ICS 33.050
M 30

团　体　标　准

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

Authentication signature specification for Android Applications—Part 3: Digital signature format specification

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 3 部分。T/TAF 084 已发布了以下部分：

——第 1 部分：数字签名应用要求；

——第 2 部分：数字证书格式规范。

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、博雅中科（北京）信息技术有限公司、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：邓佑军、浦雨三，程科伟，王平山，张猛、康亮。

引　　言

安卓应用程序认证签名是利用公钥密码机制来保证应用程序的完整性和行为的不可伪造、不可否认性。在实际应用中，安卓应用程序在生命周期中需经过开发、检测、分发等多个环节，每个环节都存在完整性、不可伪造、不可否认性需求，从而需要对安卓应用程序多次签名并留痕。

本文件作为安卓应用程序认证签名技术规范的第3部分，旨在指导安卓应用程序相关方在开发、检测、分发安卓应用程序时，采取相同的数据格式来对安卓应用程序签名，便于安卓应用程序在生命周期的不同环节下签名互认。

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

1　范围

本文件规定了基于安卓操作系统的应用程序数字签名格式规范、数字签名对象规范、数字签名数据机构规范等。

本文件适用于安卓应用程序相关方规范使用安卓应用程序数字签名格式。可用于指导专业机构、系统开发商、安全厂商、电子认证服务机构开发建设APP签名服务系统。

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。

GB/T 20520-2006　信息安全技术 公钥基础设施 时间戳规范

GB/T 35275-2017　信息安全技术 SM2密码算法加密签名消息语法规范

GB/T 35276-2017　信息安全技术 SM2密码算法使用规范

3　术语和定义

下列术语和定义适用于本文件。

3.1

数字签名　digital signature

附在数据单元后面的数据，或对数据单元进行密码变换得到的数据。允许数据的接收者验证数据的来源和完整性，保护数据不被篡改、伪造，并保证数据的不可否认性。

3.2

安卓应用程序　android application

安卓应用程序是指APK、SDK、快应用、小程序等可运行或集成在安卓系统中应用程序。

4　缩略语

下列缩略语适用于本文件。

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

SDK：软件开发工具包（Software Development Kit）

5 数字签名对象

安卓应用程序数字签名对象是安卓应用程序信息。包括应用名称、应用版本、应用开发者、应用杂凑值和签名者自定义数据。

6 数字签名数据结构

安卓应用程序数字签名数据的逻辑结构见表 1：

表 1 安卓应用程序数字签名数据结构

待签名数据	签名信息	时间戳

安卓应用程序数字签名数据的 ASN.1 定义为：

```
APPSignature::=SEQUENCE{
    tbsData       AS_TBSData,          --待签名数据
    signInfo      AS_SignInfo,         --签名信息
    timeStamp     OCTET STRING         --对签名信息的时间戳，时间戳遵循GB/T 20520-2006 《信息安全技术 公钥基础设施 时间戳规范》
}
```

6.1 待签名数据

待签名数据的逻辑结构见表 2：

表 2 待签名数据结构

头信息	应用程序信息

待签名数据的 ASN.1 定义为：

```
AS_TBSData::=SEQUENCE{
    header        AS_Header,           --头信息
    appInfo       AS_APPInfo           --应用程序信息
}
```

6.1.1 头信息

头信息的结构如表 3 所示：

表 3 头信息结构

标识	版本号

头信息的 ASN.1 定义为：

```
AS_Header::=SEQUENCE{
    id            IA5String(AS),       --数据标识
    version       INTEGER{v1(1)},      --版本号标识
}
```

其中：

id　　：固定值“AS”；

version　　：版本号，当前版本固定为“1”。

6.1.2 安卓应用程序信息

安卓应用程序信息的结构如表 4 所示：

表 4 安卓应用程序信息结构

应用名称	应用版本	应用开发者	应用杂凑值	自定义数据（可选）

应用程序信息的 ASN.1 定义为：

```
AS_APPInfo::=SEQUENCE{
    appName       IA5String,          --应用名称
    appVersion    INTEGER,            --应用版本
    appDeveloper  IA5String,          --应用开发者
    messageImprint                    MessageImprint,    --应用杂凑值
    extDatas      ExtensionDatas OPTIONAL--自定义数据
}
MessageImprint ::＝SEQUENCE {
                  hashAlgorithm         DigestAlgorithmIdentifier,
                  hashedMessage         OCTET STRING
}

ExtensionDatas::＝SET OF ExtensionData
ExtensionData::＝SEQUENCE {
                  item                  IA5String,
                  value                 OCTET STRING
 }
```

6.2 签名信息

签名信息的结构如表 5 所示：

表 5 签名信息结构

签名证书信息	签名算法标识	签名值

签名信息的 ASN.1 定义为：

```
AS_SignInfo::=SEQUENCE{
    certID          IssuerAndSerialNumber,  --签名证书标识
    signatureAlgorithm   DigestEncryptionAlgorithmIdentifier, --签名算法标识
    signatureValue     OCTET STRING          --签名值
    }
```

其中：

certID ：代表对数据进行签名的证书签发者和序列号信息。
signatureAlgorithm ： 代表签名算法 OID 标识。
signatureValue ：代表签名者对格式中待签名数据 tbsData 的数字签名。

如果签名算法使用SM2，则遵循GB/T 35275-2017《 信息安全技术 SM2密码算法加密签名消息语法规范》和GB/T 35276-2017 《信息安全技术 SM2密码算法使用规范》；如果签名算法使用RSA，则遵循PKCS#1: RSA Cryptography Standard和PKCS #7: Cryptographic Message Syntax。

7 数字签名处理流程

7.1 数字签名流程

应用程序数字签名流程如下：

a）从应用程序中提取应用程序信息，组装成“待签名数据”。
b）签名者使用私钥对“待签名数据”做数字签名，组装成“签名信息”。
c）申请制作“签名信息”的时间戳。
d）将“待签名数据”、“签名信息”和时间戳组装成应用程序数字签名数据。

7.2 数字签名验证流程

应用程序数字签名验证流程如下：

a）验证应用程序数字签名数据格式的正确性
- 根据数字签名数据结构格式来解析应用程序数字签名数据；
- 如果应用程序数字签名数据格式不正确，则验证失败并退出验证流程。

b）验证时间戳的正确性。
c）验证签名信息是否正确
- 从应用程序数字签名数据格式提取待验证数据，验证签名信息是否正确；
- 如果签名信息不正确则验证失败，并将失败原因返回上层应用并退出验证流程。

d）验证签名者数字证书有效性
- 从应用程序数字签名数据中获取签名者数字证书，验证签名者证书有效性，验证项至少包括：证书信任链验证、证书有效性验证、证书是否被吊销、密钥用法是否正确；
- 如果是由于证书信任链验证或密钥用法不正确导致的签名者证书有效性验证失败，则返回失败原因并退出验证流程；
- 如果是由于证书有效期或证书状态已吊销导致的签名者证书有效性验证失败，则还需要进一步结合签名时间进行判断。签名时证书未吊销，签名后再被吊销，则证书有效.签名时证书已吊销，则证书无效。

如果上述各步骤验证均有效，则签名验证结果为有效，可正常退出验证流程。

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3部分：数字签名格式规范

T/TAF 084.3-2021

*

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