域上的写入能力有限。

6.2 非对称加密命令

非对称加密命令集由专门用于生成或使用 ECC 密钥的命令组成。密钥通常存储在数据区域槽中，但对于某些命令，也可以存储在 SRAM 阵列中。

表 6-3. 非对称加密命令

命令名称	说明
ECDH	使用存储的私钥和输入公钥生成 ECDH 预主机密信息
GenKey	生成 ECC 私钥，也可选择通过存储的私钥生成 ECC 公钥
SecureBoot	上电时验证代码签名或代码摘要
Sign	使用 ECC 私钥和 ECDSA 签名计算对内部或外部报文摘要进行签名
Verify	使用 ECC 公钥和 ECDSA 验证计算对内部或外部报文摘要进行验证

6.2.1 ECDH 命令

ECDH 命令用于生成两个器件之间的共用机密信息。通过传递另一个器件中的 ECC 公钥并将其与存储在槽中的 ECC 私钥或存储在 TempKey 中的临时密钥进行组合，然后在另一个器件上执行相反的操作，即可让两个器件生成相同的共用预主机密信息。该机密信息随后可以进一步与双方的其他公共数据相结合，以生成两个器件之间的共用会话密钥。KDF 命令通常与 TLS 会话一起使用，以进一步实现共用机密信息的多样化。

6.2.2 GenKey 命令

GenKey 命令用于生成 ECC 私钥和通过私钥生成 ECC 公钥，或者生成公钥摘要。该命令仅适用于专用于 ECC 私钥或公钥的槽。在非 ECC 槽上运行该命令将导致错误。

6.2.3 SecureBoot 命令

SecureBoot 命令用于为外部 MCU 或 MPU 的安全引导提供支持。一般方法如下：系统内的引导代码将使用 ECC608-TMNGTLS 来协助验证随后要执行的应用程序代码。ECC608-TMNGTLS 器件配置为在安全引导和存储摘要模式下工作。 摘要将存储在 Slot 13 中，而验证安全引导所需的公钥将存储在 Slot 15 中。

可以选择通过写入 TempKey 的 Nonce、I/O 保护机密信息和各种其他数据（具体取决于命令的模式）代替返回代码来生成 MAC，以防止篡改主机与 ECC608-TMNGTLS 之间的线路。

6.2.4 Sign 命令

Sign 命令使用 ECDSA 算法生成签名。由 KeyID 指定的槽中的 ECC 私钥用于生成签名。该器件可提供多种模式，具体取决于要签名的内容。

6.2.5 Verify 命令

Verify 命令接受 ECDSA [R,S]签名并在给定输入报文摘要和公钥时验证是否已正确生成该签名。在所有情况下，签名均是命令的输入。公钥可存储在器件上或作为输入提供。

Verify 命令可返回可选 MAC 来防御中间人攻击。如果验证计算表明已基于输入摘要正确生成了签名，将根据 TempKey 中存储的输入 Nonce 以及 ECC608-TMNGTLS 和主机 MCU 中存储的 I/O 保护机密信息的值计算 MAC。只能在外部模式和存储模式下生成 MAC 输出。必须使能 I/O 保护功能才能计算 MAC。

使用存储在 Slot 4 和 Slot 9 中的 AES 密钥之前必须先对其进行验证。

6.3 对称加密命令

对称加密命令集由与生成或使用对称密钥有关的命令组成。密钥通常存储在数据区域槽中，但对于某些命令，也可以存储在 SRAM 存储单元中。

表 6-4. 对称加密命令

命令名称	说明
AES	执行 AES-ECB 加密或解密功能。计算 Galois 域乘法。
CheckMac	验证在另一个 CryptoAuthentication™器件上计算的 MAC。
GenDig	通过随机或输入种子和存储的值生成数据摘要。
KDF	实现 PRF 或 HKDF 密钥派生函数
MAC	使用 SHA-256 计算密钥和其他内部数据的摘要（响应）。

6.3.1 AES 命令

AES 命令可用于利用 AES 密钥对 16 字节的数据块进行加密和/或解密。请注意，密钥存储在给定槽的 16 字节（128 位）存储单元内或 TempKey 的前 16 个字节内。可将多个密钥存储在一个给定槽中，并按 16 字节边界连续访问（从字节 0-15 开始，一直到该槽的最后 16 个字节），但任何槽中的密钥数量都不超过四个。对于 ECC608-TMNGTLS，可将 AES 密钥存储在 Slot 4、Slot 5 或 Slot 9 中。Slot 4 和 Slot 5 最多可容纳 2 个 AES 密钥，Slot 9 最多可容纳 4 个 AES 密钥。

除了 AES 加密和解密外，AES 命令还可用于生成 Galois 域乘法（Galois Field Multiply，GFM），以支持其他加密操作。

6.3.2 CheckMac 命令

CheckMac 命令可计算不同 CryptoAuthentication 器件 [1] 上生成的 MAC 响应，然后将结果与输入值进行比较。该命令会返回一个布尔结果来指示比较成功还是失败。

如果将 TempKey 中的值用作 CheckMac 的输入，则 Nonce 和/或 GenDig 命令必须在 CheckMac 命令之前运行。

6.3.3 GenDig 命令

GenDig 命令使用 SHA-256 哈希运算将存储的或输入的值与 TempKey 的内容相结合，这些内容在执行此命令之前必须有效。存储的值可以来自其中一个数据槽、配置区域、任一 OTP 页或单调计数器。器件的具体模式决定了 GenDig 计算中将包含的数据。

[1] 生成兼容 MAC 响应的器件包括 ATECC608A/B/C、ATECC508A、ATSHA204A 和 SHA104。其中包括与产品相关的可信型号。

在某些情况下，在执行一些命令之前，需要先运行 GenDig。该命令可运行多次，以在执行给定命令前在摘要中包含更多数据。得到的摘要保留在 TempKey 中，可以通过以下四种方式之一使用：

1. 它可以作为 MAC、Sign 或 CheckMac 命令使用的报文的一部分包含在内。由于 MAC 响应输出结合了 GenDig 计算中使用的数据与 MAC 命令的机密信息密钥，因此将用于验证数据和/或 OTP 区域中存储的数据。
2. 后续 Read 或 Write 命令可以使用摘要来为数据提供认证和/或加密，在这种情况下，相应摘要称为数据保护摘要。
3. 可以使用此命令通过传输密钥阵列中的值进行安全个性化。得到的数据保护摘要将供写操作使用。
4. 输入值（通常是远程器件中的 Nonce）与当前 TempKey 值相结合以创建共用 Nonce，其中两个器件均可以证明包含 RNG。

6.3.4 KDF 命令

对于 ECC608-TMNGTLS，KDF 命令实现了多个密钥派生函数，包括 PRF（用于 TLS 1.2）、HKDF（用于 TLS 1.3）和 AES。 CryptoAuthLib 中支持该函数。 有关更多信息，请参见 7.2.3. CryptoAuthLib。

有关 KDF 命令的更多信息，请联系 Microchip 销售人员。

6.3.5 MAC 命令

报文身份验证代码（MAC）命令用于为由存储在器件中的密钥、质询和器件上的其他信息组成的报文生成 SHA-256 摘要。此命令的输出为此报文的摘要。

使用此命令的正常流程如下所示：

1. 运行 Nonce 命令以加载输入质询，并视情况将其与生成的随机数组合。此操作的结果是在器件内部存储的一个临时值。
2. 视情况运行 GenDig 命令一次或多次，将器件中的存储 EEPROM 单元与 Nonce 组合。结果存储在器件内部。此功能允许将 2 个或多个密钥用作响应生成的一部分。
3. 运行此 MAC 命令，将步骤 1（以及步骤 2，需要时）的输出与 EEPROM 密钥组合，以生成一个输出响应（即摘要）。

或者，可以通过相同的 GenDig 机制将任何槽中的数据（不必是机密信息）累积到响应中。其作用是验证存储在相应单元的值。

7. 应用信息

ECC608-TMNGTLS 是 Microchip 的 CryptoAuthentication™ Trust Platform 产品系列的成员。Trust Manager 产品是自助式加密密钥管理器件。这些器件易于实现，甚至允许小批量生产的客户在其最终系统中实现安全身份验证，同时可利用 Microchip 和 Kudelski IoT 的专业知识和配置基础架构。

ECC608-TMNGTLS 器件旨在省去为 IoT 联网产品增加安全性时的猜测工作。该产品已经过预先配置，可以通过 DTLS 连接轻松连接到任何云端基础架构。

将实际的安全器件与 Kudelski IoT keySTREAM SaaS 服务相结合时，即可打造出一套针对产品生命周期的完整可信解决方案。该解决方案支持多种用例。

7.1 用例

ECC608-TMNGTLS 专门面向 IoT 市场而定义。通过使用 Kudelski keySTREAM SaaS，可以访问各种云网络和特定的身份验证服务。系统固有的灵活性允许在现场建立自定义 PKI，无需在 Microchip 的工厂进行干预。这样方便修改和轮换证书，以及更新和维护各种应用及其用例的安全策略。下面简要介绍了该器件解决的一些用例。这些用例既可以单独实现，也可以相互组合实现。为了对这些用例进行原型设计并加以实现，Microchip 提供了硬件和软件工具。

安全 TLS 连接

ECC608-TMNGTLS 允许采用 TLS 协议创建安全身份验证。该器件将存储 Microchip 在自家经认证的安全配置工厂内生成的初始私钥。该密钥将向 keySTREAM SaaS 发出 ECC-P256 签名，以便对 ECC608 TrustManager 进行身份验证。SaaS 随后将创建自定义 PKI，并在器件中配置新的自定义证书。这是自定义 PKI 的现场配置。与根证书和中间证书关联的私钥受 Kudelski IoT HSM 保护（在客户帐户设置期间设置）。因此，可以连接到各种云提供商。通过不同模式的密钥派生函数（Key Derivation Function，KDF），可以生成适当的密钥来支持 TLS1.2、TLS1.3 和更早的安全连接 Internet 协议。

证书管理

通过使用在设置帐户时由 keySTREAM SaaS 设置的自定义 PKI，可以使用 SaaS 来管理和监视证书到期日期、证书撤销和证书更新。

设置初始帐户后，可以设置证书的到期日期并将其存储在 ECC608-TMNGTLS 中。当证书到期时，可将其配置为按照 Kudelski IoT 政策规定自动更新，以防止因证书过期而导致服务丢失。

如果发生保证会撤销证书的安全漏洞或其他事故，则可以通过使用 KeySTREAM SaaS 撤销 ECC608-TMNGTLS 器件证书。撤销证书将阻止器件连接到云端。如果需要恢复器件的安全身份验证，则可通过颁发新证书替换器件中当前存储的证书来更新证书。在证书被撤销后进行更新实现了证书轮换。

私钥轮换

keySTREAM SaaS 能够控制 ECC608-TMNGTLS 内部私钥的轮换。如果确定最终产品私钥不再可信，则可通过使用 keySTREAM SaaS 重新生成新私钥（存储在 Slot 0 中）。风险在于可能会拒绝为 Slot 0 服务，即 keySTREAM SaaS 将拒绝该特定器件访问 SaaS。

安全引导

保护单片机或微处理器的固件映像是许多供应商关注的问题。通过提供一种机制来验证正在运行的代码真实且未被修改，可以维护系统的整体完整性。ECC608-TMNGTLS 已配置为允许通过将系统的代码摘要存储在器件的数据槽中来实现安全引导。最初执行代码后，系统可以通过系统固件重新生成摘要，并将其与存储在 ECC608-TMNGTLS 中的摘要进行比较，验证固件未遭到篡改。

IP 和数据保护

保护知识产权（Intellectual Property，IP）对于维持公司的竞争优势至关重要。IP 保护描述了防止客户开发的固件或硬件遭受复制的方法。固件 IP 保护只要使用基于软件的方法即可实现，但固件内部的密钥信息仍然非常容易遭受攻击。

ECC608-TMNGTLS 器件提供了基于硬件的安全密钥存储，可确保带有固件的产品正常运行。该器件可以执行对称身份验证和非对称身份验证，其中密钥被安全地存储在安全元件中，从而削弱了黑客提取和修改密钥的能力。在任何运行时操作期间，可以使用 Slot 9 AES 对称密钥或 Slot 15 公钥来分别验证固件映像的哈希值或已签名映像的签名。

端到端数据保护

通过使用对称密钥，可以实现安全数据通信。通过使用 ECDH 函数，可以生成对称密钥，以便对器件与端点之间的通信进行加密和解密。这样可以对云端与器件之间传输的数据提供全面保护。

通用数据存储

数据 Slot 8 用于存储多个 keySTREAM SaaS 操作所需的特定客户/应用引导流程信息。该槽不可供客户用于一般用途。有时需要为给定系统存储少量的其他信息。数据 Slot 15 可用于存储额外的客户特定信息或应用特定信息。ECC608-TMNGTLS 可利用允许读写访问的数据槽来实现该用途。这样便无需添加额外的 EEPROM 存储器件来单单存储数据。

限制：如果数据 Slot 15 用于存储通用数据，则无法实现安全引导功能。

7.2 开发工具

ECC608-TMNGTLS 受多种软硬件工具以及后端服务支持，可快速开发应用程序。初始开发可以从一系列易于使用的 Trust Platform Design Suite 工具开始。这些工具以图形方式来实现您的用例，最终会输出实现应用程序所需的 C 代码。

如果预定义的 Trust Platform Design Suite 工具无法提供您所需要的应用程序，则可以使用 CryptoAuthLib 或 Python®版本的 CryptoAuthLib 和 CryptoAuthTools 来开发应用程序。CryptoAuthLib 同时也是 Trust Platform Design Suite 工具所输出的代码的主干。

可以结合使用硬件工具和 ECC608-TMNGTLS 器件样片来全面验证您的应用程序。器件的访问策略已设置，因此，重点仅围绕开发系统级代码。

当应用程序开发完毕后，即可访问 Microchip 直销网站订购 ECC608-TMNGTLS 器件。

7.2.1 Trust Platform Design Suite

为了简化实现过程，Microchip 开发了一套基于 Web 的 Trust Platform Design Suite 工具，可引导开发人员按照流程从概念阶段过渡到生产阶段。借助这些工具，可以在 ECC608-TMNGTLS 的配置和所定义访问策略的限制下开发和构建实现特定应用程序所需的事务图和代码。

注：有关这些工具的更多信息，请访问 Microchip 的 Trust Platform 信息页面。

7.2.2 硬件工具

使用 ECC608-TMNGTLS 进行开发时，有多种硬件工具可为用户提供帮助。关于此处未提及的其他工具的可用性信息，请访问 Microchip 网站。

EA06V72A/EV10E69A——CryptoAuthentication Trust Manager Platform

EA06V72A/EV10E69A 是一款紧凑的开发系统，其中包含 ATSAMD21 单片机、ECC608-TMNGTLS Trust Manager 器件、USB 集线器、mikroBUS™连接器和板上调试器。该工具包旨在与 Trust Platform Design Suite（TPDS）工具配合使用，后者用于实现 ECC608-TMNGTLS 器件的各种用例。这是建议与 Kudelski keySTREAM SaaS 工具和 Microchip 的 Trust Platform Development Suite 工具配合使用的工具包。

EA06V72A 是为 ECC608-TMNGTLS 的早期使用者提供的电路板，但将来会逐渐被 EV10E69A 生产板取代。就搭配使用 TPDS 与 Trust Manager 开发流程和 Kudelski keySTREAM SaaS 工具而言，这两个工具包的效果相同。与 EA06V72A 相比，EV10E69A 增加了几个用户 LED 和一个用户开关。

DT100104 ATECC608 Trust Board

DT100104 ATECC608 Trust Board 的第 4 版包含一个 ECC608-TMNGTLS 器件以及其他 ATECC608C Trust 器件。Trust Manager 器件的配置与 ECC608-TMNGTLS 原型器件（位于 Trust Manager Platform 板上，也可从 Microchip 直销网站订购）相同。该板采用 mikroBUS 接口设计，可轻松连接到 CryptoAuth Trust Manager Platform 或 CryptoAuth Trust Platform（DM320118）。如果将 CryptoAuth Trust Platform 与 DT100104（版本 4）板结合使用，并进行适当的 DIP 开关设置，则效果将与 CryptoAuth Trust Manager Platform 板相同。

安全 UDFN/SOIC Click 板

要将 ECC608-TMNGTLS 的 SOIC 或 UDFN 样片与 Trust Manager Platform Development Board 配合使用，建议用户购买专门设计用于与 Trust Managerr Platform 板配合使用的 mikroBUS 插座板。这些插座板由 mikroElektronika 提供，可安装在 Trust Manager Platform 板的 mikroBUS 连接器中。这些插座板可对一个或多个器件进行编程，然后在原型板或生产板上进行使用。必须获取 ECC608-TMNGTLS 的样片才能与这些工具包配合使用。

- 安全 SOIC Click 板
- 安全 UDFN Click 板

7.2.3 CryptoAuthLib

CryptoAuthLib 是一个支持 Microchip CryptoAuthentication 器件系列的软件库。Microchip 建议在使用 ECC608-TMNGTLS 进行开发时使用该库。该库实现了执行本数据手册中详述的命令所需的 API 调用。

该库实现后可以很容易地与多款 Microchip 单片机配合使用，但也可通过硬件抽象层（Hardware Abstraction Layer，HAL）轻松扩展为支持其他单片机，包括其他供应商生产的单片机。

有关这些工具的更多详细信息，请查看以下信息：

- CryptoAuthLib——网站链接
- CryptoAuthLib——GitHub

API 调用

数据手册中的每个命令都有一个或多个与其关联的 API 调用。通常，命令有一个基本的 API 调用，可以在其中指定所有输入参数。命令和各小节中显示的参数可与该命令一起使用。每个 API 调用还有多种模式变体。下表列出了命令和基本 API 调用的示例。有关最准确的 API 信息，请参见 GitHub 信息。

表 7-1. CryptoAuthLib API 调用的示例命令

器件命令	API 调用	备注
Info	atcab_info_base()	
Write	atcab_write()	
Read	atcab_read_zone()	
SHA	atcab_sha_base()	
Sign	atcab_sign_base()	
Random	atcab_random()	
Verify	atcab_verify()	

8. I²C 接口

I²C 接口使用 SDA 和 SCL 引脚来指示 ECC608-TMNGTLS 的各种 I/O 状态。该接口设计在协议层上与其他 Microchip CryptoAuthentication 和串行 EEPROM 器件兼容。确切的命令和器件 I²C 地址可能有所不同。

由于 ECC608-TMNGTLS 从器件的输出引脚上仅包含一个漏极开路驱动器，因此 SDA 引脚通常使用外部上拉电阻拉为高电平。总线主器件可能是漏极开路型或图腾柱型。在后一种情况下，当 ECC608-TMNGTLS 在总线上驱动结果时必须是三态的。SCL 引脚为输入，必须始终由外部器件或电阻驱动为高电平和低电平。

对于 ECC608-TMNGTLS，默认 7 位 I²C 地址定义为 0x38。使用该值时，I²C 地址写入/读取字节值将分别为 0x70 和 0x71。如果需要，可使用 `UpdateExtra` 命令改写一次 I²C 地址值。

切记：对于 I²C 标准中使用的术语“Master”和“Slave”，本文档中使用了与之等效的 Microchip 术语“Host”和“Client”。

相关信息

9.3.1. 交流参数：I2C 接口

8.1 I/O 条件

器件响应以下 I/O 条件：

8.1.1 器件休眠

当器件休眠时，它将忽略除唤醒状态以外的所有状态。

- 唤醒——一旦出现 SDA 的上升沿，则在 SDA 保持低电平的时间 ≥ t_{WLO} 后，器件将退出低功耗模式。在 t_{WHI} 的延时后，器件将准备好接收 I²C 命令。
- 当器件空闲或休眠时，在 t_{WLO} 期间，器件将忽略 SCL 引脚上的任何电平或转换。在 t_{WHI} 期间的某个时刻，将使能 SCL 引脚，并且将遵循 8.1.2. 器件唤醒中列出的条件。

唤醒条件要求系统处理器手动将 SDA 引脚驱动为低电平并持续 t_{WLO}，或者以足够低的时钟速率传输 `0x00` 数据字节以使 SDA 的低电平时间持续最短周期 t_{WLO}。当器件唤醒时，正常的处理器 I²C 硬件和/或软件可用于器件通信，其中包括使器件回到低功耗（即，休眠）模式所需的 I/O 序列。

提示：要产生唤醒脉冲，一种简单的方法是以 100 kHz 的频率发送字节 `0x00`。后续命令可采用更高的频率运行。

在 I²C 模式下，器件将忽略器件已经唤醒时发送的唤醒序列。

总线上有多个器件

当总线上有多个器件并且 I²C 接口以低于 300 kHz[2] 左右的速度运行时，传输某些数据模式将导致总线上的 ECC608-TMNGTLS 器件唤醒。频率越低，器件唤醒的概率越大。由于沿总线传输的后续器件地址将只匹配所需的器件，因此 ECC608-TMNGTLS 不会作出响应但会唤醒。建议在以较低频率与另一个器件通信后发出休眠或空闲序列，以使 ECC608-TMNGTLS 回到已知状态。

重要：t_{WLO} 是系统确保 ECC608-TMNGTLS 将在所有制造和环境条件下唤醒而必须提供的最短时间。实际上，更小宽度的脉冲也可能唤醒器件。

[2] 给定器件的实际频率将因工艺和环境因素而异。该值被认为在所有条件下都是安全的。

如果 I²C 总线上有多个器件，建议在上电序列之后、与总线上的任何器件通信之前唤醒 ECC608-TMNGTLS 器件。这是为了确保 ECC608-TMNGTLS 已正确初始化。

相关信息

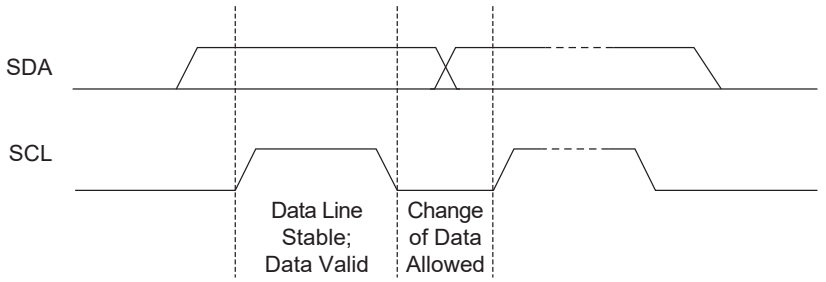
8.1.2. 器件唤醒
9.3. 交流参数：所有 I/O 接口

8.1.2 器件唤醒

当器件唤醒时，它将遵循下列条件：

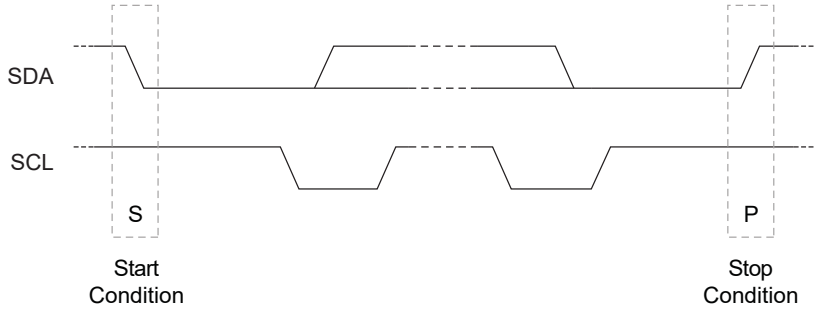
- **数据 0**：如果 SDA 为低电平且保持稳定，而 SCL 由低电平变为高电平再变为低电平，则将在总线上传输一个 0 位。当 SCL 为低电平时，SDA 可发生变化。
- **数据 1**：如果 SDA 为高电平且保持稳定，而 SCL 由低电平变为高电平再变为低电平，则将在总线上传输一个 1 位。当 SCL 为低电平时，SDA 可发生变化。

图 8-1. I²C 接口上的数据位传输



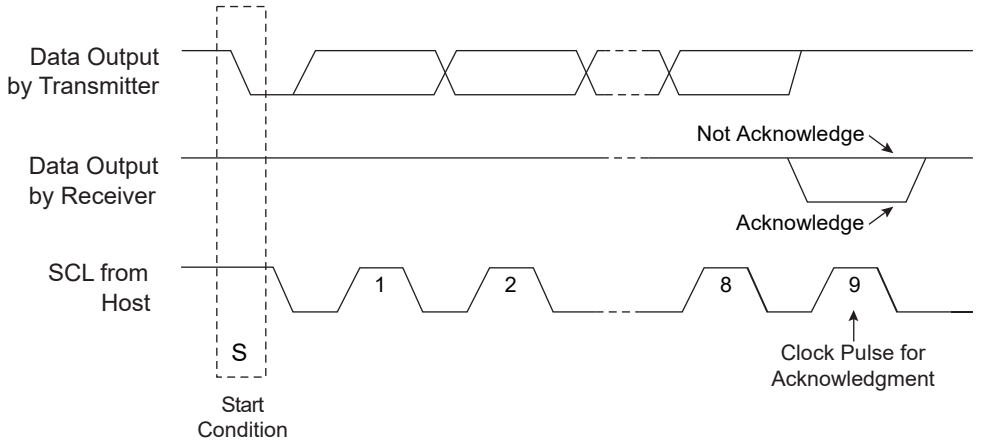
- **启动条件**：必须将 SDA 从高电平转换为低电平且 SCL 为高电平作为优先于所有命令的启动条件。
- **停止条件**：SDA 从低电平转换为高电平且 SCL 为高电平为停止条件。器件收到此条件后，当前的 I/O 事务结束。在输入端，如果器件有足够的字节来执行命令，则器件转换到繁忙状态并开始执行。必须始终在发送到器件的数据包的末尾发送停止条件。

图 8-2. I²C 接口上的启动和停止条件



- **应答（ACK）**：在每个地址或数据字节传输后的第 9 个时钟周期，接收器将拉低 SDA 引脚以确认正确接收字节。
- **不应答（NACK）**：在每个地址或数据字节传输后的第 9 个时钟周期，接收器也可使 SDA 引脚保持高电平，以指示接收字节时出现问题，或者此字节完成组传输。

图 8-3. I²C 接口上的 NACK 和 ACK 条件



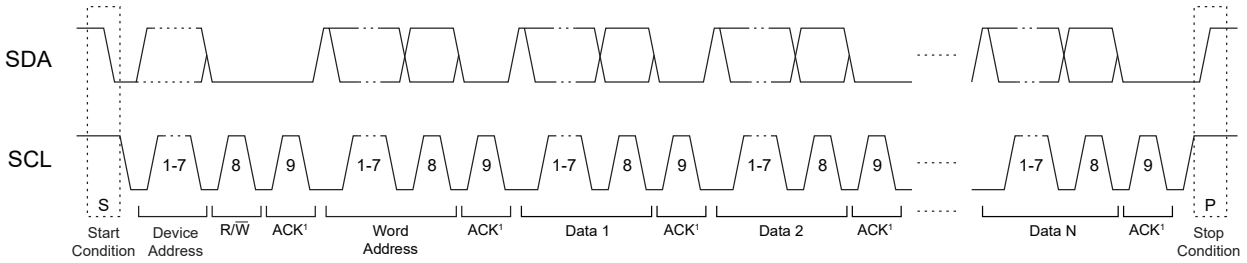
如果配置区域中的 I2C_Address 字节针对总线上的每个器件以不同方式编程，则多个 ECC608-TMNGTLS 器件可轻松共用相同 I²C 接口信号。由于器件地址的全部 7 个位均可编程，因此 ECC608-TMNGTLS 还可将 I²C 接口与任何 I²C 器件（包括任何串行 EEPROM）共用。

8.2 至 ECC608-TMNGTLS 的 I²C 传输

下图总结了从系统到 ECC608-TMNGTLS 的数据传输。传输顺序如下：

- 起始条件
- 器件地址字节
- 字地址字节
- 可选数据字节（1 至 N）
- 停止条件

图 8-4. 至 ECC608-TMNGTLS 的正常 I²C 传输



ECC608-TMNGTLS ACK 周期将 SDA 驱动为低电平。

下表标记了 I/O 事务的字节。标有“I²C 名称”的列提供了 AT24C16 数据手册中所描述字节的名称。

表 8-1. 至 ECC608-TMNGTLS 的 I²C 传输

名称	I²C 名称	说明
器件地址	器件地址	此字节选择 I²C 接口上的特定器件。如果此字节的 bit 1 至 bit 7 与配置区域中的 I2C_Address 字节的 bit 1 至 bit 7 匹配，则选择 ECC608-TMNGTLS。此字节的 bit 0 是标准 I²C R/W 位，必须为 0 以指示写操作（器件地址后的字节从主器件传输到从器件）。
字地址	字地址	要正常工作，此字节的值必须为 0x03。
命令	数据 1，N	由计数、命令数据包和 2 字节 CRC 组成的命令组。CRC 通过大小和数据包字节计算。

由于器件将命令输入缓冲区视为 FIFO，因此输入组可通过一个或多个 I²C 命令组发送到器件。发送到器件的第一个字节是计数，所以在器件接收到相应数量的字节之后，它将忽略随后接收的任何字节，直到执行完成。

系统必须在最后一个命令字节后发送一个停止条件，以确保 ECC608-TMNGTLS 将启动命令的计算。未能发送停止条件可能最终导致同步丢失；有关恢复程序，请参见 8.2.2. I2C 同步。

8.2.1 字地址值

在 I²C 写数据包期间，ECC608-TMNGTLS 会将发送的第二个字节解释为字地址，表示数据包功能，如下表所述：

表 8-2. 字地址值

名称	值	说明
复位	0x00	复位地址计数器。下一个 I²C 读取或写入事务将从 I/O 缓冲区起始处开始。
休眠（低功耗）	0x01	ECC608-TMNGTLS 进入低功耗休眠模式，忽略所有后续的 I/O 转换，直到下一个唤醒标志。器件的整个易失性状态将复位。
空闲	0x02	ECC608-TMNGTLS 进入空闲模式，忽略所有后续的 I/O 转换，直到下一个唤醒标志。TempKey、MessageDigestBuffer 和备用密钥寄存器的内容将保留。
命令	0x03	将后续字节写入输入命令缓冲区中先前写入内容之后的连续地址。这是正常操作。
保留	0x04 – 0xFF	这些地址不得发送到器件。

8.2.2 I²C 同步

系统可能会由于系统复位、I/O 噪声或其他条件而失去与 ECC608-TMNGTLS I/O 端口的同步。在这种情况下，ECC608-TMNGTLS 可能不会按预期响应，可能处于休眠状态，也可能在系统期望发送数据的时间间隔期间传输数据。要重新同步，可按照以下步骤操作：

1. 为了确保 I/O 通道复位，系统必须发送标准 I²C 软件复位序列，具体如下：
   - 一个启动位条件
   - 九个 SCL 周期，通过系统上拉电阻使 SDA 保持高电平
   - 另一个启动位条件
   - 一个停止位条件

   然后可能可以发送一个读序列，如果同步正确完成，ECC608-TMNGTLS 将确认器件地址。在数据周期内，器件可能返回数据，也可能使总线悬空（系统会将其解释为数据值 0xFF）。

   如果器件确认了器件地址，系统必须复位内部地址计数器，强制 ECC608-TMNGTLS 忽略可能已发送的任何部分输入命令。这可以通过将一个写序列发送到字地址 0x00（复位），然后再发送一个停止条件来实现。
2. 如果器件不通过 ACK 来响应器件地址，则它可能处于休眠状态。在这种情况下，系统必须发送一个完整的 Wake 令牌并在上升沿后等待 t_{WHI}。系统随后可以发送另一个读序列，如果同步完成，器件将确认器件地址。
3. 如果器件仍不通过 ACK 来响应器件地址，则它可能忙于执行命令。系统必须等待最长 t_{EXEC}（最大值），然后发送读取序列，这将由器件确认。

相关信息

8.1.1. 器件休眠

8.1.2. 器件唤醒

8.3 自 ECC608-TMNGTLS 的 I²C 传输

当 ECC608-TMNGTLS 唤醒且不繁忙时，主器件可以使用 I²C 读取从器件中获取当前输出缓冲区内容。如果有效的命令结果可用，则返回的组大小由已经运行的特定命令决定。否则，组大小（以及返回的第一个字节）将始终为 4：计数、状态/错误和 2 字节 CRC。

表 8-3. 自 ECC608-TMNGTLS 的 I²C 传输

名称	I²C 名称	方向	说明
器件地址	器件地址	至从器件	此字节选择 I²C 接口上的特定器件，如果此字节的 bit 1 至 bit 7 与配置区域中的 I2C_Address 字节的 bit 1 至 bit 7 匹配，则将选择 ECC608-TMNGTLS。此字节的 bit 0 是标准 I²C R/W 引脚，必须为 1 以指示器件地址后的字节从从器件传输到主器件（读操作）。
数据	数据 1，N	至主器件	由计数、状态/错误字节或输出数据包（后跟 2 字节的 CRC）组成的输出组。

主器件可以重复读取状态、错误或命令输出。每次 `Read` 命令沿 I²C 接口发送到 ECC608-TMNGTLS 时，器件均会发送输出缓冲区中的下一个连续字节。有关器件如何处理地址计数器的详细信息，请参见后续章节。

如果 ECC608-TMNGTLS 处于繁忙、空闲或休眠状态，它将不会确认读序列上的器件地址。如果部分命令已经发送到器件，并且读取序列`[Start + DeviceAddress(R/W == R)]`发送到器件，则 ECC608-TMNGTLS 将不会确认器件地址以指示没有数据可供读取。

8.4 休眠序列

系统完成使用 ECC608-TMNGTLS 后，建议发出休眠序列，使器件进入低功耗模式。此序列包含正确的器件地址，接着是值 0x01（作为字地址），然后是停止条件。这种到低功耗状态的转换会导致器件的内部命令引擎和输入/输出缓冲区完全复位。当器件唤醒且不忙时，此序列可随时发送到器件。

相关信息

8.1.1. 器件休眠
8.1.2. 器件唤醒

8.5 空闲序列

如果所需命令的总序列超过 $t_{WATCHDOG}$，则器件将自动进入休眠状态，并丢失存储在易失性寄存器中的任何信息。在看门狗时间间隔完成之前将器件置于空闲模式可防止此操作。当器件收到 Wake 令牌时，它将重新启动看门狗定时器，并继续执行。

此空闲序列包含正确的器件地址，接着是值 0x02（作为字地址），然后是停止条件。当器件唤醒且不忙时，此序列可随时发送到器件。

9. 电气特性

9.1 绝对最大值

工作温度	-40°C 至+85°C
储存温度	-65°C 至+150°C
最大工作电压	6.0V
直流输出电流	5.0 mA
任一引脚上的电压 -0.5V 至（V_{CC} + 0.5V）	-0.5V 至（V_{CC} + 0.5V）
ESD 额定值：	
人体模型（Human Body Model，HBM）ESD	>4 kV
充电器件模型（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。器件长时间工作在最大值条件下，其可靠性可能受到影响。

9.2 可靠性

ECC608-TMNGTLS 采用 Microchip 公司具有极高可靠性的 CMOS EEPROM 制造技术生产。

表 9-1. EEPROM 可靠性

参数	最小值	典型值	最大值	单位
+85°C 时的耐写入次数（每个字节）	400,000	—	—	写周期
+70°C 时的数据保持时间	15	—	—	年
+55°C 时的数据保持时间	45	—	—	年
耐读取次数	无限			读周期

9.3 交流参数：所有 I/O 接口

图 9-1. 唤醒时序：所有接口

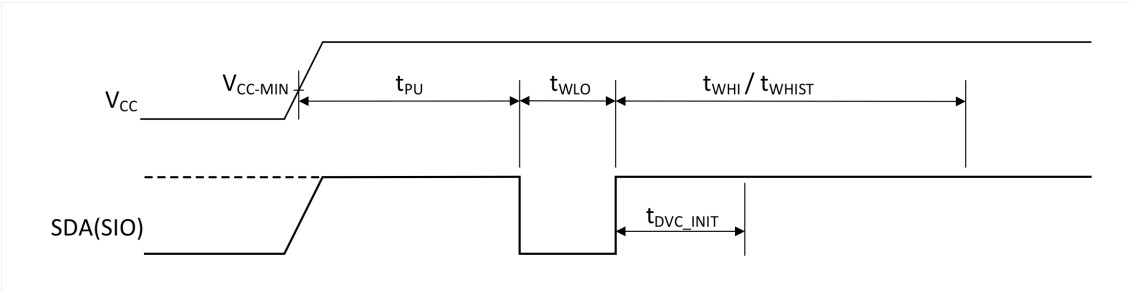


图 9-2. 输入噪声抑制：所有接口

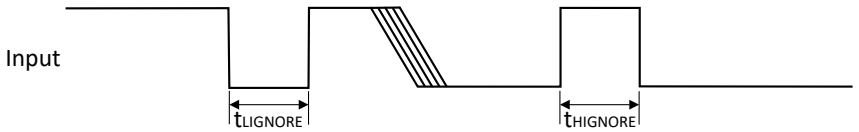


表 9-2. 交流参数：所有 I/O 接口

参数	符号	方向	最小值	典型值	最大值	单位	条件
上电延时	t_{PU}	至加密器件	100	—	—	µs	从 V_{CC} > V_{CC} 最小值到 t_{WLO} 开始的最短时间。
唤醒为低电平的持续时间	t_{WLO}	至加密器件	60	—	—	µs	—
初始化时间(1)	t_{DVC_INIT}	内部	—	—	400	µs	从唤醒脉冲的上升沿到器件初始化的最长时间。(2)
唤醒为高电平到数据通信的延时	t_{WHI}	至加密器件	1500	—	—	µs	除非实现了轮询，否则建议使 SDA 在整个过程中保持稳定的高电平状态。上电时不使能自检。
使能自检时唤醒为高电平的延时	t_{WHIST}	至加密器件	20	—	—	ms	除非实现了轮询，否则建议使 SDA 在整个过程中保持稳定的高电平状态。
上桥臂毛刺滤波器激活时间(1)	$t_{HIGNORE\_A}$	至加密器件	45	—	—	ns	无论激活时的状态如何，宽度短于此时间的脉冲都将被器件忽略。
下桥臂毛刺滤波器激活时间(1)	$t_{LIGNORE\_A}$	至加密器件	45	—	—	ns	无论激活时的状态如何，宽度短于此时间的脉冲都将被器件忽略。
下桥臂毛刺滤波器休眠时间(1)	$t_{LIGNORE\_S}$	至加密器件	15	—	—	µs	处于休眠模式时，宽度短于此时间的脉冲将被器件忽略。
看门狗超时	$t_{WATCHDOG}$	至加密器件	0.7	1.3	1.7	s	从唤醒到强制器件进入休眠模式的时间（Config.ChipMode[2]为 0 时）。

注：

1. 这些参数通过表征确定，但未经生产测试。
2. 在 t_{DVC_INIT} 时间结束之前，除了唤醒脉冲之外，建议不要在 I^2C 总线上进行任何通信。

9.3.1 交流参数：I²C 接口

图 9-3. I²C 同步数据时序

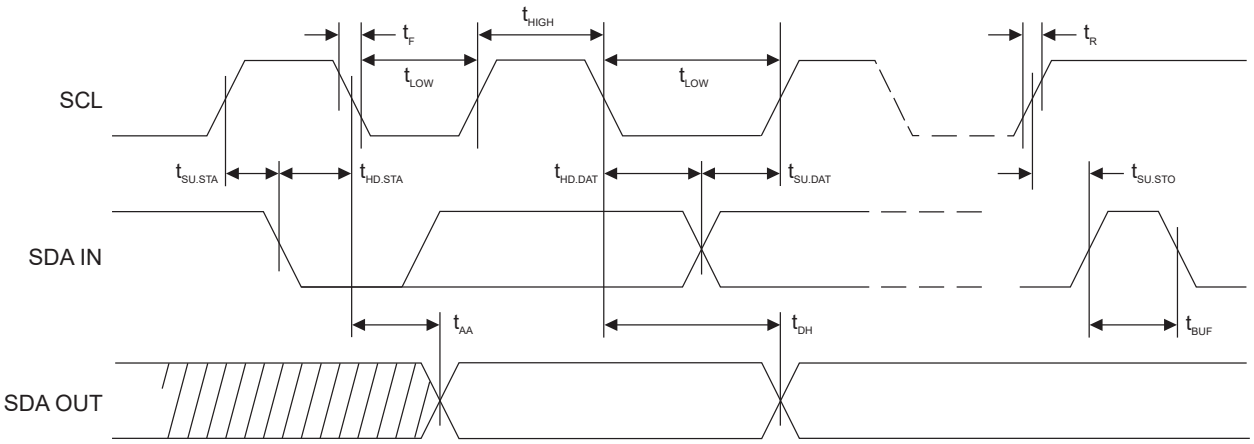


表 9-3. I²C 接口的交流特性**(2)**

除非另外说明，否则适用的推荐工作范围为：T_A = -40°C 至+85°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
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
时钟低电平到数据输出有效的时间	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	35	ms
在新传输开始前时间总线必须保持空闲的时间 [1]	t_{BUF}	500	—	ns

注：

1. 上述值均基于表征，但未经测试。
2. 交流测量条件：
   - R_L（连接 SDA 和 V_{CC}）：1.2 kΩ（对于 V_{CC} = +2.0V 至+5.0V）
   - 输入脉冲电压：0.3V_{CC} 至 0.7V_{CC}
   - 输入上升和下降时间： ≤ 50 ns
   - 输入和输出时序参考电压：0.5V_{CC}

9.4 直流参数：所有 I/O 接口

表 9-4. 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
电源电压	V_{CC}	2.0	—	5.5	V	—
电源工作电流	I_{CC}	—	2	3	mA	在 I/O 传输或非 ECC 命令执行期间等待 I/O。与时钟分频值无关。
		—	—	14	mA	在 ECC 命令执行期间。时钟分频比 = 0x0
电源空闲电流	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
休眠电流	I_{SLEEP}	—	30	150	nA	当器件处于休眠模式时，V_{CC} ≤ 3.6V，V_{SDA} 和 V_{SCL} < 0.4V 或 > V_{CC} - 0.4，T_A ≤ +55°C
		—	—	2	µA	当器件处于休眠模式时。 在整个 V_{CC} 电压范围和-40°C 至 85°C 温度范围内。
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
热阻	Θ_{JA}	—	166	—	°C/W	SOIC（SS）
		—	173	—	°C/W	UDFN（MA）

9.4.1 V_{IH} 和 V_{IL} 规格

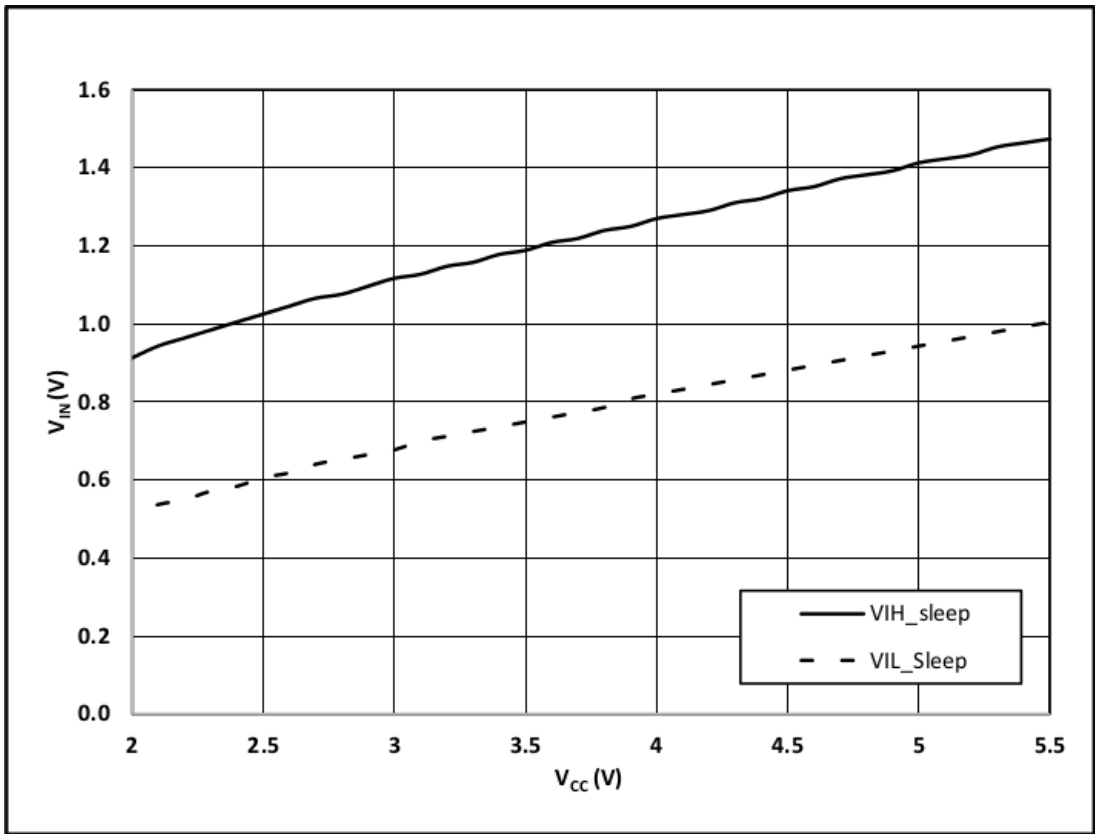
器件的输入电平因器件模式和电压而异。在休眠或空闲模式下，输入电压阈值取决于 V_{CC} 电平，如图 9-4 所示。在休眠或空闲模式下，TTLenable 位不起作用。

ECC608-TMNGTLS 的有效输入电平为固定值，不会随 V_{CC} 电平变化。发送至器件的输入电平必须符合下表。

表 9-5. 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 9-4. 休眠模式和空闲模式下的 V_{IH} 和 V_{IL}



10. 封装图

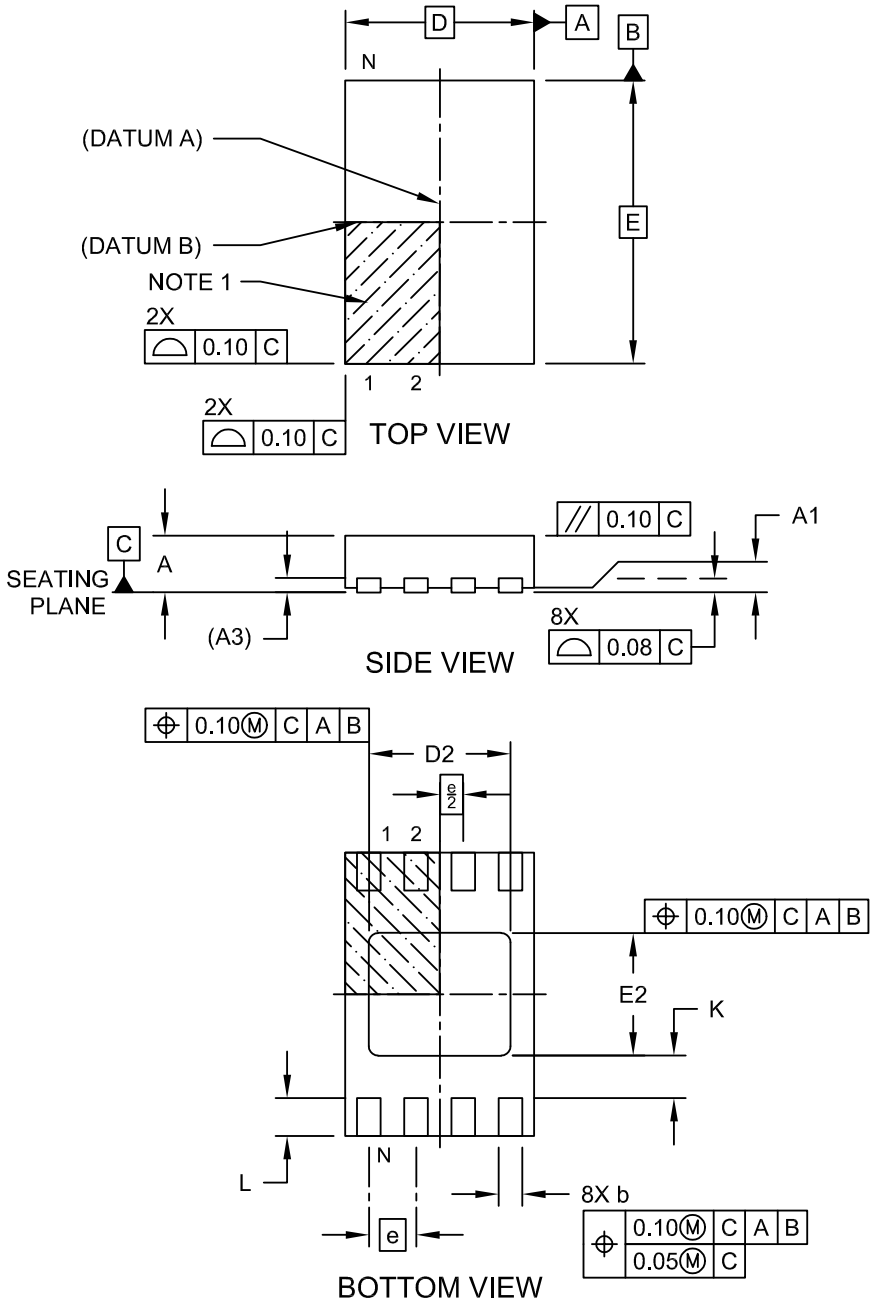
10.1 封装标识信息

作为 Microchip 整体安全功能的一部分，所有加密器件的器件标识都有意进行了模糊处理。封装顶部的标识不提供有关器件的实际类型或制造商的任何信息。封装上的字母数字代码提供制造信息，并随装配批次变化。建议不使用封装标识作为即将进行的任何检查步骤的一部分。

10.2 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

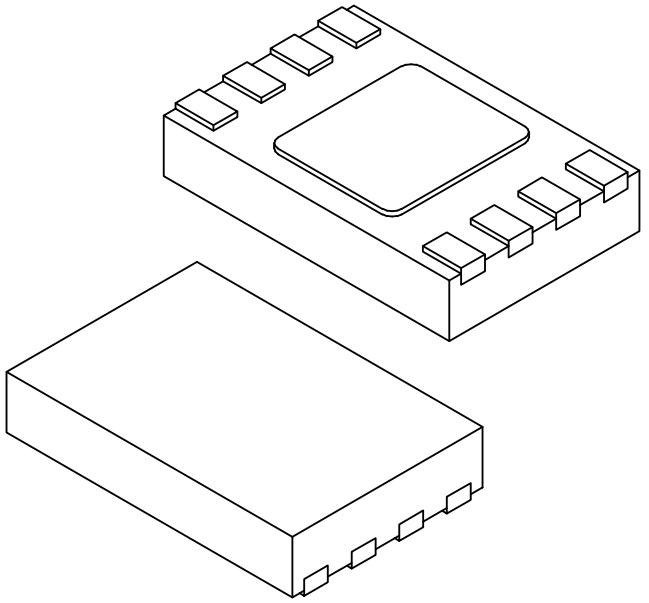
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing C04-21355-Q4B Rev C 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	0.25	0.35	0.45
Terminal-to-Exposed-Pad	K	0.20	-	-

Notes:

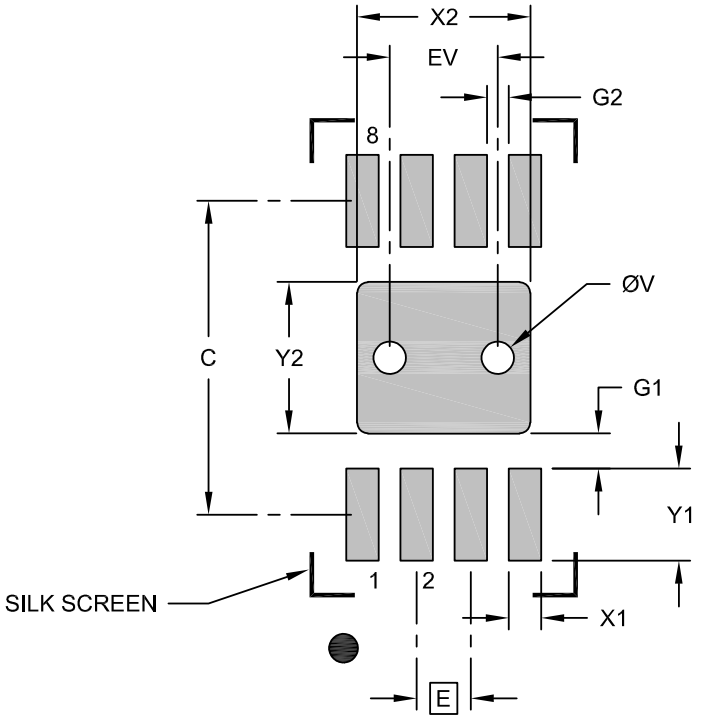
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M

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 C 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:

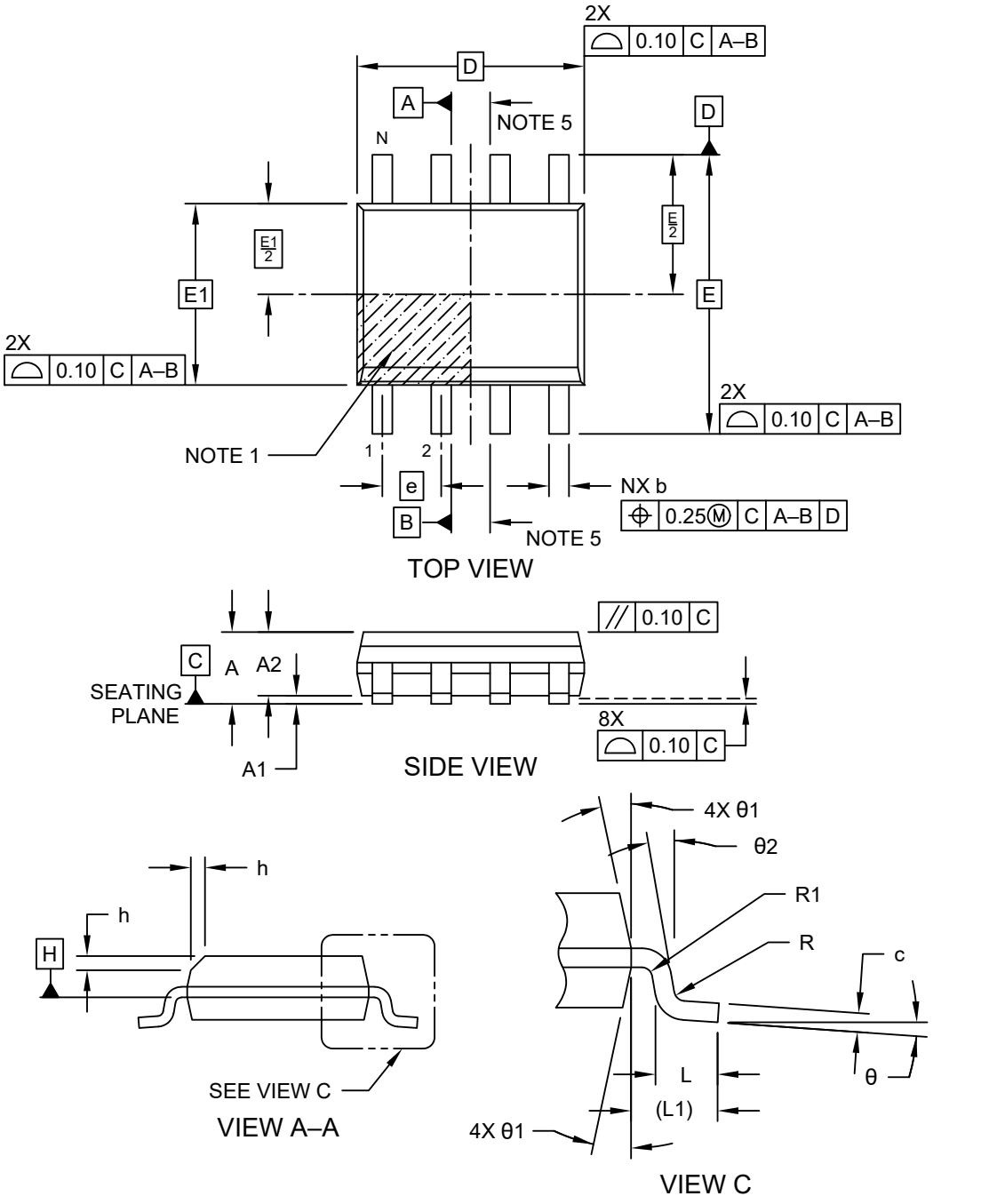
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
2. For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

Microchip Technology Drawing C04-23355-Q4B Rev C

10.3 8 引脚 SOIC

8-Lead Plastic Small Outline (C2X) - 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

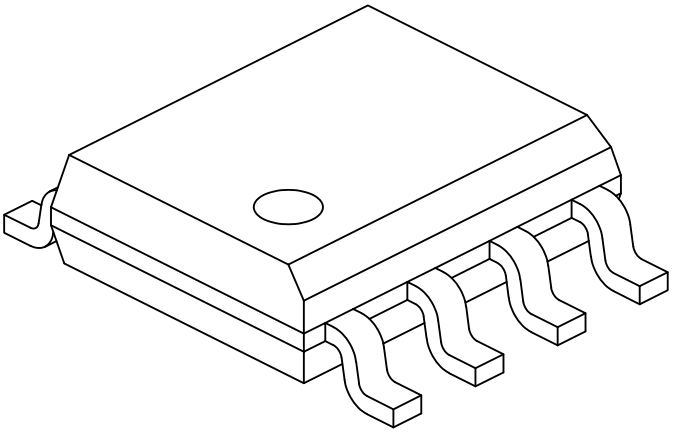


Microchip Technology Drawing No. C04-057-C2X Rev K Sheet 1 of 2

Packaging Diagrams and Parameters

8-Lead Plastic Small Outline (C2X) - 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	
Lead Thickness	c	0.17	–	0.25
Lead Width	b	0.31	–	0.51
Lead Bend Radius	R	0.07	–	–
Lead Bend Radius	R1	0.07	–	–
Foot Angle	θ	0°	–	8°
Mold Draft Angle	θ1	5°	–	15°
Lead Angle	θ2	0°	–	–

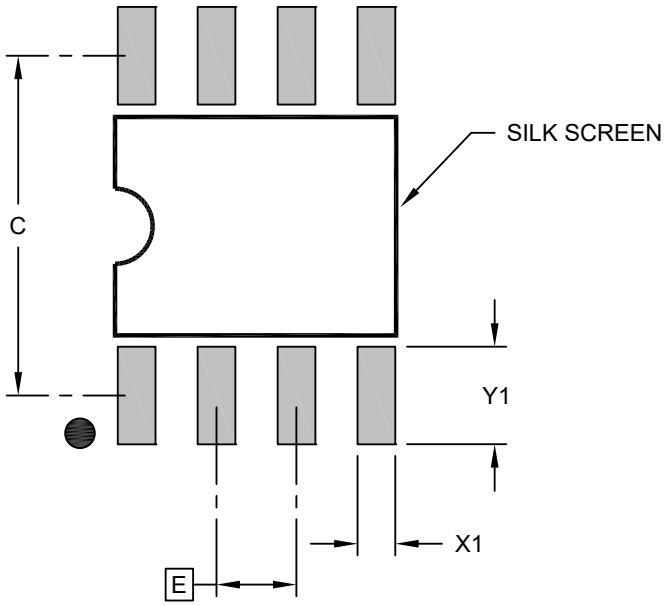
Notes:

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-C2X Rev K Sheet 2 of 2

8-Lead Plastic Small Outline (C2X) - Narrow, 3.90 mm (.150 In.) Body [SOIC]

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-C2X Rev K

11. 版本历史

版本 A（2024 年 3 月）

- 本文档的初始版本

Microchip 信息

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	-	Trust Type	Trust Option	Package Type	-	Shipping Option
xxxxx	-	ttt	vvv	p	-	x

器件：	ECC608：具有基于硬件的安全密钥存储功能的预配置加密协处理器	
可信类型	TMNG	Microchip 可信产品的类型
可信选项	TLS	与可信产品相关的配置。
封装选项	U	8 焊盘（主体 2 x 3 x 0.6 mm）增强散热型塑封超薄双列扁平无引线封装（UDFN）
	S	8 引脚（主体宽 0.150”）塑封鸥翼小外形封装（JEDEC SOIC）
交付选项(1,2)		最小起订量（MOQ）为 2k 件。
	B	每批 10 件——原型器件

示例：

- ECC608-TMNGTLSU：Trust Manager TLS，预配置，8-UDFN，2k MOQ，I^2C 接口
- ECC608-TMNGTLSU-B：Trust Manager TLS，预配置原型，8-UDFN，每批 10 件，I^2C 接口
- ECC608-TMNGTLSS：Trust Manager TLS，预配置，8-SOIC，2k MOQ，I^2C 接口
- ECC608-TMNGTLSS-B：Trust Manager TLS，预配置原型，8-SOIC，每批 10 件，I^2C 接口

注：

1. 生产订单将以卷带形式交付。卷盘的实际尺寸将取决于具体的客户订单。最小起订量（MOQ）为 2k 件。
2. 原型器件仅提供 10 件样片，带 I^2C 接口，并且可提供 SOIC 或 UDFN 封装选项。

Microchip 器件代码保护功能

请注意以下有关 Microchip 产品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：在正常使用且符合工作规范的情况下，Microchip 系列产品非常安全。
- Microchip 注重并积极保护其知识产权。严禁任何试图破坏 Microchip 产品代码保护功能的行为，这种行为可能会违反《数字千年版权法案》（Digital Millennium Copyright Act）。
- 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。

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。

本出版物及其提供的信息仅适用于 Microchip 产品，包括设计、测试以及将 Microchip 产品集成到您的应用中。以其他任何方式使用这些信息都将被视为违反条款。本出版物中的器件应用信息仅为您提供便利，将来可能会发生更新。如需额外的支持，请联系当地的 Microchip 销售办事处，或访问 www.microchip.com/en-us/support/design-help/client-support-services。

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、AVR、AVR 徽标、AVR Freaks、BesTime、BitCloud、CryptoMemory、CryptoRF、dsPIC、flexPWR、HELDO、IGLOO、JukeBlox、KeeLoq、Kleer、LANCheck、LinkMD、maXStylus、maXTouch、MediaLB、megaAVR、Microsemi、Microsemi 徽标、MOST、MOST 徽标、MPLAB、OptoLyzer、PIC、picoPower、PICSTART、PIC32 徽标、PolarFire、Prochip Designer、QTouch、SAM-BA、SenGenuity、SpyNIC、SST、SST 徽标、SuperFlash、Symmetricom、SyncServer、Tachyon、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。

AgileSwitch、ClockWorks、The Embedded Control Solutions Company、EtherSynch、Flashtec、Hyper Speed Control、HyperLight Load、Libero、motorBench、mTouch、Powermite 3、Precision Edge、ProASIC、ProASIC Plus、ProASIC Plus 徽标、Quiet-Wire、SmartFusion、SyncWorld、TimeCesium、TimeHub、TimePictra、TimeProvider 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、Augmented Switching、BlueSky、BodyCom、Clockstudio、CodeGuard、CryptoAuthentication、CryptoAutomotive、CryptoCompanion、CryptoController、dsPICDEM、dsPICDEM.net、Dynamic Average Matching、DAM、ECAN、Espresso T1S、EtherGREEN、EyeOpen、GridTime、IdealBridge、IGaT、In-Circuit Serial Programming、ICSP、INICnet、Intelligent Paralleling、

ISBN： 978-1-6683-0018-3

质量管理体系

有关 Microchip 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	**澳大利亚 - 悉尼** 电话：61-2-9868-6733	**印度 - 班加罗尔** 电话：91-80-3090-4444	**奥地利 - 韦尔斯** 电话：43-7242-2244-39 传真：43-7242-2244-393
亚特兰大 德卢斯，佐治亚州 电话：678-957-9614 传真：678-957-1455	**中国 - 北京** 电话：86-10-8569-7000	**印度 - 新德里** 电话：91-11-4160-8631	**丹麦 - 哥本哈根** 电话：45-4485-5910 传真：45-4485-2829
奥斯汀，德克萨斯州 电话：512-257-3370	**中国 - 成都** 电话：86-28-8665-5511	**印度 - 浦那** 电话：91-20-4121-0141	**芬兰 - 埃斯波** 电话：358-9-4520-820
波士顿 韦斯特伯鲁，马萨诸塞州 电话：774-760-0087 传真：774-760-0088	**中国 - 重庆** 电话：86-23-8980-9588	**日本 - 大阪** 电话：81-6-6152-7160	**法国 - 巴黎** 电话：33-1-69-53-63-20 传真：33-1-69-30-90-79
芝加哥 艾塔斯卡，伊利诺伊州 电话：630-285-0071 传真：630-285-0075	**中国 - 东莞** 电话：86-769-8702-9880	**日本 - 东京** 电话：81-3-6880-3770	**德国 - 加兴** 电话：49-8931-9700
达拉斯 阿迪森，德克萨斯州 电话：972-818-7423 传真：972-818-2924	**中国 - 广州** 电话：86-20-8755-8029	**韩国 - 大邱** 电话：82-53-744-4301	**德国 - 哈恩** 电话：49-2129-3766400
底特律 诺维，密歇根州 电话：248-848-4000	**中国 - 杭州** 电话：86-571-8792-8115	**韩国 - 首尔** 电话：82-2-554-7200	**德国 - 海尔布隆** 电话：49-7131-72400
休斯顿，德克萨斯州 电话：281-894-5983	**中国 - 香港特别行政区** 电话：852-2943-5100	**马来西亚 - 吉隆坡** 电话：60-3-7651-7906	**德国 - 卡尔斯鲁厄** 电话：49-721-625370
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	**中国 - 南京** 电话：86-25-8473-2460	**马来西亚 - 槟榔屿** 电话：60-4-227-8870	**德国 - 慕尼黑** 电话：49-89-627-144-0 传真：49-89-627-144-44
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	**中国 - 青岛** 电话：86-532-8502-7355	**菲律宾 - 马尼拉** 电话：63-2-634-9065	**德国 - 罗森海姆** 电话：49-8031-354-560
罗利，北卡罗来纳州 电话：919-844-7510	**中国 - 上海** 电话：86-21-3326-8000	**新加坡** 电话：65-6334-8870	**以色列 - 霍德夏沙隆** 电话：972-9-775-5100
纽约，纽约州 电话：631-435-6000	**中国 - 沈阳** 电话：86-24-2334-2829	**台湾地区 - 新竹** 电话：886-3-577-8366	**意大利 - 米兰** 电话：39-0331-742611 传真：39-0331-466781
圣何塞，加利福尼亚州 电话：408-735-9110 电话：408-436-4270	**中国 - 深圳** 电话：86-755-8864-2200	**台湾地区 - 高雄** 电话：886-7-213-7830	**意大利 - 帕多瓦** 电话：39-049-7625286
加拿大 - 多伦多 电话：905-695-1980 传真：905-695-2078	**中国 - 苏州** 电话：86-186-6233-1526	**台湾地区 - 台北** 电话：886-2-2508-8600	**荷兰 - 德卢内市** 电话：31-416-690399 传真：31-416-690340
	中国 - 武汉 电话：86-27-5980-5300	**泰国 - 曼谷** 电话：66-2-694-1351	**挪威 - 特隆赫姆** 电话：47-72884388
	中国 - 西安 电话：86-29-8833-7252	**越南 - 胡志明市** 电话：84-28-5448-2100	**波兰 - 华沙** 电话：48-22-3325737
	中国 - 厦门 电话：86-592-2388138		**罗马尼亚 - 布加勒斯特** 电话：40-21-407-87-50
	中国 - 珠海 电话：86-756-3210040		**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