ICS 35.040
L 80
备案号:44637—2014

GM

中华人民共和国密码行业标准

GM/T 0035.2—2014

射频识别系统密码应用技术要求 第2部分:电子标签芯片密码应用技术要求

Specifications of cryptographic application for RFID systems—Part 2: Specification of cryptographic application for RFID tag chip

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发布

目　　次

前　言

GM/T 0035《射频识别系统密码应用技术要求》分为五个部分：

——第1部分：密码安全保护框架及安全级别；

——第2部分：电子标签芯片密码应用技术要求；

——第3部分：读写器密码应用技术要求；

——第4部分：电子标签与读写器通信密码应用技术要求；

——第5部分：密钥管理技术要求。

本部分为GM/T 0035的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由密码行业标准化技术委员会提出并归口。

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、上海华虹集成电路有限责任公司、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、航天信息股份有限公司、北京华大智宝电子系统有限公司。

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

射频识别系统密码应用技术要求
第2部分:电子标签芯片密码应用技术要求

1 范围

GM/T 0035的本部分规定了采用密码技术的电子标签芯片涉及的密码算法、安全认证、数据存储和通信安全的技术要求。附录A给出了一个电子标签芯片示例。

本部分适用于采用密码安全技术的电子标签芯片的设计开发、生产制造和应用。

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。

GM/T 0035.1—2014 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

GM/T 0035.4—2014 射频识别系统密码应用技术要求 第4部分:电子标签与读写器通信密码应用技术要求

GM/T 0035.5—2014 射频识别系统密码应用技术要求 第5部分:密钥管理技术要求

3 术语和定义

GM/T 0035.1—2014界定的术语和定义适用于本文件。

4 符号和缩略语

GM/T 0035.1—2014界定的符号和缩略语适用于本文件。

5 密码安全要素

5.1 机密性

5.1.1 存储信息的机密性

电子标签对存储在电子标签内的敏感信息采用密码算法进行加密保护,确保除合法读写器外,其余任何读写器不能获得该数据。

存储信息的机密性保护应采用密码算法加密完成。

采用对称密码算法分组加密方式时,用L_D表示明文数据的长度,在明文数据前加上L_D产生新的数据块,并将该数据块按照密码算法分组长度要求进行分组,如果最后一组数据长度小于密码算法分组长度,则应进行填充补齐。填充方式为在最后一组数据后填充一个字节十六进制'80',如果仍小于密码算法分组长度,则填充'00'至分组长度。在数据分组完成后,采用密码算法和加密密钥对该数据逐组加密后存储。在读取该数据时,对于存储的密文数据,采用同样的密码算法和加密密钥对其进行解密,并