ICS 35.040
L 80
备案号:44640—2014

GM

中华人民共和国密码行业标准

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

Specifications of cryptographic application for RFID systems—Part 5:Specification for key management

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5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：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、北京中电华大电子设计有限责任公司、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。

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、王会波。

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

1 范围

GM/T 0035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。附录A给出了一个射频识别系统密钥管理示例。

本部分适用于指导射频识别系统密钥管理的设计、实现和应用。

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

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 密钥体制

5.1 对称密钥体制

适用于电子标签与读写器之间的身份鉴别、访问控制、机密性及完整性的安全保护。按照射频识别系统中对称密钥产生方式的要求不同,可以将对称密钥分为根密钥、分散密钥和传输保护密钥等,密钥类别及产生方式见表1。

表1 密钥类别与产生方式

密钥类别	产生方式
根密钥	由密钥生成系统通过随机数发生器生成
分散密钥	由根密钥经密钥分散因子分散产生
传输保护密钥	在电子标签与读写器进行信息传输前临时协商产生,用于信息传输的加密保护

其中,分散密钥由根密钥和16字节的密钥分散因子经符合国家密码管理主管部门指定的密码算法运算产生,应保证分散密钥被泄露不会导致根密钥和其他分散密钥的泄露。

分散密钥产生过程见图1。