ICS 35.040
L 80

中华人民共和国国家标准

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

Information security technology—Technical requirements for cryptographic application for radio frequency identification systems—Part 1:Cryptographic protection framework and security levels

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 37033《信息安全技术　射频识别系统密码应用技术要求》分为3个部分：

——第1部分：密码安全保护框架及安全级别；

——第2部分：电子标签与读写器及其通信密码应用技术要求；

——第3部分：密钥管理技术要求。

本部分为GB/T 37033的第1部分。

本部分按照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。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：上海华申智能卡应用系统有限公司、上海复旦微电子集团股份有限公司、北京中电华大电子设计有限责任公司、北京同方微电子有限公司、复旦大学、兴唐通信科技有限公司、上海华虹集成电路有限责任公司、航天信息股份有限公司、北京华大智宝电子系统有限公司、华大半导体有限公司。

本部分主要起草人：顾震、董浩然、王俊宇、谢文录、王云松、梁少峰、俞军、吴行军、王俊峰、周建锁、徐树民、陈跃、柳逊。

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

1 范围

GB/T 37033的本部分规定了射频识别系统密码安全保护框架、安全级别划分、不同级别密码安全技术要求和密码算法配用要求。

本部分适用于射频识别系统密码安全的设计、实现、测评与应用。

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 25069—2010 信息安全技术 术语

GB/T 29261.3—2012 信息技术 自动识别和数据采集技术 词汇 第3部分:射频识别

GB/T 32905—2016 信息安全技术 SM3密码杂凑算法

GB/T 32907—2016 信息安全技术 SM4分组密码算法

GB/T 32918—2016 信息安全技术 SM2椭圆曲线公钥密码算法

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

3 术语和定义

GB/T 25069—2010、GB/T 29261.3—2012中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

嵌入在读写器内的密码安全模块,为读写器提供安全服务。

3.2

对称密码算法 symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

3.3

非对称密码算法 asymmetric cryptographic algorithm

公钥密码算法 public key cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥(公钥)可以公开,另一个密钥(私钥)必须保密,且由公钥求解私钥是计算不可行的。

3.4

会话密钥 session key

在一次会话中使用的数据加密密钥。