安卓软件数字签名消息语法规范

草案(v0.2)

Android software digitally signature message syntax specification

目录

前　　言

安卓软件数字签名消息语法规范定义了一种数字签名格式用于认证安卓软件的完整性、有效性、合法性、可追溯性。此种数字签名格式是基于公钥密码标准(PKCS#7)的签名数据格式（signedData），在兼容安卓软件原生签名验证的基础上，为不同角色提供副署时间戳签名。本文将详细说明这种数字签名格式，并描述其签名和验证流程。

本规范按照 GB/T 1.1-2009 的规则编写。

本规范起草单位：江苏先安科技有限公司。

1 范围

本标准定义了对安卓软件原生数字签名进行二次乃至多次数字签名副署的格式。本标准适用于对安卓软件进行数字签名和对安卓软件进行合法化、有效性、完整性验证。

2 规范性应用文件

下列文件对于本文的应用是必不可少的。

PKCS #7 Cryptographic Message Syntax Version 1.5 （RFC2315）

PKCS #6 Extended-Certificate Syntax

PKCS #9 Selected Attribute Types

GM/T 0010 SM2 密码算法签名加密语法消息规范

3 术语和定义

下列术语适用于本文件。

3.1 算法标识 algorithm identifier

用于表明算法机制的数字化信息。

3.2 副署签名 counter signature

检测机构、应用商店或者管理部门对安卓软件原生数字签名进行副署时间戳签名。

3.3 安卓软件原生数字签名

通过调用安卓软件开发包中 jarsigner 对 APK 文件生成的数字签名，详情可见: http://developer.android.com/tools/publishing/app-signing.html

4 符合和缩略语

OID 对象标识符（Object Identity）

5 OID 定义

本规范对 pkcs-9-at-counterSignature，pkcs-9-at-contentType，pkcs-9-at-signingTime，pkcs-9-at-messageDigest 进行了定义，详见表 1。

表 1 副署时间戳签名对象标识符

对象标识符 OID	对象标识符定义
1.2.840.113549.1.9.6	副署时间戳签名 OID 值（pkcs-9-at-counterSignature）
1.2.840.113549.1.9.3	副署时间戳内容类型 OID 值(pkcs-9-at-contentType)
1.2.840.113549.1.9.5	副署时间戳签发时间 OID 值(pkcs-9-at-signingTime)
1.2.840.113549.1.9.4	副署时间戳摘要 OID 值（pkcs-9-at-messageDigest）

6 基本类型定义

6.1 CertificateRevocationLists

CertificateRevocationLists 类型标明一个证书撤销列表的集合。
CertificateRevocationLists::= SET OF CertificateRevocationList

6.2 DigestAlgorithmIdentifier

DigestAlgorithmIdentifier 类型标明一个消息摘要算法
DigestAlgorithmIdentifier::= AlgorithmIdentifier

6.3 DigestEncryptionAlgorithmIdentifier

DigestEncryptionAlgorithmIdentifier 类型标明一个消息签名算法
DigestEncryptionAlgorithmIdentifier::= AlgorithmIdentifier

6.4 ExtendedCertificateOrCertificate

ExtendedCertificateOrCertificate 类型指定一个 PKCS#6 扩展证书或者一个 X.509 证书。这一类型见 PKCS#6 第六节[1]推荐的语法：

```
ExtendedCertificateOrCertificate::=CHOICE {
    certificate Certificate, --X.509
    extendedCertificate [0] IMPLICIT ExtendedCertificate
}
```

6.5 ExtenedCertificatesAndCertificates

ExtenedCertificatesAndCertificates 类型指定一个扩展证书和 X.509 证书的集合。它表示集合足以包含从可识别的“根”和“顶级 CA“到所有签名者的证书链。

```
ExtenedCertificatesAndCertificates ::= SET OF ExtendedCertificateOrCertificate
```

6.6 IssuerAndSerialNumber

IssuerAndSerialNumber 类型标明一个证书颁发者可识别名和颁发者确定的证书序列号，可据此确定一份和此证书对应的实体及公钥。

```
IssuerAndSerialNumber::=SEQUENCE{
    Issuer Name,
    serialNumber CertificateSerialNumber
}
```

6.7 Version

Version 类型标明语法版本号,本规范定义为 1。

```
Version ::=INTERGER(1)
```

6.8 ContentInfo

ContentInfo 类型标明内容交换通用语法结构，内容交换的通用语法结构定义如下：

```
ContentInfo::=SEQUENCE{
    contentType ContentType,
    content[0] Explicit ANY DEFINED BY contentType OPTIONAL
```

}
ContentType::= OBJECT IDENTIFIER
其中：ContentType 内容类型是一个对象表示符.

7 安卓软件数字签名格式

安卓软件原生数字签名格式属于是 PKCS#7 signedData 类型,下面我们就描述这种类型.

7.1 PKCS#7 signedData 类型

signedData 数据类型由任意类型的数据和至少一个签名者的签名者组成。任意类型的数据能够同时被任意数量的签名者签名。

signedData 数据类型结构定义如下：

```
signedData::=SEQUENCE {
    version Version,
    digestAlgorithms DigestAlgorithmIdentifiers,
    contentInfo ContentInfo,
    certificates [0] IMPLICIT ExtendedCertficatesAndCertficates OPTIONS,
    crl [1] IMPLICIT CertificateRevocationLists OPTIONS,
    signerInfos SignerInfos
}
DigestAlgorithmIdentifiers::=SET of DigestAlgorithmIdentifiers
SignerInfos::=SET of SignerInfo
```

结构中个项含义见表 2.

表 2 signedData 数据类型

字段名称	数据类型	含义
version	Version	语法的版本号
digestAlgorithms	DigestAlgorithmIdentifiers	消息摘要算法标识符集合
contentinfo	ContentInfo	被签名的数据内容，如果是 RSA 算法，ContentInfo 的 OID 为 1.2.840.113549.1.7.1，当使用 SM2 算法时，ContentInfo 的 OID 为 1.2.156.10197.6.1.4.2.1
certificates	ExtendedCertificatesAndCertificates	PKCS#6 扩展证书和 X。509 证书的集合,在安卓软件原签名时，包含软件发布者

		的签名证书，当有副署时间戳签名时，必须包含副署时间戳签发者的签名证书
crls	CertificateRevocationLists	证书撤销列表集合
signerInfos	SignerInfoS	每一个签名者信息的集合

7.2 SignerInfo 类型

Signerinfo 的结构内容如下：

```
SignerInfo::=SEQUENCE{
    version Version,
    issuerAndSerialNumber IssuerAndSerialNumber,
    digestAlgorithm DigestAlgorithmIdentifier,
    authenticatedAttributes[0] IMPLICIT Attributes OPTIONAL,
    digestEncryptionAlgorithm DigestEncryptionAlgorithmIdentifier,
    encryptedDigest EncryptedDigest,
    unauthenticatedAttributes[1] IMPLICIT Attrubutes OPTIONAL
}
EncryptedDigest::=OCTET STRING
unauthenticatedAttributes::= SET OF ATTRIBUTE
```

结构体中各项含义见表 3.

表 3 SignerInfo 数据类型

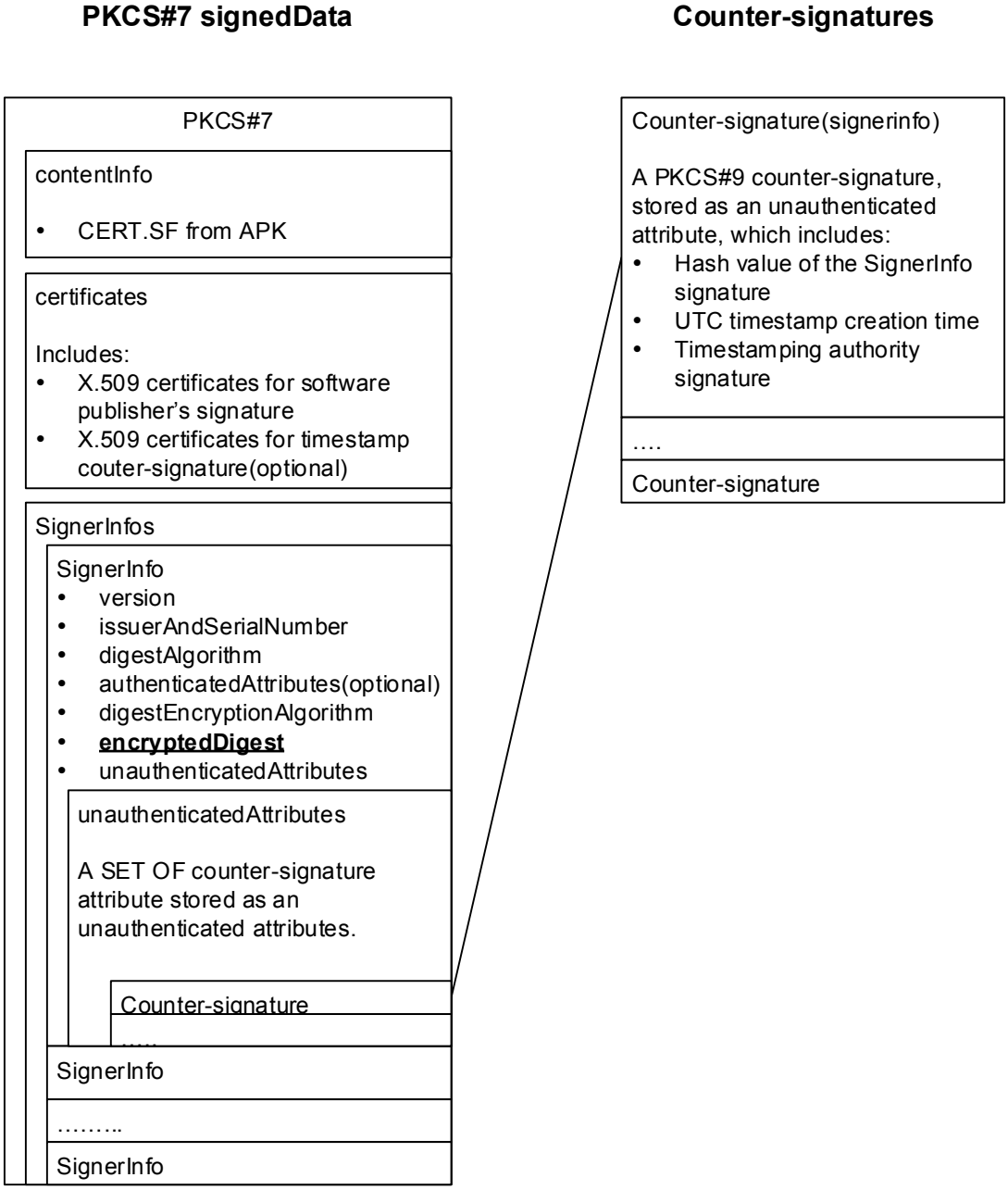
字段名称	数据类型	含义
version	Version	语法的版本号
issuerAndSerialNumber	IssuerAndSerialNumber	一个证书颁发者可识别名和颁发者确定的证书序列号，可据此确定一份证书和与此证书对应的实体及公钥
digestAlgorithm	DigestAlgorithmIdentifier	对内容进行摘要计算的消息摘要算法,当使用 RSA 时，推荐使用 SHA1 摘要算法，当使用 SM2 算法时，使用 SM3 摘要算法
authenticatedAttributes	Attributes	是经由签名者签名的属性的集合，

		该域中摘要的计算方法是对原文进行摘要计算结果（可选）
digestEncryptionAlgorithm	DigestEncryptionAlgorithmIdentifier	数字签名算法标识，当使用 RSA 时，OID 为 1.2.840.113549.1.1.1，当使用 SM2 算法时，OID 为 1.2.156.10197.1.301.1
encryptedDigest	OCTET STRING	数字签名计算结果，如果有 authenticatedAttributes,则数字签名是对 authenticatedAttributes 数据进行签名，如果没有 authenticatedAttributes 属性，则对原文进行签名
unauthenticatedAttributes	Attributes	副署时间戳签名集合。

7.3 副署时间戳签名（counter-signature）

副署时间戳签名是一种 PKCS#9 签名,放置在 PKCS#7 signerinfo 结构的 unauthenticatedAttributes 中，unauthenticatedAttributes 由一组副署时间戳签名的集合（counter-signatures）。副署时间戳签名在安卓软件的位置如下图 1 所示：

图 1 副署时间戳签名在安卓签名的位置图



其 Counter-signatue 结构如下：

counterSignature ATTRIBUTE ::= {

WITH SYNTAX SignerInfo

OID pkcs-9-at-counterSignature

}

其中属性 OID 为 1.2.840.113549.1.9.6，其值为是符合 PKCS#9 标准的 signerinfo 结构，此 signerinfo 结构必须包含 authenticatedAttributes 成员，此成员中必须包含下列三个属性：

- contentType (1.2.840.113549.1.9.3)

contentType ATTRIBUTE ::= {
WITH SYNTAX ContentType
SINGLE VALUE TRUE
OID pkcs-9-at-contentType
}

ContentType ::= AlgorithmIdentifier

其属性 OID 为 1.2.840.113549.1.9.3，其值是算法标识符（唯一），当签名算法是 RSA 时，此算法标识符为（1.2.840.113549.1.7.1）；当签名算法是 SM2 时，此算法标识符为（1.2.156.10197.6.1.4.2.1）。

- messageDigest(1.2.840.113549.1.9.4)

messageDigest ATTRIBUTE ::= {
WITH SYNTAX MessageDigest
EQUALITY MATCHING RULE octetStringMatch
OID pkcs-9-at-messageDigest
}

MessageDigest ::= OCTET STRING

其属性 OID 为 pkcs-9-at-messageDigest（1.2.840.113549.1.9.4），属性类型为 OCTET STRING（唯一），内容是软件发布者对其安卓软件签名的 signerinfo 结构中的 encryptedDigest 签名值再根据 counter-signature 中 signerinfod 的摘要算法计算摘要的结果，其位置见图 1 中粗体、下划线的字段。

- signingTime(1.2.840.113549.1.9.5)

signingTime ATTRIBUTE ::= {
WITH SYNTAX SigningTime
EQUALITY MATCHING RULE uTCTimeMatch
SINGLE VALUE TRUE
OID pkcs-9-at-signingTime
}

SigningTime ::= UTCTime

其 OID 为 pkcs-9-at-signingTime（1.2.840.113549.1.9.5），属性类型为 UTCTime, 为副署签名时间（唯一）。

8 安卓软件副署时间戳的签名和验证流程

8.1 安卓软件副署时间戳签名流程

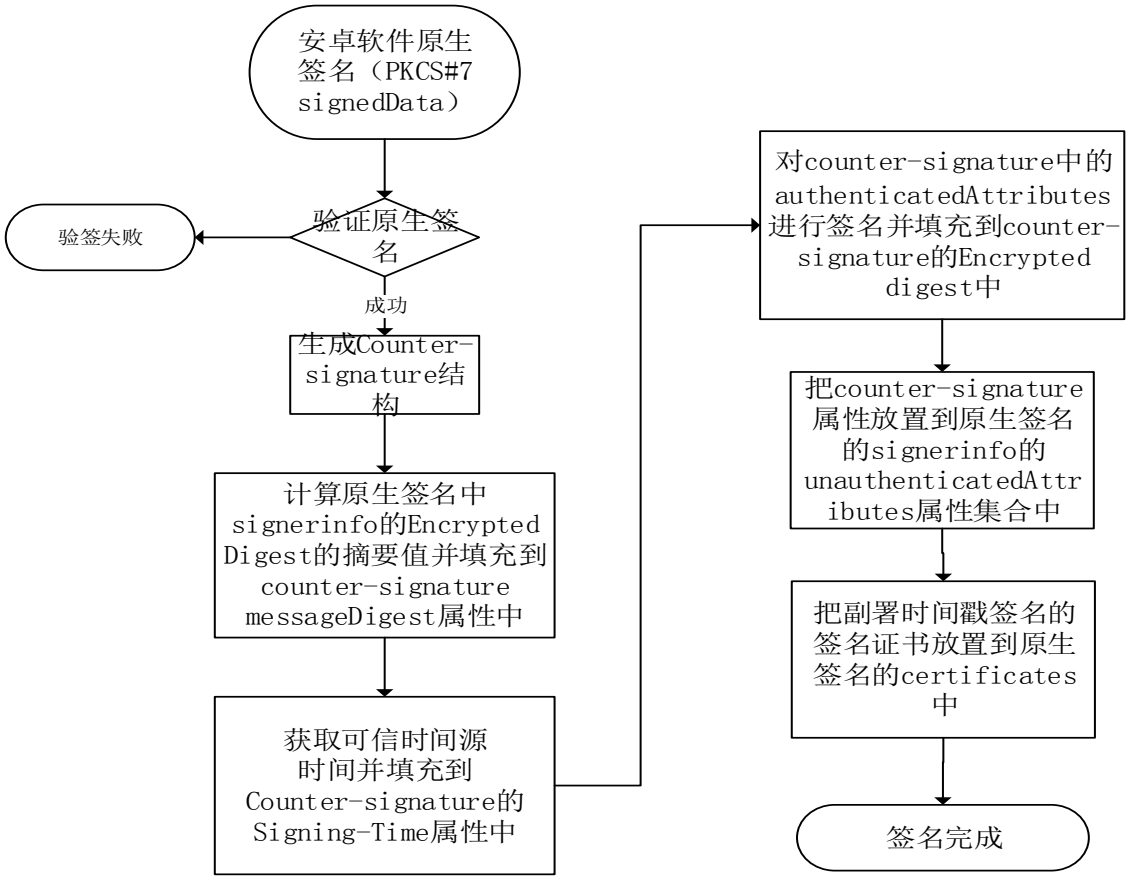


图 2、安卓软件副署时间戳签名流程

首先对安卓软件数字原生签名进行验证，如果验证成功，则构造 counter-signature 属性，对原生签名 signerinfo 结构中的 EncryptDigest（签名值）计算摘要（使用副署时间戳中的摘要算法）并放置到 counter-signature 的 messageDigest 属性中，获取可信时间源时间填充到 signing-time 属性中，对 counter-signature 中的 authenticatedAttributes 进行签名，填充到 counter-signature 中的 EncryptedDigest 中，把生成的 counter-signature 属性放置到原生签名的 unauthenticatedAttributes 属性集合中，最后把签发副署时间戳的签名证书放置到原生签名的 certificates 内，完成副署时间戳的签名。

8.2 安卓软件数字副署时间戳验证流程

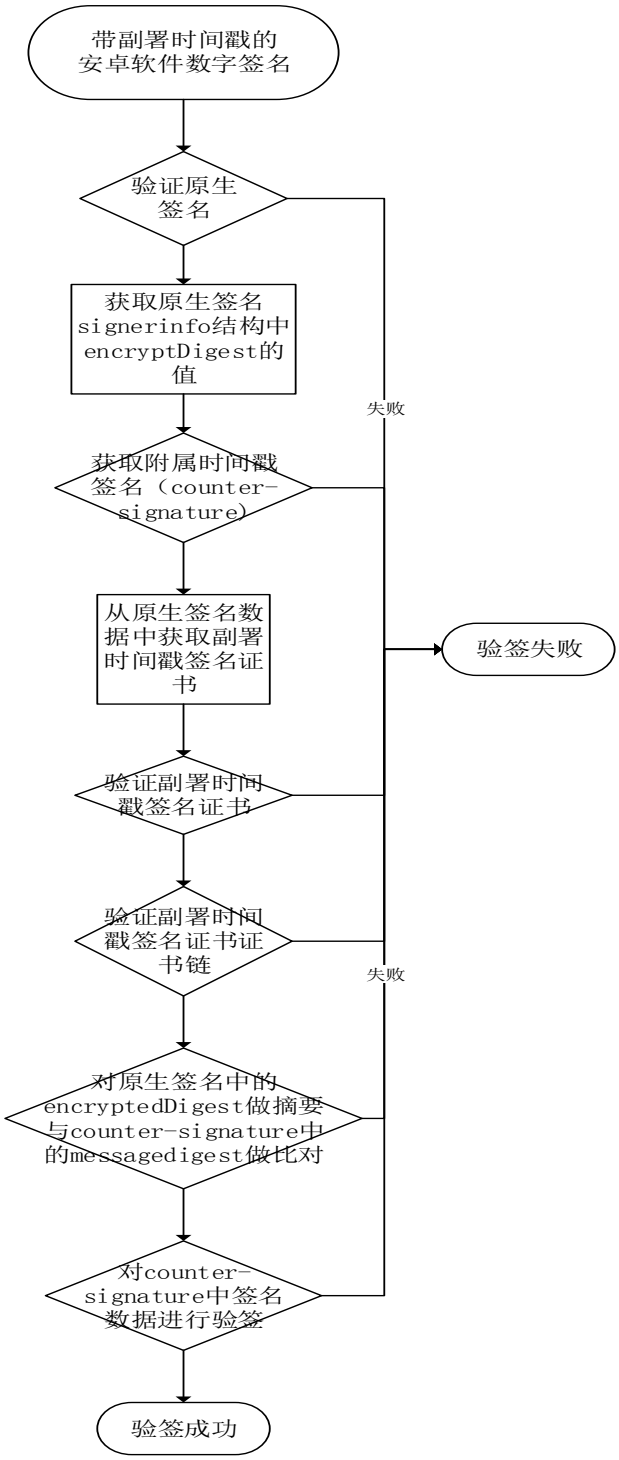


图 3、安卓软件时间戳副署签名验签流程

首先进行原生签名验签，验证开发者信息之后从原生签名中获取副署时间戳签名（counter-signature），从原生签名和副署时间戳签名中获取副署时间戳的签名证书，验证其证书和证书链，之后从原生签名的 signerinfo 结构中获取

encryptedDigest 的值，对 encryptedDigest 做摘要运算（使用副署时间戳签名中的摘要算法），与副署时间戳签名中的 messagedigest 属性进行比对，如果摘要不一致则验签失败，再对副署时间戳签名中数字签名进行验证，查看是否验证成功，完成验签步骤。