ICS 35.040
L 80
备案号:49739—2015

中华人民共和国密码行业标准

GM/T 0040—2015

射频识别标签模块密码检测准则

Cipher test specification of radio frequency identification tag module

2015-04-01 发布　　2015-04-01 实施

国家密码管理局　　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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：北京中电华大电子设计有限责任公司、国家密码管理局商用密码检测中心、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、上海复旦微电子集团股份有限公司、上海华申智能卡应用系统有限责任公司、航天信息股份有限公司、国民技术股份有限公司。

本标准主要起草人：董浩然、罗鹏、周建锁、兰天、费渡、毛颖颖、莫凡、邓开勇、顾震、杨贤伟、邵波、柳逊、刘颖、岳超。

射频识别标签模块密码检测准则

1 范围

本标准规定了采用密码技术的射频识别标签模块产品密码检测的检测内容和要求。

本标准适用于射频识别标签模块的密码及安全功能检测。也可用于符合 GB/T 28925—2012 和 GB/T 29768—2013 射频识别空中接口协议产品的密码检测。

本标准所描述的算法是国家密码管理主管部门认可的密码算法。

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。

GB/T 28925—2012 信息技术 射频识别 2.45 GHz 空中接口协议

GB/T 29768—2013 信息技术 射频识别 800/900 MHz 空中接口协议

GM/T 0005—2012 随机性检测规范

GM/T 0008—2012 安全芯片密码检测准则

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 0035.2—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 0035.4—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/Z 4001 密码术语

3 术语和定义

GM/Z 4001 所界定的以及下列术语和定义适用于本文件。

3.1

对称密码算法 symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

3.2

单向鉴别 unidirectional authentication

由读写器发起对标签的身份鉴别。

3.3

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。

3.4

抗原发抵赖 non-repudiation of origin

一种密码学的方法，用来防止消息的原发者否认其创建并且已经发送了该消息。