ICS 35.040
L 80
备案号:44639—2014

GM

中华人民共和国密码行业标准

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

Specifications of cryptographic application for RFID systems—Part 4:Specification of cryptographic application for communication between RFID tag and reader

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4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。

本部分主要起草单位：北京同方微电子有限公司、兴唐通信科技有限公司、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、航天信息股份有限公司、上海华申智能卡应用系统有限公司、复旦大学、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：吴行军、董浩然、王俊峰、周建锁、陈跃、俞军、梁少峰、谢文录、王云松、徐树民、顾震、王俊宇、柳逊、王会波。

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

1 范围

GM/T 0035的本部分规定了电子标签与读写器之间的身份鉴别、传输信息的机密性和完整性等安全要求及实现方式。

本部分适用于射频识别系统中电子标签与读写器间通信的安全设计、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

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 传输信息的机密性

电子标签与读写器通信时,电子标签和读写器对相互之间传输的敏感信息采用密码算法进行加密保护,保证该传输数据在被截获后无法得到明文数据,达到传输信息的机密性要求。

传输信息的机密性保护须通过对传输的明文数据进行加密完成,采用流加密或分组加密的方式进行。

传输信息机密性的实现方式见7.1。

5.2 传输信息的完整性

电子标签与读写器通信时,电子标签和读写器对相互之间传输的信息采用密码算法进行校验计算,以发现信息被篡改、删除和插入等情况,达到传输过程中的信息完整性要求。

传输信息完整性校验的实现方式见7.2。