ICS 33.050
M 30

团　体　标　准

T/TAF 084.1-2021

安卓应用程序认证签名技术规范 第1部分：数字签名应用要求

Authentication signature specification for Android Applications—
Part 1: Application specification of digital signature

2021-05-12 发布　　2021-05-12 实施

电信终端产业协会　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。

本文件是 T/TAF 084《安卓应用程序认证签名技术规范》的第 1 部分。T/TAF 084 已发布了以下部分：

——第 2 部分：数字证书格式规范；

——第 3 部分：数字签名格式规范。

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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、华为技术有限公司、小米通讯技术有限公司、荣耀终端有限公司、OPPO广东移动通信有限公司。

本文件主要起草人：邓佑军、刘陶、武林娜、吴怡、衣强、刘琼、周圣炎、刘俊伟、赵晓娜、侯振靖、梁顺龙。

引　　言

近年来，安卓应用程序各种违法违规问题层出不穷，不光给消费者造成经济上的损失、隐私上的侵扰，也给移动互联网行业造成了不安全、不可信的危机。安卓应用程序签名者向依法设立的电子认证服务机构申请APP签名证书并对自己开发的、检测的、分发的安卓应用程序签名，可以有效避免安卓应用程序被假冒或篡改，保障自身利益和合法权益。

本文件作为安卓应用程序认证签名技术规范的第1部分，旨在对相关方在安卓应用程序数字签名活动中提供指导。

安卓应用程序认证签名技术规范　第1部分：数字签名应用要求

1　范围

本文件定义了安卓应用程序签名过程中各参与方的工作机制的操作流程。

本文件适用于安卓应用程序开发者、检测者、分发者、终端厂家和 APP 签名服务系统运营者，实现安卓应用程序的签名、验签及标识展示。

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，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

T/TAF 084.2-2021　安卓应用程序认证签名技术规范　第2部分：数字证书格式规范

T/TAF 084.3-2021　安卓应用程序认证签名技术规范　第3部分：数字签名格式规范

3　术语和定义

下列术语和定义适用于本文件。

3.1

数字证书　digital certificate

数字证书是指在互联网通讯中标志通讯各方身份信息的一个数字标识。由电子认证服务机构依据一定的认证规则进行认证后签发，数字证书包含拥有者信息、拥有者公开密钥、签发机构信息、有效期以及一些扩展信息。

3.2

认证签名　authentication signature

利用数字证书来参与数字签名活动的行为称为认证签名。

3.3

安卓应用程序　android application

安卓应用程序（简称APP）是指APK、SDK、快应用、小程序形式的等可运行或集成在安卓系统中应用程序。

3.4

开发者 application developer

从事 APP 研发和运营的个人或者机构。

3.5

检测者 application Tester

从事 APP 合规性检测的机构，一般具有相关检测方面的能力或资质。

3.6

分发者 application distributor

从事 APP 分发管理的机构，如应用商店运营者、APP 下载网站运营者等。

3.7

签名者 application signer

对 APP 进行签名的相关角色，包括开发者、检测者和分发者。

3.8

APP 签名服务系统 APP signature service system

为签名者、应用分发平台和应用检测平台提供 APP 签名、验签和签名者数据服务的管理系统。

4 缩略语

下列缩略语适用于本文件。

APK：Android应用程序包（Android application package）

CA：证书认证机构（Certificate Authority）

SDK：软件开发工具包（Software Development Kit）

5 签名应用要求

5.1 概述

签名是非对称密钥加密技术与数字摘要技术的相结合的一种常见技术，认证签名可表明签名者的身份真实可靠，签名者行为是本人意愿，签名具有防篡改、防抵赖等特性，广泛应用与社会生产生活实践中。APP 通过认证签名应用，可以对 APP 进行溯源，减少违法违规应用给用户造成的侵害，同时还可以有效避免 APP 被假冒或篡改，保障开发者自身利益和合法权益，为安卓生态闭环管理提供了安全信任基础。

5.2 整体架构

APP 认证签名体系整体架构分为四层，第一层是签名角色层。包括开发者、检测者和分发者。在 APP 签名活动中，数字证书表明了他们具备开展 APP 活动的身份和能力，签名代表了他们在开展活动中的行

为。第二层是签名服务层。签名服务层由证书服务系统和 APP 签名服务系统组成，证书服务系统为签名角色层提供身份认证服务，身份认证通过后签发数字证书，APP 签名服务系统为签名角色层提供 APP 签名服务、为 APP 管理层提供 APP 签名数据同步服务。第三层 APP 管理层。由应用分发平台和应用检测平台组成，实时从 APP 签名服务系统中同步 APP 签名数据，在开展 APP 管理过程中，负责上架审核、更新审核管理和应用检测等，同时为 APP 应用层提供 APP 查验服务。第四层是 APP 应用层、是指 APP 实际安装和运行的终端系统，在安装前从应用分发平台查验 APP 的分发来源和相关意见。APP 认证签名整体架构如图 1 所示。

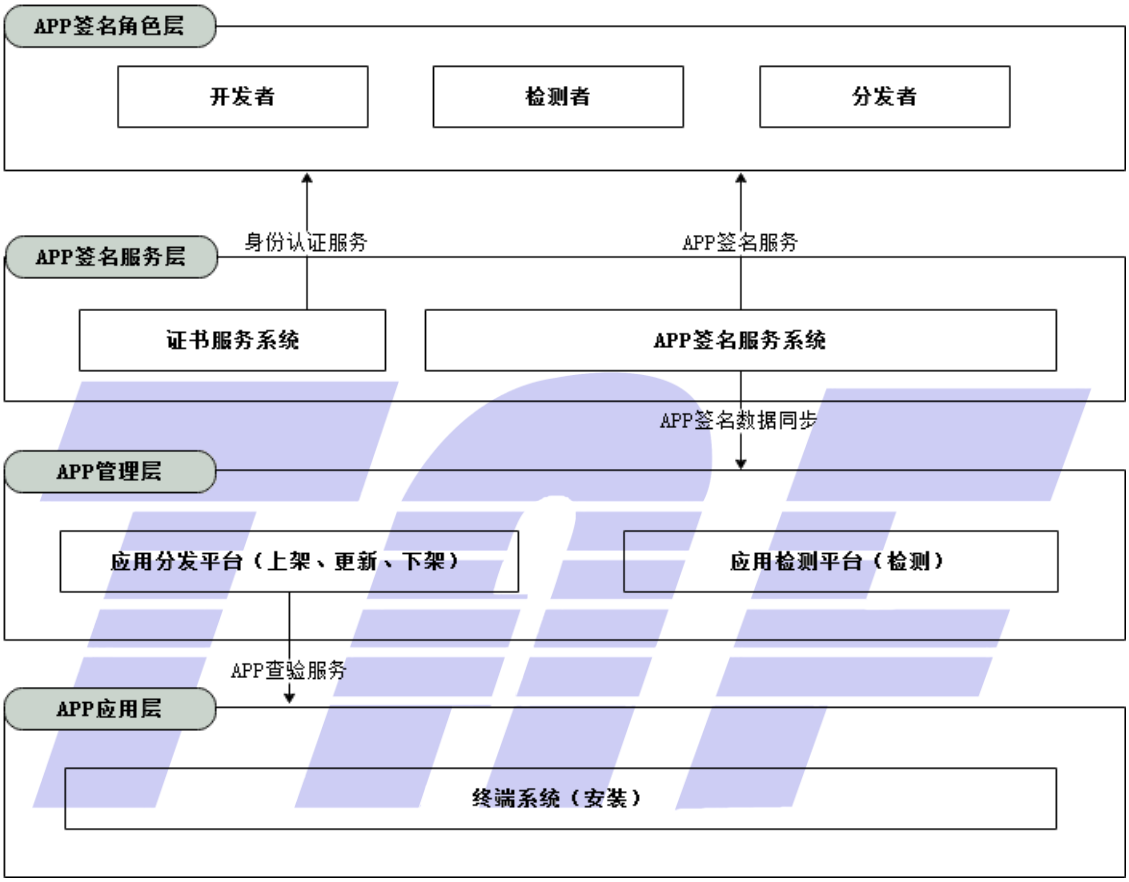

图 1　APP 认证签名整体架构图

5.3 应用流程

5.3.1　身份认证流程

签名者在开展 APP 签名活动前，首先向 APP 签名服务系统中的电子认证服务机构申请电子认证，由电子认证服务机构审核并发放专用的 APP 签名数字证书。身份认证流程如图 2 所示。

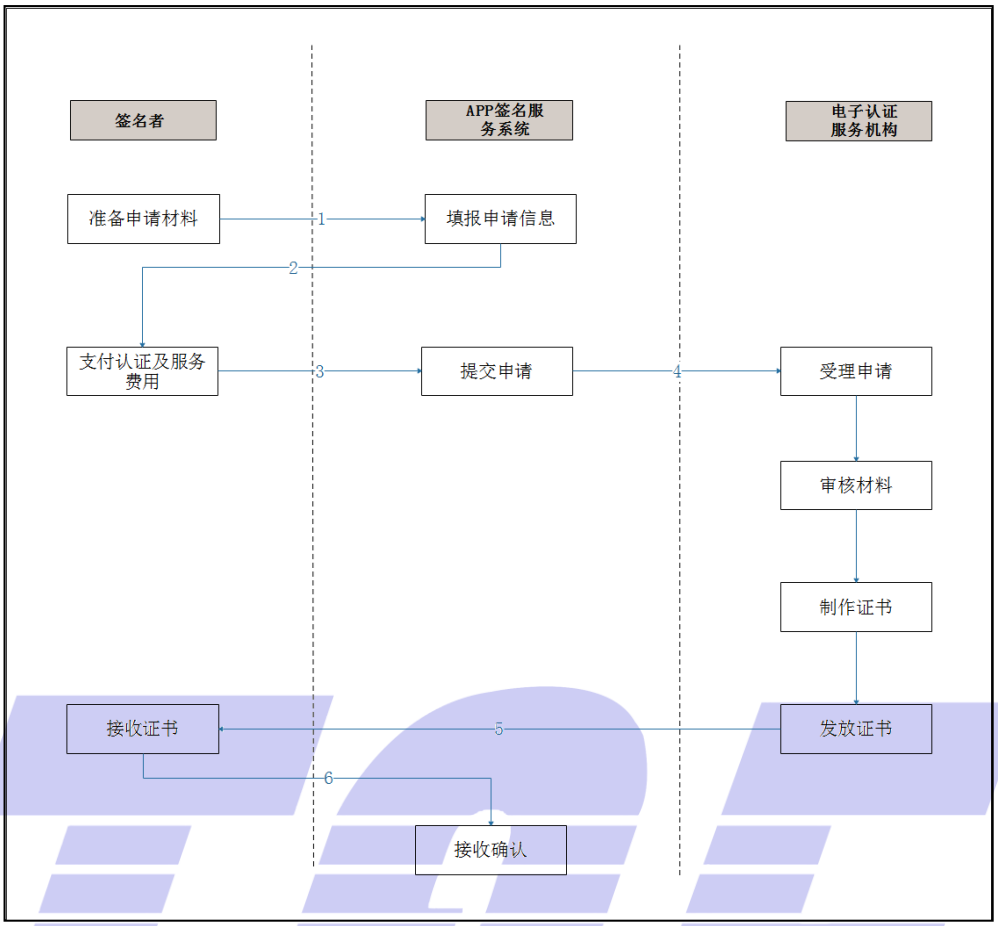

图 2　身份认证流程图

a）签名者按照电子认证服务机构的相关要求，准备实名认证所需的材料。

b）签名者在 APP 签名服务系统注册账号，按照流程填报相关信息并上传相关身份证明材料。

c）签名者根据申请的证书类型和数量，支付相应的认证及服务费用。

d）签名者通过 APP 签名服务系统向电子认证服务机构提交认证申请。

e）电子认证服务机构受理、审核、制作完成数字证书后，通过邮寄或现场交付等方式发放给签名者。

f）签名者接收到数字证书后，在 APP 签名服务系统中进行确认，完成签名者 CA 身份认证。

5.3.2　签名和查验流程

应用分发平台和应用检测平台在开展 APP 管理活动前，应先通过 APP 签名服务系统实现 APP 签名数据实时同步。签名和查验流程如图 3 所示。

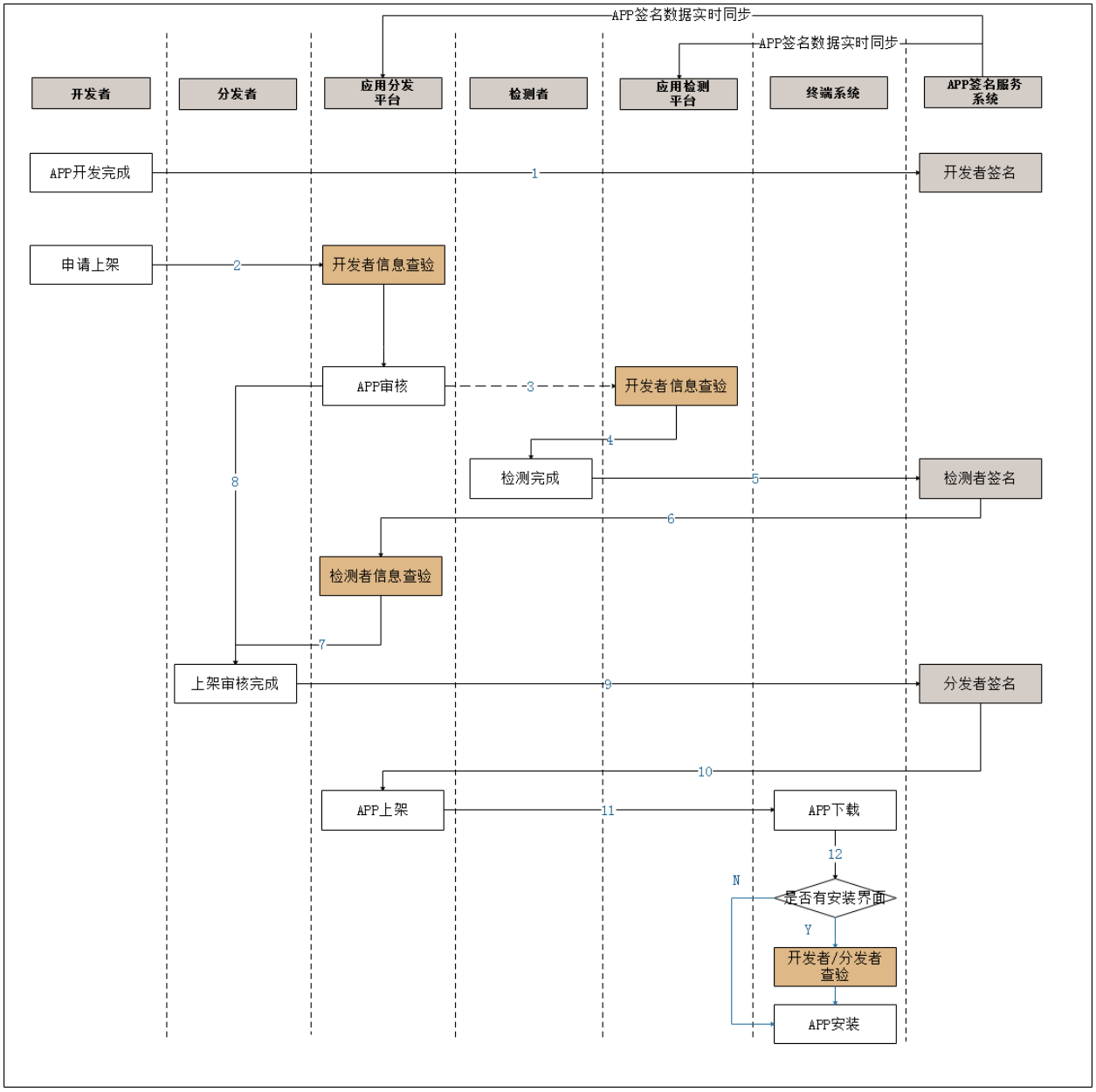

图 3　签名和查验流程图

a）开发者在开发完成或更新 APP 后，在 APP 签名服务系统中上传 APP 并完成开发者签名。

b）开发者向应用分发平台提交 APP 上架申请，由应用分发平台查验 APP 是否经过开发者签名，无签名时，引导开发者申请 CA 认证并完成签名。完成签名后，应用分发平台审核 APP 资质及其他要求。

c）应用分发平台向应用检测平台提交 APP 合规性检测。（可选，不申请则跳到第 h 步）

d）应用检测平台查验 APP 是否经过开发者签名，无签名时，引导开发者申请 CA 认证并完成签名。完成签名后，应用检测平台根据相关检测依据对 APP 进行合规性检测。

e）应用检测平台检测完成后，检测者在 APP 签名服务系统上传应用检测信息进行检测者签名。

f）应用分发平台查验检测者的应用检测信息。

g）应用分发平台在 APP 上架审核过程中参考检测者的应用检测信息。

h）应用分发平台完成 APP 上架审核。

i）分发者在 APP 签名服务系统中上传应用分发信息并对 APP 进行分发者签名。
j）应用分发平台对 APP 进行上架展示。
k）终端系统通过应用分发平台下载 APP。
l）终端系统安装 APP。如果 APP 安装时无安装界面，则直接安装，如果 APP 安装时有安装界面，则需要查验 APP 是否存在开发者或分发者的签名信息。查验渠道包括应用分发平台、应用检测平台和终端云管理平台。

5.4 CA 认证要求

a）签名者在签名前应向电子认证服务机构如实提交申请材料并签订电子认证服务协议，申请电子认证。
b)电子认证服务机构应按照公开发布的《电子认证业务规则》对签名者进行身份鉴证,并按照《T/TAF 084.2-2021 安卓应用程序认证签名技术规范-第二部分 数字证书格式规范》签发签名者数字证书。
c）签名者应妥善保管自己的数字证书，确保密钥信息不被他人获取及使用。

5.5 APP 签名服务系统功能要求

a）APP签名服务系统应提供签名者注册和数字证书申请功能。
b）APP签名服务系统应提供基于签名者数字证书安全登录的功能。
c）APP签名服务系统应提供签名者应用管理及批量签名功能。满足一个APP只能有一个开发者角色的签名，支持一个或多个检测者和分发者签名。签名数据格式应遵循《T/TAF 084.3-2021 安卓应用程序认证签名技术规范-第三部分 数字签名格式规范》。
d）APP签名服务系统应提供签名者签名数据有效性验证功能。
e）APP 签名服务系统应提供签名数据同步功能。

5.6 签名要求

a）开发者在 APP 开发完成后应及时通过 APP 签名服务系统对 APP 进行签名。
b）检测者在 APP 检测完成后应及时通过 APP 签名服务系统对 APP 进行签名。
c）分发者在 APP 上架审核完成后应及时通过 APP 签名服务系统对 APP 进行签名。

5.7 签名内容要求

a）签名者应按照《T/TAF 084.3-2021 安卓应用程序认证签名技术规范-第三部分 数字签名格式规范》的要求对应用名称、版本、开发者名称、应用摘要值等内容进行签名。
b）检测者签名内容还应包括检测说明。检测说明包括但不限于“检测未发现问题”、“检测发现问题”等内容。
c）分发者签名内容还应包含分发说明。分发说明包括但不限于“上架中”、“已上架”等内容。

5.8 验签和同步要求

a）APP 签名服务系统应实时验证签名者签名的有效性，验签成功后保存签名数据。
b）APP 签名服务系统应实时将有效签名数据同步到所有应用分发平台、应用检测平台和终端云管理平台，数据同步过程中应确保数据的私密性和完整性。

5.9 查验和展示要求

a）开发者在 SDK 集成前，应先通过 APP 签名服务系统查验 SDK 是否经过开发者签名。未完成开发

者签名的 SDK，引导开发者申请 CA 认证并完成开发者签名。

b）检测者在 APP 检测前，应先通过应用检测平台查验 APP 是否经过开发者签名。未完成开发者签名的 APP，引导开发者申请 CA 认证并完成开发者签名。

c）分发者在 APP 上架前，应先通过应用分发平台查验 APP 是否经过开发者签名。未完成开发者签名的 APP，引导开发者申请 CA 认证并完成开发者签名。完成开发者签名的 APP，应用分发平台上架中应展示开发者认证标识。

d）终端系统在安装 APP 时，对于有安装界面的 APP，应先查验 APP 是否经过开发者或分发者的签名。未完成开发者或分发者签名的 APP，应提示用户。

电信终端产业协会团体标准

安卓应用程序认证签名技术规范　第 1 部分：数字签名应用要求

T/TAF 084.1-2021

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn