ICS 35.040
L 80

中华人民共和国国家标准

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

Information security technology—Technical requirements for cryptographic application for radio frequency identification systems—Part 3:Technical requirements for key management

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3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：北京中电华大电子设计有限责任公司、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、上海复旦微电子集团股份有限公司、北京同方微电子有限公司、复旦大学、航天信息股份有限公司、上海华虹集成电路有限责任公司、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：王俊峰、董浩然、陈跃、顾震、周建锁、刘丽娜、俞军、吴行军、王云松、徐树民、谢文录、梁少峰、王俊宇、柳逊。

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

1 范围

GB/T 37033的本部分规定了射频识别系统在采用密码机制时电子标签、读写器及其通信相关的密钥管理要求。

本部分适用于射频识别系统密钥管理的设计、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

3 术语和定义

GB/T 37033.1—2018中界定的以及下列术语和定义适用于本文件。

3.1

安全密码设备 secure cryptographic device

为诸如密钥这样的秘密信息提供安全存储,以及基于这些秘密信息提供安全服务的设备。

3.2

密钥分割 split knowledge

两个或更多的实体分别地拥有密钥片段,仅通过单个密钥片段不能合成密钥信息。

3.3

密钥组件 key component

至少两个随机或伪随机过程产生的参数中的一个,它们能与一个或多个其他参数结合形成一个密钥。

3.4

双重控制 dual control

利用两个或更多的独立实体(通常是人),协同操作以保护敏感功能和信息的过程。

注:单独的实体不能存取和使用这些功能或信息(例如密钥)。

4 符号和缩略语

下列符号和缩略语适用于本文件。

CA:证书认证机构(Certification Authority)