GY

中华人民共和国广播电视和网络视听行业标准

GY/T 389—2023

应急广播系统数字签名技术规范

Technical specification for digital signature of emergency broadcasting system

2023-11-30 发布　　2023-11-30 实施

国家广播电视总局　　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。

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。

本文件由全国广播电影电视标准化技术委员会（SAC/TC 239）归口。

本文件起草单位：国家广播电视总局广播电视科学研究院、江西省广播电视局、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。

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

应急广播系统数字签名技术规范

1 范围

本文件规定了应急广播业务数据和应急广播传输覆盖主体指令的数字签名安全保护机制。

本文件适用于应急广播从应急信息接入、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 32905—2016 信息安全技术 SM3密码杂凑算法

GB/T 32918.2—2016 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

GY/T 383—2023 应急广播系统总体技术规范

3 术语和定义

GY/T 383—2023界定的以及下列术语和定义适用于本文件。

3.1

应急信息 emergency information

县级以上人民政府或其指定的部门因突发事件/紧急情况而发布的信息。

注：应急信息按照紧急程度、发展态势、危害程度等，分为紧急类和非紧急类。

[来源：GY/T 383—2023，3.1]

3.2

应急广播 emergency broadcasting

利用广播电视、网络视听等信息传送方式，向公众或特定区域、特定人群播发应急信息的传送播出系统。

[来源：GY/T 383—2023，3.2]

3.3

应急广播消息 emergency broadcasting message；EBM

各级应急广播平台之间，以及应急广播平台到广播电视播出系统、应急广播传输覆盖网之间传递的，根据应急信息生成的应急广播播发相关数据。

注：包括应急广播消息指令文件、应急广播消息指令签名文件、应急广播节目资源文件等。

[来源：GY/T 383—2023，3.3]

3.4

应急广播适配器 emergency broadcasting adapter

接收、解析、验证应急广播消息，并向广播电视和网络视听系统进行协议转换、签名、封装和存储的设备。

[来源：GY/T 383—2023，3.5]

3.5

SM2 算法　SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为 256bit。

[来源：GM/Z 0001—2013，2.118]

3.6

SM3 算法　SM3 algorithm

一种密码杂凑算法，其输出为 256bit。

[来源：GM/Z 0001—2013，2.119]

3.7

数字签名　digital signature

附加在数据单元上的一些数据，或是对数据单元做密码变换，这种附加数据或密码变换被数据单元的接收者用以确认数据单元的来源和完整性，达到保护数据、防止被非法伪造的目的。

[来源：GY/T 383—2023，3.6]

3.8

应急广播接收终端　emergency broadcasting receiving terminal

能够接收应急广播消息的接收设备，包括收音机类、电视机类、机顶盒类、视听载体类、移动接收类、大喇叭类、显示屏类等。

[来源：GY/T 383—2023，3.7]

3.9

应急广播数字证书　emergency broadcasting certificate

面向应急广播系统中的应急广播平台、应急广播适配器、应急广播接收终端发放的具有特定格式的非对称公钥文件。

3.10

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

对各级应急广播平台、应急广播适配器和应急广播接收终端数字证书生成、发放和撤销等进行管理的系统。

3.11

应急广播数字证书授权列表　emergency broadcasting certificates authorization list

由应急广播数字证书管理系统签发的数字证书编号列表，包括：接收端数字证书编号、数字证书授权列表序列号、数字证书数量、数字证书编号列表、签名证书编号、数字签名值，用于规定各级应急广播系统发送端和接收端的信任关系。

3.12

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

为应急广播系统中的密码设备和密码模块生成应急广播证书授权列表申请文件，并向应急广播系统转发应急广播数字证书管理系统签发的应急广播数字证书授权列表。

3.13

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

在各类传输覆盖网络中实际传输的指令，由应急广播传输覆盖主体指令和签名信息组成。

注：签名信息包括签名时间、数字证书编号和数字签名值。

3.14

应急广播传输覆盖主体指令　emergency broadcasting transmission coverage subject command

面向不同类型的传输覆盖网络，将应急广播消息进行适配处理后生成的原始指令。

3.15

应急广播业务数据　emergency broadcasting data；EBD

应急广播运行管理过程产生的相关数据，主要包括应急广播消息、应急广播消息播发状态查询、应急广播消息播发状态反馈、运维数据请求、应急广播平台信息、台站（前端）信息、应急广播适配器信息、传输覆盖播出设备信息、平台设备及终端信息、播发记录、应急广播平台状态、应急广播适配器状态、传输覆盖播出设备状态、平台设备及终端状态、行政区域信息、应急广播数字证书授权列表文件、心跳检测、处理结果通知、接收回执等。

[来源：GY/T 384—2023，3.8]

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）

UTC　协调世界时（Universal Time Coordinated）

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

5　通则

应急广播系统采用数字签名技术对传输的应急广播业务数据和应急广播传输覆盖主体指令进行安全保护。应急广播数字签名框架见图1。

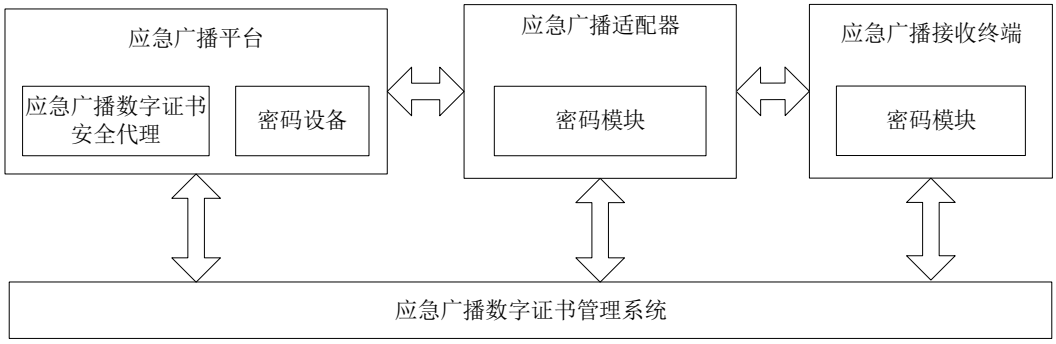

图1　应急广播数字签名框架

应急广播数字签名框架由应急广播数字证书管理系统、应急广播数字证书安全代理、密码设备、密码模块组成。密码设备和密码模块中的应急广播数字证书由应急广播数字证书管理系统统一签发和维护，数字证书管理机制应符合6.1的规定，数字证书格式应符合7.1的规定。

应急广播平台、应急广播适配器和应急广播接收终端之间传输应急广播业务数据和应急广播传输覆盖主体指令时，发送端使用自身私钥对发送的应急广播业务数据和应急广播传输覆盖主体指令进行签名，将签名信息与应急广播业务数据和应急广播传输覆盖主体指令一同发送。接收端使用发送端数字证书对接收到的应急广播业务数据和应急广播传输覆盖主体指令进行数字签名验证。数字签名的密码算法采用GB/T 32918.2—2016、GB/T 32905—2016规定的SM2算法、SM3算法。应急广播业务数据的数字签名机制应符合6.4的规定，数字签名格式应符合7.3的规定。应急广播传输覆盖主体指令的数字签名机制应符合6.5的规定，数字签名格式应符合7.4的规定。

应急广播系统中的接收端应存储多个可信任的发送端的数字证书，数字证书间的信任关系由应急广播数字证书管理系统统一管理和授权，并生成统一格式的信任关系列表，通过应急广播数字证书安全代理发送到各接收端。数字证书授权机制应符合6.6的规定，数字证书授权文件格式应符合7.5的规定。

6 应急广播数字签名保护机制

6.1 应急广播数字证书签发机制

应急广播数字证书管理系统负责应急广播数字证书签发，应急广播数字证书管理系统中内置应急广播数字证书管理系统证书。签发机制说明如下：

a) 应急广播系统建设方在建设应急广播系统时，应向应急广播数字证书管理系统提交密码设备和密码模块私钥及数字证书申请；

b) 应急广播数字证书管理系统按照应急广播系统建设方的要求，生成对应应急广播平台、应急广播适配器和应急广播接收终端中密码设备和密码模块的公私钥对，并签发数字证书；

c) 应急广播数字证书管理系统采用数字信封的方式，将加密后的私钥和数字证书交付给应急广播系统建设方；

d) 应急广播系统建设方将收到的私钥和数字证书解密后，安全导入到对应的密码设备和密码模块中。

注：数字信封是一种数据结构，包含用对称密钥加密的密文和公钥加密的该对称密钥。

6.2 应急广播数字签名计算与验证机制

应急广播系统发送应急广播业务数据和应急广播传输覆盖主体指令时需要对数据和指令进行数字签名。应急广播系统将待签名数据（应急广播业务数据或应急广播传输覆盖主体指令）传入密码设备或密码模块，密码设备或密码模块将待签名数据和签名时间作为参与数字签名计算的数据进行数字签名计算，然后将签名时间、数字证书编号和数字签名值返回到应急广播系统。

应急广播数字签名流程见图 2。

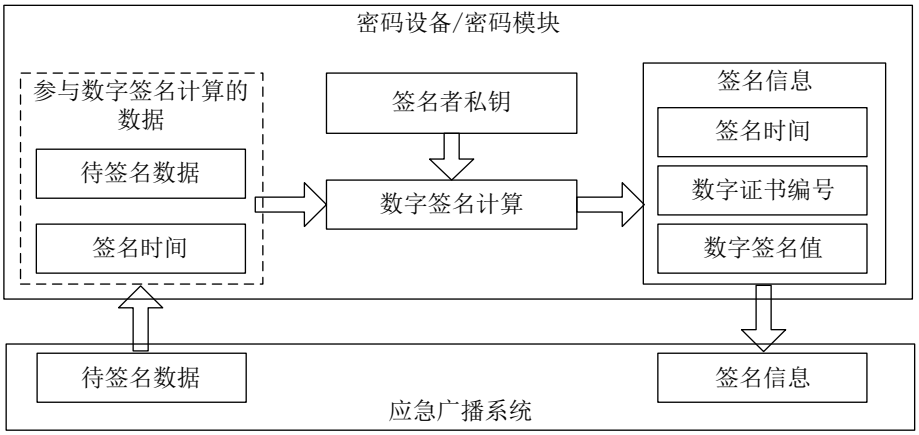

图2 应急广播数字签名流程

应急广播系统收到应急广播业务数据和应急广播传输覆盖指令时需要进行数字签名验证。应急广播系统将待验证数据传入密码设备或密码模块，密码设备或密码模块使用数字证书进行数字签名验证，将验证结果返回到应急广播系统。

应急广播数字签名验证流程见图 3。

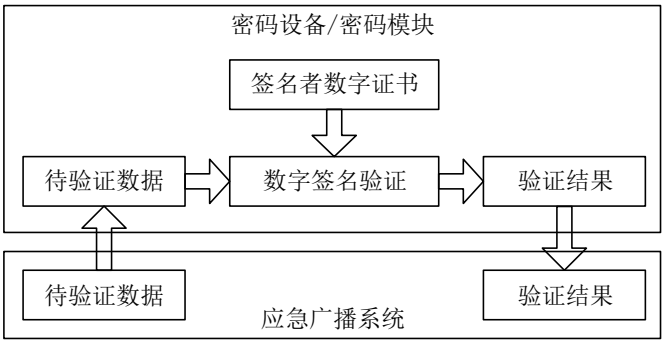

图3　应急广播数字签名验证流程

6.3　应急广播消息指令文件的数字签名机制

应急广播消息指令文件采用数字签名方式实现安全保护。应急广播消息文件由应急广播消息指令文件、应急广播消息指令签名文件和应急广播节目资源文件组成。发送端采用私钥对应急广播消息指令文件进行数字签名，生成应急广播消息指令签名文件。接收端使用应急广播消息文件发送端的数字证书对应急广播消息指令签名文件进行数字签名验证。

应急广播消息指令文件的数字签名流程见图4。

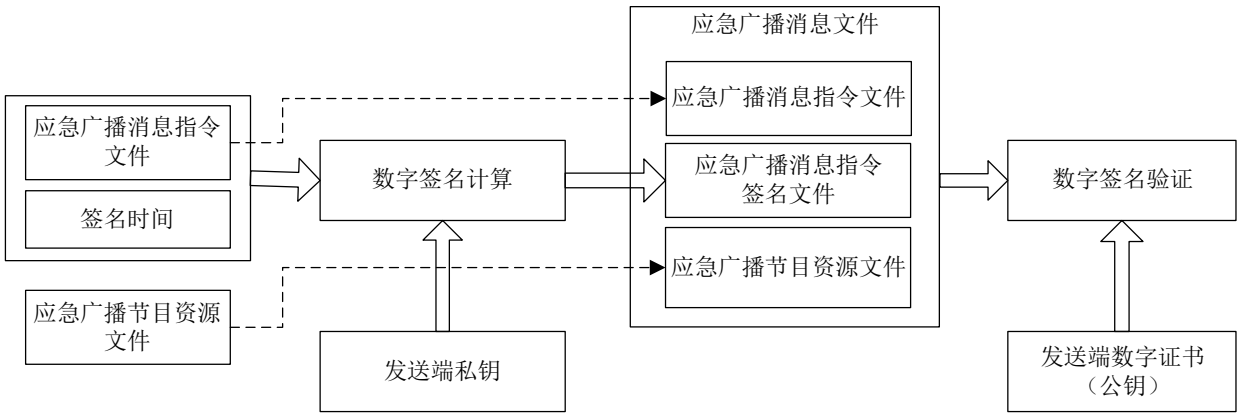

图4　应急广播消息指令文件的数字签名流程

6.4　应急广播业务数据文件的数字签名机制

应急广播业务数据文件采用数字签名方式实现安全保护。应急广播业务数据文件采用文件发送端的私钥进行数字签名，签名信息存储在应急广播业务数据签名文件中，接收端通过使用文件发送端的数字证书对应急广播业务数据文件进行数字签名验证。

应急广播业务数据文件的数字签名流程见图5。

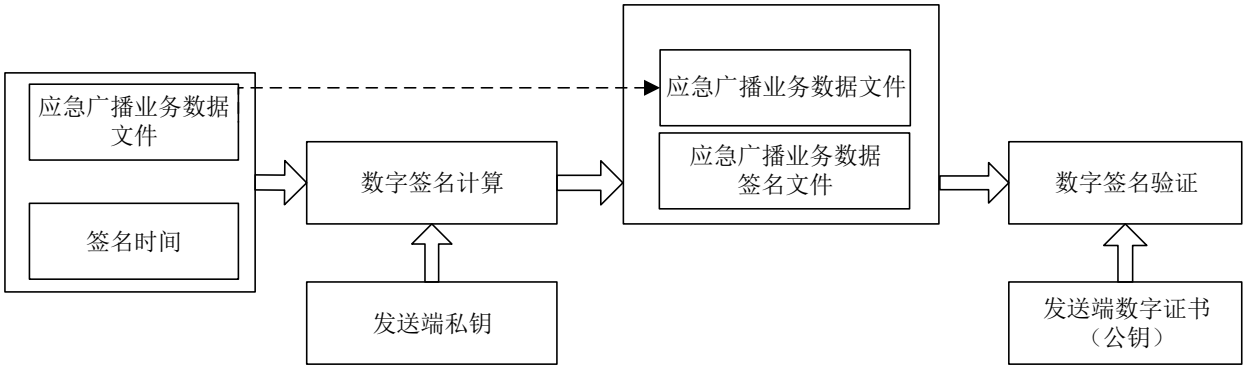

图5　应急广播业务数据文件的数字签名流程

6.5　应急广播传输覆盖主体指令数字签名机制

应急广播传输覆盖主体指令采用数字签名机制实现安全保护。发送端将应急广播传输覆盖主体指令、签名时间等进行封装，使用发送端私钥进行数字签名计算；发送端将应急广播传输覆盖主体指令和签名信息封装后传输；接收端使用发送端数字证书对接收到的应急广播传输覆盖指令进行数字签名验证。

应急广播传输覆盖主体指令数字签名流程见图6。

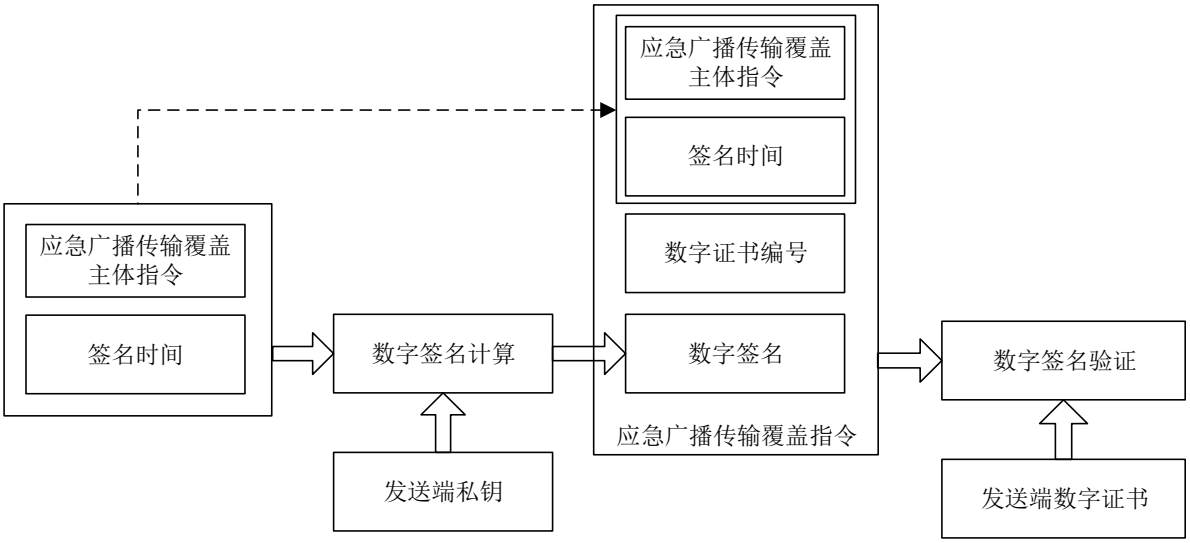

图6　应急广播传输覆盖主体指令数字签名流程

6.6　应急广播数字证书授权机制

应急广播系统采用数字证书授权列表建立各级应急广播系统设备间的数字证书的信任机制。授权机制说明如下：

a）　应急广播平台、应急广播适配器和应急广播接收终端完成部署后，记录其部署的数字证书编号；

b）　根据应急广播业务需求，申请方生成拟需要写入各个应急广播平台、应急广播适配器和应急广播接收终端内部的数字证书授权列表申请文件；

c）　申请方将生成的数字证书授权列表申请文件提交至应急广播数字证书管理系统；

d）　应急广播数字证书管理系统将数字证书授权列表申请文件存档，并生成数字证书授权列表；

e）　应急广播系统将数字证书授权列表与列表中对应的数字证书封装成响应文件反馈至申请方，数字证书授权列表格式、响应文件格式应符合 7.5 中的规定；

f) 申请方将响应文件分发到应急广播系统中的密码设备和密码模块中；

g) 密码设备和密码模块使用应急广播数字证书管理系统证书对响应文件中的数字证书授权列表进行数字签名验证，验证通过后再对响应文件中的数字证书进行验证，验证通过后将数字证书写入内部安全存储区保存。

密码设备和密码模块应保存应急广播数字证书管理系统证书、应急广播数字证书授权列表和授权证书。

7 应急广播数字签名格式

7.1 应急广播数字证书格式

应急广播数字证书包括：应急广播数字证书版本号、应急广播数字证书签发者编号、应急广播数字证书编号、应急广播数字证书有效期、应急广播数字证书公钥数据、应急广播数字证书数字签名值等，应急广播数字证书格式应符合表1的规定。

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
SignatureResult	512	uimsbf	应急广播数字证书数字签名值

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8bit表示，其中高4位为大版本编号，低4位为小版本编号，应用本文件版本取值为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48bit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48bit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16bit表示，其中高8位表示年份，是年份减去2000的二进制数，低8位表示月份，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信息,指当前应急广播数字证书的公钥,本文件中采用SM2算法，公钥长度512bit。

SignatureResult：应急广播数字证书数字签名值，指数字证书签发者使用其自身私钥对应急广播数字证书版本号、应急广播数字证书签发者编号、应急广播数字证书编号、应急广播数字证书有效期、应急广播数字证书公钥数据进行数字签名计算得到的结果。长度为512bit,签名算法默认为SM2算法/SM3算法。

7.2 应急广播数字签名信息语法格式

应急广播系统对待签名数据和签名时间进行数字签名计算，生成签名信息，数字签名信息语法格式应符合表2的规定。

表2　数字签名信息语法格式

字段	比特数	类型	备注
Data	N	uimsbf	待签名数据
SignatureValue{	—	—	签名信息
SignTime	32	uimsbf	签名时间
CertificateSN	48	uimsbf	数字证书编号
SignatureResult	512	uimsbf	数字签名值
}	—	—	—

Data：待签名数据，是指需要进行数字签名保护的数据。

SignatureValue：签名信息，包括签名时间、签名者数字证书编号、数字签名值。

SignTime：签名时间，是指签名时的时间，用32bit UTC时间表示。

CertificateSN：数字证书编号，指的是对签名对应的数字证书的编号，用48bit表示。

SignatureResult：数字签名值，用512bit表示。

7.3　应急广播消息指令文件和应急广播业务数据文件数字签名格式

应急广播消息指令签名文件和应急广播业务数据签名文件语法格式应符合表3的规定。

表3　签名文件语法格式

名称	层次关系	属性	可选/必备	定义
Signature	Signature	复合类型	必备	签名文件结构体
Version	Signature.Version	整数	必备	协议版本号
RelatedEBD	Signature.RelatedEBD	复合类型	必备	关联的应急广播消息指令和应急广播业务数据
EBDID	Signature.RelatedEBD.EBDID	字符串	必备	关联的应急广播消息指令文件和应急广播业务数据文件编号
CertSN	Signature.CertSN	字符串	必备	数字证书编号
SignatureAlgorithm	Signature.SignatureAlgorithm	字符串	必备	数字签名算法
SignatureValue	Signature.SignatureValue	字符串	必备	签名信息

Signature.Version：协议版本号，整数类型，应用本文件版本取值为1。

Signature.RelatedEBD：关联的应急广播消息指令和应急广播业务数据。

Signature.RelatedEBD.EBDID：关联的应急广播消息指令文件和应急广播业务数据文件编号，字符串类型。

Signature.CertSN：数字证书编号，为签名应急广播业务数据所用的数字证书编号，证书编号为表1中应急广播数字证书编号的十六进制字符串表示。

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

Signature.SignatureValue：签名信息，Base64编码，签名信息的语法格式应符合表4的规定。

应急广播消息指令签名文件和应急广播业务数据签名文件Schema应符合附录A的规定，示例见附录B。

7.4　应急广播传输覆盖主体指令数字签名格式

7.4.1 调频与中波方式

在调频与中波传输方式中,应急广播传输覆盖主体指令的签名信息附加在应急广播传输覆盖主体指令尾部，数字签名信息语法格式应符合表4的规定。

表4 调频与中波方式数字签名信息语法格式

字段	比特数	类型	备注
Data	N	uimsbf	调频与中波应急广播传输覆盖主体指令数据
SignatureValue{	—	—	签名信息
SignTime	32	uimsbf	签名时间
CertificateSN	48	uimsbf	发送端数字证书编号
SignatureResult	512	uimsbf	数字签名值
}	—	—	—

Data：调频与中波应急广播覆盖主体指令数据。

SignTime：签名时间，指签名应急广播传输覆盖主体指令时的当前时间，用32bit UTC时间表示。

CertificateSN：发送端数字证书编号，指的是对当前应急广播传输覆盖主体指令进行签名对应的数字证书的编号，用48bit表示。

SignatureResult：数字签名值，用512bit表示。

7.4.2 有线和地面数字电视方式

在有线和地面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、签名信息两个字段构成，数字签名信息语法格式应符合表5的规定。

表5 有线和地面数字电视方式数字签名信息语法格式

字段	比特数	类型	备注
Data	N	uimsbf	有线和地面数字电视应急广播传输覆盖主体指令数据
SignatureLength	16	uimsbf	数字签名长度
SignatureValue{	—	—	签名信息
SignTime	32	uimsbf	签名时间
CertificateSN	48	uimsbf	发送端数字证书编号
SignatureResult	512	uimsbf	数字签名值
}	—	—	—

Data：有线和地面数字电视应急广播传输覆盖主体指令数据。

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

SignTime：签名时间，是指签名时的时间，用32bit UTC时间表示。

CertificateSN：发送端数字证书编号，指的是对签名对应的数字证书的编号，用48bit表示。

SignatureResult：数字签名值，用512bit表示。

7.5 应急广播数字证书授权文件格式

7.5.1 应急广播数字证书授权列表申请文件格式

应急广播数字证书授权列表申请文件为TXT文件，文本格式见图7。

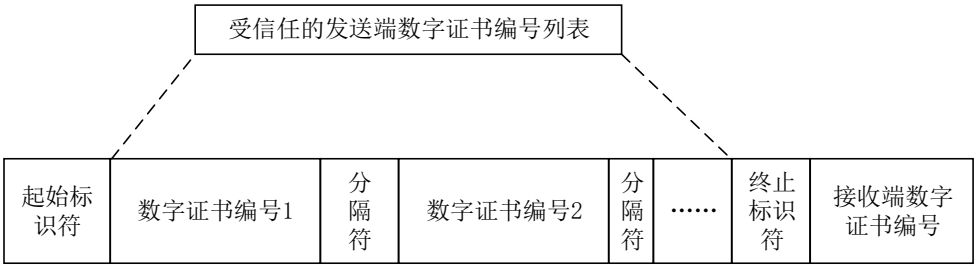

图7 应急广播数字证书申请列表文件格式

起始标识符：“path=”。

受信任的发送端数字证书编号列表：列表由一个或多个受信任的发送端数字证书编号组成，编号之间采用分隔符分隔。

分隔符：数字证书编号间的分隔符为“.”。

终止标识符：终止标识符统一为“&opt=reg&SMSN=”。

接收端数字证书编号：应急广播数字证书管理系统为接收端分配的数字证书编号。

应急广播数字证书授权列表申请文件示例见附录C。

7.5.2 应急广播数字证书授权列表响应文件格式

应急广播数字证书授权列表响应文件采用TXT文件，格式应符合表6的规定，示例见附录C。

表6 应急广播数字证书授权列表响应文件格式

字段	类型	备注	分隔符
Status	字符	响应状态	/n
CertificateSN	字符	签发者数字证书编号	,
SIGN_LIST	Base64 编码	数字签名值	,
LIST	Base64 编码	数字证书授权列表	,
SIGN_CERT	Base64 编码	签发者数字证书	,
XML	字符	数字证书数据	—

Status：响应状态成功为RET_OK，执行状态失败为RET_NOK。

CertificateSN：签发者数字证书编号。

SIGN_LIST：响应文件中LIST内容的数字签名值。

LIST：数字证书授权列表的Base64编码形式。

SIGN_CERT：签发者数字证书。

XML：以XML文件格式表示的证书授权列表中指定的信任证书数据，文件格式应符合表7的规定。

表7 XML 文件格式

名称	层次关系	属性	可选/必备	定义
DLBResponseData	DLBResponseData	复合类型	—	响应数据结构体
ResponseSignTime	DLBResponseData.ResponseSignTime	时间格式	必备	响应文件生成时间
ResponseCertPath	DLBResponseData.ResponseCertPath	字符串	必备	数字证书编号列表
Cert	DLBResponseData.cert	复合类型	必备	数字证书信息
CertSN	DLBResponseData.cert.CertSN	字符串	必备	数字证书编号
CertUsage	DLBResponseData.cert.CertUsage	字符串	必备	数字证书可用状态
CertCtx	DLBResponseData.cert.CertCtx	字符串	必备	数字证书
CertState	DLBResponseData.cert.CertState	字符串	必备	数字证书状态
SignDate	DLBResponseData.cert.SignDate	时间格式	必备	数字证书生成时间，格式为YYYY-MM-DD HH:MI:SS.m
ValidDate	DLBResponseData.cert.ValidDate	时间格式	必备	数字证书有效期，格式为YYYY-MM-DD HH:MI:SS.m

DLBResponseData：响应数据结构体。

ResponseSignTime：响应文件生成时间，时间格式为YYYY-MM-DD HH:MI:SS。

ResponseCertPath：数字证书编号列表，中间用“,”分隔。

Cert：数字证书信息，包括数字证书编号、可用状态、证书内容等。

CertSN：数字证书编号。

CertUsage：数字证书可用状态，0为正常，1为异常。

CertCtx：数字证书。

CertState：数字证书状态，0为正常，1为异常。

SignDate：数字证书生成时间，格式为YYYY-MM-DD HH:MI:SS.m。

ValidDate：数字证书有效期，格式为YYYY-MM-DD HH:MI:SS.m。

7.5.3 应急广播数字证书授权列表格式

应急广播数字证书授权列表包括:接收端数字证书编号、数字证书授权列表序列号、数字证书数量、数字证书编号列表、签名证书编号、数字签名值，应急广播数字证书授权列表格式应符合表8的规定。

表8 应急广播数字证书授权列表格式

字段	比特数	类型	备注
ReceiverSN	48	uimsbf	接收端数字证书编号
CertsAuthSN	8	uimsbf	数字证书授权列表序列号
CertsCount	8	uimsbf	数字证书数量
CertSNs	N×48	uimsbf	数字证书编号列表
SignSN	48	uimsbf	签名证书编号
SignatureResult	512	uimsbf	数字签名值

ReceiverSN：接收端数字证书编号，48bit，指的是接收证书授权列表的设备的数字证书编号。

CertsAuthSN：数字证书授权列表序列号，8bit，按顺序递增。

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

CertSNs：数字证书编号列表，CertsCount ×48bit，指的是证书授权列表中所有的证书序列号。

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

SignatureResult：数字签名值，512bit，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。

附 录 A
（规范性）
应急广播消息指令签名文件和应急广播业务数据签名文件 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）
应急广播消息指令签名文件和应急广播业务数据签名文件示例

下面给出了应急广播消息指令签名文件和应急广播业务数据签名文件示例，包含了协议版本号、关联应急广播业务数据、关联业务数据包 ID、数字证书编号、签名算法、签名值的表示。

示例：

```
<?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>AAAJ3QAAAAAAQnlutM+foGrysMo74xiKrnzpdmNg4OXGLPIHOYCgIowBStaYPpGpWgIMoZfpN/E6RJk
GHFLwkenYM/K3gMFipJQ=</SignatureValue>
</Signature>
```

附 录 C
（资料性）
应急广播数字证书授权列表示例

下面给出了应急广播数字证书授权列表申请文件示例，包括发送端数字证书编号和接收端数字证书编号。

示例：

```
path=000011011360.000011011361.000011011363&opt=reg&SMSN=000011011ABA
path=000011011360.000011011361.000011011363&opt=reg&SMSN=000011011CBC
```

下面给出了应急广播数字证书授权列表响应文件示例，包括响应状态、数字证书授权列表以及证书信息。

示例：

```
RET_OK
SN=000000000001,SIGN_LIST=MEUCIQDjcfx4tOYxk5TQ+Aw2FFzE/MAw/Nd09ryIYPVGKBL2VgIgAhtAxPihts/6vWdqLN+wKbKYHG/vpq58B0T1lWkkGN0=,LIST=AAARARq6AAMAABEBE2AAABEBE2EAABEBE2MAAAAAAAHjcfx4tOYxk5TQ+Aw2FFzE/MAw/Nd09ryIYPVGKBL2VgIbQMT4obbP+rlnaizfsCmymBxv76aufAdE9ZVpJBjd,SIGN_CERT=MEYCIQCF4GvadWXVctnZPG2Vjq4HIRoAiJc+FlmJ8rp2d4QoewIhAJ4Z+FUEZa9+0npr0PxMXjZ7Ni0iUHVCPPdM7hRIlAaG,<?xml version="1.0" encoding="GBK"?><DLBResponseData><ResponseSignTime>2019-08-21 15:22:44</ResponseSignTime><ResponseCertPath>000011011360,000011011361,000011011363</ResponseCertPath><cert SN="000011011360"><CertSN>000011011360</CertSN><CertUsage>0</CertUsage><CertCtx>1000000000000100001101136049 01FCD12111DF00A1DEC876FD6FC384EB137B3ECD3565E4C8AE87478489EE92529F9540C364084EB4B5DBF9707A2AACD9E9D87179CBCE28C1E09CD53BC2C838CE35B05FEAEC98E5F69D53CD6AA182B76A72B1D82E4290D54B6A65804E77C79E68C7C3AC0DB91579ED78E13A3606E20A5844B6079B146C519D0F5AEE97B11D1F5EB8</CertCtx><CertState>0</CertState><SignDate>2019-01-29 17:37:43.0</SignDate><ValidDate>2049-01-31 23:59:59.0</ValidDate></cert><cert SN="000011011361"><CertSN>000011011361</CertSN><CertUsage>0</CertUsage><CertCtx>1000000000000100001101136149 01CB0353FD6EC017359C9D24EE0BB261E2A6B7CFD1DD995F5B8BC0FE624991891F2EF872AB6163491AF932C1618C74DB08A4F8D7D65C1ECCEE253FEA97A494A1E67370FF53082CD99526916665C8622E3D96FEE4FB786815E18F6AEF6178B7688A41DBAA2B0F0C78980D86EEBE67995336D70FE7B762F50CC6D1F7B3B8911AB8FD</CertCtx><CertState>0</CertState><SignDate>2019-01-29 17:37:43.0</SignDate><ValidDate>2049-01-31 23:59:59.0</ValidDate></cert><cert SN="000011011363"><CertSN>000011011363</CertSN><CertUsage>0</CertUsage><CertCtx>1000000000000100001101136349 013481AA415871374D13DA723F135810EB1E5CD6E615A946F7DDA05F2985BC3050BDB14929F2C2653BC26A49BBAF786D73A766E4E7F59A68A01AFCA7B10713960249614F4F617DEA0DABC187EAC201480F3103014E359955D2F7B39A7A3ACF9D114F77B439760E611382478198872FAC23ECEE06A0D15D4286A7EAAD8AFD9B9667</CertCtx><CertState>0</CertState><SignDate>2019-01-29 17:37:43.0</SignDate><ValidDate>2049-01-31 23:59:59.0</ValidDate></cert></DLBResponseData>
```

参 考 文 献

[1] GB/T 25069—2022 信息安全技术 术语
[2] GM/Z 0001—2013 密码术语
[3] GY/T 384—2023 应急广播平台接口规范
[4] GY/T 385—2023 应急广播消息格式规范