ICS 35.040
L 80
备案号:44636—2014

GM

中华人民共和国密码行业标准

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

Specifications of cryptographic application for RFID systems—Part 1: Cryptographic protection framework and security levels

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1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、兴唐通信科技有限公司、北京同方微电子有限公司、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：顾震、董浩然、王俊宇、谢文录、王云松、梁少峰、俞军、吴行军、王俊峰、周建锁、徐树民、陈跃、柳逊、王会波。

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

1 范围

GM/T 0035的本部分规定了射频识别系统密码安全保护框架及安全级别,以及与GM/T 0035.2—2014、GM/T 0035.3—2014、GM/T 0035.4—2014和GM/T 0035.5—2014之间的相互关系。附录A给出了一个射频识别系统密码安全方案示例。

本部分适用于射频识别系统密码安全的设计、实现与应用。

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 0035.2—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

GM/T 0035.3—2014 射频识别系统密码应用技术要求 第3部分:读写器密码应用技术要求

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

下列术语和定义适用于本文件。

3.1

安全存取模块 secure access module

嵌入在读写器内的密码模块,为读写器提供安全服务。

3.2

电子标签 RFID tag

一种用于射频识别,载有与预期应用相关的电子识别信息的载体,每个标签具有唯一的电子编码。通常由耦合元件及芯片组成,包括非接触CPU卡和非接触存储卡。

3.3

读写器 reader

与电子标签进行数据通信并对标签进行读、写操作的设备。

3.4

对称密码算法 symmetric cryptographic algorithm

加解密使用相同密钥的密码算法。

3.5

非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm

加解密使用不同密钥的密码算法。其中一个密钥(公钥)可以公开,另一个密钥(私钥)必须保密,且