ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0121—2022

密 码 卡 检 测 规 范

Test specification for cryptographic board

2022-11-20 发布　　2023-06-01 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。

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：国家密码管理局商用密码检测中心、山东渔翁信息技术股份有限公司、北京三未信安科技发展有限公司、北京江南天安科技有限公司、兴唐通信科技有限公司、成都卫士通信息产业股份有限公司、鼎铉商用密码测评技术（深圳）有限公司、智巡密码（上海）检测技术有限公司。

本文件主要起草人：陈妍、李国友、李冬、邓开勇、顾伟平、齐晶晶、宋志华、吴震、高志权、张玉国、桑洪波、马晓艳、姚长远、何济尘、高伟、孟琦、秦放、凌杭、包斯刚、韩玮。

密码卡检测规范

1 范围

本文件规定了密码卡的检测内容、检测方法、检测要求及文档要求。

本文件适用于密码卡的检测，以及该类密码设备的研制，也可用于指导基于该类密码设备的应用开发。

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。

GB/T 15852.2 信息技术 安全技术 消息鉴别码 第2部分：采用专用杂凑函数的机制

GB/T 17964 信息安全技术 分组密码算法的工作模式

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32918(所有部分) 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 33133(所有部分) 信息安全技术 祖冲之序列密码算法

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 35275 信息安全技术 SM2密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2密码算法使用规范

GB/T 38635(所有部分) 信息安全技术 SM9标识密码算法

GB/T 36624 信息技术 安全技术 可鉴别的加密机制

GM/T 0005 随机性检测规范

GM/T 0018 密码设备应用接口规范

GM/T 0039 密码模块安全检测要求

GM/T 0050 密码设备管理 设备管理技术规范

GM/T 0062 密码产品随机数检测要求

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

密码卡 cryptographic board card

具有密码运算功能、密钥管理和自身安全防护等功能的硬件板卡设备。

3.2

保护密钥 protection key

用于加密保护设备中其他密钥和敏感信息安全的密钥。

3.3

设备密钥对　device key pair

用于表明设备身份、对设备进行管理的非对称密钥对，包含签名密钥对和加密密钥对。

3.4

密钥加密密钥　key encrypting key；KEK

用于对密钥进行加密或解密的密钥。

3.5

会话密钥　session key

在一次会话中使用的数据加密密钥。

3.6

用户密钥对　user key pair

存储在设备内部的用于应用密码运算的非对称密钥对，包含签名密钥对和加密密钥对。

3.7

私钥访问控制码　private key access password

用于验证私钥使用权限的口令字。

3.8

智能密码钥匙　cryptographic smart token

实现密码运算、密钥管理功能，提供密码服务的终端密码设备，一般使用 USB 接口形态。

3.9

智能 IC 卡　smart card

实现密码运算和密钥管理的含 CPU(中央处理器)的集成电路卡。

4　缩略语

下列缩略语适用于本文件。

API：应用程序编程接口(Application Programming Interface)

CBC：密文分组链接工作模式(Cipher Block Chaining Operation Mode)

CFB：密文反馈工作模式(Cipher Feedback Operation Mode)

CPCI：紧凑型外设部件互连(Compact Peripheral Component Interconnect)

CTR：计数器工作模式(Counter Operation Mode)

ECB：电码本工作模式(Electronic Codebook Operation Mode)

HMAC：带密钥的杂凑算法(keyed-Hash Message Authentication Code)

Mini PCI-E：微型高性能外设部件互连(Mini Peripheral Component Interconnection Express)

OFB：输出反馈工作模式(Output Feedback Operation Mode)

PCI：外设部件互连(Peripheral Component Interconnection)

PCI-E：高性能外设部件互连(Peripheral Component Interconnection Express)

SATA：串行 ATA(Serial Advanced Technology Attachment)

USB：通用串行总线(Universal Serial Bus)

5　检测环境

密码卡常规检测平台由检测控制台和运行测试程序的检测服务器组成，用于检测密码卡的功能、性能，通过服务器提供的 PCI、PCI-E、USB 等接口或转接卡连接密码卡，并在服务器上安装密码设备应用

接口 API 库文件及对应的驱动程序(若密码卡无需驱动程序,则无需在服务器上进行安装)。检测控制台向服务器上运行的测试程序发送测试指令,测试程序根据测试指令调用密码卡的 API 接口对密码卡功能及性能进行测试。检测环境见图 1。

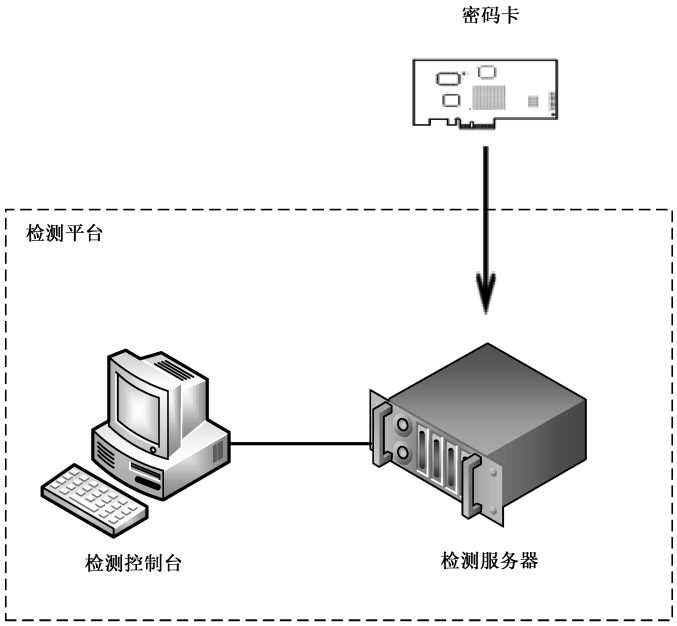

图 1　密码卡常规检测环境拓扑图

6　检测内容

6.1　概述

密码卡检测项目可包括:

a)　功能检测:初始化检测、密码算法检测、密钥管理检测、随机数质量检测、接口检测、管理安全检测;

b)　性能检测:包含随机数产生性能、对称密钥产生性能、非对称密钥对产生性能、对称算法加解密性能、非对称算法加解密性能、非对称算法签名及验证性能、杂凑算法运算性能的检测;

c)　安全性检测;

d)　虚拟化检测。

6.2　功能检测

6.2.1　初始化检测

检测要求:

a)　应能正确地在检测平台内安装,其设备驱动程序在指定的操作系统中应能够正确地安装和卸载;

b)　在开机上电后应进行自检(包括密码算法、随机数、静态存储数据和软件固件完整性及其他需要进行自检的功能部件)并输出状态指示;未通过上电自检,密码卡应拒绝一切密码功能调用服务;

c)　应至少支持初始和就绪两个状态;未安装设备密钥对和保护密钥的密码卡处于初始状态,已安装设备密钥对和保护密钥的密码卡处于就绪状态;在初始状态下,只可读取设备信息、添加管

理员及操作员(若支持操作员角色)、生成或恢复设备密钥对和保护密钥;在就绪状态下,除设备密钥对和保护密钥的生成或恢复操作不能执行外,应能根据角色权限执行相关操作,满足管理员权限时,能够提供密钥管理和密码运算等功能,满足操作员权限时,能够提供密码运算等操作;在就绪状态下可通过恢复出厂设置或置零等操作使密码卡进入初始状态;

d) 驱动程序宜支持多个密码卡设备同时使用和操作的基本要求,宜与密码卡具备安全绑定机制。

检测步骤:

a) 将密码卡插到检测服务器中,应成功安装或卸载驱动程序;

b) 密码卡应正确执行硬件上电自检,输出自检状态结果;如果自检状态结果显示自检失败,则进一步进行密码功能调用服务,操作应失败;

c) 在未安装设备密钥对和保护密钥的情况下,应成功读取设备信息、生成或恢复设备密钥对和保护密钥,执行其他任何安全服务或密钥管理操作应失败;

d) 应通过管理工具添加管理员和操作员权限,并成功生成(或恢复)设备密钥对和保护密钥,进入就绪状态;

e) 在就绪状态下,未通过管理员身份认证,执行密钥管理操作和密码运算等安全服务操作应失败;通过管理员权限认证,执行密钥管理操作和密码运算等安全服务操作成功;

f) 若支持操作员角色,在就绪状态下,未通过操作员身份认证,执行密钥管理和密码运算等安全服务操作应失败;通过操作员身份认证后,应成功执行密码运算等安全服务,执行密钥管理操作应失败;

g) 在就绪状态下,执行恢复出厂设置或触发毁钥机制等置零操作密码卡内所有密钥及敏感信息,密码卡进入初始状态;

h) 核查驱动程序文件,可通过驱动获取密码卡内部唯一标识等方式验证驱动和密码卡的绑定关系。

6.2.2 密码算法检测

检测要求:

密码卡应使用符合国家密码管理要求的密码算法,宜采用经密码检测认证的密码算法芯片、安全芯片、密码模块等作为主要密码部件。

a) 应支持至少一种对称密码算法,如分组密码算法、序列密码算法等。分组密码算法应至少支持ECB和CBC两种工作模式,宜扩展支持CFB、OFB、CTR等工作模式,工作模式应符合GB/T 17964。应按照指定的工作模式对数据进行正确的加解密运算。采用SM4算法时,其实现应符合GB/T 32907,采用祖冲之算法时,其实现应符合GB/T 33133,采用可鉴别的加密机制时,其实现应符合GB/T 36624。算法标识应符合GB/T 33560。

b) 应支持至少一种密码杂凑算法,宜支持GB/T 15852.2规定的HMAC。杂凑函数采用SM3算法时,其实现应符合GB/T 32905要求。算法标识应符合GB/T 33560。

c) 应支持至少一种非对称密码算法,支持加解密、签名/验证和密钥协商等运算。非对称密码算法采用SM2算法时,其实现应符合GB/T 32918(所有部分)、GB/T 35275、GB/T 35276,采用SM9算法时,其实现应符合GB/T 38635(所有部分)。标识应符合GB/T 33560。

d) 应支持密码算法上电/复位自检和周期性自检,自检失败,应停止提供安全服务,进入错误状态,输出错误指示。

检测步骤:

a) 密码卡应按照指定的对称密码算法工作模式对数据进行加解密,检测其运算结果的正确性:

1) 对给定的密钥和明文经指定的算法和工作模式加密,结果和给定密文完全相同;

2) 对给定的密钥和密文经指定的算法和工作模式解密,结果和给定明文完全相同。

b) 密码卡应对消息进行杂凑运算，检测其运算结果的正确性，对给定消息和参数(或空)调用杂凑算法计算杂凑值，结果和给定杂凑值完全相同。

c) 密码卡应使用非对称密码算法对数据进行加解密、签名/验证和密钥协商运算，检测其运算结果的正确性：

1) 对给定的密钥和明文调用密码算法加密后，调用密码算法进行解密运算，解密结果和给定明文完全相同；

2) 对给定的密钥和明文调用密码算法加密后，检测平台对密文进行解密运算，解密结果和给定明文完全相同；

3) 使用给定的密钥对待签名消息调用密码算法签名后，调用密码算法对该签名值进行验签运算，验签通过；

4) 使用给定的密钥对待签名消息调用密码算法签名后，检测平台对签名值进行验签，验签通过；

5) 使用给定的密钥和密钥协商参数，调用密钥协商算法与检测平台进行密钥协商，协商结果正确。

d) 密码卡应正确执行密码算法上电/复位自检和周期性自检，核查自检状态结果或状态指示，如果自检失败，调用密码卡执行密码运算操作应失败。

6.2.3 密钥管理检测

6.2.3.1 密钥结构

密码卡应具备完善的密钥管理功能，应至少支持三级密钥结构：

——第一级是保护密钥，用于保护密码卡中其他密钥和敏感信息的安全，包括对其他密钥的管理等。

——第二级是用户密钥对、密钥加密密钥和设备密钥对。用户密钥对包括签名密钥对和加密密钥对，用于实现用户数字签名、签名验证，以及会话密钥的保护等功能；密钥加密密钥是定期更换的对称密钥，用于对会话密钥的保护；设备密钥对，作为密码卡的身份密钥，包括签名密钥对和加密密钥对，用于设备管理，不对上层应用开放。

——第三级是会话密钥，用于数据加解密。

密码卡应支持有效的安全机制和措施，保证密钥在密钥产生、安装、导入、导出、存储、使用、更新、备份恢复以及销毁整个生命周期中的安全。

6.2.3.2 密钥产生及存储

检测要求：

a) 应支持按照指定的索引号、密钥长度等参数生成密钥(如对称密钥、非对称密钥)；

b) 对称密钥和非对称密钥生成中所使用到的随机数，应使用经密码检测认证具有物理噪声源功能的芯片生成；

c) 应在初始状态以安全形式生成或安装保护密钥，并以安全形式存储，不能以明文形式出现在密码卡外部；

d) 应在初始状态通过管理工具生成或安装设备密钥对，并以密文或微电保护等安全方式存储于密码卡内的密钥存储区，设备密钥对私钥不能以明文形式出现在密码卡外部；

e) 用户密钥对应由管理工具安装或调用密码卡生成，私钥应以密文或微电保护等安全方式存储在密码卡内部的密钥存储区，不能以明文形式出现在密码卡外部；

f) 用户密钥对和设备密钥对中的加密密钥对应由独立的密钥管理系统产生并按照 GM/T 0018

中规定的保护结构下发到密码卡中；

g) 密钥加密密钥应由管理工具安装或调用密码卡生成，并以密文或微电保护等安全方式存储于密码卡内部的密钥存储区；

h) 应支持使用 API 接口函数生成会话密钥；

i) 除公钥外的密钥均不能以明文形式出现在密码卡外；

j) 应支持安全存储一定数量的对称密钥和非对称密钥对；

k) 应具备有效的密钥存储保护机制，防止解剖、探测和非法读取；

l) 内部存储的密钥应具有权限控制机制，防止非法使用和导出。

检测步骤：

a) 使用指定的参数生成对称或非对称密钥并能正确存储和显示密钥存储状态；

b) 在初始状态，生成或安装保护密钥，并安全存储；

c) 在初始状态操作管理工具，生成或安装设备密钥对，并存储，核查密钥存储状态；

d) 在就绪状态操作管理工具，生成或安装用户密钥对和密钥加密密钥并存储，核查密钥存储状态和数量；

e) 检测平台调用 API 接口，密码卡生成或计算会话密钥，会话密钥能使用句柄正确检索；

f) 根据密码卡实际存储能力，调用密码卡生成一定数量的对称密钥和非对称密钥并存储，核查密钥存储状态和数量；

g) 验证密钥保护机制，能有效防止非法访问与泄露；

h) 验证权限控制机制，能有效防止非法使用和导出。

6.2.3.3 密钥导入及导出

检测要求：

a) 用户密钥对和设备密钥对的公钥应能被导出到密码卡外使用；

b) 会话密钥的导出应采用加密等安全方式实现；

c) 用户密钥和设备密钥的加密密钥对、密钥加密密钥、会话密钥的导入应采用加密等安全方式实现。

检测步骤：

a) 通过检测平台调用 API 接口导出内部存储的用户密钥对和设备密钥对的公钥，并使用导出的公钥进行运算验证；

b) 通过检测平台调用 API 接口，使用用户密钥或密钥加密密钥加密会话密钥，并成功导入导出会话密钥密文。

c) 用户密钥对和设备密钥对中的加密密钥对能通过 GM/T 0018 中规定的保护结构导入到密码卡中；

d) 若密钥加密密钥支持导入，应能以加密等安全方式正确导入，并使用导入的密钥加密密钥进行运算验证。

6.2.3.4 密钥使用及更新

检测要求：

a) 应采用访问控制技术控制内部存储密钥的访问和使用；用户密钥对和设备密钥对的私钥应具备私钥访问控制码的控制机制，防止非法使用，其访问控制码的设置应由密码卡管理工具完成，可采用口令方式，口令长度应不低于 8 字符，至少包含字母、数字及特殊字符中的两种；

b) 密码卡内部存储的密钥加密密钥和用户密钥对应以密钥索引号作为唯一标识进行调用，同时满足运算操作权限；

c) 会话密钥应支持一次会话更换一次；

d) 密码卡应支持多个用户密钥对的使用和操作；
e) 用户密钥对和密钥加密密钥应支持更新。

检测步骤：

a) 获取操作权限后，能对内部存储密钥进行访问和使用；未获取操作权限，对内部存储密钥的访问和使用应失败；
b) 获取操作权限后，检测平台调用 API 接口，使用正确的私钥访问控制码调用用户密钥的私钥进行算法运算，并返回成功；使用错误的私钥访问控制码调用用户密钥的私钥进行算法运算，应返回失败；
c) 获取操作权限后，检测平台调用 API 接口，应通过已生成的密钥加密密钥、用户密钥索引号进行正确的算法运算；
d) 检测平台调用 API 接口，建立多个会话，能成功产生会话密钥，对同一明文数据进行对称加解密运算，多个密文结果比较，结果应不一致；
e) 检测平台调用 API 接口，生成多个用户密钥对，根据不同密钥索引号，生成会话密钥并使用用户密钥公钥加密导出，并能成功导入会话密钥密文，使用对应的用户密钥私钥成功解密；
f) 操作管理工具成功，能正确有效地更新密码卡内部存储的用户密钥对和密钥加密密钥。

6.2.3.5 密钥备份及恢复

检测要求：

a) 应支持以密文等安全形式备份密码卡内部长期存储的用户密钥对和密钥加密密钥；
b) 应支持将备份的密钥恢复到密码卡；
c) 同厂商同型号的密码卡之间应支持互相备份恢复；
d) 备份恢复只能在密码卡内进行。

检测步骤：

a) 通过管理工具执行密钥备份操作，能成功地以密文形式备份；
b) 通过管理工具执行密钥恢复操作，能将其恢复到原密码卡或相同型号的密码卡中，对恢复密钥进行正确性验证。

6.2.3.6 密钥销毁

检测要求：

a) 密码卡内的密钥采用加密方式存储时，应对用于加密存储的密钥提供安全有效的销毁措施；
b) 对密码卡内以密文形式存储的密钥，在需要销毁时应提供安全有效的销毁措施；
c) 若密码卡采用微电保护措施存储密钥，应具备销毁密钥的触发装置，密码卡触发毁钥后，应立即清除微电保护存储的所有密钥，采用微电保护的密钥可以不加密；
d) 对出现在密码卡内密码运算部件中的明文密钥，使用完应及时销毁。

检测步骤：

a) 执行密码卡提供的密钥销毁操作，应成功销毁对应密钥并进行核查验证；
b) 若支持微电保护存储措施，应触发密钥销毁机制，核查验证密码卡应立即并有效地销毁微电保护存储的所有密钥。

6.2.4 随机数质量检测

检测要求：

a) 密码卡应至少采用两个独立的经密码检测认证具有物理噪声源功能的芯片生成随机数。随机数质量检测结果应符合 GM/T 0005。

b) 应支持随机数的上电/复位自检、使用自检(包括周期自检和单次自检)和接受指令后的自检,应符合 GM/T 0062 中的 D 类产品的检测要求;自检失败,应停止提供安全服务,进入错误状态,输出错误指示。

检测步骤:

a) 调用 API 生成随机数接口,采集 1 000 个 128 KB 大小的随机数文件;

b) 对所采集的随机数文件进行检测,检测结果应符合 GM/T 0005 的要求。

6.2.5 接口检测

6.2.5.1 应用接口检测

检测要求:

应用接口应符合 GM/T 0018,应以 API 库文件的形式提供给检测平台,当以动态链接库形式提供时,应提供至少一种操作系统环境下的动态库文件,操作系统类型和版本以检测平台为准。

检测步骤:

将 API 库文件安装在检测平台,成功加载和获取 GM/T 0018 中定义的各类函数接口,完成 API 初始化和接口测试。

6.2.5.2 物理接口检测

检测要求:

密码卡应至少具备 PCI、PCI-E、Mini PCI-E、SATA、USB、CPCI 或 M.2 等接口的一种,且物理接口能正常工作。

检测步骤:

应能通过物理接口接入检测环境,通过检测平台访问密码卡,实现初始化、密码算法、密钥管理、随机数、应用接口、管理安全和性能等检测。

6.2.6 管理安全检测

6.2.6.1 权限管理

检测要求:

密码卡应支持权限配置、访问控制配置等管理功能。应至少支持管理员,宜支持操作员。各角色应持有表征身份信息的硬件装置,如经密码检测认证的智能密码钥匙或智能 IC 卡等,宜与密码卡两部分硬件实体结合实现身份认证:

a) 管理员应能执行密码初始化、操作员管理、密钥管理和安全服务等功能;

b) 若支持操作员角色,操作员应能执行密码运算等安全服务。

检测步骤:

a) 登录管理员角色,成功执行密码初始化、操作员管理、密钥管理和安全服务等功能;

b) 若支持操作员角色,则登录操作员角色,成功且仅能执行密码运算等安全服务。

6.2.6.2 设备管理

密码卡如支持远程配置管理功能,宜符合 GM/T 0050 设备管理技术要求,支持或通过管理代理向上层管理应用提供设备管理应用接口。

6.3 性能检测

密码卡的性能检测应包括:密码卡随机数产生性能、对称密钥产生性能、非对称密钥对产生性能、对

称算法的加解密性能、非对称算法的加解密性能、非对称算法签名及验证性能、杂凑算法运算性能。

a) 随机数产生性能检测：密码卡生成并输出长度为 L（字节）的符合随机特性的随机序列，多线程（线程数 X）并行，连续执行 N 次，测量其完成时间 T（秒）。性能指标公式为：$S=8*L*X*N/(1\ 024*1\ 024*T)$；单位为 Mb/s。

b) 对称密钥产生性能检测：密码卡生成并输出密钥，多线程（线程数 X）并行，连续执行 N 次，测量其完成时间 T（秒）。性能指标公式为：$S=X*N/T$；单位为（组/秒）。

c) 非对称密钥对产生性能检测：密码卡生成并输出密钥对，多线程（线程数 X）并行，连续执行 N 次，测量其完成时间 T（秒）。性能指标公式为：$S=X*N/T$；单位为（对/秒）。

d) 对称算法加解密性能检测：将一个长度为 L（字节）的数据报文，发送给密码卡进行加/解密操作，多线程（线程数 X）并行，连续执行 N 次，测量其完成时间 T（秒）。需分别测对称算法所支持的各种工作模式的性能，性能指标公式为：$S=8*L*X*N/(1\ 024*1\ 024*T)$；单位为 Mbps。

e) 非对称算法加密/解密性能检测：将一个长度为 L 字节的数据报文，发送给密码卡进行加密/解密操作，多线程（线程数 X）并行，连续执行 N 次，测量其完成时间 T（秒）。性能指标公式为：$S=8*L*X*N/(1\ 024*1\ 024*T)$；单位为 Mbps。

f) 非对称算法签名/验证性能检测：将一个定长的数据报文，发送给密码卡进行签名/验证操作，多线程（线程数 X）并行，连续执行 N 次，测量其完成时间 T（秒）。性能指标公式为：$S=X*N/T$；单位为（次/秒）。

g) 杂凑算法运算性能检测：将一个长度为 L（字节）的数据报文，发送给密码卡进行摘要运算，多线程（线程数 X）并行，连续执行 N 次，测量其完成时间 T（秒）。性能指标公式为：$S=8*L*X*N/(1\ 024*1\ 024*T)$；单位为 Mb/s。

6.4 安全性检测

密码卡安全性检测应符合 GM/T 0039。

6.5 密码卡虚拟化检测

若密码卡支持虚拟化功能，不同的虚拟密码卡之间应实现密钥隔离、管理隔离、使用隔离等功能。密码卡能通过管理程序等方式，核查所支持虚拟密码卡的最大数量，虚拟密码卡应通过密码卡功能和性能检测要求。

7 送检技术文档要求

研制单位按照商用密码检测认证机构要求提交相关文档资料，作为密码卡的检测依据。

8 合格判定条件

本文件中，除 6.3 和 6.5 以外的各项检测中，其任意一项检测结果不合格，判定为产品不合格。