ICS 35.040
L 80

中华人民共和国国家标准

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

Information security technology—Technical requirements for cryptographic application for radio frequency identification systems—Part 2:Technical requirements for cryptographic application for RF tag,reader and communication

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2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、上海华申智能卡应用系统有限公司、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：董浩然、俞军、周建锁、吴行军、顾震、柳逊、王俊宇、王俊峰、陈跃、谢文录、王云松、刘丽娜、姚爽、梁少峰、徐树民、沈红伟。

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

1 范围

GB/T 37033的本部分规定了采用密码技术的电子标签和读写器及其通信的密码安全要素,规定了不同安全级别的射频识别系统对电子标签和读写器及其通信的密码安全技术要求,并规定了电子标签与读写器之间通信的密码安全实现方式。

本部分适用于采用密码安全技术的电子标签和读写器的设计、实现、生产制造、测评和应用,以及射频识别系统中电子标签与读写器间通信的设计、实现、测评和应用。

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 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 37033.3—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

GM/T 0008—2012 安全芯片密码检测准则

GM/T 0040—2015 射频识别标签模块密码检测准则

3 术语和定义

GB/T 37033.1—2018中界定的术语和定义适用于本文件。

4 符号和缩略语

下列符号和缩略语适用于本文件。

CBC-MAC:采用对称算法密码块链接模式生成的消息鉴别码(Cipher Block Chaining Message Authentication Code)

CRC:即循环冗余校验(Cyclic Redundancy Check)

Dec(X, K):解密运算符,用密钥K对X进行解密运算

Enc(X, K):加密运算符,用密钥K对X进行加密运算

HMAC:采用密码杂凑函数生成的消息鉴别码(Hash Message Authentication Code)

MAC:消息鉴别码(Message Authentication Code)

OFB:输出反馈工作模式(Output Feedback Operation Mode)

RFID:射频识别(Radio Frequency IDentification)