ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0040—2024
代替 GM/T 0040—2015

射频识别标签模块密码检测规范

Cipher test specification of radio frequency identification tag module

2024-12-27 发布　　2025-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本文按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GM/T 0040—2015《射频识别标签模块密码检测准则》，与GM/T 0040—2015相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了标签模块分类，把标签模块新划分为4大类，其中Ⅰ类被分为Ⅰ-A类和Ⅰ-B类，保留原Ⅱ-A和Ⅱ-B的分类，增加了Ⅲ类和Ⅳ类（见第5章，2015年版的第5章）；

b) 更改了“检测要求和判定准则”，增加了Ⅲ类和Ⅳ类标签模块的检测项，更改了Ⅱ类标签模块的随机数测试内容（见第6章，2015年版的第6章）；

c) 更改了“随机数测试”中的“检测项目要求”和“检测条件要求”，并删除了相应的表1和表3，表2和表4（见2015年版的6.2.2.2和6.2.2.3），直接引用标准GM/T 0005—2021附录A中A.1 20 000比特样本检测设置和A.2 1 000 000比特样本检测设置（见6.2.2）；

d) 增加了“审计记录”，并按照GM/T 0035.2—2014的要求来判定，且只有第Ⅳ类标签才需要符合审计要求（见6.9）；

e) 更改了“密钥管理”中各检测项的要求，不要求符合“GM/T 0008—2012”，删除了对“GM/T 0008—2012”的引用（见6.10，2015年版的6.9）；

f) 删除“开发环境保障”的内容（见2015年版的6.10）；

g) 更改了“标签模块分类及检测项”的内容（见附录A，2015年版的附录A）。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：华大恒芯科技有限公司、商用密码检测认证中心、苏州安超微电子有限公司、紫光同芯微电子有限公司、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、国民技术股份有限公司、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责任公司。

本文件主要起草人：张建平、周建锁、雷银花、毛颖颖、陈小庆、杨贤伟、邵波、柳逊、孙磊、董浩然、罗鹏、兰天、费渡、莫凡、邓开勇、顾震、刘颖、岳超。

本文件及其所替代文件的历次版本发布情况为：

——2015年首次发布为GM/T 0040—2015；

——本次为第一次修订。

射频识别标签模块密码检测规范

1 范围

本文件规定了采用密码技术的射频识别标签模块产品的分类和密码检测的检测内容、检测要求以及判定准则。

本文件适用于包括高频，超高频，微波等频段的射频识别标签模块的密码及安全功能检测。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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—2021 随机性检测规范

GM/T 0035—2014(所有部分) 射频识别系统密码应用技术要求

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

单向鉴别 unidirectional authentication

由读写器发起对标签的身份鉴别。

3.2

数据源鉴别 data origin authentication

确认接收到的数据的来源与其声明的一致。

3.3

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。

3.4

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。

3.5

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。

注：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。