GD

中华人民共和国广播电视暂行技术文件

GD/J 081—2018

应急广播安全保护技术规范　数字签名

Technical specification for emergencey broadcasting security protection
—Digital signature

2018－10－12 发布　　2018－10－12 实施

国家广播电视总局科技司　　发 布

目　　次

前　言

本技术文件按照GB/T 1.1—2009给出的规则起草。

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这些专利的责任。

本技术文件由国家广播电视总局科技司归口。

本技术文件起草单位：国家广播电视总局广播科学研究院、江西省新闻出版广电局、北京江南天安科技有限公司、杭州图南电子股份有限公司、杭州工信光电子有限公司、北京数码视讯科技股份有限公司、成都德芯数字科技股份有限公司。

本技术文件主要起草人：郭沛宇、李晓鸣、张乃光、赵云辉、蔡旦颖、李国、朱家雄、赵震、蒋金甫、刘春江、丁森华、马艳、席岩、栗志国、赵镜平、张振兴。

应急广播安全保护技术规范　数字签名

1　范围

本技术文件规定了应急广播信息主体文件、应急广播消息指令文件和传输覆盖指令的数字签名安全保护机制。

本技术文件适用于应急广播从应急信息接入、制播、调度控制、传输覆盖到接收全流程的安全保护。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 32905—2016　信息安全技术　SM3密码杂凑算法

GB/T 32918（所有部分）　信息安全技术　SM2椭圆曲线公钥密码算法

3　术语和定义

下列术语和定义适用于本文件。

3.1

应急广播消息　emergency broadcasting message

各级应急广播平台之间，以及应急广播平台到广播电视频率频道播出系统、各类应急广播传输覆盖资源和终端之间传递的播发指令等相关数据。应急广播消息包括应急广播信息主体文件、应急广播信息主体签名文件、应急广播节目资源文件、应急广播消息指令文件、应急广播消息指令签名文件。

3.2

应急广播数字证书　emergency broadcasting certificate

由数字证书签发编号和数字证书编号唯一标识，包括数字证书格式版本号、数字证书签发编号、数字证书编号、数字证书有效期、公钥信息、数字签名信息等，用于应急广播各级系统之间、系统与终端之间的认证。

3.3

数字签名　digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

3.4

应急广播数字证书管理系统　emergency broadcasting certificate management system

进行应急广播各级系统和接收端数字证书生成、发放和撤销的管理系统。

3.5

应急广播证书授权列表　emergency broadcasting certificates authorization list

由应急广播数字证书管理系统签发的证书授权列表，包括：接收端编号、证书授权序列号、证书数量、证书编号列表、数字签名，用于规定应急广播各级系统和接收端的信任关系。

3.6

应急广播数字证书安全代理　emergency broadcasting　certificate security proxy

应急广播数字证书管理系统与应急广播各级系统的安全通信代理，向应急广播证书管理系统申请本级系统的数字证书，以及申请本级系统各设备和接收端的证书授权列表。

3.7

应急广播传输覆盖指令　emergency broadcasting transmission coverage command

面向不同的传输覆盖网络类型，将应急广播消息指令进行适配处理后生成的控制指令。

4　缩略语

下列缩略语适用于本文件。

uimsbf　无符号整数，高位在前（unsigned integer most significant bit first）

XML　可扩展标记语言（Extensible Markup Language）

5　应急广播数字签名保护机制

5.1　概述

为保障国家应急广播体系各级系统之间应急广播消息和传输覆盖指令传输的安全性，确保应急广播各级系统仅接收和处理合法的应急广播消息和指令，防止非法攻击干扰正常社会秩序，需要采用相应的安全手段保障应急广播消息和指令的真实性、合法性、完整性。

应急广播消息和指令的安全保护机制采用数字签名和数字证书技术实现。应急广播各平台之间传递的应急广播消息以及在广播电视传输覆盖网中传递的应急广播传输覆盖指令采用基于非对称密码算法的数字签名技术实现真实性、合法性和完整性保护。应急广播消息和指令的发送端采用自身的私钥，对应急广播信息主体文件、应急广播节目资源文件、应急广播消息指令文件和应急广播传输覆盖指令计算数字签名，并将数字签名附带在应急广播消息和传输覆盖数据中传递，应急广播消息和应急广播传输覆盖数据的接收端采用发送端的公钥对数字签名进行验证，确保接收端只接收合法的应急广播消息，只处理合法的应急广播指令。应急广播数字签名的密码算法采用GB/T 32918、GB/T 32905—2016规定的SM2、SM3算法。

应急广播各级系统及接收端采用数字证书技术实现数字签名用密钥的分发、认证与撤销。应急广播数字证书管理系统负责应急广播各级系统及接收端数字证书的申请、生成、分发与撤销，应急广播数字证书及应急广播证书授权列表的传递及更新。

5.2　应急广播信息的数字签名机制

应急广播信息采用数字签名方式实现其真实性、合法性和完整性保护。应急广播节目资源文件的摘要存储在应急广播信息主体文件中，应急广播信息主体文件采用应急广播平台制作播发系统的私钥进行签名，该签名存储在应急广播信息签名文件中，应急广播信息签名文件中包含了应急广播信息主体文件的标识。

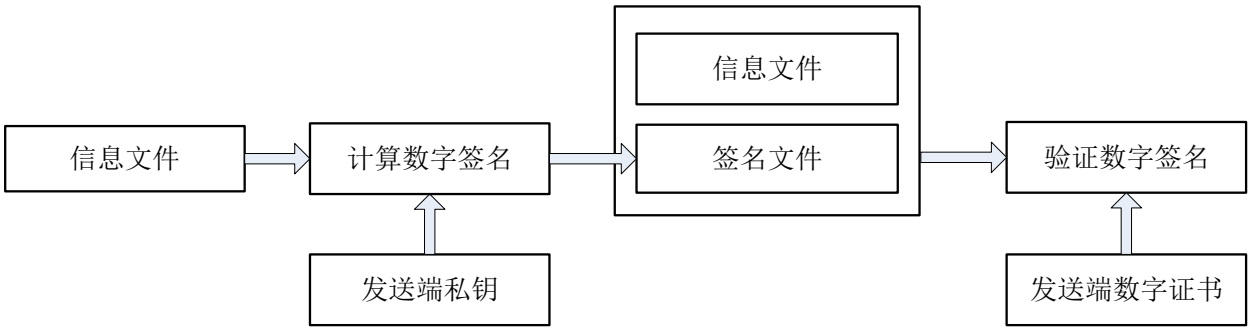

图1　应急广播信息的数字签名机制

应急广播信息签名文件格式见6.3。

5.3　应急广播消息的数字签名机制

应急广播各级系统之间的应急广播消息传递采用XML文件签名的方式进行保护，应急广播平台调度控制系统组织好待签名的XML格式应急广播消息后，使用应急广播平台调度控制系统的私钥进行签名，签名结果以XML签名文件形式与应急广播消息文件一起发送。接收时使用应急广播平台调度控制系统数字证书和XML签名文件对应急广播消息文件进行签名验证，确认应急广播消息的真实性、合法性和完整性，应急广播消息的数字签名机制如图2所示。

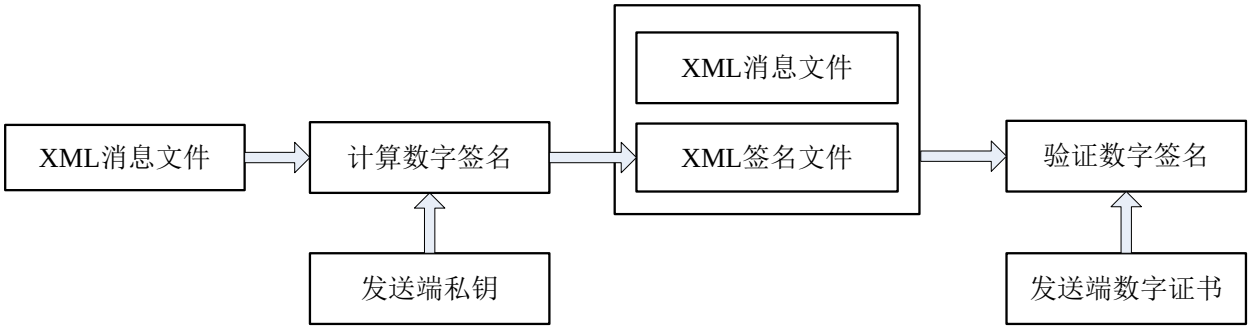

图2　应急广播消息的数字签名机制

应急广播消息签名文件格式见6.4。

5.4　应急广播传输覆盖指令数字签名机制

应急广播传输覆盖指令采用数字签名机制实现安全保护。应急广播传输覆盖指令发送端将应急广播传输覆盖指令、签名时间等打包，用应急广播传输覆盖指令发送端私钥计算数字签名；应急广播传输覆盖指令发送端将计算出的数字签名与应急广播指令、签名时间和应急广播传输覆盖指令发送端数字证书编号打包传输；应急广播传输覆盖指令接收端接收到应急广播传输覆盖指令后，采用应急广播传输覆盖指令发送端数字证书进行签名验证，如果验证成功则接收端进行处理，接收端不应该执行和处理验证失败的指令。

应急广播传输覆盖指令数字签名机制如图3所示。

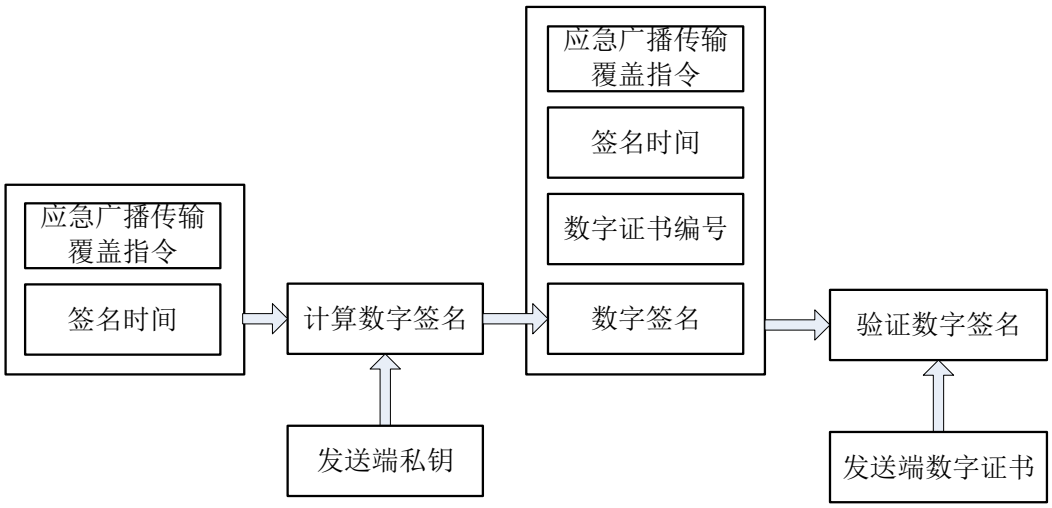

图3　应急广播传输覆盖指令数字签名机制

5.5　应急广播的证书授权机制

应急广播证书授权的步骤如下：

a）注册：将应急广播各级设备信息注册到应急广播数字证书安全代理；

b）数字证书授权列表生成及签名：证书安全代理根据应急广播平台各级设备的部署方式为各级系统和终端生成其对应的证书授权列表，并向应急广播证书管理系统申请对证书授权列表签名；

c）数字证书下发：证书安全代理根据授权列表从应急广播数字证书管理系统获取相应数字证书，将签名的证书授权列表和数字证书发送到应急广播平台，由应急广播平台将证书授权列表数字证书下发到下级平台和终端。

6　应急广播数字签名协议

6.1　应急广播数字证书格式

应急广播数字证书包括：数字证书格式版本号、数字证书签发编号、数字证书编号、数字证书有效期、公钥信息、数字签名信息等，应急广播数字证书格式见表1。

表1　应急广播数字证书格式

字段	比特数	类型	备注
CertificateVersion	8	uimsbf	应急广播数字证书版本号
IssuerSN	48	uimsbf	应急广播数字证书签发者编号
CertificateSN	48	uimsbf	应急广播数字证书编号
CertificateValidate	16	uimsbf	应急广播数字证书有效期
PublicKey	512	uimsbf	应急广播数字证书公钥数据
SignatureData	512	uimsbf	应急广播数字证书签名数据

CertificateVersion：应急广播数字证书版本号，指的是当前应急广播数字证书版本，用8个比特表示，其中高4位为大版本编号，低4位为小版本编号，应用本标准版本取值为0x00。

IssuerSN：应急广播数字证书签发者编号，指的是签发当前数字证书的数字证书编号，用48比特表示。

CertificateSN：应急广播数字证书编号，指的是当前数字证书编号，用48比特表示，编号0x00 00 00 00 00 00～0x00 00 00 00 00 FF的数字证书编号保留为应急广播数字证书管理系统使用，其余编号使用不受限制。

CertificateValidate：应急广播数字证书有效期，用16比特表示，其中高8比特表示年份，是年份减去2000的二进制数，低8比特表示月份，是月份的二进制表示，如2018年8月表示为0x12 08。

PublicKey：应急广播数字证书公钥数据，指当前应急广播数字证书的公钥，本标准中采用SM2算法，公钥长度512比特。

SignatureData：应急及广播数字证书签名数据，指数字证书签发者用其自身私有计算的该数字证书格式版本号、数字证书签发编号、数字证书编号、数字证书有效期、公钥信息等的数字签名，长度为512比特，签名算法默认为SM2/SM3算法。

6.2 应急广播传输覆盖指令封装协议

6.2.1 调频与中波方式

本节规定应急广播指令数字签名数据封装协议。应急广播指令的数字签名数据附加在应急广播指令尾部，数字签名数据包括：签名时间、数字证书编号、数字签名三个部分；编码规定见表2。

表2 数字签名数据编码规定

字段	比特数	类型	备注
signature_data{			
SigTime	32	uimsbf	签名时间
CertificateSN	48	uimsbf	发送端数字证书编号
Signature	512	uimsbf	数字签名数据
}			

SigTime：签名时间，指签名应急广播指令时的当前时间，用32比特UTC时间表示。

CertificateSN：发送端数字证书编号，指的是当前指令签名对应的数字证书的编号，用48比特表示。

Signature：数字签名数据，指的是当前指令的数字签名，用512比特表示。

6.2.2 数字电视方式

在数字电视传输方式中，在应急广播表（包含应急广播索引表和应急广播内容表）数据后面增加数字签名，实现应急广播表数据的安全保护，数字签名由数字签名长度、数字签名数据两个字段构成，数字签名长度用于指示应急广播表中数字签名数据的长度；数字签名数据包含应急广播表的数字签名信息，用于保障当前表数据的真实性、合法性和完整性。接收端接收到应急广播表后应验证其中数字签名的有效性，如果签名验证不通过，应放弃对当前表分段的处理。应急广播表中增加的数字签名语法见表3。

表3　应急广播表数字签名语法

语法	位数	标识符

signature_length
for (l=0;l<q;l++){
signature_data()
}
	16	uimsbf

signature_length：数字签名长度，16位字段，用于指示应急广播消息表数字签名数据的字节长度。

signature_data()：数字签名数据，数字签名数据包含应急广播消息表的数字签名信息。数字签名数据的语法格式见表2。

6.3　应急广播信息签名文件格式

应急广播信息签名文件中包括：版本号、关联应急广播信息主体文件索引信息、签名证书序列号、签名算法和签名值，以XML语法进行描述，语法结构见表4。

表4　应急广播信息签名文件语法结构

名称	层次关系	属性	可选/必选	定义
Signature	Signature	复合类型	必选	应急广播信息签名数据结构体
Version	Signature.Version	整数	必选	协议版本号
RelatedEBInfo	Signature.RelatedEBInfo	复合类型	必选	关联应急广播信息文件索引列表
EBInfoID	Signature.RelatedEBInfo.EBInfoID	字符串	必选	关联应急广播信息主体文件索引信息
CertSN	Signature.CertSN	字符串	必选	证书序列号
SignatureAlgorithm	Signature.SignatureAlgorithm	字符串	必选	签名算法
SignatureValue	Signature. SignatureValue	字符串	必选	签名值

Signature.Version： 应急广播信息签名文件格式版本号，整数类型应用本标准版本时为1。

Signature.RelatedEBInfo：关联应急广播信息主体文件索引信息，其下级元素为被签名的应急广播信息主体文件索引信息。

Signature.RelatedEBInfo.EBInfoID：关联应急广播信息主体文件ID，字符串类型。

Signature.CertSN：证书序列号，为签名应急广播信息所用的证书的序列号，证书序列号为表1中证书序列号的十六进制字符串表示。

Signature.SignatureAlgorithm：签名算法固定为字符串“SM2-SM3”。

Signature. SignatureValue：签名值为签名数据的Base64编码，签名数据的语法格式见表2。

应急广播信息签名文件Schema见资料性附录C，实例见资料性附录D。

6.4　应急广播消息签名文件格式

应急广播消息签名文件中包括版本号、关联应急广播业务数据包索引信息、签名证书序列号、签名算法和签名值，以XML语法进行描述，语法结构见表5。

表5　应急广播消息签名文件语法结构

名称	层次关系	属性	可选/必选	定义
Signature	Signature	复合类型	必选	应急广播消息签名数据结构体
Version	Signature.Version	整数	必选	协议版本号
RelatedEBD	Signature.RelatedEBD	复合类型	必选	关联应急广播业务数据
EBDID	Signature.RelatedEBD.EBDID	字符串	必选	关联业务数据包 ID
CertSN	Signature.CertSN	字符串	必选	证书序列号
SignatureAlgorithm	Signature.SignatureAlgorithm	字符串	必选	签名算法
SignatureValue	Signature.SignatureValue	字符串	必选	签名值

Signature.Version： 应急广播消息签名文件格式版本号，整数类型，应用本标准版本取值为1。

Signature.RelatedEBD：关联应急广播业务数据索引信息，其下级元素为被签名的应急广播业务数据包ID。

Signature.RelatedEBD.EBDID：关联应急广播业务数据包ID，字符串类型。

Signature.CertSN：证书序列号，为签名应急广播消息所用的证书的序列号，证书序列号为表1中证书序列号的十六进制字符串表示。

Signature.SignatureAlgorithm：签名算法固定为字符串“SM2-SM3”。

Signature. SignatureValue：签名值为签名数据的Base64编码，签名数据的语法格式见表2。

应急广播消息签名文件Schema见规范性附录A，实例见资料性附录B。

6.5　应急广播证书授权协议

该协议主要用于应急广播系统中更新应急广播发送端的数字证书到应急广播各级接收系统,应急广播数字证书授权列表包括：接收端编号、证书授权序列号、证书数量、证书编号列表、数字签名，证书授权列表格式如表6所示。

表6　应急广播数字证书授权列表

字段	比特数	类型	备注
ReceiverSN	48	uimsbf	接收端编号
CertsAuthSN	8	uimsbf	证书授权序列号
CertsCount	8	uimsbf	证书数量
CertSNs	N*48	uimsbf	证书编号列表
SigSN	48	uimsbf	签名证书编号
Signature	512	uimsbf	数字签名

ReceiverSN：接收端编号，48比特，指的是接收证书授权列表的设备的证书编号。

CertsAuthSN：证书授权序列号，8比特，按顺序递增。

CertsCount:证书数量，8比特，指的是该证书授权列表中包含的证书的数量。

CertSNs:证书编号列表，N*48比特，指的是证书授权列表中所有的证书序列号，这里的N指的是证书数量。

SigSN：签名证书编号，48比特，指的是签名该证书授权列表所使用的证书的编号。

Signature：数字签名数据，512比特，指的是对数字签名数据之前的所有字段所计算的数字签名，该数字签名采用SM2数字签名算法。

附 录 A
（规范性附录）
应急广播消息签名文件 Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="Signature">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Version" type="xs:string"/>
    <xs:element name="RelatedEBD">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="EBDID" type="xs:string"/>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
    <xs:element name="CertSN" type="xs:string"/>
    <xs:element name="SignatureAlgorithm" type="xs:string"/>
    <xs:element name="SignatureValue" type="xs:string"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

附 录 B
（资料性附录）
应急广播消息签名文件实例

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<Signature>
    <Version>1</Version>
    <RelatedEBD>
        <EBDID>10010232000000000001000000000000943</EBDID>
    </RelatedEBD>
    <CertSN>0001230000000001</CertSN>
    <SignatureAlgorithm>SM2-SM3</SignatureAlgorithm>
    <SignatureValue>AAAJ3QAAAAAAQn1utM+foGrysMo74xiKrnzpdmNg4OXGLPIHOYCgIowBStaYPpGpWgIMoZfpN/E6RJk
GHFLwkenYM/K3gMFipJQ=</SignatureValue>
</Signature>
```

附 录 C
（规范性附录）
应急广播信息签名文件 Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="Signature">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Version" type="xs:string"/>
    <xs:element name="RelatedEBInfo">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="EBInfoID" type="xs:string"/>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
    <xs:element name="CertSN" type="xs:string"/>
    <xs:element name="SignatureAlgorithm" type="xs:string"/>
    <xs:element name="SignatureValue" type="xs:string"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

附 录 D
（资料性附录）
应急广播信息签名文件实例

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<Signature>
    <Version>1</Version>
    <RelatedEBInfo>
        <EBInfoID>11A0120150415001</EBInfoID>
        <EBInfoID>11A0120150415002</EBInfoID>
        <EBInfoID>11B0220150415001</EBInfoID>
    </RelatedEBInfo>
    <CertSN>0001230000000001</CertSN>
    <SignatureAlgorithm>SM2-SM3</SignatureAlgorithm>
    <SignatureValue>AAAJ3QAAAAAAQn1utM+foGrysMo74xiKrnzpdmNg4OXGLPIHOYCgIowBStaYPpGpWgIM
oZfpN/E6RJkGHFLwkenYM/K3gMFipJQ=</SignatureValue>
</Signature>
```