GY

中华人民共和国广播电视和网络视听行业标准

GY/T 388—2023

应急广播系统密码应用技术规范

Technical specification for cryptography appllication 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、安徽省广播电视局、北京江南天安科技有限公司、北京交大思源科技有限公司、北京数码视讯科技股份有限公司、杭州图南电子股份有限公司。

本文件主要起草人：宫铭豪、李晓鸣、王晓艳、蒋麟、丁森华、赵云辉、任斌、赵镜平、胡宝胜、梅岩、张卫蓬、马吉伟、汤俊锋、陈龙斌。

应急广播系统密码应用技术规范

1 范围

本文件规定了应急广播系统密码应用的技术要求。

本文件适用于指导、规范应急广播系统密码的应用、运行及测评。

注：本文件中，“密码”指“商用密码”。

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 37092 信息安全技术 密码模块安全要求

GY/T 383—2023 应急广播系统总体技术规范

GY/T 389—2023 应急广播系统数字签名技术规范

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]

3.2

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]

3.3

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。

3.4

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]

3.5

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]

3.6

SM4 算法 SM4 algorithm

一种分组密码算法，分组长度为128bit，密钥长度为128bit。

[来源：GM/Z 0001—2013，2.120]

3.7

数据完整性 data integrity

数据没有遭受以非授权方式所作的改变的性质。

[来源：GB/T 39786—2021，3.2]

3.8

真实性 authenticity

一个实体是其所声称实体的这种特性。

注：真实性适用于用户、进程、系统和信息之类的实体。

[来源：GB/T 39786—2021，3.3]

3.9

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]

3.10

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]

3.11

身份鉴别 identity authentication

确认一个实体所声称身份的过程。

[来源：GB/T 39786—2021，3.8]

3.12

密钥 key

控制密码算法运算的关键信息或参数。

[来源：GB/T 39786—2021，3.6]

3.13

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。

4 通则

要求如下。

a) 应急广播系统应在系统规划阶段制定密码应用方案，并经第三方对方案进行评审。

b) 应急广播系统在系统建设阶段应按照通过评审的密码应用方案进行建设，应在系统投入运行前开展密码应用安全性评估，评估通过后方可正式上线运行，并应在系统运行过程中定期开展密码应用安全性评估。

c) 应急广播系统上线前应进行数字签名标准符合性测试，并出具测试报告。

d) 应急广播系统中所用的动态令牌、智能密码钥匙、虚拟专用网络（VPN）、密码模块、服务器密码机、签名验签服务器等密码产品应具有商用密码产品认证证书。

e) 国家级及省级应急广播系统所使用的动态令牌、智能密码钥匙、VPN、密码模块、服务器密码机、签名验签服务器等密码产品应达到GB/T 37092规定的二级及以上安全要求。市、县级应急广播系统所使用的动态令牌、智能密码钥匙、VPN、密码模块、服务器密码机、签名验签服务器等密码产品应达到GB/T 37092规定的一级及以上安全要求。

5 密码应用技术要求

5.1 应急广播平台密码应用技术要求

5.1.1 身份鉴别

要求如下：

a) 应采用密码技术对登录应急广播平台的用户进行身份鉴别，保证用户身份的真实性，宜采用的密码技术包括动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制；
b) 应采用密码技术实现应急广播平台身份鉴别信息的机密性保护，宜采用的密码技术包括基于对称密码算法或密码杂凑算法的 MAC 机制、基于公钥密码算法的数字签名机制；
c) 身份鉴别过程应使用 SM2 算法/SM3 算法/SM4 算法。

5.1.2 数据保护

应急广播平台需要使用密码技术进行保护的数据为应急广播业务数据、应急广播传输覆盖指令、应急广播数字证书授权列表、应急广播关键日志数据，其中关键日志数据包括应急广播平台用户登录行为数据、应急广播业务数据的播发行为数据。

要求如下。

a) 应采用数字签名技术实现对所传输和保存的应急广播业务数据、应急广播传输覆盖指令和应急广播数字证书授权列表的数据完整性、真实性和不可否认性保护，数字签名运算应在密码产品内部进行。数字签名机制应符合 GY/T 389—2023 的规定。
b) 应采用密码技术实现对应急广播平台所存储的关键日志数据的数据完整性保护。宜采用的密码技术包括基于对称密码算法或密码杂凑算法的 MAC 机制、基于公钥密码算法的数字签名机制。
c) 数据保护过程应使用 SM2 算法/SM3 算法/SM4 算法。

注：不可否认性是指证明一个已经发生的操作行为无法否认的性质。

5.1.3 数据验证

要求如下：

a) 应急广播平台在接收到应急广播业务数据、应急广播传输覆盖指令和应急广播数字证书授权列表后，应先对其进行数字签名验证，确定其合法性后才可以进行后续操作；
b) 应急广播平台应对关键日志数据的数据完整性进行验证，并在日志查询页面显示验证结果。

5.1.4 安全运行

国家级及省级应急广播平台应使用安全运维审计系统对应急广播平台相关设备进行集中运行和管理，安全运维审计系统应使用超文本传输安全协议（HTTPS）协议。

5.2 应急广播适配器密码应用技术要求

应急广播适配器应集成相关密码技术和装备，对传输的数据进行安全保护，要求如下。

a) 应急广播适配器应内置自身的设备私钥、应急广播数字证书授权列表以及应急广播数字证书授权列表对应的应急广播数字证书。
b) 应急广播适配器应具备对接收到的应急广播业务数据、应急广播传输覆盖指令和应急广播数字证书授权列表进行合法性验证的能力。
c) 应急广播适配器应对输出的应急广播业务数据和应急广播传输覆盖指令采用数字签名技术进行保护。数字签名机制应符合 GY/T 389—2023 的要求。

5.3 应急广播接收终端密码应用技术要求

应急广播接收终端应集成相关密码技术和装备，对接收的数据进行安全校验，要求如下：

a) 应急广播接收终端应内置自身的设备私钥、应急广播数字证书授权列表以及应急广播数字证书授权列表对应的应急广播数字证书，多模方式的应急广播接收终端应内置所有通道的应急广播数字证书授权列表以及应急广播数字证书授权列表对应的应急广播数字证书；

b) 应急广播接收终端应具备对接收到的应急广播业务数据、应急广播传输覆盖指令和应急广播数字证书授权列表进行合法性验证的能力。

6 密钥管理要求

6.1 密钥生成

应急广播系统密码应用的密钥生成和签发机制应符合 GY/T 389—2023 中 6.1 的规定。

6.2 密钥存储

应急广播平台、应急广播适配器、应急广播接收终端的密码产品中，用于数字签名计算的私钥以及用于对称密码算法或密码杂凑算法的MAC机制的对称密钥，应禁止明文出现在密码设备和密码模块之外。

6.3 密钥使用

应急广播系统中的每个密钥应只有单一用途。

6.4 密钥撤销

应急广播系统通过更新应急广播数字证书授权列表实现密钥撤销。

参 考 文 献

[1] GB/T 25069—2022 信息安全技术 术语
[2] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
[3] GM/Z 0001—2013 密码术语