ACL16_AEC & ACL16_AHM 设备认证类安全芯片 FAQ 整理 V1.1

20240326

流程篇：

- 请问 AEC 的公钥和私钥是怎么产生的？

A：支持外部写入，或内部随机产生私钥并生成公钥

- 安全芯片会不会被人通过直接模拟单总线上的数据来仿冒或破解？

A：每次质询的随机数不同，且有密钥参与。不知道密钥的情况下无法模拟

- AEC 非对称安全芯片的优势有哪些？

A：密钥分发安全方便，且通过证书链便于管理。私钥由芯片内部产生，最安全

- 在使用的过程中，密钥是固定的还是可以随时变化？

A：密钥是固定的，但认证的数据是变化的

- AEC 密钥被配置为不可读出后，客户如何使用？

A：可以通过命令获得对应的公钥来实现验证功能

- 怎样实现远程验证？

A：可以用非对称或对称算法，通过随机数质询的方式进行认证，或通过证书认证的方式进行认证

- 安全芯片的密钥是如何产生的？同一个型号的器件密钥都是不同的吗？

A：如果是非对称式密钥，且由芯片内部自己产生，则每个芯片的私钥是不同的

- AEC 和 AHM 芯片，是不是无论与任何 MCU 都可以一起配合使用？

A：是的，接口是单总线通信

- 客户如果选择了安全芯片，主控 MCU 的软件也必须增加解密的代码？

A：是的

- AEC 和 AHM 每个器件的密钥是生产的时候就决定的？还是可配置的？

A：AEC 的密钥是由芯片在内部由芯片自己生成的。AHM 的密钥是外部写入的

- 对于 AEC 安全芯片，私钥是固定不变的？还是每次应用时都会新生成？

A：通常私钥是固定的，但每次应用时都会加入随机数，外部看到的密钥是在变化的

- 两边都需要预先设置一个互相信任的密钥吗？还是自动生成？

A：需要，但不一定是预置的，可以通过证书信任链的方式去实现，安全芯片的私钥可以自己产生

- 签名和完整性验签有区别吗？

A：有，签名是用来验证身份的合法性，完整性验签是用来验证文本是否被修改

- 能大概说下工厂产线生成密钥的流程吗？是否需要专用设备？

A：对称和非对称芯片密钥流程不一样。对环境和设备都有要求，需要专用设备

- 密钥可以设置几种不同安全级别的密钥吗？不同的密钥有不同的权限？

A：可以根据实际应用去设定密钥的访问权限；通常而言私钥是无法外部访问的，只能有条件的内部使用

- 固件 IP 保护是怎么做到的？

A：在 PCB 上放置安全芯片，固件运行时需要验证安全芯片是否有正确的密钥，以此来实现代码的保护。即使固件被复制也会因为没有密钥而无法运行

- 安全芯片的密钥有有效期吗？

A：在整个产品生命周期内都是有效的

硬件篇：

- ACL16_Axx 系列安全芯片支持哪些加密算法类型？

A：AEC ： ECDSA，支持 ECC Sign & Verify； AHM ： SHA256，支持 HMAC

- 安全芯片静态功耗参数如何？是否支持自动休眠？

A：AEC /AHM 支持自动进入 StandBy 模式（50uA），也支持指令进入 PowerOff 模式（2uA）

- 安全芯片封装尺寸是多少？

A：LGA4封装，1.22*1.22*0.35mm

- 安全芯片支持哪一种通讯方式？

A：仅支持单总线通讯

- 安全芯片最多可以预置多少组密钥？

A：AEC 采用非对称算法体系，私钥签名，公钥验签，密钥组数 1 组；AHM 采用对称算法体系，使用对称密钥，参与运算的对称密钥只有 1 组

- 安全芯片采用何种内核？

A：AEC /AHM 均为 ASIC 芯片，无内核版本

- AEC /AHM 是专门的安全芯片？还是必须集成到 MCU？

A：AEC /AHM 均为独立的、专用的安全芯片，需要外接在主控 MCU 上使用

- AEC 和 AHM 可以实现 PIN2PIN 的替代么？

A：AEC 和 AHM 硬件电路是 PIN TO PIN 兼容的，算法实现方案不一样

- 整个验证完成的时间是多久？

A：AEC -ECDSA 签名时间约 250ms，AHM -HMAC 时间约 5ms

- 工作温度范围是多少？ESD 静电防护等级是多少？

A：工作温度：-40℃ ~ +85℃。ESD：±8KV（HBM）

- 安全芯片生命周期是多久？

A：存储寿命至少 10 年

- 可以防破解吗？芯片级破解会有效吗？

A：可以防破解，安全芯片内部有加入安全防护措施，这也是安全芯片必须具备的功能

- 芯片读写次数是否有限制？

A：读没有限制，写次数至少 10 万次

- 请问芯片 128bit 序列号是如何产生的？

A：根据 WAFER 坐标等信息生成，序列号不支持读出

- 安全芯片的算法是可以选择的，还是固定的？

A：固定的。根据芯片型号有不同选择，AEC 支持 ECC-P256，AHM 支持 SHA256

- 不使用的时候 ，能否直接断电？

A：可以，断电后密钥、证书和数据不会丢失

- 安全芯片可以写数据吗？类似存放一些证书之类的？

A：可以写数据。可以存放证书，页数据支持权限设置

- 安全芯片的内部信息可以读取吗？

A：根据页数据的配置权限决定该页数据是否可以被外部读出

- 安全芯片的随机数发生器是真随机数发生器还是伪随机数发生器，是否有通过国家级等级认证？

A：是真随机数，有通过资质认证

- 在安全性方面采取了哪些措施？

A：安全芯片在设计时考虑了防止物理攻击的措施，比如：防 DPA/SPA 攻击，防 DFA 错误注入攻击；存储器保护功能；128 位唯一芯片序列号；真随机数发生器；国际认可的 ECC 安全算法等

- 单总线通信的命令是带 CRC 校验吗？

A：是，CRC16

- 硬件防护隔离密钥有效期多长？

A：在整个产品寿命周期内都是安全且有效的

软件篇：

- 有相对的开发应用软件吗？有没有 sample code 提供？

A：可以提供主控/上位机参考代码。可以提供 sample code 参考

- 密钥需要存放在服务器端吗？密钥会被破解吗？

A：不需要存放在服务器端。密钥独立存放在芯片内部且配置成不可读模式，物理上也很难破解获取密钥

- 安全芯片接到加密指令后，主控 MCU 需要加入等待时间再读取加密结果？

A：每条指令等待的时间不一样，主控 SDK 开发包中会给出具体等待时间

- 对主控 MCU 控制器的程序设计有无影响，是否会增加 MCU 的代码量？

A：因为增加了安全功能，主控 MCU 也要增加相应的安全功能代码。Flash 代码预计增加十几 KB，SRAM 预计几 KB，具体与主控 MCU 驱动库有关，当然也可以根据需要精简

- AEC 签名可以离线认证吗？

A：可以

- 开发难易度如何？

A：开发有对应的代码和说明作为参考，非常简单容易

商业篇：

- 安全芯片有相关的认证吗？

A：航芯安全产品均有相关的资质证书

- 这个方案有实际应用案例吗？

A：设备认证，配件认证，IP 保护，易耗品认证、电子烟耗材认证等

- 供货稳定么？芯片成本如何？

A：供货非常稳定。成本问题可咨询航芯销售人员

- NDA 是什么？有什么具体要求？

A：NDA 是一个保密协议，用于限制将安全芯片资料、源码等透漏给第三方。具体可咨询航芯销售人员

- 针对其他厂家的主控 MCU 配置的驱动包都可以支持吗？

A：标准 C 语言编写，移植简单、使用方便

- 多少用量起订？是否支持单独定制密钥？或支持用户自己写入密钥？

A：不同型号有不同的起定量，具体可咨询航芯销售人员。可以支持定制密钥；也可以开放给客户自己定义密钥，但安全性需要客户自己保证

- 开发板和工具套件是否免费提供或申请？

A：具体可咨询航芯销售人员

- 原厂能提供什么样的技术支持？

A：具体要看需要何种应用需求，可咨询航芯销售人员

- 是否有针对国密的产品？

A：有，具体可登录航芯官网或咨询航芯销售人员

- 芯片的可靠性如何，如果芯片出现问题，是否会影响系统的功能？

A：如果芯片出现问题，是会影响系统的运行的。航芯产品有严格的生产测试标准，每年出货量很大，且在多个行业均有量产出货，可靠性有保证

- AEC 和 AHM 相较于目前市面上的安全芯片具有什么优点？

A：我们有丰富的安全芯片设计经验，大批量使用的成功案例。芯片安全性高、ECC 硬实现速度快等

- 安全性的测试有提供测试报告吗？

A：有第三方的测试报告，具体可咨询航芯销售人员