ICS 35.040
L 80
备案号:44641—2014

GM

中华人民共和国密码行业标准

GM/T 0036—2014

采用非接触卡的门禁系统密码应用技术指南

Technical guidance of cryptographic application for access control systems based on contactless smart card

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发布

目　　次

前言 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　符号和缩略语 …… 3
5　密码系统概述 …… 3
6　与密码相关的安全技术要求 …… 4
7　密码应用参考方案 …… 5
8　其他应考虑的安全因素 …… 5
附录 A（资料性附录）　基于 SM7 算法的非接触式逻辑加密卡方案 …… 6
附录 B（资料性附录）　基于 SM1/SM4 算法的非接触式 CPU 卡方案 …… 8

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：上海复旦微电子集团股份有限公司，上海华虹集成电路有限责任公司，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，上海华申智能卡应用系统有限公司，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，复旦大学。

本标准主要起草人：俞军、董浩然、梁少峰、吴行军、周建锁、王俊峰、谢文录、柳逊、陈跃、顾震、王云松、徐树民、王俊宇。

采用非接触卡的门禁系统密码应用技术指南

1 范围

本标准规定了针对采用非接触式卡的门禁系统，采用密码安全技术时，系统中使用的密码设备、密码算法、密码协议和密钥管理的相关要求。

本标准适用于指导采用非接触卡的门禁系统相关产品的研制、使用和管理。

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 0002—2012 SM4 分组密码算法

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

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

分散密钥 derived key

由根密钥和非保密可变数据生成的对称密钥。

3.6

根密钥 derivation key

用来生成分散密钥的密钥。

3.7

机密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。