设备身份认证安全解决方案

版本号： V1.0

中云信安（深圳）科技有限公司

一、方案概述

设备身份认证主要完成原装设备的合法性认证，用于防止第三方兼容设备（破解设备、盗版设备）的非法接入，典型的设备认证如苹果 MFI 认证、耗材的防伪认证等。

基于目前相关产品设备的认证方案，本方案主要通过安全芯片作为硬件载体 SE（Secure Element）安全存储关键的设备和密钥信息，基于密码学(非对称密码算法)对设备进行接入认证,达到对接入系统的设备进行授权控制,防止非法未授权设备的系统接入。

方案涉及密码算法及应用:

RSA\SM2：非对称密码算法，公私钥签名验签，达到设备身份认证目的。

AES\DES\SM4：对称算法，可完成数据流加密需求。

SHA\SM3：杂凑算法（HASH），用于签名认证数据哈希。

二、系统方案架构

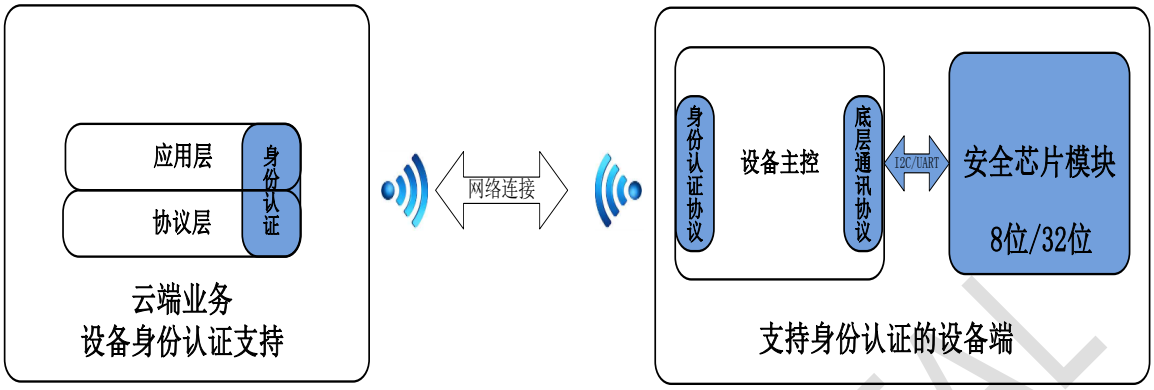

图 2-1 支持身份认证的设备方案框图

2.1 支持身份认证的设备端

2.1.1 安全芯片模块（Secure Element）

安全芯片模块（可选用 8 位/32 位 安全 MCU）需要通过 FIPS140-2、国密认证、EAL4+认证、银行卡检测中心等安全认证，具备高安全性、防抄板等特性高安全等级芯片，集成硬件的密码算法引擎，具备较高的密码运算速度和丰富的硬件算法加速引擎，支持国际（RSA/ECC/AES/DES/3DES/SHA 等）、国密（SM1/2/3/4）密码算法。

密码芯片模块包括灵活的软件固件配置，进一步提供高安全的密钥存储、非对称密码算法、对称密码算法运算接口供应用调用，提供支持身份认证的解决方案。

安全芯片模块（可选用 8 位/32 位 安全 MCU）通过设备主控端定义的底层通讯协议完成与设备主控的通讯，达到不同安全芯片模块的兼容性。

2.1.2 设备主控

设备主控在原有设备端业务的基础上，通过增加与安全芯片模块的通讯接口（如 I2C、UART 等）和底层通讯协议，并与云端业务设备在原有通讯信道上通过扩充的身份认证协议通讯，完成设备身份认证的信息交互。

2.2 云端业务（设备身份认证支持）

在原有系统云端业务的基础上，不改变原有软件架构，仅在应用层、协议层扩充设备身份认证应用层业务，达到对远端设备的身份认证目的，拒绝非法设备的接入。

三、通用安全芯片产品认证方案要点

3.1 设备认证流程

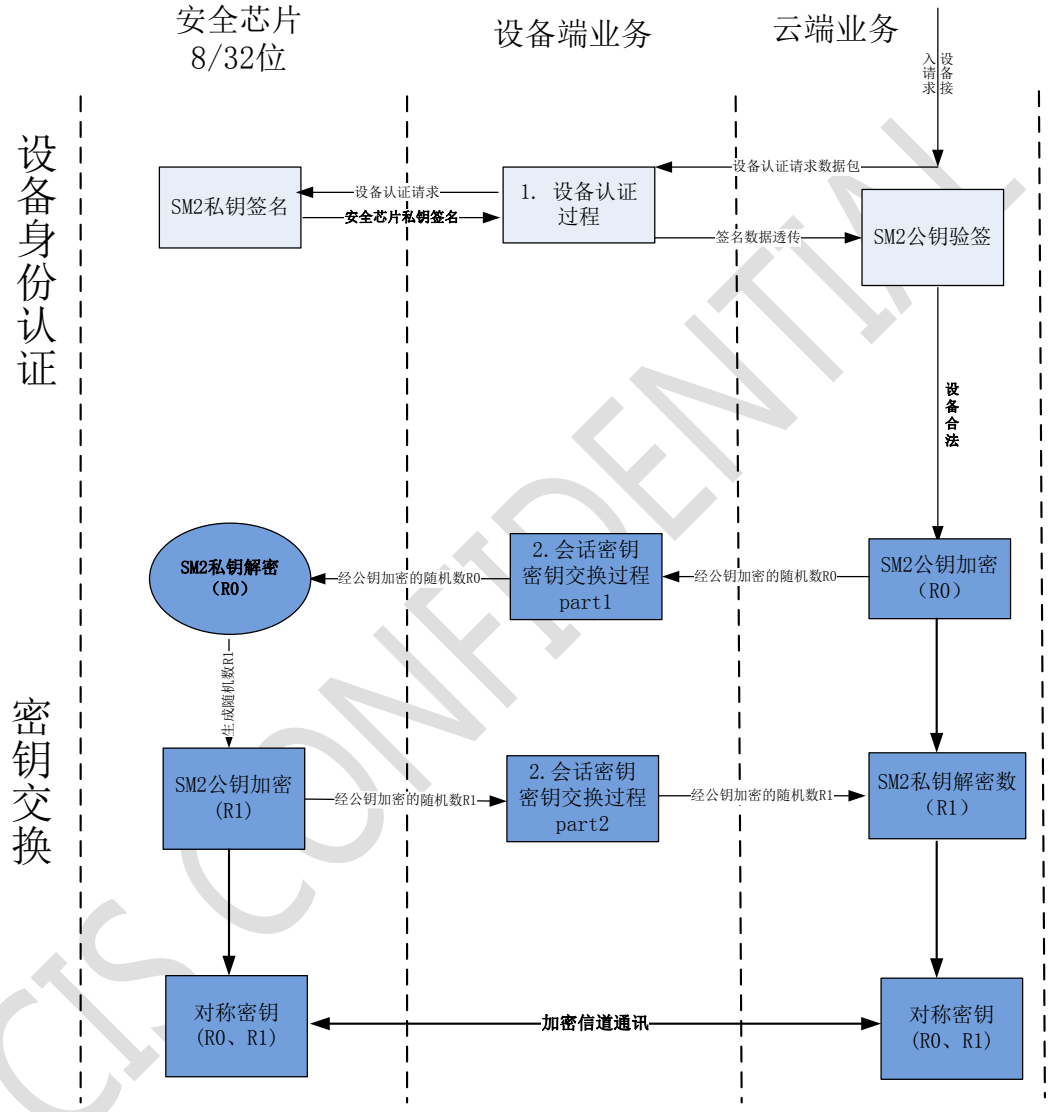

图 3-1 设备认证及加解密流程

3.2 安全芯片模块

3.2.1 安全芯片安全性说明

由于采用非对称 SM2 算法，因此设备认证的安全性，仅且唯一取决于 SM2 算法

私钥的安全性，SM2 私钥保存在安全芯片的安全 FLASH 中，可保证正常使用阶段的安全性，防止第三方破解，但在私钥的使用中，以下两点务必保证：

1. SM2 公私钥对生成阶段，务必保证私钥的安全性。
2. SM2 私钥需要保证生产阶段的安全性。

3.2.2 安全芯片硬件接口

安全芯片模块可以采用 I2C、UART、SPI 等接口，可根据设备端通讯接口情况和通讯协议进行适配，保证不同安全芯片（8/32、不同厂家）模块的间兼容性。

3.2.3 安全芯片模块使用流程说明

安全芯片模块用在设备认证方案，推荐安全芯片模块的使用流程参考“图 3-1 设备认证及加解密流程”所示，以便达到较高等级的设备认证，也可以基于安全芯片模块提供的密码算法接口和安全存储功能，实现私有的设备认证及加解密应用方案。

设备认证阶段：

1. 云端：存储设备公钥，生成随机数 32Bytes，作为待签名数据，通过公钥加密带签名数据；
2. 密码模块：通过私钥解密加密的待签名数据，调用 SM2 签名接口，对随机数进行签名，签名数据回送云端；
3. 云端：使用公钥对密码模块签名数据进行验证，确认签名数据 PASS 或 FAIL。
4. 设备认证结束。

会话密钥交换阶段（可选）：

1. 云端：生成随机数 R0，通过 SM2 公钥加密随机数 $R0^*$；
2. 密码模块：SM2 私钥解密 $R0^*$，得到随机数 R0；
3. 密码模块：生成随机数 R1，通过 SM2 公钥加密随机数 $R1^*$；
4. 云端：SM2 私钥解密 $R1^*$，得到随机数 R1；
5. 完成密钥交换，密钥为（R0、R1）。