ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0041—2024
代替 GM/T 0041—2015

智能 IC 卡密码检测规范

Cryptographic test specification for smart card

2024-12-27 发布　　2025-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照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 0041—2015《智能IC卡密码检测规范》，与GM/T 0041—2015相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了“检测环境”一章（见第5章）；

b) 更改了内部认证测试要求，增加了标准测试数据的含义和测试步骤（见7.2.2，2015年版的6.2.2）；

c) 更改了非对称密钥使用权限测试方法，增加了私钥使用权限的测试步骤（见7.3.3.5，2015年版的6.3.3.5）；

d) 更改了素数采集要求，增加了单组数据的数据量大小要求（见7.4.1，2015年版的6.4.1）；

e) 更改了随机数采集要求，增加了对于三级密码模块产品大数据量采集测试要求（见7.5.1，2015年版的6.5.1）；

f) 更改了非对称密码算法实现正确性的验证方法（见7.6.2，2015年版的6.6.2）；

g) 更改了非对称密码算法密钥生成的正确性测试方法，增加了测试次数和配对一致性检测步骤，并将配对一致性检测列为单独的测试项（见7.6.6，2015年版的6.6.5）；

h) 增加了“送检技术文档要求”一章（见第8章）。

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：北京华大智宝电子系统有限公司、商用密码检测认证中心、武汉天喻信息产业股份有限公司、东信和平科技股份有限公司、北京握奇数据系统有限公司、航天信息股份有限公司、北京中电华大电子设计有限责任公司、上海华虹集成电路有限责任公司。

本文件主要起草人：陈跃、陈保儒、王雪聪、李大为、邓开勇、罗鹏、雷银花、林春、刘文娟、李晓俊、张汉就、刘蕾、罗世新、王晓燕、梁少峰、费林深。

本文件及其所代替文件的历次版本发布情况为：

——2015年首次发布为GM/T 0041—2015；

——本次为第一次修订。

智能 IC 卡密码检测规范

1 范围

本文件规定了智能 IC 卡产品的检测项目、检测方法、送检技术文档要求和判定规则。

本文件适用于智能 IC 卡产品的密码检测，也用于指导智能 IC 卡产品的研发。

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。

GM/T 0005 随机数检测规范

GM/T 0039 密码模块安全检测要求

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 界定的术语和定义适用于本文件。

注：本文件中测试对象指智能 IC 卡。

4 缩略语

下列缩略语适用于本文件。

APDU：应用协议数据单元（Application Protocol Data Unit）

COS：芯片操作系统（Chip Operating System）

DDF：目录定义文件（Directory Definition File）

IC：集成电路（Integrated Circuit）

Lc：命令数据的长度（Length of Command Data）

MAC：报文鉴别代码（Message Authenticate Code）

PIN：个人识别号（Personal Indentify Number）

RSA：非对称密码算法（Rivest-Shamir-Adleman Algorithm）

5 检测环境

5.1 检测环境拓扑图

智能 IC 卡密码检测环境参考拓扑图如图 1 所示。