ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0124—2022

安全隔离与信息交换产品密码检测规范

Cryptography test specification for secure separation and information exchange product

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、奇安信网神信息技术（北京）股份有限公司、南瑞集团有限公司、北京安盟信息技术股份有限公司。

本文件主要起草人：孙浩、燕爽、邓开勇、李冬、李国友、杨维永、朱孟江、唐磊、张璐、张大伟、韩斐、刘智飞。

安全隔离与信息交换产品
密码检测规范

1 范围

本文件规定了安全隔离与信息交换产品的密码检测内容、检测要求、检测方法及文档要求。

本文件适用于安全隔离与信息交换产品的检测，以及该类产品的研制。

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 15843（所有部分） 信息技术 安全技术 实体鉴别

GB/T 20279—2015 信息安全技术 网络和终端隔离产品安全技术要求

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 32915 信息安全技术 二元序列随机性检测方法

GB/T 32918（所有部分） 信息安全技术 SM2 椭圆曲线公钥密码算法

GM/T 0062 密码产品随机数检测要求

GM/Z 4001—2013 密码术语

3 术语和定义

GM/Z 4001 界定的及以下术语和定义适用于本文件。

3.1

安全隔离与信息交换产品 secure separation and information exchange product

能够保证不同网络之间在网络协议终止的基础上，通过安全通道在实现网络隔离的同时进行安全数据交换的软硬件组合。

3.2

安全域 security domain

具有相同的安全保护需求和相同的安全策略的计算机或网络区域。

3.3

安全等级 security level

网络隔离与信息交换产品的安全等级划分为基本级和增强级。

4 检测内容

4.1 概述

安全隔离与信息交换产品检测的主要内容包括 12 项：

a） 产品外观及结构检查；
b） 产品管理功能检查；
c） 产品状态检测；
d） 产品自检检测；
e） 产品配置管理检测；
f） 产品密码算法正确性与一致性检测；
g） 产品随机数质量检测；
h） 产品角色鉴别检测；
i） 产品密钥管理检测；
j） 产品日志审计检测；
k） 产品功能检测；
l） 产品性能检测。

典型的运行环境见图 1。

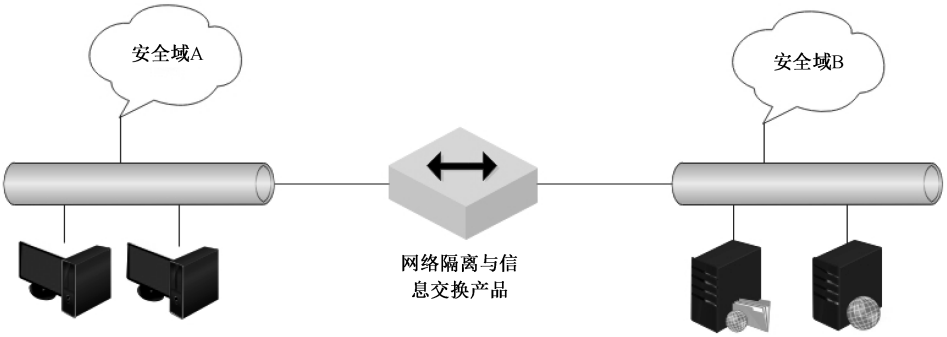

图 1 安全隔离与信息交换产品典型运行环境

4.2 产品外观及结构检查

4.2.1 检测要求

检测要求如下：

a） 产品应具备以下主要部件或接口：
   1） 应具备内部处理单元、外部处理单元和专用隔离部件；
   2） 应支持状态指示灯，可识别产品正常工作状态和故障状态；
   3） 应支持电源指示灯，可识别产品是否上电。
b） 产品宜具备以下主要部件或接口：
   1） 宜支持最少 4 个 RJ45 网络接口；
   2） 宜支持 2 个串口(RJ45 或 DB9 形态)作为管理控制口；
   3） 宜支持冗余电源。

4.2.2 检测方法

根据产品的物理参数对产品的外观、尺寸、内部部件及附件进行检查。

4.3 产品管理功能检查

4.3.1 检测要求

产品应使用与工作接口独立的管理接口进行产品管理，管理界面宜支持以下主要管理功能：

a) 产品的安装及初始化、系统启动和关闭、备份和恢复功能；
b) 产品双机热备或负载均衡等可用性参数设置；
c) 若产品支持远程管理，应有关闭远程管理接口的能力，应限制可进行远程管理的地址，应通过建立安全通道方式开展远程管理，安全通道采用的密码协议应符合国家密码管理相关规定；
d) 产品状态查询功能管理，包括产品配用算法、密钥管理、硬件密码部件状态等查询；
e) 日志管理管理功能，包括日志记录、日志查询和日志导出等。

4.3.2 检测方法

通过产品管理界面检查产品支持的管理功能。

4.4 产品状态检测

4.4.1 检测要求

产品宜具备初始状态和就绪状态，且只能由初始状态向就绪状态转换。

4.4.2 检测方法

检测方法如下。

a) 产品首次加电启动后进入初始状态，此时产品不能为两个安全域提供隔离服务；产品完成自检并由管理员对网络配置、交换策略、安全策略等进行配置后，进入就绪状态。
b) 产品完成初始化配置，加电启动并经过产品自检后，进入就绪状态并提供隔离服务。

4.5 产品自检检测

4.5.1 检测要求

检测要求如下。

a) 产品应支持自检功能，应包括密码算法正确性、随机数质量、鉴别数据、密钥和信息传输策略(安全属性)完整性自检等。其中，随机数质量自检应符合 GM/T 0062 E 类产品的要求。
b) 产品应支持上电自检、周期自检和条件自检功能。

4.5.2 检测方法

检测方法如下。

a) 产品上电后，自动执行上电自检。自检成功，产品自动进入就绪状态；自检失败，产品记录日志并告警。
b) 产品在运行过程中，按设定的周期自动执行周期自检。如果自检失败，产品记录日志并告警。
c) 产品在运行过程中根据条件进行自检。如果自检失败，产品记录日志并告警。

4.6 产品配置管理检测

4.6.1 检测要求

检测要求如下。

a) 产品应包含但不限于产品权限配置、网络配置、访问控制配置等管理功能。
b) 权限配置宜具备：
   1) 支持 2 个串口(RJ45 或 DB9 形态)作为管理控制口；
   2) 支持冗余电源；
   3) 设置管理员、安全员、审计员三类角色；管理员负责安装及初始化、系统启动和关闭、备份和恢复、状态管理及角色的添加、修改和删除；安全员负责产品网络配置、双机热备或负载

均衡等可用性参数、产品访问控制配置等；审计员负责日志审计。

c） 网络配置宜具备通信接口和管理接口 IP 地址、掩码及端口配置。

d） 访问控制配置宜具备 IP 地址访问控制授权表配置。

4.6.2 检测方法

根据产品的物理参数对产品的外观进行检查，通过产品管理界面检查产品的权限配置、网络配置、访问控制配置功能。

4.7 产品密码算法的正确性和一致性检测

4.7.1 密码算法要求

产品使用的密码算法应由密码模块提供，密码模块应经国家商用密码认证机构认证。

4.7.2 对称密码算法的正确性和一致性

4.7.2.1 检测要求

产品如使用对称密码算法，应支持 SM4 密码算法，其实现应符合 GB/T 32907；产品应能使用 SM4 算法对数据进行加解密运算，应能支持给定密钥和明文（密文），检测其运算结果的正确性。

4.7.2.2 检测方法

检测方法如下：

a） 产品对给定的密钥和明文经 SM4 算法加密，结果与给定的密文完全相同；

b） 产品对给定的密钥和密文经 SM4 算法解密，结果与给定的明文完全相同。

4.7.3 非对称密码算法的正确性和一致性

4.7.3.1 检测要求

产品如使用非对称密码算法，应支持 SM2 密码算法，其实现应符合 GB/T 32918（所有部分）；产品应能使用 SM2 算法对数据进行加解密、签名/验签等运算，应能支持给定密钥和明文（密文），检测其运算结果的正确性。

4.7.3.2 检测方法

支持 SM2 算法的加解密运算时：

a） 产品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，解密结果与给定明文完全相同；

b） 产品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，解密结果与给定明文完全相同。

支持 SM2 算法的签名/验签运算时：

a） 产品使用给定的密钥对待签名消息调用密码算法签名后，检测平台对签名结果进行验签，验签通过；

b） 产品使用给定的密钥对待签名消息调用密码算法签名后，调用密码算法进行验签运算，验签通过。

4.7.4 杂凑密码算法的正确性和一致性

4.7.4.1 检测要求

产品如使用杂凑密码算法，应支持 SM3 密码算法，其实现应符合 GB/T 32905。

4.7.4.2 检测方法

产品对给定消息调用杂凑算法计算杂凑值，结果与给定杂凑值完全相同。

4.8 产品随机数质量检测

4.8.1 检测要求

产品生成和使用的随机数应由密码模块提供，密码模块应经过国家商用密码认证机构认证。

4.8.2 检测方法

调用产品随机数生成接口，采集 1000 个 128 KB 大小的随机数文件；对所采集的随机数文件进行检测，检测结果应符合 GB/T 32915 的要求。

4.9 产品角色鉴别检测

4.9.1 基本级要求

4.9.1.1 检测要求

安全等级为基本级的产品应设定有角色并具备相应的鉴别机制，不同的访问或操作应有不同的权限。产品应拒绝任何不具备相应权限的访问或操作，防止未经授权的恶意人员登录，破坏产品的安全性。

4.9.1.2 检测方法

检测方法如下：

a) 通过产品管理界面输入错误的用户名和随机的登录口令，登录失败；
b) 通过产品管理界面输入正确的用户名和随机的登录口令，登录失败；
c) 通过产品管理界面输入正确的用户名和正确的登录口令，登录成功。

4.9.2 增强级要求

4.9.2.1 检测要求

安全等级为增强级的产品应采用经过国家商用密码认证机构认证的智能密码钥匙等表征身份的硬件装置，结合登录口令实现多因素的鉴别机制，其中口令长度应大于 6 位，口令应至少包含数字、大小写字母，也可包含特殊字符。产品应实现 GB/T 15843 中规定的一种核准的鉴别机制。

4.9.2.2 检测方法

检测方法如下：

a) 获取产品身份鉴别过程中的协议数据，核查产品实现的鉴别机制符合 GB/T 15843 中的规定；
b) 使用正确的身份硬件装置，通过产品管理界面输入错误的用户名和随机的登录口令，登录失败；
c) 使用正确的身份硬件装置，通过产品管理界面输入正确的用户名和随机的登录口令，登录失败；
d) 使用正确的身份硬件装置，通过产品管理界面输入正确的用户名和正确的登录口令，登录成功；
e) 使用错误的身份硬件装置，通过产品管理界面输入正确的用户名和正确的登录口令，登录失败。

4.10 产品密钥管理检测

4.10.1 检测要求

产品应具备完善的密钥管理功能，密钥管理包括密钥的生成、存储、使用、更新、备份、恢复和销毁。产品保证密钥在生命周期的各个环节的安全性。

4.10.2 检测方法

检测方法如下。

a) 密钥生成：使用产品密钥管理工具正确生成所用的各类密钥，生成的密钥与密码算法强度相匹配。
b) 密钥存储：使用产品密钥管理工具查看密钥存储状态，密钥安全存储。除公钥外的密钥未以明文形式出现在密码模块外。
c) 密钥使用：使用经鉴别通过的角色，成功访问和使用产品内部存储的密钥；使用未经鉴别的角色，访问和使用失败。
d) 密钥更新：使用产品密钥管理工具执行密钥更新操作，成功更新指定密钥。
e) 密钥备份：使用产品密钥管理工具执行密钥备份操作，成功以密文形式备份。
f) 密钥恢复：使用产品密钥管理工具执行密钥恢复操作，成功恢复至密码模块中。
g) 密钥销毁：使用产品密钥管理工具执行密钥销毁操作，成功销毁指定密钥。

4.11 产品日志审计检测

4.11.1 检测要求

产品应提供日志记录、查看和导出功能，应能保证日志未被非法篡改。

4.11.2 检测方法

通过产品管理界面查看日志内容，应包括：

a) 管理员操作行为，包括登录认证、配置管理等操作；
b) 异常事件，包括自检失败、认证失败等异常事件的记录。

日志内容宜包括：

a) 修改安全属性的所有尝试行为，包括修改前后的安全属性值；
b) 密码算法正确性检测、随机数质量检测、鉴别数据、密钥完整性自检的结果数据，包括自检项目及检测结果。

4.12 产品功能检测

4.12.1 总体要求

产品应实现两个安全域之间的安全数据交换，并且保证安全隔离与信息交换产品内外两个处理系统不同时连通。

4.12.2 基本级要求

4.12.2.1 检测要求

安全等级为基本级的产品应符合 GB/T 20279—2015 中 5.2.2.1.1.1、5.2.2.1.1.2 的规定。

4.12.2.2 检测方法

检测方法如下：

a) 模拟生成设备所支持的信息流，经过产品的发送方和接收方之间的所有信息流应执行 GB/T 20279—2015 中 5.2.2.1.1.1 中规定的控制策略；

b) 获取接收方信息流数据，核查产品实现 GB/T 20279—2015 中 5.2.2.1.1.2 中规定的控制功能。

4.12.3 增强级要求

4.12.3.1 检测要求

安全等级为增强级的产品应符合 GB/T 20279—2015 中 5.2.2.2.1.1、5.2.2.2.1.2 的规定。

4.12.3.2 检测方法

检测方法如下：

a) 模拟生成设备所支持的信息流，经过产品的发送方和接收方之间的所有信息流应执行 GB/T 20279—2015 中 5.2.2.2.1.1 中规定的控制策略；

b) 获取接收方信息流数据，核查产品实现 GB/T 20279—2015 中 5.2.2.2.1.2 中规定的控制功能。

4.13 产品性能检测

产品的交换速率与硬件切换时间应符合 GB/T 20279—2015 中 5.5 的规定。

5 文档要求

5.1 系统框架结构

开发者应以结构图的形式，说明产品的系统框架结构，包括安全隔离与信息交换产品的各个子系统的构成、各子系统的功能和各子系统的实现原理，并附以详细的文字说明。

详细描述安全隔离与信息交换产品的安全机制、密码体制和密钥管理。

5.2 密码子系统框架结构

开发者应详细说明安全隔离与信息交换产品密码子系统的整体框架结构以及功能模块流程，并附以详细的文字说明。

a) 密码子系统的整体框架结构说明书：以结构图的形式，说明安全隔离与信息交换产品中密码子系统的框架结构，包括密码子系统的各个功能模块的构成、各功能模块的功能和各功能模块的实现原理，并附以详细的文字说明。

b) 密码子系统的功能模块流程说明书：以流程图的形式详细描述各子模块的工作原理和工作流程，详细说明各模块所调用的函数名称和调用顺序，包括密钥生成、更新、销毁等整个密钥生存周期各阶段所用到的函数，以及加密初始化函数、加密函数、解密函数、杂凑函数、签名函数、签名验证函数和加密后处理函数等。

5.3 源代码

开发者应提供产品与密码实现和使用相关的源代码，并提供源代码的说明文档。

5.4 不存在隐式通道的声明

开发者应提供产品涉及密码的部分不存在隐式通道的声明文件。

5.5 密码自测试或自评估报告

开发者应提供产品的密码自测试或自评估报告，自测试项目应包含但不限于产品所使用的密码算法和随机数自测试。