ICS 33.160.99
CCS M73

团　　体　　标　　准

T/ZSA 303-2025

移动智能终端安全摄像头系统技术要求

Technical requirements for smart mobile terminal security camera system

2025-06-11 发布　　2025-06-12 实施

中关村标准化协会　　发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中关村标准化协会互联网可信认证技术委员会提出并归口。

本文件起草单位：蚂蚁科技集团股份有限公司、荣耀终端有限公司、捷付睿通(内蒙古)支付股份有限公司、北京一砂信息技术有限公司、萨思数字科技（北京）有限公司。

本文件主要起草人：窦方钰、李志雄、王振亚、林冠辰、吴思捷、徐亦佳、彭晋、李志超、赵晓娜、罗广文、潘双全、石新凌、成雅琴、张楚、王军、路如毅。

移动智能终端安全摄像头系统技术要求

1 范围

本文件规定了移动智能终端安全摄像头系统的总体框架、功能要求、接口协议以及安全要求。

本文件适用于移动智能终端基于TEE安全环境的从图像采集到处理、传输及验证的全流程防篡改方案设计，适配于各种图像业务场景应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注明日期的引用文件表示仅该日期对应的版本适用于本文件；未注明日期的引用文件表示其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 31168 信息安全技术 云计算服务安全能力要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 35281 信息安全技术 移动互联网应用服务器安全技术要求

GB/T 37036.3 信息技术 移动设备生物特征识别 第3部分：人脸

GB/T 38671 信息安全技术 远程人脸识别系统技术要求

IFAA本地免密协议2.0

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全摄像头系统 security camera system

基于硬件摄像头进行图片信息采集，并完成硬件级安全下的图片处理、签名、传输、存储和管理的系统，硬件级安全摄像头由终端设备、服务器端（硬件级安全摄像头鉴权服务器、业务服务器）、TEE环境等部分组成。

3.2

移动智能终端 mobile intelligent terminal

接入移动通信网，能够提供应用程序开发接口的开放操作系统，并能够安装和运行应用软件的移动终端。

3.3

可信环境 trusted environment

用户设备上的安全区域，可保证加载到其内部数据的安全性，包括保密性、完整性和可用性等，如可信执行环境（TEE）、安全元件（SE）、可信密码模块（TCM）或其他具备安全边界的保护区域。
[来源：GB/T 36651-2018，3.1]

3.4

安全摄像头 SDK security camera software development kit

运行在移动智能终端REE侧，包含在应用程序内的安全摄像头软件SDK。

3.5

应用程序 application

运行在移动智能终端REE侧的移动互联网应用程序。

4 缩略语

下列缩略语适用于本文件。

AIDL：Android接口定义语言（Android Interface Definition Language）
API： 应用编程接口（Application Programming Interface）
APP： 应用程序（Application）
JPEG：面向连续色调静止图像的一种压缩标准（Joint Photographic Experts Group）
REE： 富执行环境（Rich Execution Environment）
RPMB：重放保护内存块(Replay Protected Memory Block)
SDK： 软件开发工具包（Software Development Kit）
SE： 安全单元（Security Element）
SFS： 文件存储服务（File Storage Service）
TA： 可信应用（Trusted Application）
TEE： 可信执行环境（Trusted Execution Environment）
TLV： 一种数据结构的缩写（Tag,Length,Value）
YUV： 一种颜色编码方法

5 总体框架

移动智能终端安全摄像头系统总体框架见**错误!未找到引用源。**

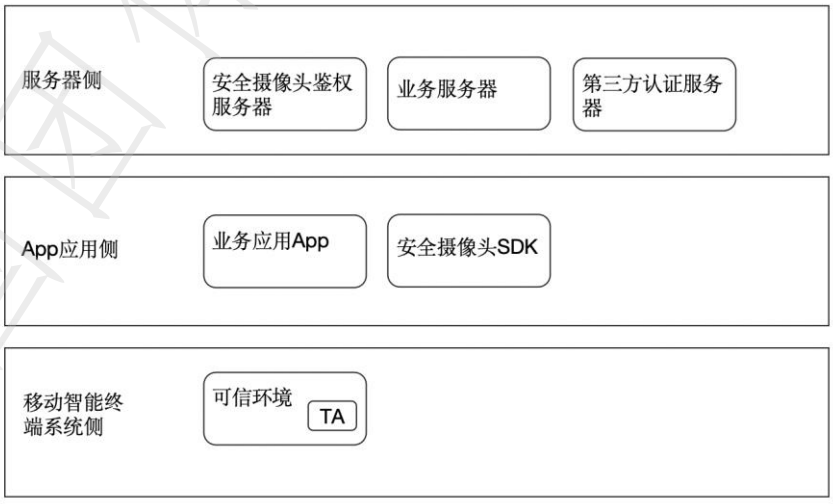


图1 安全摄像头系统总体框架

安全摄像头总体框架，包含了IIFAA（互联网可信认证联盟）第三方认证服务器、业务服务器、应用程序、安全SDK以及位于可信环境下的TA应用。此方案往往涉及多个业务实现主体，有一个或多个业务方案解决方参与，彼此间通过接口实现调用。

具体实现是应保障人脸识别业务从摄像头传感器上发起并写入安全内存，TEE环境中TA直接进行读取及操作。可完成从图片的读取，以及图片经过活体选择后可进行裁剪和签名，确保图片信息的防篡改。各实现主体包含多部分，移动智能应用程序侧，包含具体移动互联网应用（应用程序），以及和移动智能终端系统侧交互的安全摄像头SDK；移动智能终端系统侧，则包含可信环境以及该环境中的具体可信应用；在服务器侧，应包括IIFAA第三方认证服务器，安全摄像头鉴权服务器，以及具体业务服务器。

业务服务器及应用程序为具体业务（例如人脸识别、人证比对等）的主体。应用程序中应包含安全摄像头SDK，以便于使用其能力。安全摄像头服务器主要对下行数据进行签名确保其可信，同时验证上行数据的可信。安全摄像头SDK，提供了解析、组装安全摄像头服务区下发上行数据、供应图片等能力，且保证和终端Service的连接。可信环境中的安全摄像头TA，应具备对图片基本处理的功能（包括JPEG转换等），同时须具备验证服务器签名，以及为图像信息进行签名的能力。

移动智能终端安全摄像头系统厂商实现流程和细节见附录A。

6 功能要求

6.1 移动智能终端

移动智能终端安装具体应用程序，采用的芯片应具备采集图片并写入安全内存的硬件级安全摄像头接口，以及基于IIFAA协议的基础密钥体系，要求如下：

a） 应提供图片的安全采集及安全写入功能；
b） 应提供IIFAA密钥体系的实现及使用接口，包含根密钥等；
c） 应满足终端业务逻辑的请求、接收、处理响应等网络及权限需求；
d） 应提供硬件级安全摄像头系统应用程序和TA交互必要的系统服务；
e） 应具备可信环境（如TEE）和硬件级安全摄像头TA。

6.2 安全摄像头 TA

硬件级安全摄像头TA可用于图片处理，它具备验证服务器下发数据的验签能力、图片签名、解析及组装TLV逻辑的能力的同时，还具备密钥的读取、创建及操作能力，具体能力描述如下：

a） 读取硬件级安全摄像头从传感器写入图片信息；
b） 根据安全摄像头SDK发送的图片处理信息，从而进行具体处理逻辑；
c） 读取IIFAA设备根密钥且进行签名能力；
d） 生成业务密钥对能力；
e） 验证服务器下发签名数据；
f） 解析TLV信息能力，且具备组装上传TLV数据能力。

6.3 业务服务器

业务服务器可用于实现图片的具体业务逻辑，如在人脸识别、证件识别等业务中，包含了从比对，到移动智能终端安全摄像头验签等具体业务逻辑，要求如下：

a） 应能处理图片业务逻辑的请求以及响应；
b） 应能验证图片的合法性及正确性，如人脸比对；
c） 应能支持更新图片信息；
d） 应具备安全措施保证图片信息的安全性和隐私性；
e） 应能向移动智能终端安全摄像头服务器进行可用性查询、验签、透传等逻辑；
f） 应能实现具体业务结果传递，如核身结果的传出；
g） 应支持应用程序发送信息的解析以及响应。

6.4 硬件级安全摄像头鉴权服务器

具备基于IIFAA本地免密协议的硬件级安全摄像头相关功能，要求如下：

a） 应具备可用性接口，判断设备是否支持硬件级安全摄像头；

b） 应支持随机生成挑战码，用于下发数据中使用；

c） 应提供校验设备密钥签名、图片签名等验签能力接口。

6.5 安全摄像头 SDK

安全摄像头客户端SDK应具有多方面能力，包括对安全摄像头服务器数据的解析以及返回，和手机系统的连接、交互，以及图片的数据解析、供应上次应用取图和对终端业务的接口暴露等逻辑。应用程序通过安全摄像头SDK获取图片及签名等信息，要求如下：

a）应包含初始化、打开相机、获取图片等接口；

b）应支持对安全摄像头服务器下发数据的解析与组装；

c）应支持接收并执行安全摄像头服务器下发的安全摄像头初始化请求消息；

d）应支持接收并执行安全摄像头服务器下发的安全摄像头环境信息请求消息；

e）应提供可进行图片具体处理逻辑的接口；

f）应提供连接并调用系统服务的能力。

7 接口协议

7.1 业务服务器与移动智能终端安全摄像头服务器之间

7.1.1 数据元素

数据元素见表 1。

表 1 数据元素

请求参数		
字段	类型	备注
version	String	协议版本
action	String	请求action 可用性查询：USABLE_CONSULT 初始化：INITIALIZE 验签：VERIFY
transaction/payload	String	业务附加信息
IIFAA/version	String	IIFAA版本
IIFAA/device-id	String	设备ID
IIFAA/message	String	IIFAA协议信息（请求时）/执行结果 （响应时）
IIFAA/code	Int	响应码
TLV[a]/pubAlgEncode	Int	公钥编码
TLV/pubkey	String	公钥数据
TLV/deviceId	String	设备id

[a] 注：TLV 为一种可变的格式，意为：Type 类型， Lenght 长度，Value 值。其中 Type 字段是关于标签和编码格式的信息，Length 字段是定义数值的长度， Value 字段表示实际的数值。

TLV/bizChallengeCode	String	挑战码，端生成非对称密钥使用
TLV/bizChallengeSignature	String	挑战码的IIFAA签名
TLV/authChallengeCode	String	验证挑战码
picBase64	String	base64编码的图片
TLV/bizPubKey	String	端上签名图片使用的业务公钥
TLV/bizPubAlg	String	公钥算法
TLV/bizChallengeCode	String	挑战码
TLV/bizPubKeySignature	String	业务挑战码+业务公钥使用设备私钥的签名
TLV/authChallengeCode	String	验证挑战码
TLV/authSignature	String	图片+验证挑战码使用业务私钥的签名

7.1.2 报文接口

7.1.2.1 硬件级安全摄像头可用性查询

状态查询请求参数见表 2。

表 2 状态查询请求参数

请求参数		
字段	类型	备注
action	String	请求action
transaction/payload	String	业务附加信息
Seccam/version	String	硬件级安全摄像头版本
IIFAA/device-id	String	设备ID
IIFAA/device-model	String	机型设备

响应参数见表 3。

表 3 状态查询响应参数

响应参数		
字段	类型	备注
version	String	版本信息
IIFAA/code	Int	响应码
IIFAA/message	String	异常描述（当服务器报错/服务器端无注册信息时）

7.1.2.2 初始化

硬件级安全摄像头鉴权服务器请求获取初始化请求消息参数见表 4。

表 4 初始化请求参数

请求参数		
字段	类型	备注
action	String	请求action

transaction/payload	String	业务附加信息
IIFAA/version	String	IIFAA版本
IIFAA/device-id	String	设备ID
IIFAA/message	String	IIFAA协议信息
IIFAA/device-model	String	机型信息

硬件级安全摄像头鉴权服务器返回的初始化响应见
表 5。

表 5 注册相应消息参数

响应参数		
字段	类型	备注
version	String	IIFAA版本信息
IIFAA/code	Int	响应码
IIFAA/device-id	String	设备ID
TLV/bizChallengeCode	String	挑战码，端生成非对称密钥使用
TLV/bizChallengeSignature	String	挑战码的IIFAA签名
TLV/authChallengeCode	String	验证挑战码

7.1.2.3 验签

验证签名请求参数见表 6。

表 6 验证签名请求参数

请求参数		
字段	类型	备注
version	String	协议版本
action	String	请求action
transaction/payload	String	业务附加信息
picBase64	String	base64编码的图片
IIFAA/version	String	IIFAA版本
IIFAA/device-id	String	设备ID
IIFAA/device-model	String	设备机型信息
TLV/bizPubKey	String	端上签名图片使用的业务公钥
TLV/bizPubAlg	String	公钥算法
TLV/bizChallengeCode	String	挑战码
TLV/bizPubKeySignature	String	业务挑战码+业务公钥使用设备私钥的签名
TLV/authChallengeCode	String	验证挑战码
TLV/authSignature	String	图片+验证挑战码使用业务私钥的签名

验证签名响应参数见表 7。

表 7 获取认证响应参数

响应参数		
字段	类型	备注
version	String	IIFAA版本信息
IIFAA/code	Int	响应码
IIFAA/message	String	认证初始化数据（一个数组）

7.2 应用程序与安全摄像头 SDK 之间接口

7.2.1 概述

应用程序与安全摄像头SDK之间的调用，应包含获取环境信息、打开相机、初始化等多个基础步骤，对应的底层操作为获取设备信息和创建密钥对等操作。

7.2.2 初始化

初始化响应参数见表 8。

表 8 初始化响应参数

响应参数		
字段	类型	备注
Context	Context	系统上下文
Value	Byte[]	初始化信息（由服务器组装下发）
InitListener	String	初始化回调函数

7.2.3 打开摄像头

打开摄像头响应参数见表 9。

表 9 打开摄像头响应参数

响应参数		
字段	类型	备注
cameraId	Int	需要传入cameraid，0为后置摄像头，1为前置摄像头
Listener	OpenSecCamListener	打开相机回调函数

7.2.4 获取图片

获取图片响应参数见表 10。

表 10 获取图片响应参数

响应参数		
字段	类型	备注

Ionfd	Int	需传入打开相机后返回的ionfd
value	byte[]	服务器生成的challenge

7.3 安全摄像头 SDK 与系统之间接口

安全摄像头SDK与系统之间接口，应满足基本调用要求，形式上可以使用反射、AIDL等多种方式实现。

8 安全要求

8.1 一般要求

8.1.1 个人信息保护和人脸识别系统要求

个人信息保护应符合GB/T 35273的要求。

移动智能终端上人脸识别应符合GB/T 37036.3的相关要求，移动智能终端远程人脸识别系统还应符合GB/T 38671的相关要求。

8.1.2 通信安全认证

通信安全认证要求如下：

a) 移动智能终端与服务器端应使用加密算法和安全协议保护移动智能终端与服务器之间所有连接，保证传输数据的机密性和完整性，例如：使用TLS安全协议；

b) 硬件级安全摄像头服务器，移动智能终端与TEE终端之间应建立安全的、定向的通信连接。通信前应采用密码技术的双向认证机制，确保TEE终端可验证硬件级安全摄像头服务器的身份，硬件级安全摄像头服务器也可以验证向它发送数据的TEE及移动智能终端的身份。

8.1.3 密码应用

本文件中涉及的密码应用，应依据国家密码管理局规定实施，采用的国家密码算法包括 SM2、SM3 等。

8.2 移动智能终端侧基本安全要求

8.2.1 图片产生

硬件级安全摄像头应将摄像头置于硬件级安全模式下，同时硬件级安全摄像头将图片写入安全内存中，供TEE环境下TA进行读取，从而保证图片采集的安全性，该部分多与芯片厂商实现相关联。

8.2.2 云到端可信

硬件级安全摄像头鉴权服务器通过生成挑战码，以及对数据和挑战码进行签名，确保云到端的可信。

c) 通过IIFAA认证中心对下发数据进行签名，从而确保下发数据不可篡改；

d) 通过更新挑战码，确保防重放攻击。

8.2.3 端到云可信

终端产生业务密钥对图片进行签名，同时公钥通过设备根密钥进行签名，从而保证端到云的可信，该逻辑流程中，满足数据从TA上传到服务器的数据可信，具体要求如下：

a) 签名过程应使用挑战码或计数器等机制，防止重放攻击。业务密钥使用以及挑战码应设立有效使用时长限制；
b) 同时应采取措施保证通信中数据的完整性，防止数据在通信过程中被劫持、篡改和注入，若数据完整性被破坏，应及时进行丢弃处理或其他安全流程操作；
c) 设备根密钥在移动智能终端生产过程中烧入，应保存于RPMB中。

8.2.4 安全环境

安全环境分为基本要求和增强要求，分别如下：
a) 基本要求：采用可信执行环境（TEE）实现终端非对称密码算法公私密钥对的生成、存储和非对称加密以及对称加密算法的运算；
b) 增强要求：采用安全芯片（SE）实现终端非对称密码算法公私密钥对的生成、存储和非对称加密以及对称加密算法的运算。

8.2.5 应用程序安全

应用程序安全要求如下：
a) 应保证移动智能终端安装、运行的移动应用软件来自可靠证书签名或可靠分发渠道；
b) 应保证移动智能终端安装、运行的移动应用软件由可靠的开发者开发；
c) 具备防范越权操控和身份伪冒的能力；
d) 对设备密码、设备认证信息进行加密处理，不应在日志和配置文件中明文记录敏感信息；
e) 在数据传输之前应进行双向认证，并且传输数据也应进行加密传输；
f) 对设备生成和用户输入的用户敏感信息应加密存储；
g) 具备防止身份验证暴力攻击的能力；
h) 具备对输入数据的安全性检验能力；
i) 应对应用程序进行安全加固，加固后应用程序的代码及敏感信息应具备防篡改、防逆向、防动态调试等能力。

8.2.6 数据存储安全

数据存储安全要求如下：
a) 将硬件级安全摄像头产生的未签名图片，以及业务密钥对的私钥应存储在移动智能终端可信环境内，应为保存数据的文件设置适当的权限，以防止未授权的访问和篡改。保存的文件应加密存储；
b) 移动智能终端不应有未向用户明示且未经用户同意，擅自修改用户数据的行为。

8.3 安全摄像头移动智能终端

8.3.1 密钥存储安全

密钥存储安全要求如下：
a) 设备RPMB区域用于存放有防止非法篡改需求的数据信息，比如设备信息、设备私钥信息等。该区域对写入有权限要求，但对于读取则没有，一般存储其中的数据需要加密。基于此特性，IIFAA设备根密钥应由设备厂商烧录于此；
b) 业务密钥对的私钥存储，若需要持久化存储，则应存储于SFS中。该区域为安全加密文件系统，其中存放的数据会被加密，只有创建数据的应用才可以看到。

8.4 安全摄像头服务器端

8.4.1 总体要求

服务器端安全要求应符合GB/T 22239-2019 第三级要求以及GB/T 35281的要求。基于云计算实现的服务平台，还应符合GB/T 31168的要求。

8.4.2 数据传输安全

对于服务器之间以及服务器同终端之间的数据传输，应满足如下安全要求：

a) 应对传输的敏感信息（敏感信息包括后台系统管理员认证信息、操作系统登录认证信息，网络设备认证信息、用户敏感信息等）进行机密性保护；
b) 应对传输的敏感信息进行完整性保护，如使用哈希算法、时间戳、计数器等，防止未授权的第三方对数据进行修改、破坏和消息重放等；在存储或传输时应具备数据包排序及差错校验功能，避免信息包的丢失、乱序等。

8.4.3 数据访问控制

应支持权限控制功能，如在虚拟化系统上对于数据库设置不同的访问策略，保证用户仅能对该业务系统对应的数据库进行权限以内的相关操作，不能访问其他未被授权的业务系统数据。

8.4.4 数据存储安全

对服务器端的数据存储，应满足如下安全要求：

a) 应支持分级的数据加密方法，根据数据密级采用不同的安全存储机制；
b) 应支持密钥安全存储，保证密钥不被泄露；
c) 应支持数据完整性保护，对极敏感数据提供完整性检测机制，极敏感数据损坏和丢失时能够及时发现；
d) 应具备完备的数据备份和恢复功能，一旦发生数据丢失或破坏，可以利用备份恢复数据，保证数据在故障发生后不会丢失；
e) 应具备对各类数据和文件进行归档的能力和定期对临时数据及文件自动清理的功能，数据删除后系统内的文件、目录和数据库等资源所在存储空间被释放或重新分配，应能够完全清除，不可恢复。

附录 A
（资料性）
厂商流程与实现细节

A.1 厂商流程与实现细节

A.1.1 概述

相比于传统系统侧获取图片而言，目前可信SecCam方案将安全加密签名模块基于ARM TrustZone技术，当使用硬件级安全摄像头时，图像数据从camera sensor产生，通过共享内存将图像数据传入到TEE(Trust Execution Environment)中，在TEE里对图像数据进行加密和签名，保证数据产生源的可信。

A.1.2 流程

硬件级安全摄像头工作流程和交互流程分别见图A.1，主要流程包括如下步骤：

a) 对可信摄像头进行初始化操作，包括对调用方的校验以及业务密钥对的生成和返回；
b) openSecCam打开硬件级安全摄像头，Camera sensor开始采集图像数据，同时通过dma向安全内存写入图片信息。openSecCam还会执行初始化系统硬件级安全摄像头接口；
c) openSecCam成功后，callback 注册成功，硬件级安全摄像头数据帧刷新时，callback会不断回调并返回fd，通过fd 能反查到该帧数据所在的共享内存物理地址供getSecImg使用；
d) 调用getSecImg获取安全图像，通过IonFd反查到图像数据帧所在的共享内存的地址，从硬件级安全摄像头TA拿到安全图像的数据buffer，获取硬件级安全摄像头中的一帧安全图像secImg，以及相关的签名数据，返回上层应用使用。

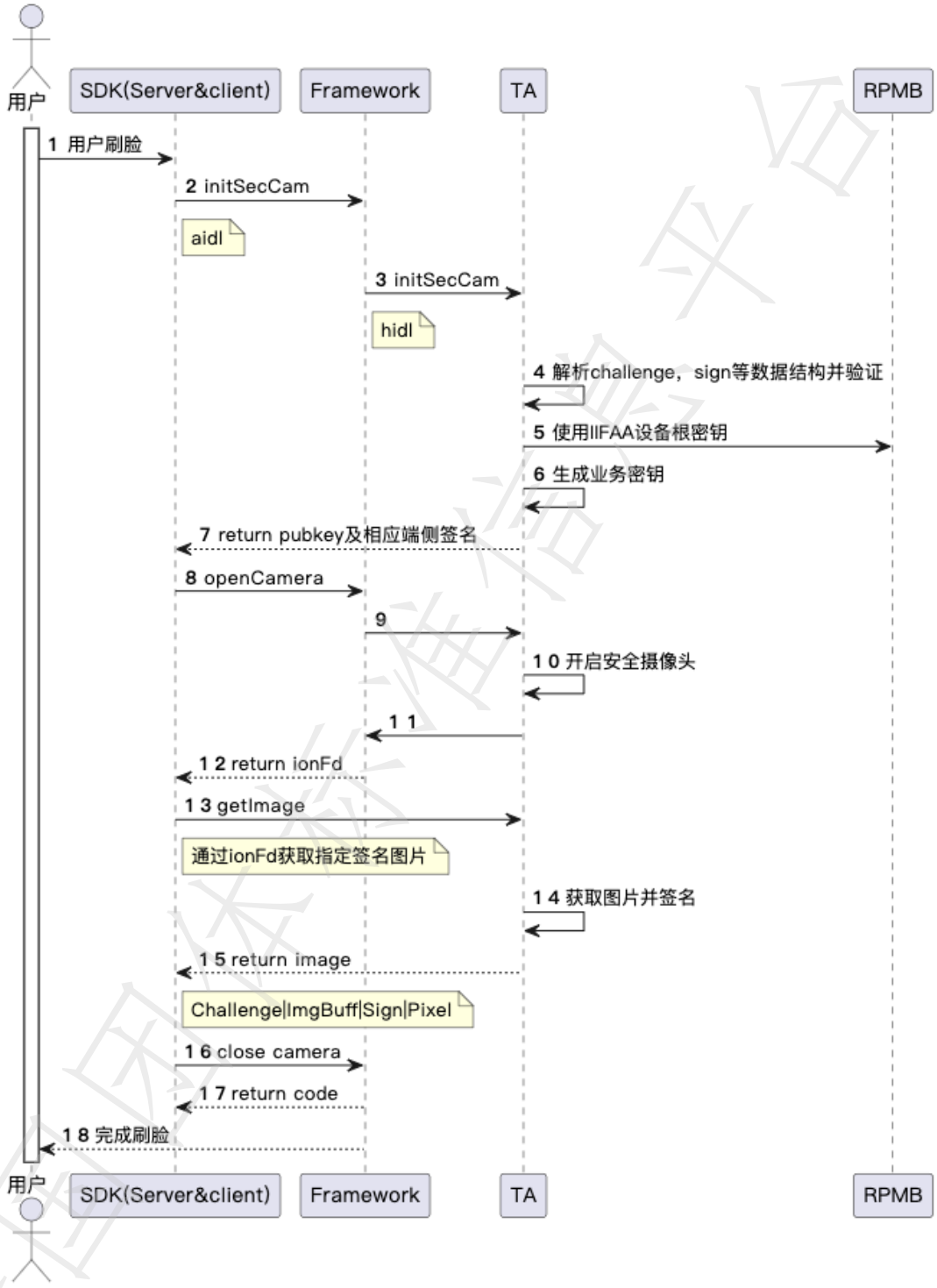


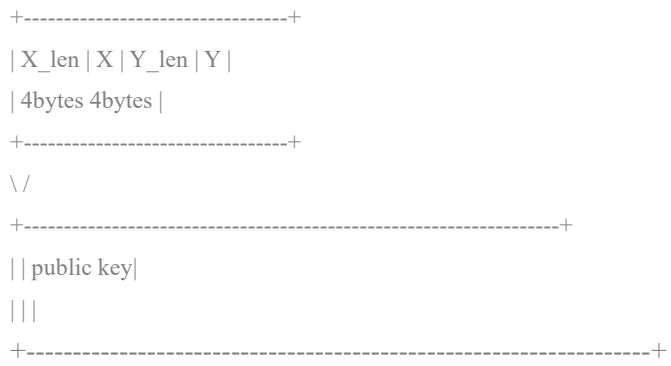
图 A.1 硬件级安全摄像头交互流程

A.1.3 数据结构

REE 至 TEE 交互数据结构上采用 TLV 的形式。

分布上为：

Tag1Length1Value1Tag2Length2Value2...TagNLengthNValueN



A.1.4 密钥使用及存储

IIFAA 设备根密钥保存与 RPMB 中，而初始化流程中创建的业务密钥对，私钥和业务 Token 会放置于 SFS 文件系统中（实际上只需要保证通过 Token 可以找到业务私钥）。

A.1.5 数据的传递

Android 于 API 27 引入 SharedMemory 的上层 framework API 供应用侧使用，利用 SharedMemory 本质上是在 native 创建了一块匿名共享内存，在两个进程间进行数据共享。这样能实现 Binder 传输大内存，并且不会进行一次拷贝，对性能有较大的提升。因此，公钥及图像 TLV 数据的传输均使用 SharedMemory。