ICS 33.050
M 30

团　体　标　准

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

Authentication signature specification for Android Applications—
Part 2: Digital certificate 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 2 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 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、博雅中科（北京）信息技术有限公司、长春吉大正元信息技术股份有限公司、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、王浩仟、汪海、张洋、胡越男、武小芳、浦雨三、赵丽丽、康亮。

引　　言

随着移动互联网的快速发展，安卓应用程序大量涌现，在安卓应用程序开发环节嵌入恶意代码，或通过篡改正常应用程序嵌入恶意代码，是目前制作安卓恶意程序的主要手段，采用CA机构签发的代码签名证书对安卓应用程序进行数字签名，能够保证开发者的身份真实可信，数字签名技术可以有效防止安卓移动应用程序被非法篡改，并对安卓移动应用程序的开发者有效溯源。

本文件作为安卓应用程序认证签名技术规范的第2部分，旨在指导国内现有CA机构签发安卓应用程序签名者数字证书的格式，便于安卓应用程序数字签名验签系统快速识别数字证书所对应的角色和身份信息。

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

1 范围

本文件定义了安卓应用程序电子认证服务体系中使用的数字证书的类型、数字证书和证书撤销列表的格式，制定了数字证书及证书撤销列表格式模板，用于指导电子认证服务机构签发统一格式的数字证书和证书撤销列表，以保障数字证书在安卓应用程序在流通结点之间的互信互认。

本文件适用于电子认证服务机构签发安卓移动应用程序开发者、检测者和分发者证书。

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 16262.1-2006 信息技术 抽象语法记法-（ASN.1）第1部分_ 基本记法规范

GB/T 20518-2018 信息安全技术 公钥基础设施 数字证书格式

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

数字证书是由权威的电子认证服务机构进行数字签名，包含拥有者信息、拥有者公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

3.2

证书撤销列表 certificate revocation list；CRL

CA对撤销的证书而签发的一个列表文件。

4 缩略语

下列缩略语适用于本文件。

ASN.1：抽象语法标记（Abstract Syntax Notation One）

CA：证书认证机构（Certificate Authority）

CRL：证书撤销列表（Certificate Revocation List）

5 数字证书类型

根据安卓应用程序用户特点及应用需求，数字证书可分成如下三类：

a）开发者证书

b）检测者证书

c）分发者证书

其中开发者包括个人和机构，检测者和分发者一般为机构。

6 数字证书格式

本文件采用GB/T 16262.1-2006的特定编码规则（DER）对下列证书项中的各项信息进行编码，组成特定的证书数据结构。ASN.1 DER编码是关于每个元素的标记、长度和值的编码系统。

6.1 数字证书基本结构

安卓应用程序用户证书的基本结构由三部分组成：基本证书域、签名算法域、签名值域。遵循 GB/T 20518-2018 中 5.2.1 章节规范。

6.1.1 基本证书域

基本证书域包括基本域和扩展域。本项未特别定义的数据项遵循 GB/T 20518-2018 中 5.2.2 章节规范。

6.1.1.1 基本域

基本域应包含如下部分组成：

a）版本 Version；

b）序列号 SerialNumber；

c）签名算法 SignatureAlgorithm；

d）颁发者 Issuer；

e）有效期 Validity；

f）主体 Subject；

g）主体公钥信息 SubjectPublicKeyInfo。

6.1.1.1.1 版本

本项描述了数字证书的版本号。

数字证书应使用版本 3。

6.1.1.1.2 序列号

本项是 CA 系统分配给每个证书的一个正整数，一个 CA 系统签发的每张证书的序列号应是唯一的。序列号最长可为 20 个 8 位字节的序列号值。证书更新时序列号应改变。

6.1.1.1.3 签名算法

本项包含 CA 签发该证书所使用的密码算法的标识符，算法标识符应与证书中 SignatureAlgorithm 项的算法标识符相同。

应采用国家密码主管部门认可签名算法。

6.1.1.1.4 颁发者

本项标识了证书签名和证书颁发的实体。它应包含一个非空的可甄别名。该项被定义为 X.500 的 Name 类型。本项遵循 GB/T 20518-2018 的 5.2.3.4 章节规范。

6.1.1.1.5 有效期

本项是指一个时间段，在这个时间段内，CA 系统担保它将维护关于证书状态的信息。该项被表示成一个具有两个时间值的 SEQUENCE 类型数据：证书有效期的起始时间（notBefore）和证书有效期的终止时间（notAfter）。本项遵循 GB/T 20518-2018 的 5.2.3.5 章节规范。

6.1.1.1.6 主体

本项描述了与主体公钥项中的公钥相对应的实体。主体名称可以出现在主体项或主体替换名称扩展项中（SubjectAltName）。如果主体是一个 CA，那么主体项应与其签发的所有证书的颁发者相同，一个 CA 认证的每个主体实体的甄别名称应是唯一的。一个 CA 可以为同一个主体实体以相同的甄别名称签发多个证书。该项不能为空。

本项代表一个证书持有者身份的唯一标识，在 Android 移动应用中，本标识可为 Android 移动应用依赖方提供方便快捷的身份验证。主体（DN）命名规范见表 1。

表 1　主体（DN）命名规范表

主体项	命名规则	说明
CN	用户名称@用户编号	用户名称是证书所有者的全称，个人为姓名，机构为机构全称。 用户编号是一个证书实体的证书序号，企业用户编号为 4 位流水号。个人用户编号为身份证后四位+2 位流水号。
O	用户所属组织	Developer 代表安卓移动应用开发者； Tester 代表安卓移动应用检测者； Distributor 代表安卓移动应用分发者。
L	用户所在城市	城市名称。
S	用户所在省份	省份名称。
C	国家	固定值“CN”

主体（DN）命名示例参考附录 A。

6.1.1.1.7 主体公钥信息

本项用来标识公钥和相应的公钥算法。本项遵循GB/T 20518-2018的5.2.3.7章节规范。

6.1.1.2 扩展域

数字证书中应定义如下一些标准的扩展项：

a）密钥用法

b）主体密钥标识符

c）颁发机构密钥标识符

d）个人身份标识码

e）企业组织机构代码

6.1.1.2.1 密钥用法

本项说明已认证的公开密钥用于何种用途。

所有证书应具有密钥用法扩展项。用户证书则根据证书用途，分“签名”证书和“加密”证书，选择对应的密钥用途进行签发。本项遵循 GB/T 20518-2018 的 5.2.4.2.4 章节规范。

6.1.1.2.2 主体密钥标识符

本项提供一种识别包含有一个特定公钥的证书的方法。此扩展标识了被认证的公开密钥，它能够区分同一主体使用的不同密钥。

所有的 CA 证书应包括本扩展，此扩展项为非关键项。本项遵循 GB/T 20518-2018 的 5.2.4.2.3 章节规范。

6.1.1.2.3 颁发机构密钥标识符

本项提供了一种方式，以识别与证书签名私钥相应的公钥。当颁发者由于有多个密钥共存或由于发生变化而具有多个签名密钥时使用该扩展。识别可基于颁发者证书中的主体密钥标识符或基于颁发者的名称和序列号。本项遵循 GB/T 20518-2018 的 5.2.4.2.2 章节规范。

6.1.1.2.4 个人身份标识码

个人身份标识码项用于表示个人身份的有效身份证件号码。是个人主体唯一标识。本项遵循 GB/T 20518-2018 的 5.2.4.2.18 章节的定义。个人证书应包含此扩展。

6.1.1.2.5 企业组织机构代码

企业组织机构代码号扩展项用于表示企业组织机构代码。是机构主体唯一标识。本项遵循 GB/T 20518-2018 的 5.2.4.2.21 章节的定义。机构证书应包含此扩展。

6.1.1.2.6 主体替换名称

数字证书在更新时，如果企业名称发生了变更，主体替换名称应设置为原证书主体中的 CN 值。

6.1.2 签名算法域

包含证书签发机构签发该证书所使用的密码算法的标识符。算法标识符用来标识一个密码算法，无可选参数。本项遵循 GB/T 20518-2018 的 5.2.2 章节 SignatureAlgorithm 域的规范。

6.1.3 签名值域

本项包含对基本证书域进行数字签名的结果。经 ASN.1 DER 编码的基本证书域作为数字签名算法的输入，签名的结果按照 ASN.1 编码成 BIT STRING 类型并保存在签名值域内。本项遵循 GB/T 20518-2018 的 5.2.2 章节 SignatureValue 域的规范。

6.2 数字证书模板

根据数字证书类型可分为个人证书模板和机构证书模板，证书模板定义参考附录 B。

7 CRL 格式

7.1 CRL 基本机构

CRL 是 CA 对吊销的证书而签发的一个列表文件，该文件可用于业务系统鉴别用户证书的有效性。

CRL 文件结构主要包括：

a）版本号

b）颁发者

c）生效日期

d）下次更新日期

e）签名算法

f）扩展项

g）被吊销的证书列表

本项遵循 GB/T 20518-2018 的 5.3.2 章节规范。

7.2 CRL 模板

CRL 模板定义参考附录 B。

附 录 A
（规范性）
证书主体 DN 命名示例

A.1 开发者证书主体 DN 示例

开发者信息示例见表 A.1：

表 A.1 开发者信息示例表

名称：	XXX 有限公司
地址：	河北省邢台市
角色：	开发者
其他信息：	申请本角色第（2）张有效证书

DN 命名示例如下：

DN=CN=XXX 有限公司@02,O=Developer,L=邢台市,S=河北省,C=CN

A.2 检测者证书主体 DN 示例

检测者信息见表 A.2：

表 A.2 检测者信息示例表

名称：	XXXX 有限公司
地址：	河北省邢台市
角色：	检测者
其他信息：	申请本角色第（5）张有效证书

DN 命名示例如下：

DN=CN=XXXX 有限公司@05,O=Tester,L=邢台市,S=河北省,C=CN

A.3 分发者证书主体 DN 示例

分发者信息见表 A.3：

表 A.3 分发者信息示例表

名称：	XXXXX 有限公司
地址：	河北省邢台市
角色：	分发者
其他信息：	申请本角色第（1）张有效证书

DN 命名示例如下：

DN=CN=XXXXX 有限公司@01,O=Distributor,L=邢台市,S=河北省,C=CN

附 录 B
（资料性）
模板定义示例

B.1 个人证书模板

个人证书模板示意表见表 B.1

表 B.1 个人证书模板示意表

证书域名	含义	说明	字段内容（示例）
Version	版本号	证书版本号	V3
Serial Number	证书序列号	有颁发机构生成	330c177d2ec4c963
Signature	签名算法	符合国家标准	1.2.156.10197.1.501
Issuer	颁发者	有效国家二级根	CN=XXCA,O=XX 公司,C=CN
Validity	有效期限		最长 3 年
notBefore	有效期起始日期	签发日期	2017 年 6 月 23 日 16:10:34
notAfter	有效期终止日期	起始日期+X 个月	2019 年 6 月 23 日 16:10:34
Subject	主体	DN	
	C	国家	CN
	S	省份	北京
	L	城市	北京
	O	组织	Developer
	CN	通用名称	张三@3311
KeyUsage	密钥用法	关键扩展域	签名证书包含： Digital Signature, Non-Repudiation 加密证书包含： Key Encipherment, Data Encipherment Key Agreement
IdentifyCode	个人身份标识码	关键扩展项	0110123199910100031
SubjectKeyIdentifier	主体密钥标识符	关键扩展项，用户证书公钥的哈希值	1c 5d d3 5f 44 c9 2c 0d 34 9b c9 37 1c a8 b8 8d 1e 74 9b 10
AuthorityKeyIdentifier	颁发机构主体密钥标识符	关键扩展项，颁发机构证书公钥的哈希值	KeyID=8b 69 10 6b a5 42 df 2e a6 f7 a0 d9 b3 8c a4 08 bb 3d 50 39
SignatureAlgorithm	签名算法	对证书基本信息的数字签名的签名算法	
Issuer’s Signature	签名值	颁发机构对证书基本信息的数字签名	

B.2 机构证书模板

机构证书模板示意表见表 B.2

表 B.2 机构证书模板示意表

证书域名	含义	说明	字段内容（示例）
Version	版本号	证书版本号	V3
Serial Number	证书序列号	有颁发机构生成	330c177d2ec4c963
Signature	签名算法	符合国家标准	1.2.156.10197.1.501
Issuer	颁发者	有效国家二级根	CN=XXCA,O=XX 公司,C=CN
Validity	有效期限		最长 3 年
notBefore	有效期起始日期	签发日期	2017 年 6 月 23 日 16:10:34
notAfter	有效期终止日期	起始日期+X 个月	2019 年 6 月 23 日 16:10:34
Subject	主体	DN	
	C	国家	CN
	S	省份	北京
	L	城市	北京
	O	组织	Developer
	CN	通用名称	XXX 有限公司@01
KeyUsage	密钥用法	关键扩展域	签名证书包含： Digital Signature, Non-Repudiation 加密证书包含： Key Encipherment, Data Encipherment Key Agreement
OrganizationCode	企业组织机构代码	关键扩展项	2342342023948J
SubjectKeyIdentifier	主体密钥标识符	关键扩展项，用户证书公钥的哈希值	1c 5d d3 5f 44 c9 2c 0d 34 9b c9 37 1c a8 b8 8d 1e 74 9b 10
AuthorityKeyIdentifier	颁发机构主体密钥标识符	关键扩展项，颁发机构证书公钥的哈希值	KeyID=8b 69 10 6b a5 42 df 2e a6 f7 a0 d9 b3 8c a4 08 bb 3d 50 39
SignatureAlgorithm	签名算法	对证书基本信息的数字签名的签名算法	
Issuer's Signature	签名值	颁发机构对证书基本信息的数字签名	

B.3 CRL 模板示意表

CRL 模板示意表见表 B.3

表 B.3 CRL 模板示意表

证书域名	含义	说明（示例）
Version	版本号	1（表示 V2 版本）
Signature	签名算法	1.2.156.10197.1.501

表B.3 CRL模板示意表（续）

证书域名	含义	说明（示例）
Issuer	签发机构	有效国家二级根
Validity	有效期限	
ThisUpdate	本次更新日期	签发时确定
NextUpdate	下次更新日期	根据签发 CRL 策略确定
Revoke cert List	被吊销的证书列表	
Cert info	证书信息	被撤消的证书关键信息
SeriaNumber	序列号	被撤消的证书序列号
Revocationdate	时间	吊销时间
extnValue	扩展项	CRL 理由码
AuthorityKeyIdentifier	颁发机构主体密钥标识符	关键扩展项，颁发机构证书公钥的哈希值
SignatureAlgorithm	签名算法	对 CRL 基本信息的数字签名的签名算法
SignatureValue	签名值	对 CRL 基本信息的数字签名的签名值

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2部分：数字证书格式规范

T/TAF 084.2-2021

*

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