ICS 35.040
CCS L 80

GM

# 中华人民共和国密码行业标准

GM/T 0096—2020

# 射频识别防伪系统密码应用指南

**Guide for RFID anti-counterfeiting cipher application**

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　发 布

中华人民共和国密码
行业标准
**射频识别防伪系统密码应用指南**
GM/T 0096—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2021年4月第一版
*
书号:155066·2-35975

# 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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京中电华大电子设计有限责任公司、安徽云盾信息技术有限公司、上海复旦微电子集团股份有限公司、上海华申智能卡应用系统有限公司、复旦大学、兴唐通信科技有限公司、紫光同芯微电子有限公司、华大半导体有限公司、北京华大智宝电子系统有限公司、上海坤锐电子科技有限公司、成都卫士通信息产业股份有限公司、北京三未信安科技发展有限公司、中国电力科学研究院有限公司、中国电子技术标准化研究院。

本文件主要起草人：周建锁、董浩然、沈宁、柳逊、顾震、陈波涛、费渡、孙孝年、王政、王俊宇、王俊峰、吕永其、盛敬刚、李静进、李强、刘晓东、赵兵、陈跃、沈磊。

# 射频识别防伪系统密码应用指南

## 1 范围

本文件规定了射频识别防伪应用的安全类别、系统规划与实施。

本文件适用于射频识别防伪应用中密码安全方案设计、密码产品选用与系统实施。

## 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 28925 信息技术 射频识别 2.45 GHz 空中接口协议

GB/T 29768 信息技术 射频识别 800/900 MHz 空中接口协议

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 37033.1—2018 信息安全技术 射频识别系统密码应用技术要求 第 1 部分：密码安全保护框架及安全级别

GB/T 37033.2—2018 信息安全技术 射频识别系统密码应用技术要求 第 2 部分：电子标签与读写器及其通信密码应用技术要求

GB/T 37033.3—2018 信息安全技术 射频识别系统密码应用技术要求 第 3 部分：密钥管理技术要求

GB/T 37092 信息安全技术 密码模块安全要求

GM/T 0008 安全芯片密码检测准则

GM/T 0014 数字证书认证系统密码协议规范

GM/T 0030 服务器密码机技术规范

GM/T 0039 密码模块安全检测要求

GM/T 0040—2015 射频识别标签模块密码检测准则

GM/Z 4001—2013 密码术语

SB/T 10768—2012 基于射频识别的瓶装酒追溯与防伪标签技术要求

## 3 术语和定义

GB/T 37033.1—2018 和 GM/Z 4001—2013 界定的以及下列术语和定义适用于本文件。

3.1

**安全存取模块 secure access module**

嵌入在电子标签读写器内的密码模块，为读写器提供安全服务。

3.2

**单向鉴别 unidirectional authentication**

由读写器发起对标签的身份鉴别。