SE050

即插即信安全元件

第 1.3 版——2019 年 6 月 7 日 客观数据手册
504913

1. 简介

SE050 是一款即用型物联网安全元件解决方案。它在 IC 级别提供信任根。通过开箱即用的方式，为物联网系统提供从边缘到云的最新安全功能。

SE050 支持安全存储和配置凭据，并为安全关键通信和控制功能运行加密操作。SE050 在物联网用例中的用途广泛，适用于安全连接到公有/私有云、设备到设备认证或传感器数据保护。

SE050 拥有操作系统级别的独立通用标准 EAL6+安全认证，并支持具有高密钥长度和可经未来 ECC 曲线证明的 RSA 和 ECC 非对称密码算法。即使面对复杂的非侵入式和侵入式攻击，这一最新的安全措施也能保护 IC。

SE050 是一个一站式解决方案，附带 Java Card 操作系统和针对预安装物联网安全用例进行优化的小程序。此外，产品还获得全面产品支持包的补充，可通过用于主机应用的即插即信中介层、简单易用的开发套件、参考设计以及用于产品评估的大量文档来实现快速上市和轻松设计。

SE050 是一个产品平台，提供多种引脚对引脚兼容的产品变型，请参见[4]。

可以在 www.nxp.com 上的应用笔记中找到有关集成的其他信息。另请参见[3]。

1.1 SE050 用例

- 安全连接到公有/私有云、边缘计算平台、基础设施
- 设备至设备认证
- 安全数据保护
- 安全调试支持
- 安全 CL/MIFARE/Wi-Fi 互动
- 区块链的器件 ID
- 关键密钥存储
- 安全凭证配置
- 生态系统保护

1.2 SE050 目标应用

- 智能工业
- 智能家居
- 智慧城市
- 智能供应链

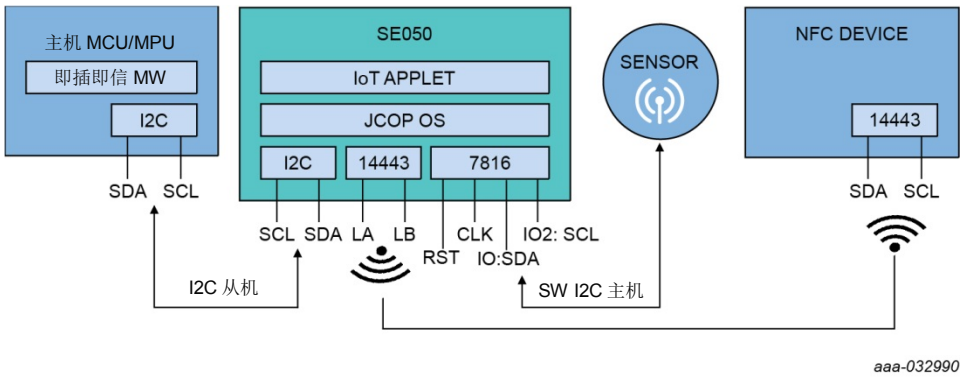

图 1.SE050 解决方案框图

注：SE050 设计用作物联网系统的一部分。它的作用是连接到主机控制器的辅助安全器件。主机控制器通过 I²C 接口与 SE050 通信（主机控制器为主机，SE050 为从机）。除了与主机控制器的强制连接之外，SE050 器件还可以选择通过单独的 I²C 接口连接到传感器节点或类似元件。在这种情况下，SE050 器件是主机，传感器节点是从机。最后，SE050 配备用于本地非接触式天线的连接，可提供无线接口以连接智能手机之类的外部器件。

1.3 SE050 命名约定

下表解释了 SE050 平台的商品名命名约定。每款 SE050 产品都会被分配一个这样的商品名，其中包括特定应用数据。

SE050 商业名称格式如下。

Sx05yagddd/Zrrff

所有字母的释义请见表 1。

表 1. SE050 商业名称格式

变量	含义	值	说明
x	接口	E	E=I²C 主机，从机
y	JCOP 版本	0	
a	小程序配置	A B C	具有不同密钥配置选项的配置选项，见[4]
g	温度范围	1 2	标准工作环境温度 1 = -25 °C - 90 °C , 2 = -40 °C - 105 °C
ddd	交付类型	HQ1	HX2QFN20
mrrff		字母和数字	用于识别各个配置的恩智浦内部代码

2. 特性和优势

2.1 主要优势

- 即插即信，提供完整的产品支持包，可快速轻松地进行设计
- 易于与不同的 MCU 和 MPU 平台以及 OS（Linux、RTOS、Windows、Android 等）集成
- 一站式解决方案，是系统级安全的理想选择，无需编写安全代码
- 在 IC 级别进行安全凭证注入以建立信任根
- 与公有云和私有云的安全零接触连接
- 真正从传感器到云的端到端安全性
- 为每个关键用例提供现成的示例代码

2.2 主要特性

SE050 基于恩智浦的整体安全体系结构 3.0™，可为各种安全威胁提供安全有效的保护。安全措施的效率已通用标准 EAL6+认证的证明。

SE050 基于集成的 Javacard 操作系统和小程序实现完全自动运行。只有通过小程序的固定功能，才能实现直接存储器访问。因此，存储器的内容与主机系统是完全隔离的。

- 恩智浦整体安全体系结构 3.0™
- 使用先进的 40 nm 芯片制造技术
- 将获得 CC EAL6+认证的硬件和操作系统用作恩智浦物联网应用的运行环境，支持完全加密通信和安全生命周期管理
- 有效防御高级攻击，包括各种功率分析和故障攻击
- 多个逻辑和物理保护层，包括金属屏蔽、端到端加密、内存加密、篡改检测
- 支持 RSA 和 ECC 非对称密码算法，未来曲线和较长的密钥长度，例如 Brainpool、Edwards 和 Montgomery 曲线
- 支持使用 AES 和 DES 对称密码算法进行加密和解密
- HMAC、CMAC、SHA-1、SHA-224/256/384/512 操作
- 各类密钥派生功能选项，包括 HKDF、MIFARE KDF、PRF(TLS-PSK)
- 适用于工业应用的可选扩展温度范围（-40°C 至+105°C）
- 小尺寸 HX2QFN20 封装(3x3 mm)
- 标准物理接口 I^2C 从机（高速模式，3.4 Mbps），I^2C 主从机（快速模式，400 kbps）。两者可以同时激活
- 用于物联网用例的专用 CL 无线接口，可简化配置、现场维护和后期配置
- 高达 50 kB 的安全用户闪存，用于加密数据或密钥存储
- 支持 SCP03 协议（总线加密和加密凭据注入），将主机与安全元件安全绑定
- 支持小程序级的安全传送信息通道，可在多租户生态系统中进行端到端的加密通信

2.3 功能详解

表 2. 功能概述

分类	子类别	值
标准	安全认证	CC EAL6+ (HW+JCOP)
	JavaCard 版本	3.0.5
	GlobalPlatform 规范版本	GP 3.0
加密	ECC	ECDSA、ECDH、ECDHE、ECDAA、EDDSA
	Hash	HMAC、安全 HMAC、CMAC
	SHA	SHA-1、SHA-224、SHA-256、SHA-384、SHA-512
	密钥派生	HKDF、PBKDF、Wi-Fi KDF、OPC_UA KDF PRF (TLS-PSK)
	AES	用于解密/加密的 AES 密码
	RSA	用于解密/加密的 RSA 密码（最高 4096 位）
加密曲线	ECC	ECC NIST（192 至 521 位）
		Brainpool（160 至 512 位）
		Twisted Edwards Ed25519
		Montgomery 曲线 25519
		Koblitz（192 至 256 位）
		Barreto-Naehrig 曲线（256 位）
用户存储器		50 kB
存储器可靠性		高达 100 百万写入周期/ 25 年
接口	I^2C 从机	高速模式(3.4 Mbps)
	I^2C 主机	快速模式(400 kbit/s)
	非接触式	ISO14443
节电模式	空闲	~1.8 mA
	掉电（带状态保持）	~430 µA
	深度掉电（无状态保留）	<5 µA
温度	标准	-25 - 85 °C
	扩展范围	-40 - +105 °C
封装	塑料 QFN	3x3 mm (HX2QFN20)

3. 功能说明

3.1 功能框图

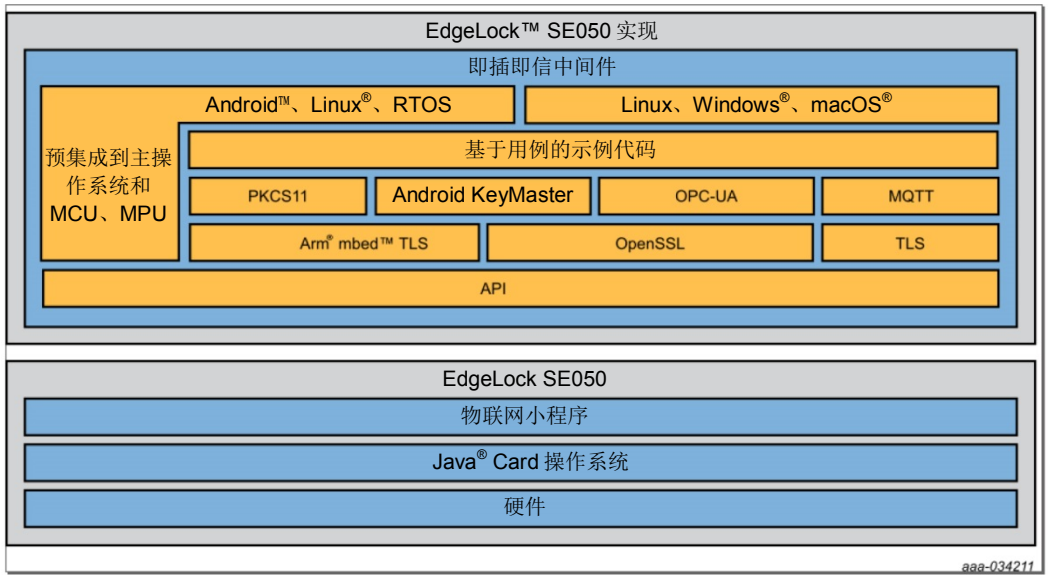

图 2.SE050 功能图——示例 Open SSL

SE050 使用 I^2C 作为通信接口。第 4 节将提供更多详细信息。SE050 命令使用 Smartcard T=1 over I² C (T=1o I^2C)协议进行打包。恩智浦 DocStore 中提供了 SE050 命令的详细文档（见[3]）和基于 T=1 over I^2C 协议封装。

为了简化产品使用，SE050 提供了一个主机库，该主机库抽象了 SE050 命令和 T=1 over I^2C 协议封装。支持各类平台的主机库已提供下载，包括 SE050 网站上提供的完整源代码。

SE050 物联网小程序配备通用文件系统，能够安全地存储安全对象和相关的权限管理。所有对象都可以存储在永久性存储器或 RAM 中，并提供安全导出和导入功能，以便存储在外部存储器中。所有安全对象均配备基本的文件操作，例如写入、读取、删除和更新。

3.1.1 受支持的安全对象类型

安全对象是 SE050 文件系统中的一个条目。每个安全对象都具有特定功能。可以使用以下安全对象类型：

- 对称密钥（AES、DES）
- ECC 密钥
- RSA 密钥
- HMAC 密钥
- 二进制文件
- 用户 ID
- 计数器
- 哈希扩展寄存器

3.1.1.1 对称密钥

对称密钥对象可以安全地存储 AES 128、192 和 256 位对称密钥以及带有单个 DES、2K3DES 和 3K3DES 的 DES 密钥。可在对称密钥对象上进行以下特定操作：

- 加密
- 解密
- 派生
- CMAC
- 安全导入

3.1.1.2 ECC 密钥

ECC 密钥对象具有安全存储 ECC 密钥（使用以下曲线和密钥大小）的能力：

- ECC NIST 曲线：NIST P-192、NIST P-224、NIST P-256、NIST P-384、NIST P-521
- ECC Brainpool 曲线：160 位、192 位、224 位、256 位、320 位、384 位、512 位
- ECC Ed25519 曲线：256 位
- ECC Montgomery 曲线 25519：256 位
- ECC Koblitz 曲线：secp160k1、secp192k1、secp224k1、secp256k1
- ECC 曲线：secp192r1、secp224r1、secp256r1、secp384r1、secp521r1
- ECC Barreto-Naehrig 256 位曲线

可在 ECC 密钥对象上进行以下操作（并非所有操作都适用于所有曲线）：

- ECDSA/EDDSA 签名
- ECDSA/EDDSA 验证
- ECDH 生成共享秘密
- ECDAA 签名
- ECDAA 验证
- 生成密钥
- 安全导入

3.1.1.3 RSA 密钥

RSA 密钥对象具有安全存储高达 4096 位 RSA 密钥的能力。可在 RSA 密钥对象上进行以下特定操作：

- RSA 签名
- RSA 验证
- RSA 加密
- RSA 解密
- 安全导入

3.1.1.4 HMAC 密钥对象

HMAC 密钥对象允许安全地存储 HMAC 密钥。可在 HMAC 密钥对象上进行以下操作来计算 HMAC：

- 初始化

- 更新
- 完成

3.1.1.5 二进制文件对象

二进制文件对象是通用类型的字节数组。与在标准文件系统中一样，可以使用读/写操作来访问这些值。

3.1.1.6 计数器对象

计数器对象是特殊类型的二进制文件对象，具有解释文件内容的特定功能。

计数器对象支持的操作是：

- 置位
- 取值
- 递增

3.1.1.7 哈希扩展寄存器

哈希扩展寄存器安全对象存储提供给该安全对象的所有数据的哈希值。因此，它包含自上次重启或创建以来提供给该寄存器的值的完整历史记录，并且可用于证明目的。

3.1.1.8 用户 ID 安全对象

在需要多租户支持且无需使用加密凭据的情况下，可以使用用户 ID 安全对象，基于用户 ID 创建会话。

3.1.2 访问控制

每个安全对象都可以链接到特定于对象的访问控制策略。访问控制策略将由认证标识的用户与一组权限（例如读、写…）关联在一起。

为了将功能扩展到广泛的生态系统中，产品提供一组不同的认证选项：

- 基于用户 ID 的认证
- 基于对称密钥的身份验证（带和不带安全传送信息）
- 基于非对称密钥的身份验证（带和不带安全传送信息）
  在创建安全对象时，一组可选策略将与安全对象相关联。每个策略可将对象所允许的的一组操作分配给认证对象。

3.1.3 会话和多线程

SE050 物联网小程序专为需要在 APDU 级别上使用多线程和多租户用例的生态系统而准备。为了实现这一系统，小程序支持 2 个同时进行的会话（这些会话可以跨越完整的安全传送信息会话）、为不需要持久会话的租户提供经过自我认证的 APDU，以及对于单租户用例的置顶默认会话。

3.1.4 认证和信任配置

SE050 小程序随附了一组进行了信任配置的根凭据，使器件所有者可以安全地认证生成的所有安全密钥。除此之外，客户可以定义自己的认证密钥。

3.1.5 应用支持

对于特定的生态系统，SE050 物联网小程序配备内置加密功能，以简化特定用例的部署，例如

- MIFARE SAM 功能
- Wifi 密码保护
- 基于 ECC 密钥和 RSA 密钥的云连接
- 使用 I^2C 主机读取安全传感器
- 远程认证和信任配置
- 平台配置寄存器

3.2 凭证存储和存储器

在 SE050 中，所有凭据和安全对象都存储在动态文件结构中。在创建时，用户必须将文件标识符与创建的对象相关联。然后，此标识符将在后续操作中用于访问对象。可以分配的对象数量仅受系统中可用存储器的限制。在完成使用后，就可以删除对象，重新释放关联的存储器。

在使用过程中也有可能创建临时对象。临时对象的对象描述符存储在非挥发性记忆体中，但是对象内容存储在 RAM 中。与 SE050 的导入/导出功能一起使用，就可以使用临时对象将密钥安全地存储在远程存储器系统中。

3.3 简单易用的配置

所有 SE050 变体都已预配置，以便在开发阶段易于使用。

因此，客户将在主要用例中，获得 SE050 所需的所有预插入密钥。

4. 通信接口

4.1 I^2C 接口

SE050 配置一个支持从机的 I^2C 接口和一个支持主机的 I^2C 接口。

I^2C 从机接口是器件的主要通信接口，由主机控制器用来将任意 APDU 发送到器件。在高速模式(HS)下运行时，支持高达 3.4 MHz 的时钟频率。I^2C 接口使用 Smartcard T=1 over I^2C 协议。

SE050 的默认从机地址配置为 0x48。

I^2C 主机接口应该与需要安全写入和读取的从机器件一起使用。该接口的最大 SCL 时钟速率为 400 kHz。

4.1.1 支持的 I²C 频率

SE050 的 I²C 从机接口支持 I²C 高速模式。当启用时钟扩展时，最大 SCL 时钟高达 3.4 MHz。

如果禁用时钟扩展功能，则支持的最大 SCL 时钟频率为 1.7 MHz。

默认启用时钟扩展。对于超过 600 kHz 的频率将发生时钟扩展。如果 I²C 主机不支持时钟扩展，必须使用禁用时钟扩展的专用配置来确保上述最大时钟频率。

SE050 的 I²C 主机接口支持最大 400 kHz 的 SCL 时钟频率。

4.2 ISO7816 和 ISO14443 接口

除了支持 I²C 接口之外，SE050 还支持 ISO7816 和 ISO14443 智能卡接口。对于 ISO7816 接口，支持 SmartCard 协议 T=0 和 T=1。对于 ISO14443 接口协议，使用协议 T=CL。支持的谐振输入电容为 56 pF。此外，还支持一个额外的 GPIO 焊盘 IO2。

如果启用 ISO7816 接口，则 RST_N 引脚只能用作外部复位源。如果仅启用 I²C 接口，则 RST_N 焊盘无效。如果 SE050 保持复位状态，则电流消耗与空闲状态的定义相同，见表 12。

5. 节电模式

该器件提供两种节电操作模式。掉电模式（带状态保留）和深度掉电模式（无状态保留）。这些模式可通过焊盘 ENA（深度掉电模式）或由 SW（掉电模式）激活。

5.1 掉电模式

掉电模式具备以下特性：

- 所有内部时钟将被冻结
- CPU 进入节电模式，程序执行被中止
- CPU 寄存器保留其内容
- RAM 保留其内容

当 SE050 通过 T=1 over I²C 协议接收“APDU 会话请求结束”，即进入掉电模式。在掉电模式下，所有内部时钟将被冻结。IO 保持其在掉电模式被激活的逻辑状态。

退出掉电模式有两种方法：

- RST_N 上的复位信号（如果启用了 ISO7816 接口）。通过 RST_N 从掉电模式唤醒后，器件处于空闲模式（见表 12）
- I²C_SDA 的下降沿触发外部中断边沿

5.2 深度掉电模式

SE050 提供特殊的节电模式，实现最大程度的节能。此模式通过将启用引脚(ENA)拉至逻辑零电平进行激活。

在深度掉电模式下，内部电源完全关闭，只有 I^2C 焊盘保持供电。

要退出深度掉电模式，必须将焊盘 ENA 上拉至逻辑“1”电平。

要使用深度掉电模式，必须通过焊盘 V_{in} 和焊盘 V_{out} 为 SE050 供电。

6. 订购信息

6.1 订购选项

表 3. SE050 订购信息

12NC	型号	SE050 变体	可订购的器件编号
9353 867 22472	SE050A1HQ1/Z01SG	SE050A1	SE050A1HQ1/Z01SGZ
9353 869 84472	SE050A2HQ1/Z01SH	SE050A2	SE050A2HQ1/Z01SHZ
9353 869 85472	SE050B1HQ1/Z01SE	SE050B1	SE050B1HQ1/Z01SEZ
9353 869 86472	SE050B2HQ1/Z01SF	SE050B2	SE050B2HQ1/Z01SFZ
9353 869 87472	SE050C1HQ1/Z01SC	SE050C1	SE050C1HQ1/Z01SCZ
9353 869 88472	SE050C2HQ1/Z01SD	SE050C2	SE050C2HQ1/Z01SDZ

表 4. SE050 开发套件订购信息

12NC	型号	说明
9353 832 82598	OM-SE050ARD	SE050 兼容 Arduino 的开发套件，SE050C 配置

6.2 订购 SE050 样品

可以使用 SE050 产品信息页上的“直接购买”按钮，通过 nxp.com 从恩智浦半导体订购样品。请注意，恩智浦半导体可免费提供 5 件样品。大量样品必须付费订购。

6.3 配置

有关 SE050 的配置和可用变体的详细信息，请参见单独的恩智浦应用笔记([4])