PCI密码卡技术规范

Technical Specification for PCI Cryptographic Module

国 家 密 码 管 理 局

2022年8月

目　次

前　　言 II
引　　言 IV
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　符号和缩略语 3
5　PCI密码卡概述 3
6　功能要求 4
6.1　密码运算功能 4
6.2　密钥管理功能 5
6.3　随机数生成和检验功能 6
6.4　设备标志信息存储功能 6
7　硬件要求 6
7.1　PCI 接口要求 7
7.2　硬件组成要求 7
7.3　环境要求 7
7.4　可靠性要求 7
7.5　电路原理图和印制版图要求 7
8　软件要求 8
8.1　底层软件 8
8.2　驱动程序 8
8.3　应用编程接口（API） 8
9　安全性要求 9
9.1　密码算法安全 9
9.2　产品安全 9
9.3　使用安全 9
10　检测要求 9
10.1　硬件检测 9
10.2　功能检测 10
10.3　性能检测 10
10.4　算法正确性检测 11
10.5　安全性检测 11
附录 A （规范性附录） PCI密码卡产品检测专用API函数集 13

前　言

本规范是国家密码管理局提出并制定的系列规范之一。本规范制定了PCI密码卡的技术规范，为信息安全基础设施PCI密码卡的研制和开发提供指导和依据。

本规范的附录A为规范性附录。附录A为 PCI密码卡产品检测专用API函数集。

本规范由国家密码管理局提出并归口。

本规范起草单位：国家密码管理局商用密码检测中心、成都卫士通信息产业股份有限公司、无锡江南计算机技术研究所、兴唐通信科技股份有限公司、济南得安计算机技术有限公司。

本规范主要起草人：霍卫华、徐强、高志权、李玉峰、陈妍。

本规范责任专家：刘平。

本规范凡涉及密码算法相关内容，按国家密码有关管理法规实施。

引　言

本规范的目标是为信息安全基础设施PCI密码卡设备制定统一的功能要求、硬件要求、软件要求（含应用接口要求）、安全性要求（含密钥结构）、检测要求等有关内容，通过统一的API函数集调用PCI密码卡设备，向上层提供基础密码服务，实现不同生产厂商的PCI密码卡设备互操作，方便应用。为该类密码设备的开发、使用及检测提供标准依据和指导，有利于提高该类密码设备的产品化、标准化和系列化水平。

本规范编制过程中得到了国家商用密码应用技术体系总体工作组的指导。

PCI密码卡技术规范

1 范围

本规范规定了PCI密码卡的功能要求、硬件要求、软件要求（含应用接口要求）、安全性要求（含密钥结构）、检测要求等有关内容。

本规范适用于PCI密码卡的研制设计、应用开发，也可用于指导PCI密码卡的使用和检测。

2 规范性引用文件

下列标准所包含的条文，通过本规范中的引用而构成为本规范的条文。在标准出版时，所示版本均为有效。考虑到标准的修订，使用本规范时，应研究使用下列标准最新版本的可能性。

GB/T 9813.4　计算机通用规范 第4部分：工业应用微型计算机

GB/T 17964　信息安全技术 分组密码算法的工作模式

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 0028　密码模块安全技术要求

GM/T 0062　密码产品随机数检测要求

GM/Z 4001　密码术语

ISO/IEC 7816-3　Electronic signals and transmission protocols

3 术语和定义

GM/Z 4001界定的以及以下术语和定义适用于本规范。

3.1

算法标识 algorithm identifier

用于对密码算法进行唯一标识的符号。

3.2

大端字节序 big-endian

也称网络字节序，指内存的低地址存放最高有效字节（MSB），即常说的高位在先，低位在后。

3.3

非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）必须保密，且由公钥求解私钥是计算不可行的。

3.4

解密 decipherment/decryption

加密过程对应的逆过程。

3.5

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。

3.6

数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果， 该结果只能用签名者的公钥进行验证， 用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

3.7

加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。

3.8

密码杂凑算法 hash algorithm

又称杂凑算法、密码散列算法或哈希算法。该算法将一个任意长的比特串映射到一个固定长的比特串，且满足下列三个特性：

（1）为一个给定的输出找出能映射到该输出的一个输入是计算上困难的；

（2）为一个给定的输入找出能映射到同一个输出的另一个输入是计算上困难的；

（3）要发现不同的输入映射到同一输出是计算上困难的。

3.9

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。

3.10

小端字节序 little-endian

指内存的低地址存放最低有效字节（LSB），即常说的低位在先，高位在后。

3.11

消息鉴别算法 MAC algorithm

使用密码算法计算消息鉴别码的计算方法，可用于数据完整性的鉴别。

3.12

PCI密码卡 PCI cryptographic module

以PCI/PCI-E总线接口与相关设备相连接的、能够独立提供密码服务和密钥管理功能的板卡设备。

3.13

PCI Express

PCI Express是PCI局域总线的改进版，是一种高性能的局域I/O总线互连技术，保持PCI软件的使用模型并使用具有多通路高速的串行总线替代物理总线。

3.14

PCI局部总线 PCI local bus

PCI是Peripheral Component Interconnect的英文缩写，其含义为外设部件互连。PCI局部总线是和外设部件相连接的一种结构化总线，其特点是：传输带宽高、兼容性强、扩展性好。

3.15

私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

3.16

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。

3.17

公钥 public key

非对称密码算法中可以公开的密钥。

3.18

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。

3.19

会话密钥 session key

在一次会话中使用的数据加密密钥。

3.20

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。

3.21

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。

4 符号和缩略语

下列缩略语适用于本部分：

PCI	外设部件互连，是一种密码设备的硬件实体
PCI Express	PCI局域总线的改进版，是一种高性能的局域I/O总线互连技术IC集成电路
DMA	直接存储器访问
API	应用编程接口
RSA	一种公开的密钥密码体制，它由三个发明者名字的首字母缩写
ECC	椭圆曲线算法（Elliptic Curve Cryptography）
ECB	电码密本链接模式（Electronic Code Book）
CBC	密码分组链接模式（Cipher Block Chaining）
CFB	密文反馈链接模式（Ciphertext Feedback）
OFB	输出反馈链接模式（Output Feedback）
Hash	杂凑算法，又称散列函数算法
MAC	消息鉴别码（Message Authentication Code）

5 PCI密码卡概述

PCI密码卡是以PCI局部总线或者PCI Express为接口，具有密码运算功能、密钥管理功能、物理随机数产生功能和设备自身安全保护措施的密码设备。

PCI密码卡可以应用在需要密码运算和密钥管理等安全功能的、具有PCI局部总线或者PCI Express的通信设备、计算机设备、安全保密设备上，例如：虚拟专网（VPN）设备、证书中心（CA）系统的有关设备、网络密码机、安全服务器、安全终端、安全管理中心、密钥管理设备等。

6 功能要求

在本规范中，PCI密码卡的功能包括两类，分别是基本功能和扩展功能：

1) 基本功能，主要包括：a.密码运算功能，包括对称密码算法、非对称密码算法和杂凑算法；b.密钥管理功能；c.两级密钥结构体制（用户密钥对或密钥加密密钥、对称密码算法的会话密钥）的支持功能；d.真随机数生成和检验功能；e.密码卡内部敏感数据信息的安全保护功能等。
2) 扩展功能，是在基本功能的基础上，根据应用需要进行合理的扩充和增添的功能，包括:a.非对称密码算法可选择支持RSA算法或者ECC算法中的任意一种；b.三级密钥结构体制的支持功能（在两级密钥结构体制的基础上引入设备保护密钥）；c.除了应支持的对称密码算法、非对称密码算法和杂凑算法之外的其他密码运算功能等；d.密码卡内部的文件存储管理功能。

6.1 密码运算功能

PCI密码卡应支持对称密码算法、非对称密码算法和杂凑算法，在适当的驱动条件下完成相应的密码算法运算。PCI密码卡中的密码算法应为符合国家密码管理要求的密码算法。

6.1.1 对称密码算法

PCI密码卡应至少支持一种对称密码算法，如分组密码算法、序列密码算法。数据加解密算法、敏感数据信息保护算法、消息鉴别算法均可采用对称密码算法来实现。

6.1.2 分组密码算法的链接模式

PCI密码卡提供的分组密码算法应支持ECB和CBC两种链接模式，其他链接模式（例如CFB、OFB等）作为扩展功能选择支持。

分组密码的工作方式的实现应与GB/T 17964中的描述相一致。

6.1.3 杂凑算法

PCI密码卡应至少支持一种杂凑算法。

6.1.4 非对称密码算法

数字签名、签名验证、密钥安全存储管理等可采用非对称密码算法来实现。对非对称密码算法的基本要求为：

1) 非对称密码算法应至少支持一种；
2) 选择支持RSA算法时，应具备2048比特及以上的模长；
3) 选择支持ECC算法时，应具备256比特及以上的模长；
4) 应提供数字签名和签名验证功能；
5) 选择支持ECC算法时，PCI密码卡应提供ECC密钥协商生成会话密钥功能。

6.1.5 扩展密码算法

PCI密码卡只在需要时才选择支持扩展密码算法。

6.2 密钥管理功能

PCI密码卡宜具有IC卡接口或者USB接口。通过将PCI密码卡、IC卡或者USBKey两部分硬件实体结合起来，完成用户身份认证功能。只有通过用户身份认证的用户方可使用PCI密码卡提供的密钥管理服务。IC卡或者USBKey可以作为公开密钥、私钥、密钥加密密钥、用户签名信息、证书信息或其他敏感数据信息的载体。

IC卡的类型为智能IC卡；配用的智能IC卡或者USBKey应通过密码检测认证。

6.2.1 密钥的种类和作用

PCI密码卡应至少支持两级密钥结构体制：一级是用户密钥对或者密钥加密密钥，一级是会话密钥。这种密钥结构体制支持基于PCI密码卡的设备或应用系统实现端到端的数据安全保护、一次一密以及相应的密钥管理等安全服务。其中，用户密钥对或者密钥加密密钥选择支持任意一种，也可选择支持两种。

此外，作为硬件设备自身的维护管理，选择支持设备密钥对。

1) 设备密钥对

分加密密钥对和签名密钥对两种，选择支持RSA算法或者ECC算法的任意一种；用于实现数字签名、签名验证等功能；其中，私钥应受私钥访问控制码的安全访问控制。

2) 用户密钥对

分加密密钥对和签名密钥对两种，选择支持RSA算法或者ECC算法的任意一种；用于实现用户数字签名、签名验证以及会话密钥的安全保护等功能；其中，私钥应受私钥访问控制码的安全访问控制。

3) 密钥加密密钥

长度不低于128比特，用于实现会话密钥的安全保护功能。

4) 会话密钥

长度不低于128比特，用于用户数据加解密运算，或者作为其他应用系统密钥的加密保护密钥。

在上述两级密钥结构体制的基础上，选择支持增加第三级密钥，即保护密钥，作为用户密钥对或者数据加密密钥的安全存储保护密钥。

6.2.2 密钥的产生及存储

1) 设备密钥对

由设备初始化时使用的管理工具生成或者安装，存储在PCI密码卡硬件内部。

2) 用户密钥对

由密码设备管理工具生成或者安装；根据系统需要应支持一定数量用户密钥对的存储区域；用户密钥对的私钥应支持硬件内部安全存储，应支持私钥访问控制码的安全访问控制。

3) 密钥加密密钥

由密码设备管理工具生成或者安装，应支持具有物理噪声源功能的芯片生成；根据系统需要应支持一定数量密钥加密密钥的存储区域；该密钥应支持硬件内部安全存储。

4) 会话密钥

应支持使用具有物理噪声源功能的芯片生成，以确保会话密钥的质量；应支持一次会话更换一次会话密钥；不得以明文方式导出硬件；在会话密钥长期存储时，应支持用户密钥对或者密钥加密密钥加密存储等安全保护措施。

此外，对于支持非对称密码算法运算的PCI密码卡，应支持非对称密钥对的生成功能，应支持使用具有物理噪声源功能的芯片生成，应支持使用强素数。

6.2.3 密钥的使用及更换

1) 设备密钥对

定期更换不作具体规定。

2) 用户密钥对

用于用户数字签名、签名验证运算，或者作为会话密钥的加密保护密钥对；定期更换由密码设备管理工具完成，这里不作具体规定。

3) 密钥加密密钥

作为会话密钥的加密保护密钥；定期更换由密码设备管理工具完成，这里不作具体规定。

4) 会话密钥

用于用户数据加解密运算，或者作为其他应用系统密钥的加密保护密钥；在会话密钥用于用户数据的加解密运算时，应支持经常更换会话密钥，以确保用户数据加解密运算的安全性；每次会话中使用的会话密钥不相同，应支持一次会话更换一次会话密钥。

6.2.4 密钥的销毁

1) 设备密钥对

密钥销毁不作具体规定。

2) 用户密钥对

应提供紧急销毁的安全保护措施，以确保PCI密码卡自身的安全性。

3) 密钥加密密钥

应提供紧急销毁的安全保护措施，以确保PCI密码卡自身的安全性。

4) 会话密钥

应支持会话密钥的销毁，以确保用户数据加解密运算的安全性。

6.2.5 密钥的备份及恢复

1) 设备密钥对

由设备初始化时使用的管理工具完成，这里不作具体规定。

2) 用户密钥对

由密码设备管理工具完成，这里不作具体规定。

3) 密钥加密密钥

由密码设备管理工具完成，这里不作具体规定。

4) 会话密钥

由上层应用系统进行统一管理，这里不作具体规定。

6.3 随机数生成和检验功能

PCI密码卡应至少采用两个独立的具有物理噪声源功能的芯片生成随机数，具有物理噪声源功能的芯片应通过密码检测认证。PCI密码卡应支持对其生成的随机数进行统计检验，以保证其质量。随机数检验参照GM/T 0062中D类产品的检测要求。

6.4 设备标志信息存储功能

PCI密码卡应具有唯一的设备标志信息，以区分不同厂家、不同型号的PCI密码卡。设备标志信息包括以下几个部分：生产厂商、设备类型、序列号、硬件版本、软件版本、支持算法等。密码检测认证机构和用户可以通过这些信息来查验和辨识PCI密码卡。设备标志信息通过GM/T 0018中的函数SDF_GetDeviceInfo获取。

7 硬件要求

7.1 PCI接口要求

7.1.1 PCI接口规范

符合PCI或者PCI Express规范；考虑到总线规范的不断扩展修订，使用本规范时，应研究使用最新版本规范的可能性。

7.1.2 数据总线

采用PCI局域总线的PCI密码卡，其总线采用32位或者64位数据总线；采用PCI Express 规范的PCI密码卡，其总线采用多通路高速的串行总线；采用存储器方式或I/O端口方式进行访问。

基于x86及其兼容平台的PCI密码卡，总线排序方式采用Little-Endian模式；基于PowerPC及其兼容平台的PCI密码卡，总线排序方式采用Big-Endian模式。

7.1.3 通信方式

数据通信可采用查询方式或中断通信方式。

7.1.4 数据传输

采用DMA传输方式或其他方式。

7.1.5 电源

采用PCI局域总线的PCI密码卡可以工作于单一的“＋5V”电压、单一“＋3.3V”电压或两种混合电压环境；采用PCI Express规范的PCI密码卡可工作于“＋3.3V”和“＋12V”电压环境。

7.2 硬件组成要求

PCI密码卡的基本硬件组成包括以下几种部件：密码算法模块、处理器（DSP或CPU）、物理噪声源、非易失性存储器、IC卡接口或者USB接口、PCI桥接芯片或者PCI Express桥接芯片等。

在具体实现中，以上部件不一定独立存在于PCI密码卡中，但上述部件所具有的功能是必不可少的。随着技术的不断发展，不排除多个部件集成于一体的可能性。

IC卡接口应该遵循ISO/IEC 7816-3《Electronic signals and transmission protocols》中的有关规定。

7.3 环境要求

PCI密码卡的工作温度和工作相对湿度应符合GB/T 9813.4中4.8.2关于“气候环境适应性”级别1的规定要求。

7.3.1 工作温度

0℃～45℃。

7.3.2 工作相对湿度

20%～80%。

7.4 可靠性要求

PCI密码卡的可靠性指标采用平均无故障工作时间（MTBF）来衡量。PCI密码卡的平均无故障工作时间由组成密码卡的各个部件的可靠性决定。

PCI密码卡的平均无故障工作时间MTBF应大于10,000小时。

7.5 电路原理图和印制版图要求

PCI密码卡电路原理图、方框图和印制版图的设计和标注应准确清晰。

8 软件要求

PCI密码卡软件设计采用分层设计的方法。PCI密码卡的软件分为三个层次：底层软件（监控软件）、驱动程序和应用编程接口。为了保证软件部分的安全性和可扩展性，本节对各个层次的实现提出原则性的约束。

8.1 底层软件

8.1.1 模块化设计

底层软件采用模块化设计，以保证不同版本之间模块的向后兼容性。

8.1.2 随机数检验

由具有物理噪声源功能的芯片产生的随机序列应至少通过几项基本的随机性（如0和1的平衡性、连长特性等）检验，以确保其等概性和不可预测性，随机数检验的质量标准参照GM/T 0005。只有通过检验的随机序列才可用作随机密钥。

8.1.3 其他要求

底层软件应通过技术措施，防止用户的非法调用，防止系统“死机”。

8.2 驱动程序

8.2.1 透明传输

驱动程序应透明传输应用系统和PCI密码卡缓存区之间的数据，不得截获、解析应用系统的数据结构。

8.2.2 安装/卸载

应支持安装/卸载驱动程序。

8.2.3 多设备支持要求

驱动程序应该支持多个PCI密码卡设备同时使用和操作的基本要求。

8.3 应用编程接口（API）

8.3.1 字节顺序

在不同型号的PCI密码卡之间加解密互通传输时，为避免因字节顺序差异带来的影响或错误，这里定义数据的存储顺序和传输顺序按照大端字节序（big-endian）进行处理。

下面举例说明，数据0x12345678，其对应的大端字节序存储顺序如图1所示。

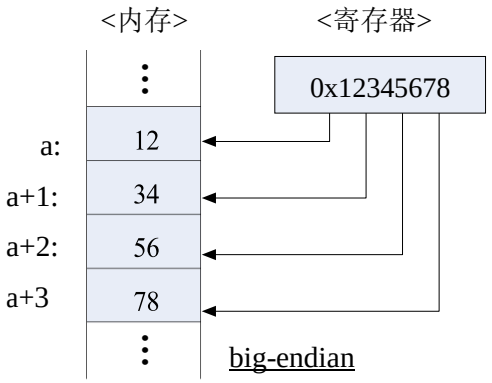

图 1 大端字节序存储示意图

8.3.2 应用编程接口（API）的目标模块

应用编程接口（API）以目标模块方式提供给用户，作为PCI密码卡用户应用系统和驱动程序之间的接口。目标模块可以是动态库、静态库或其他二进制目标代码形式，不经主管部门批准不可将源代码直接提供给用户。PCI密码卡生产厂家应对应用编程接口给出详细具体的使用说明，不得泄漏密码算法的细节和与使用无关的密钥管理的细节。

应用编程接口应遵循GM/T 0018。

8.3.3 多个私钥的支持

在PCI密码卡硬件内部选择支持多个公私钥对，应用编程接口应支持对多个公私钥对的使用和操作。

8.3.4 API函数集

PCI密码卡的API函数集定义应遵循GM/T 0018，产品检测专用函数参照附录A。

9 安全性要求

9.1 密码算法安全

应采用硬件部件实现符合国家密码管理要求的密码算法，宜采用通过检测认证的密码算法芯片、安全芯片、密码模块作为主要密码部件。

9.2 产品安全

PCI密码卡的产品安全性应遵循GM/T 0028的要求。

9.3 使用安全

基于本规范设计、开发的PCI密码卡在使用方面，应满足以下要求：

1) PCI密码卡应支持初始状态和就绪两个状态；
2) 未安装设备密钥对或用户密钥对或密钥加密密钥的PCI密码卡处于初始状态，已安装设备密钥对或用户密钥对或密钥加密密钥的PCI密码卡处于就绪状态；
3) 在初始状态下，除可读取硬件设备信息操作外，不能执行任何安全服务操作，在使用密码设备管理工具完成生成（或恢复）用户密钥对或者密钥加密密钥后，PCI密码卡就处于就绪状态；
4) 在就绪状态下，能执行与PCI密码卡硬件设备相关的安全服务操作；
5) 在就绪状态下，进行硬件存储用户密钥对的私钥操作前，应通过私钥访问控制码的安全认证。

10 检测要求

生产厂商研制生产的PCI密码卡在投入使用前应按照本规范规定的检测要求进行各项检测，检测要求规定了PCI密码卡的硬件检测、功能检测、性能检测、算法正确性检测和安全性检测等内容。

10.1硬件检测

10.1.1安装检测

PCI密码卡能正确地安装到系统的对应插槽中，其设备驱动程序在指定的操作系统中能够正确地安装和卸载。

10.1.2初始化测试

PCI密码卡出厂时处于初始状态，通过使用密码设备管理工具完成生成（或恢复）用户密钥对或者密钥加密密钥后，PCI密码卡能正确完成初始化操作，处于就绪状态。

10.1.3硬件上电自检

PCI密码卡在开机上电后应支持进行硬件自检，自检结果可以用硬件的方式给出指示；未通过上电自检，PCI密码卡应拒绝一切密码功能调用服务。上电自检应完成以下项目：

1) 物理噪声源是否失效。采集具有物理噪声源功能的芯片产生的随机数，然后进行随机性检测；
2) 密码运算单元是否失效。对特定的数据进行密码运算，检查计算结果与预知结果是否一致；
3) 静态存储数据的完整性是否被破坏。对静态存储数据计算数据的杂凑值，将计算结果与预知结果作比较；
4) 其它需要进行自检的功能部件是否工作正常。

10.2功能检测

PCI密码卡的功能检测主要通过GM/T 0018中定义的API函数集,并结合附录A的产品检测专用API函数进行访问检测。这部分测试程序由检测机构提供。API函数接口库由PCI密码卡的研制单位提供。对于正确的调用环境和调用过程，调用API函数接口应该返回正确的结果，并完成相应功能；对于设定的不正确的调用环境和调用过程，调用API函数接口应返回相应的错误代码。

10.2.1密码运算功能检测

测试程序对PCI密码卡支持的对称密码算法、非对称密码算法和杂凑算法进行基本运算检测，检测其运算的功能正确性。

10.2.2密钥管理检测

测试程序对于具有对称密码算法密钥管理功能和非对称算法密钥管理功能的PCI密码卡，通过制定测试项依次检测其生成密钥、保护导入密钥、保护导出密钥以及销毁密钥等功能项进行功能正确性检测。

10.2.3物理随机数检测

测试程序通过调用API函数接口,PCI密码卡生成并输出指定长度的比特流作为测试样本。将测试样本输入测试程序进行随机性统计特性测试。

10.2.4密码卡内敏感数据的安全保护检测

对硬件存储和使用敏感数据的实现正确性进行检测，并进行相关的抗攻击性实验。

10.3性能检测

目的是测试PCI密码卡进行各项密码运算的速度指标。每次测试应具有足够的数据量，保证PCI密码卡进入稳定工作期，防止性能波动。本节没有规定对PCI密码卡进行速度性能检测的具体操作系统。对于特殊的操作系统，应进行单独测试。

下列各项速度性能测试中的测试量由数据报文长度和测试次数决定。可以根据各个测试项的具体耗时情况，依照等比序列来选取测试次数，例如：测试次数N可以选择1次、10次、100次、1000次…等，分别测试后得到不同测试次数时的性能序列。数据报文长度的选择在各个速度性能测试项中分别定义。

在10.3.1、10.3.3中包含的各个测试项和10.3.2中的加解密性能的计算如下式所示：

$$S = 8LN/(1024\times1024T)$$

其中，S为速度，单位为Mbps(兆比特/秒)；L为数据报文的长度，单位为字节；N为测试次数；T为测量所耗费的时间，单位为秒。

在10.3.2中签名、验签性能的计算如下式所示：

$$S = N/T$$

其中，S为速度，单位为tps（次/秒）；N为测试次数；T为测量所耗费的时间，单位为秒。

10.3.1对称密码算法的加解密性能测试

将内存中的一个定长数据报文，发送给PCI密码卡进行对称密码算法的加密和解密操作，重复操作N次，测量其完成时间T。用于测试的数据由检测机构选取。测试应进行多次，结果取平均值。如PCI密码卡支持对称算法的多种工作模式，应测试所支持的各种工作模式，如：ECB、CBC、CFB、OFB等都进行测试。并且应对所支持的所有使用方式（如加密、解密等）进行逐一测试。

取不同长度的数据报文分别进行测试，并记录结果。下列典型长度的数据报文应进行测试：一个分组长度、64字节、128字节、256字节、512字节、1024字节、2048字节、4096字节、10240字节以及PCI密码卡研制单位建议的长度。

10.3.2非对称密码算法的运算性能测试

将内存中的一个定长数据报文，发送给PCI密码卡进行非对称密码算法的运算操作，重复操作N次，测量其完成时间T。用于测试的数据由检测机构选取。测试应进行多次，结果取平均值。如PCI密码卡支持多种非对称算法，应测试所支持的所有非对称密码算法及其各种应用模式，如：RSA、ECC等算法的加密、解密、签名、验证等。

10.3.3杂凑算法性能测试

将内存中的一个定长数据报文，发送给PCI密码卡进行杂凑运算，重复操作N次，测量其完成时间T。用于测试的数据由检测机构选取。测试应进行多次，结果取平均值。

取不同长度的数据报文分别进行测试，并记录结果。下列典型长度的数据报文应进行测试：一个分组长度、64字节、128字节、256字节、512字节、1024字节、2048字节、4096字节、10240字节以及PCI密码卡研制单位建议的长度。

10.3.4非对称密钥对生成性能测试

让PCI密码卡生成并输出指定数量的密钥对，测量其完成时间。测试应进行多次，结果取平均值。

10.4算法正确性检测

通过测试程序，使用PCI密码卡对已知相应正确结果的数据执行密码运算，然后比较计算结果和预知结果。如果计算结果和预知结果相同，则测试通过；否则，测试失败。密码算法实现正确性测试应测试PCI密码卡提供的每个对称和非对称密码算法的每个功能函数，如：加密、解密、杂凑、签名、验证等。如PCI密码卡支持算法的多种工作模式，应测试所有支持的工作模式，如：ECB、CBC、CFB、OFB等。

此外，对于具有ECC运算及其密钥管理的PCI卡，通过测试程序，与其他生产厂商研制的PCI密码卡进行ECC密钥协商互通测试，检测其正确性。

10.5安全性检测

通过测试程序，对初始状态的PCI密码卡进行密码运算功能检测，应检测失败；对就绪状态的PCI密码卡进行密码运算功能检测，应检测成功。

通过测试程序，对错误的私钥访问控制码，应检测失败；对正确的私钥访问控制码，应检测

成功。

通过测试程序，对错误的用户IC卡或者USBKey，应检测失败；对正确的用户IC卡或者USBKey，应检测成功。

附 录 A

（规范性附录）

PCI密码卡产品检测专用API函数集

PCI密码卡产品检测专用API函数集以动态库方式提供，可用于产品研制单位自测试和检测机构检测，也可用于采用PCI密码卡的密码设备在研制开发中的调试验证。

PCI密码卡产品检测专用API函数中密钥结构、算法标识等参数参考GM/T 0018定义，包括以下具体函数：

功能说明	函数名
导入明文会话密钥	SDF_ImportKey
外部私钥RSA运算	SDF_ExternalPrivateKeyOperation_RSA
外部密钥ECC签名	SDF_ExternalSign_ECC
外部密钥ECC私钥解密	SDF_ExternalDecrypt_ECC

检测专用函数 1：导入明文会话密钥

原型：
```
int SDF_ImportKey (
      void *hSessionHandle,
      unsigned char *pucKey,
      unsigned int uiKeyLength,
      void **phKeyHandle);
```
描述：导入明文会话密钥，同时返回密钥句柄

参数：

	hSessionHandle[in]	与设备建立的会话句柄
	pucKey[in]	缓冲区指针，用于存放输入的密钥明文
	puiKeyLength[in]	输入的密钥明文长度
	phKeyHandle[out]	返回的密钥句柄
返回值：	0	成功
	非 0	失败，返回错误代码

检测专用函数 2：外部私钥RSA运算

原型：
```
int SDF_ExternalPrivateKeyOperation_RSA(
      void *hSessionHandle,
      RSArefPrivateKey *pucPrivateKey,
      unsigned char *pucDataInput,
      unsigned int  uiInputLength,
      unsigned char *pucDataOutput,
      unsigned int  *puiOutputLength);
```
描述：指定使用外部私钥对数据进行运算

参数：

	hSessionHandle[in]	与设备建立的会话句柄
	pucPrivateKey [in]	外部RSA私钥结构
	pucDataInput [in]	缓冲区指针，用于存放输入的数据
	uiInputLength [in]	输入的数据长度
	pucDataOutput [out]	缓冲区指针，用于存放输出的数据
	puiOutputLength [out]	输出的数据长度
返回值：	0	成功

非 0　　失败，返回错误代码

备注：　数据格式由应用层封装

检测专用函数 3：外部密钥ECC签名

原型：　int SDF_ExternalSign_ECC(
　　void *hSessionHandle,
　　unsigned int uiAlgID,
　　ECCrefPrivateKey *pucPrivateKey,
　　unsigned char *pucData,
　　unsigned int uiDataLength,
　　ECCSignature *pucSignature);

描述：　使用外部ECC私钥对数据进行签名运算

参数：　hSessionHandle[in]　　与设备建立的会话句柄
　　uiAlgID[in]　　算法标识，指定使用的ECC算法
　　pucPrivateKey[in]　　外部ECC私钥结构
　　pucData[in]　　缓冲区指针，用于存放外部输入的数据
　　uiDataLength[in]　　输入的数据长度
　　pucSignature[out]　　缓冲区指针，用于存放输出的签名值数据

返回值：　0　　成功
　　非 0　　失败，返回错误代码

备注：　对原文的杂凑运算，在函数外部完成。

检测专用函数 4：外部密钥ECC私钥解密

原型：　int SDF_ExternalDecrypt_ECC(
　　void *hSessionHandle,
　　unsigned int uiAlgID,
　　ECCrefPrivateKey *pucPrivateKey,
　　ECCCipher *pucEncData,
　　unsigned char *pucData,
　　unsigned int *puiDataLength);

描述：　使用外部ECC私钥进行解密运算

参数：　hSessionHandle[in]　　与设备建立的会话句柄
　　uiAlgID[in]　　算法标识，指定使用的ECC算法
　　pucPrivateKey[in]　　外部ECC私钥结构
　　pucEncData[in]　　缓冲区指针，用于存放输入的数据密文
　　pucData[out]　　缓冲区指针，用于存放输出的数据明文
　　puiDataLength[out]　　输出的数据明文长度

返回值：　0　　成功
　　非 0　　失败，返回错误代码