ICS 35.040
L 80
备案号:49739—2015

GM

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

中华人民共和国密码
行业标准
射频识别标签模块密码检测准则
GM/T 0040—2015
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.25 字数 28 千字
2015年6月第一版 2015年6月第一次印刷
*
书号:155066·2-28791 定价 21.00 元

GM/T 0040-2015

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。

3.5

灭活　kill

对标签模块的一种操作指令，成功执行后，标签模块不再响应任何命令。

3.6

射频识别　radio frequency identification

利用射频信号通过空间耦合（交变磁场或电磁场）实现信息的无接触传递，并通过所传递的信息达到识别目的。

3.7

射频识别标签模块　RFID tag module

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。每个射频识别标签模块（以下简称标签模块）具有唯一的电子编码，可由单芯片或多芯片组成。

3.8

随机数　random number

一种数据序列，其产生不可预测，其序列没有周期性。

3.9

双向鉴别　bidirectional authentication

读写器和标签之间进行的相互身份鉴别。

4　符号和缩略语

下列缩略语适用于本文件。

RFID　射频识别（radio frequency identification）

UID　唯一标识符（unique identifier）

5　射频识别标签模块分类

5.1　Ⅰ类标签模块

Ⅰ类标签模块规定了标签模块应具备与读写器间的单向鉴别能力。适用于仅需要认证标签模块身份真实性的应用环境。

5.2　Ⅱ类标签模块

Ⅱ类标签模块规定了标签模块应具备与读写器间的双向鉴别能力，适用于需要对标签模块与读写器进行相互认证身份真实性的应用环境。该类标签模块按是否支持传输的机密性和完整性又划分为两个子类：Ⅱ-A 类和Ⅱ-B 类，其中Ⅱ-A 类标签模块不支持机密性和完整性的校验，Ⅱ-B 类标签模块可支持机密性和完整性校验。

6　检测要求

6.1　一般要求

本标准一般性检测要求如下：

a）　标签模块的检测按照 GM/T 0035.1—2014、GM/T 0035.2—2014 及本标准内容开展，本标准仅定义了标签模块的密码检测；

b） 本标准按密码算法、密码服务、敏感信息保护、生命周期安全测试、审计、密钥管理和开发环境保障等方面分别提出检测要求；

c） 标签模块应明确声明产品类型及密码功能，产品各项密码功能应正确有效；

d） 标签模块检测项见附录 A。

6.2 密码算法

6.2.1 算法实现正确性测试

6.2.1.1 Ⅰ类标签模块

Ⅰ类标签模块算法实现正确性测试方式如下：

a） 检测要求

按照标签模块提供的密码算法功能进行算法调用正确性检测。

使用读写器发起操作指令，分别测试标签模块支持的各类密码算法及其工作模式，标签模块返回的响应数据应正确有效。

b） 判定准则

标签模块能正确实现各类密码算法功能。

6.2.1.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.2.2 随机数测试

6.2.2.1 Ⅰ类标签模块

无要求。

6.2.2.2 Ⅱ-A 类标签模块

Ⅱ-A 类标签模块随机测试方式如下：

a） 检测要求

1） 显著性水平

应符合 GM/T 0005—2012 的要求。

2） 样本数量

随机数样本数量为 1 000；

3） 样本长度

应符合 GM/T 0005—2012 的要求。

4） 检测项目

检测项目见表 1，检测项目定义见 GM/T 0005—2012。

表 1 检测项目要求

序号	检测项目
1	单比特频数检测
2	扑克检测
3	重叠子序列
4	游程分布检测

5） 检测条件

每个检测项目的检测条件见表2：

表2 检测条件要求

序号	检测项目	检测条件要求
1	单比特频数检测	
2	扑克检测	$m=4$，$m=8$
3	重叠子序列	$m=2$，$m=5$
4	游程分布检测	

b） 判定准则

如果随机数通过表2中规定的所有检测项目，则随机数通过本标准检测，否则，未通过本标准检测。

6.2.2.3 Ⅱ-B类标签模块

Ⅱ-B类标签模块随机数测试方式如下：

a） 检测要求

1） 显著性水平

应符合GM/T 0005—2012的要求。

2） 样本数量

随机数样本数量为1 000。

3） 样本长度

应符合GM/T 0005—2012的要求。

4） 检测项目

检测项目见表3，检测项目定义见GM/T 0005—2012。

表3 检测项目要求

序号	检测项目
1	单比特频数检测
2	块内频数检测
3	扑克检测
4	重叠子序列
5	游程总数检测
6	游程分布检测
7	块内最大“1”游程检测
8	二元推导检测
9	自相关检测
10	矩阵秩检测
11	累加和检测
12	近似熵检测

表 3（续）

序号	检测项目
13	线性复杂度检测
14	Maurer 通用统计检测
15	离散傅立叶检测

5） 检测条件

检测条件要求见表 4：

表 4 检测条件要求

序号	检测项目	检测条件要求
1	单比特频数检测	
2	块内频数检测	$m=100$
3	扑克检测	$m=4$，$m=8$
4	重叠子序列	$m=2$，$m=5$
5	游程总数检测	
6	游程分布检测	
7	块内最大“1”游程检测	$m=10\ 000$
8	二元推导检测	$k=3$，$k=7$
9	自相关检测	$d=1$，$d=2$，$d=8$，$d=16$
10	矩阵秩检测	$M=Q=32$
11	累加和检测	
12	近似熵检测	$m=5$
13	线性复杂度检测	$m=500$
14	Maurer 通用统计检测	
15	离散傅立叶检测	

b） 判定准则

如果随机数通过表 4 规定的所有检测项目，则随机数通过本标准检测；否则，未通过本标准检测。

6.3 密码服务

6.3.1 身份鉴别测试

6.3.1.1 概述

密码服务指标签模块基于算法提供的身份鉴别、机密性和完整性等安全要素。密码服务的实现与产品具有耦合性。选用 GB/T 28925—2012、GB/T 29768—2013 中的安全鉴别协议的产品应实现该标准中规定的安全命令和机制；选用 GM/T 0035.4—2014 安全鉴别协议产品应实现该标准中规定的安全机制；选用其他安全标准或自定义安全鉴别协议的产品应实现相应的安全机制。

6.3.1.2 Ⅰ类标签模块

Ⅰ类标签模块身份鉴别测试方式如下：

a） 检测要求

采用单向鉴别方式，单向鉴别过程应使用密码，其密码功能应正确有效。测试环境需设计有效类和无效类测试用例，标签模块应对读写器发出的认证请求做出相应的正确应答。

b） 判定准则

标签模块单向鉴别机制有效。

6.3.1.3 Ⅱ类标签模块

Ⅱ类标签模块身份鉴别测试方式如下：

a） 检测要求

采用双向鉴别方式，双向鉴别过程应使用密码，其密码功能应正确有效。

测试环境需设计有效类和无效类测试用例，标签模块应对与读写器之间的双向鉴别做出相应的正确应答。

b） 判定准则

标签模块双向鉴别机制有效。

6.3.2 数据传输机密性测试

6.3.2.1 Ⅰ类标签模块

无要求。

6.3.2.2 Ⅱ-A类标签模块

无要求。

6.3.2.3 Ⅱ-B类标签模块

Ⅱ-B类标签模块传输机密性测试方式如下：

a） 检测要求

标签模块能够根据需要，为允许传输的敏感信息提供正确有效的传输机密性服务。

标签模块与读写器通信时，采用流加密或分组加密的方式对传输的敏感信息进行加密保护，其数据传输机密性服务应正确有效。

b） 判定准则

信道传输的数据在传输过程中能够采用密码算法进行机密性保护。

6.3.3 数据存储机密性测试（本项为可选项）

6.3.3.1 Ⅰ类标签模块

无要求。

6.3.3.2 Ⅱ-A类标签模块

无要求。

6.3.3.3 Ⅱ-B类标签模块

Ⅱ-B类标签模块数据存储机密性测试方式如下：

a） 检测要求

标签模块能够根据需要，为存储的敏感信息提供正确有效的数据存储机密性服务。

标签模块对存储在标签模块内的敏感信息采用密码算法进行加密保护，确保除合法读写器外，其余任何读写器不能获得该数据。

b） 判定准则

标签模块能够采用密码算法对存储的敏感信息数据进行机密性保护。

6.3.4 数据传输完整性测试（本项为可选项）

6.3.4.1 Ⅰ类标签模块

无要求。

6.3.4.2 Ⅱ-A类标签模块

无要求。

6.3.4.3 Ⅱ-B类标签模块

Ⅱ-B类标签模块数据传输完整性测试方式如下：

a） 检测要求

标签模块能够根据需要，为允许传输的敏感信息提供正确有效的数据传输完整性服务。

标签模块与读写器通信时，标签模块采用密码算法对传输的数据进行校验计算，以发现数据被篡改、删除和插入等情况，达到传输过程中的数据完整性要求。

b） 判定准则

信道传输的数据在传输过程中能够采用密码算法进行完整性保护。

6.3.5 数据存储完整性测试（本项为可选项）

6.3.5.1 Ⅰ类标签模块

无要求。

6.3.5.2 Ⅱ-A类标签模块

无要求。

6.3.5.3 Ⅱ-B类标签模块

Ⅱ-B类标签模块数据存储完整性测试方式如下：

a） 检测要求

标签模块能够根据需要，为存储的敏感信息提供正确有效的数据存储完整性服务。

标签模块采用密码算法对存储在标签模块内的敏感信息进行校验计算，以发现数据被篡改、删除和插入等情况，确保存储信息的完整性。

b） 判定准则

标签模块能够采用密码算法对存储的敏感信息数据进行完整性保护。

6.4 密码性能

6.4.1 鉴别性能测试

标签模块鉴别性能测试方式如下：

a） 检测要求

测试标签模块认证流程时长。

b） 判定准则

标签模块能够达到认证过程的时长要求。

6.4.2 数据交互性能测试

标签模块数据交互性能测试方式如下：

a） 检测要求

测试标签模块数据交互(数据传输、数据处理及读写)的速率。

b） 判定准则

标签模块能够达到数据交互的速率要求。

6.5 敏感信息保护

6.5.1 口令保护测试(本项为可选项)

6.5.1.1 Ⅰ类标签模块

Ⅰ类标签模块口令保护测试方式如下：

a） 检测要求

标签模块采用口令保护方式对数据的读、写以及数据的更新等操作设置控制权限，阻止非授权的访问。

在用户应用时，读写器只能按照标签模块发行时所设置的口令权限对标签模块进行相关操作。

标签模块能够根据需要正确、有效地操作敏感信息。

b） 判定准则

标签模块数据读、写及更新权限有效。

6.5.1.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.5.2 敏感信息保护测试

6.5.2.1 Ⅰ类标签模块

Ⅰ类标签模块敏感信息保护测试方式如下：

a） 检测要求

测试标签模块对敏感信息的防非法访问功能。

b） 判定准则

1） 标签模块具有防止存储数据被非法访问的功能；

2） 标签模块的关键参数和其他敏感信息不能通过物理或逻辑接口非法访问。

6.5.2.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.6 抗抵赖

6.6.1 抗原发抵赖测试(本项为可选项)

6.6.1.1 Ⅰ类标签模块

无要求。

6.6.1.2 Ⅱ类标签模块

Ⅱ类标签模块抗原发抵赖测试方式如下：

a） 检测要求

读取标签模块内存储的签名数据原文、数字签名和公钥证书，验证数字签名的合法性。

b） 判定准则

应符合 GM/T 0035.2—2014 中 5.3.1 的规定。

6.7 生命周期安全

6.7.1 标签模块灭活测试

6.7.1.1 Ⅰ类标签模块

Ⅰ类标签模块灭活测试方式如下：

a） 检测要求

测试标签模块灭活功能的有效性。

b） 判定准则

灭活后，被测标签模块不应有任何应答。

6.7.1.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.7.2 防非法指令测试

6.7.2.1 Ⅰ类标签模块

Ⅰ类标签模块防非法指令测试方式如下：

a） 检测要求

使用产品未定义或错误的指令，测试标签模块防非法指令的功能。

b） 判定准则

向被测标签模块发送产品未定义或错误的指令，标签模块应报错或不产生响应。

6.7.2.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.7.3 防初始使用权欺骗测试

6.7.3.1 Ⅰ类标签模块

Ⅰ类标签模块防初始使用权欺骗测试方式如下：

a） 检测要求

标签模块不提供初始化权限，对被测标签模块执行初始化操作，测试标签模块是否具备防初始化功能。

b） 判定准则

不能对被测标签模块执行初始化操作。

6.7.3.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.7.4 防生命周期越界测试

6.7.4.1 Ⅰ类标签模块

Ⅰ类标签模块防生命周期越界测试方式如下：

a) 检测要求

使用非当前生命周期阶段的指令，测试标签模块防生命周期越界功能。

b) 判定准则

向被测标签模块发送非当前生命周期阶段指令，标签模块应报错或不产生响应。

6.7.4.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.8 审计

6.8.1 标签模块唯一标识测试

6.8.1.1 Ⅰ类标签模块

Ⅰ类标签模块审计检测方式如下：

a) 检测要求

测试标签模块标识的唯一性。见 GM/T 0035.2—2014 中 5.4.1。

b) 判定准则

被测标签模块标识应与该标签模块提供的唯一标识一致。

6.8.1.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.9 密钥管理

6.9.1 密钥生成

6.9.1.1 Ⅰ类标签模块

标签模块使用的密钥数据应由经国家密码管理主管部门审批的密码设备随机生成。

6.9.1.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.9.2 密钥存储

6.9.2.1 Ⅰ类标签模块

应符合 GM/T 0008—2012 中 7.2.1 的规定。

6.9.2.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.9.3 密钥使用

6.9.3.1 Ⅰ类标签模块

应符合 GM/T 0008—2012 中 7.3.1 的规定。

6.9.3.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.9.4 密钥更新

6.9.4.1 Ⅰ类标签模块

如果标签模块具备密钥更新功能，则应符合 GM/T 0008—2012 中 7.4.1 的规定。

6.9.4.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.9.5 密钥导入

6.9.5.1 Ⅰ类标签模块

应符合 GM/T 0008—2012 中 7.5.1 的规定。

6.9.5.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.9.6 密钥清除

6.9.6.1 Ⅰ类标签模块

如果标签模块具备密钥清除功能，则应符合 GM/T 0008—2012 中 7.7.1 的规定。

6.9.6.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.10 开发环境保障

6.10.1 文档管理

6.10.1.1 Ⅰ类标签模块

Ⅰ类标签模块文档管理方式如下：

a) 标签模块的开发流程、配置管理、交付运行、算法功能开发和工具技术等各类文档齐全；
b) 在生命周期的各个阶段须具有追踪记录文档；
c) 标签模块的开发流程的各个阶段需明确界定；
d) 对标签模块产品开发过程中各阶段完成的任务及相应的输出须具有明确要求。

6.10.1.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.10.2 开发环境安全

6.10.2.1 Ⅰ类标签模块

应符合 GM/T 0008—2012 中 13.3.1 的规定。

6.10.2.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.10.3 隐蔽通道声明

6.10.3.1 Ⅰ类标签模块

应提供标签模块中涉及密码的部分不存在隐蔽通道的声明文件。

6.10.3.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.10.4 人员

6.10.4.1 Ⅰ类标签模块

应符合 GM/T 0008—2012 中 13.4.1 的规定。

6.10.4.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.10.5 源文件

6.10.5.1 Ⅰ类标签模块

应符合 GM/T 0008—2012 中 13.6.1 的规定。

6.10.5.2 Ⅱ类标签模块

同Ⅰ类标签模块。

附 录 A
（规范性附录）
射频识别标签模块密码检测项

射频识别标签模块密码检测项见表 A.1。

表 A.1 射频识别标签模块密码检测项

标签模块检测项			标签模块分类		
			Ⅰ类	Ⅱ类	
				Ⅱ-A 类	Ⅱ-B 类
密码算法	算法实现正确性测试		√	√	√
	随机数测试			√[a]	√[b]
密码服务	身份鉴别测试	单向鉴别测试	√		
		双向鉴别测试		√	√
	数据传输机密性测试				√
	数据存储机密性测试				√[c]
	数据传输完整性测试				√[c]
	数据存储完整性测试				√[c]
密码性能测试	鉴别性能测试		√	√	√
	数据交互性能测试		√	√	√
敏感信息保护	口令保护测试		√[c]	√[c]	√[c]
	敏感信息保护测试		√	√	√
抗抵赖	抗原发抵赖测试			√[c]	√[c]
生命周期安全测试	标签模块灭活测试		√	√	√
	防非法指令测试		√	√	√
	防初始使用权欺骗测试		√	√	√
	防生命周期越界测试		√	√	√
审计	唯一标识测试		√	√	√
密钥管理			√	√	√
开发环境保障			√	√	√

注：“√”表示不同类别的射频识别标签模块中应具备的密码检测项。

[a] 随机数检测Ⅱ-A 类检测 4 项。

[b] 随机数检测Ⅱ-B 类检测 15 项。

[c] 检测项可选。