ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0026—2023
代替 GM/T 0026—2014

安全认证网关产品规范

Security authentication gateway product specification

2023-12-04 发布　　2024-06-01 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。

本文件代替 GM/T 0026—2014《安全认证网关产品规范》，与 GM/T 0026—2014 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 GB/T 25069（见第 3 章）、GB/T 36624（见 6.1）、GM/T 0028（见 7.3.2.2，7.3.2.3 和 7.3.2.4）、GM/T 0062（见 7.4.2.3.3 和 8.4.7）、GM/T 0068（见 7.1.5）、GM/T 0069（见 7.1.5）和 GM/Z 4001（见第 3 章），删除了 GM/T 0014（见 2014 年版的第 2 章），更改了 GB/T 9813 为 GB/T 9813.3（见 7.5.4）；

b) 删除了术语“密码算法”（见 2014 年版的 3.1）、“带密钥的杂凑算法”（见 2014 年版的 3.2）、“非对称密码算法/公钥密码算法”（见 2014 年版的 3.3）、“对称密码算法”（见 2014 年版的 3.4）、“分组密码算法”（见 2014 年版的 3.5）、“密文分组链接工作模式”（见 2014 年版的 3.6）、“初始化向量/值”（见 2014 年版的 3.7）、“数据源鉴别”（见 2014 年版的 3.8）、“数字证书”（见 2014 年版的 3.9）、“SSL 协议”（见 2014 年版的 3.10）、“认证头”（见 2014 年版的 3.11）、“封装安装载荷”（见 2014 年版的 3.12）、“虚拟专用网络”（见 2014 年版的 3.13）、“安全报文”（见 2014 年版的 3.14）、“SM1 算法”（见 2014 年版的 3.15）、“SM2 算法”（见 2014 年版的 3.16）、“SM3 算法”（见 2014 年版的 3.17）、“SM4 算法”（见 2014 年版的 3.18）和“安全认证网关”（见 2014 年版的 3.19）；

c) 增加了缩略语“GCM”“TLCP”（见第 4 章），删除了“IV”（见 2014 年版的第 4 章）；

d) 删除了安全认证网关部署模式中“物理”两字（见 2014 年版的第 5 章）；

e) 增加了 GCM 模式（见 6.1）；

f) 更改了“密钥种类”的描述（见 6.2，见 2014 年版的 6.2）；

g) 更改了随机数生成相关的功能要求（见 7.1.7，2014 年版的 7.1.7）；

h) 增加了采用的密码协议（见 7.1.5）；

i) 增加了密钥交换的描述（见 7.1.9）；

j) 更改了密钥更新部分的描述（见 7.1.11，2014 年版的 7.1.11）；

k) 更改了 NAT 穿越的功能描述（见 7.1.12，2014 年版的 7.1.12）；

l) 增加了包过滤功能（见 7.1.14）；

m) 更改了产品性能参数的描述（见 7.2.1 和 7.2.2，2014 年版的 7.2.1 和 7.2.2）；

n) 更改了密钥安全的描述（见 7.3.1，2014 年版的 7.3.1）；

o) 增加了敏感参数配置安全（见 7.3.2.2）；

p) 增加了应符合 GM/T 0028 对硬件模块物理安全的规定（见 7.3.2.2）；

q) 增加了产品的软件或固件应符合 GM/T 0028 对软件/固件安全的规定和对软件升级安全要求进行了规定（见 7.3.2.3）；

r) 更改了 7.4.1 的标题名称（见 2014 年版的 7.4.1，2014 年版的 7.4.1）；

s) 更改了合规性验证和远程参数配置，对相关内容进行简化。[见 7.4.1a）和 b），2014 年版的 7.4.1 a）和 b）]；

t) 更改了“加密部件”的描述（见 7.5.2，2014 年版的 7.5.2）；

u) 更改了随机数发生器直接引用 GM/T 0062 E 类产品检测（见 7.5.2 和 8.4.7，2014 年版的

7.5.3 和 8.1.7)；

v) 增加了检测说明,外观和结构的检查和提交文档的检查(见 8.1,8.2 和 8.3)；

w) 增加了产品功能检测中每个功能的检测方法(见 8.4)；

x) 更改了产品性能检测的描述(见 8.5,2014 年版的 8.2)；

y) 增加了敏感参数配置安全的检测描述(见 8.6.1.3)；

z) 增加了管理安全的检测方法的描述(见 8.6.1.7)；

aa) 增加了远程管理的检测方法的描述(见 8.6.2.4)。

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:格尔软件股份有限公司、无锡江南信息安全工程技术中心、上海数字证书认证中心有限公司、北京信安世纪科技股份有限公司、中电信量子信息科技集团有限公司、飞天诚信股份有限公司、北京国脉信安科技有限公司、山东得安信息技术有限公司、山东渔翁信息技术股份有限公司、广东省电子商务认证有限公司、天融信科技集团股份有限公司、上海智巡密码检测技术有限公司、山东大学。

本文件主要起草人:郑强、谭武征、徐强、刘承、汪宗斌、罗俊、朱鹏飞、梁宁宁、药乐、胡金山、王鹏、安高峰、韩玮、孔凡玉、邱媛、韩琳、董明富。

本文件所代替文件的历次版本发布情况为:

——2014 年首次发布版为 GM/T 0026—2014；

——本次为第一次修订。

安全认证网关产品规范

1 范围

本文件规定了安全认证网关的密码算法和密钥种类、产品的要求、产品的检测及合格判定。

本文件用于安全认证网关产品的研制、检测、使用和管理。

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 9813.3 计算机通用规范 第3部分：服务器

GB/T 15153.1 远动设备及系统 第2部分：工作条件 第1篇：电源和电磁兼容性

GB/T 15843.3 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

GB/T 17964 信息安全技术 分组密码算法的工作模式

GB/T 25069 信息安全技术 术语

GB/T 36624—2018 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 0022 IPSec VPN技术规范

GM/T 0023 IPSEC VPN网关产品规范

GM/T 0024 SSL VPN技术规范

GM/T 0025 SSL VPN网关产品规范

GM/T 0028 密码模块安全技术要求

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/T 0068 开放的第三方资源授权协议框架

GM/T 0069 开放的身份鉴别框架

GM/Z 4001 密码术语

3 术语和定义

GB/T 25069 和 GM/Z 4001 界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

AH：认证头(Authentication Header)

CBC：密码分组链接(Cipher Block Chaining)

ESP：封装安全载荷(Encapsulate Security Payload)

GCM:Galois 计数器模式(Galois Counter Mode)
IPSec:IP 安全(Internet Protocol Security)
NAT:网络地址转换(Network Address Translation)
SSL:安全套接层协议(Secure Sockets Layer)
TLCP:传输层密码协议(Transport Layer Cryptography Protocol)
VPN:虚拟专用网络(Virtual Private Network)

5 部署模式

安全认证网关是采用数字证书为应用系统提供用户管理、身份鉴别、单点登录、传输加密、访问控制和信息审计等服务的产品。安全认证网关是采用了数字证书技术进行鉴别。安全认证网关的部署模式分为串联和并联两种方式。

a) 串联:指从网络拓扑上,用户应经过网关才能访问到受保护的应用。
b) 并联:指从网络拓扑上,用户可不经过网关能访问到受保护的应用,可由应用或防火墙上进行某种逻辑判断,来识别出未经网关访问的用户(例如通过来源 IP),以达到逻辑上串联的效果。

安全认证网关至少应支持串联的部署模式。同时,考虑到实际情况的需要,安全认证网关可在支持串联部署模式之外,可支持并联部署方式,但应为应用提供鉴别用户是否经由网关进行访问的技术手段。

6 密码算法和密钥种类

6.1 算法要求

安全认证网关使用的非对称密码算法、对称密码算法、密码杂凑算法和随机数生成算法应符合密码国家标准、行业标准的相关要求,算法及使用方法如下。

a) 非对称密码算法用于认证、数字签名和数字信封。
b) 对称密码算法使用分组密码算法,用于密钥交换数据的加密保护和报文数据的加密保护。算法的工作模式为 GCM 模式或 CBC 模式。GCM 应符合 GB/T 36624,CBC 应符合 GB/T 17964。
c) 密码杂凑算法用于对称密钥生成、完整性校验和数字签名。
d) 随机数生成算法用于生成符合 GM/T 0005 的检测要求的随机数。

6.2 密钥种类

对于符合 IPSec 协议的安全认证网关,密钥种类应符合 GM/T 0022;对于符合 TLCP 协议的安全认证网关,密钥种类应符合 GM/T 0024。

7 安全认证网关产品要求

7.1 产品功能要求

7.1.1 用户管理

安全认证网关应可以对访问的用户进行管理:

a) 网关能对需要访问系统的相关用户进行增删改查;

b) 网关能从其他身份管理系统(例如 CA,RA)同步证书用户的信息;

c) 网关能对用户进行一定程度的角色分组,或者按照组织机构进行管理。

7.1.2 身份鉴别

安全认证网关应提供基于数字证书的方式来进行最终用户的身份鉴别,身份鉴别协议应符合 GB/T 15843.3。当安全认证网关使用代理模式时:

对于符合 IPSec 协议的安全认证网关,应在 IKE 协商阶段鉴别最终用户的证书及签名,并进行证书黑名单(CRL)的检查。

对于符合 TLCP 协议的安全认证网关,应在每次 TLCP 握手时,鉴别最终用户的证书及签名,并进行证书黑名单(CRL)的检查。

当安全认证网关使用调用模式时,网关应在被调用时鉴别最终用户的证书及签名,并检查证书黑名单(CRL)。

在外部环境支持的条件下(OCSP 验证,或基于 CA 提供的其他接口进行实时证书状态验证),网关宜支持实时的证书状态验证方式。

7.1.3 应用管理

安全认证网关产品应可对需要保护的应用进行管理,能对应用信息进行增删改查。应用信息应包含应用地址,应用地址可分为三类:

a) 网段:按照网络地址+掩码进行标识,例如 192.168.1.0/24;

b) TCP/UDP 应用:按照协议(TCP/UDP)及端口号进行标识,例如 tcp://192.168.3.6:25/或 udp://192.168.1.9:53/;

c) WEB 应用:按照协议(HTTP/HTTPS),域名,端口号和 WEB 路径进行标识,例如 http://www.site.com:8080/myapp 或 https://www.securesite.com/mysecure。

7.1.4 访问控制

基于用户管理和应用管理的信息,网关对用户访问的应用的权限进行定义。

a) 基于单个用户或用户组(角色)定义来控制访问某一应用。

b) 访问权限的配置模式为白名单或黑名单方式。

c) 如果采用了黑白名单混用的方式(例如用户在作为角色 A 能访问应用,但作为角色 B 时禁止访问应用),则应提供对权限优先级进行排序的方式。

7.1.5 单点登录

用户访问同一台网关保护的多个应用时,应只存在一次身份鉴别过程。鉴别过程宜符合 GM/T 0068 和 GM/T 0069。

7.1.6 信息审计

安全认证网关产品中应具有信息审计功能,能对用户对系统的访问进行详细记录,记录信息宜包括但不限于:时间、用户 IP、用户证书信息、事件类型、访问资源、上传流量、下载流量、访问结果、错误原因、成功和失败标识。

7.1.7 随机数生成

安全认证网关应具备独立的随机数生成功能。

7.1.8 工作模式

符合 IPSec 协议的安全认证网关产品的工作模式应符合 GM/T 0022。符合 TLCP 协议的安全认证网关产品工作模式应符合 GM/T 0024。

7.1.9 密钥交换

安全认证网关产品应具有密钥交换功能，通过协商产生工作密钥及会话密钥。

a) 密钥交换采用 IPSEC 协议应符合 GM/T 0022，采用 TLCP 协议应符合 GM/T 0024。

b) 密钥交换产生的工作密钥及会话密钥在安全认证网关每次启动时均应置零。

7.1.10 安全报文的传输

安全认证网关产品应具有安全报文传输功能，保证数据的安全传输。

7.1.11 密钥更新

安全认证网关产品应具有根据时间周期和报文流量两种条件进行密钥的更新功能，其中根据时间周期条件进行密钥更新为必备功能，根据报文流量条件进行密钥更新为可选功能。

对于符合 IPSec 协议的安全认证网关，工作密钥的最长更新周期不超过 24h，会话密钥的最大更新周期不超过 1 h。

对于符合 TLCP 协议的安全认证网关，对于客户端-服务端模式，工作密钥的最长更新周期不超过 8 h，对于网关-网关模式，工作密钥最长时间更新周期不超过 1 h。

7.1.12 NAT 穿越

对于符合 IPSec 协议的安全认证网关产品来说，NAT 穿越是必备检测。具体的测试过程见 GM/T 0023 中 NAT 穿越的功能要求。

7.1.13 抗重放攻击

安全认证网关在安全报文传输阶段应具有对抗重放攻击的功能。

7.1.14 包过滤

IPSec VPN 网关应具有根据数据报文的五元组（源 IP 地址、目的 IP 地址、源传输层端口、目的传输层端口、传输层协议）决定其处理方式的功能。处理方式应支持丢弃、明文转发、密文转发（使用 IPSec 处理后转发）。

7.1.15 客户端主机安全检查

安全认证网关产品应具有客户端主机安全检查功能。客户端在连接服务端时，根据服务端下发的客户端安全策略检查用户操作系统的安全性。不符合安全策略的用户将无法使用安全认证网关。

客户端安全策略应至少包括下列条件之一：

a) 已安装并启用反病毒软件；

b) 已安装并启用个人防火墙；

c) 已安装最新的操作系统安全补丁；

d) 已为系统设置了登录口令。

7.2 产品性能参数要求

7.2.1 符合IPSec协议的产品性能参数

符合 IPSec 协议的安全认证网关产品性能参数包括加解密吞吐量、加解密时延、加解密丢包率、每秒新建隧道数和最大并发隧道数，每个参数的具体要求见 GM/T 0023。

7.2.2 符合TLCP协议的产品性能参数

符合 TLCP 协议的安全认证网关产品性能参数包括最大并发用户数、最大并发连接数、每秒新建连接数和加解密吞吐率，每个参数的具体要求见 GM/T 0025。

7.3 产品安全性要求

7.3.1 密钥安全

符合 IPSec 协议的安全认证网关产品密钥管理安全要求见 GM/T 0023，符合 TLCP 协议的安全认证网关产品密钥安全要求见 GM/T 0025。

7.3.2 配置安全

7.3.2.1 配置数据安全

所有的配置数据应保证其在设备中的完整性、可靠性。应有管理界面对配置数据进行配置和管理，管理员进入管理界面应通过身份鉴别。

7.3.2.2 敏感参数配置安全

安全认证网关包括密钥在内的敏感安全参数的生成、建立、输入、输出、存储和置零的全生命周期的管理应符合 GM/T 0028 的要求。

7.3.2.3 硬件安全

硬件安全的要求如下。

a) 安全网关产品硬件应符合 GM/T 0028 对硬件模块物理安全的规定。
b) 安全认证网关产品应提供安全措施，保证密码算法、密钥、关键数据的存储安全。
c) 所有密码运算应在独立的密码部件中进行。
d) 除必需的通信接口和管理接口以外，不提供任何可供调试、跟踪的外部接口。内部的调试、检测接口应在产品定型后封闭。符合 IPSec 协议的安全认证网关产品的远程维护接口应采用加密通道和身份鉴别安全措施。

7.3.2.4 软件安全

软件安全的要求如下。

a) 安全认证网关产品的软件或固件应符合 GM/T 0028 对软件/固件安全的规定。
b) 操作系统应进行安全加固，裁减一切不需要的模块，关闭所有不需要的端口和服务。
c) 任何操作指令及其任意组合，不能泄露密钥和敏感信息。
d) 软件升级应具备修复安全漏洞的能力，在升级前应对升级包文件进行完整性校验。

7.3.2.5 客户端安全

安全认证网关的客户端产品应具有完整性的自校验功能，包括厂商对客户端软件的签名，以保护信息的完整性。

7.3.3 管理安全

7.3.3.1 分权管理

分权管理的要求如下。

a) 应实现系统管理员、安全管理员、系统审计员分权管理。
b) 系统管理员负责对软件环境日常运行的管理和维护，以及对系统的备份和操作系统恢复。
c) 系统审计员负责对系统中的日志进行安全审计。
d) 安全管理员负责业务配置、应用管理、授权管理管理操作。

7.3.3.2 管理员登录安全

管理员通过数字证书技术进行鉴别，登录到安全认证网关进行管理配置，管理员通过被授权的终端登录到安全认证网关进行相应的配置操作。

7.4 产品管理要求

7.4.1 远程管理

远程管理：安全认证网关产品应提供协议接口接受管理中心通过网络远程对其设备状态、网络配置、安全策略进行查询、监控和管理。对密码设备的管理宜符合 GM/T 0050 的设备管理技术规范。

a) 合规性验证

安全认证网关产品宜提供远程调用接口对 SM2、SM3、SM4 和密钥随机性进行合规性验证，验证协议和接口应符合密码国家标准、行业标准的相关要求。

b) 远程参数配置

安全认证网关产品宜提供协议和接口接受管理中心远程对其参数进行配置。

c) 远程监控

1) 参数查询

安全认证网关产品宜提供协议和接口接受管理中心对其安全策略、安全参数、网络参数、用户参数配置信息和日志进行查询，并可提供分类查询和关键字检索手段。

2) 状态监测

安全认证网关产品宜提供协议和接口接受管理中心远程对其运行状态(CPU、内存和非易失性存储介质系统资源的占有率)、系统信息(开机时间、运行时间、系统时间和设备名字及 IP)、网络流量、是否在线、隧道状态(建立时间、加密流量、有效期)进行远程实时查询，并在设备状态明显异常时可向管理中心报警。

3) 远程控制

安全认证网关产品宜提供协议和接口接受管理中心远程对其进行重启、故障诊断、各项功能的关闭和启用操作。

4) 时间同步

安全认证网关产品宜提供远程调用接口接受管理中心对其进行远程时间同步。

7.4.2 管理内容

7.4.2.1 日志管理

安全认证网关产品应提供日志记录、查看和导出功能。日志内容包括：

a) 操作行为，包括登录认证、参数配置、系统配置、策略配置、密钥管理操作；
b) 用户访问行为，包括用户、时间、访问资源、结果；
c) 安全事件，密钥交换成功及失败、密钥过期、隧道建立及删除事件；
d) 异常事件，解密失败、完整性校验失败、认证失败、非法访问异常事件的统计。

7.4.2.2 管理员管理

管理员管理的要求如下。

a) 安全认证网关产品应设置管理员，进行设备参数配置、策略配置、系统配置、设备密钥的生成、导入、备份和恢复操作。管理员应持有表征用户身份信息的硬件装置，与登录口令相结合登录系统，进行管理操作前应通过身份鉴别。
b) 登录口令长度应不少于8个字符，且至少由数字、字母和特殊字符其中的两种类型组成。
c) 使用错误口令或非法身份登录的次数限制应小于或等于8。

7.4.2.3 设备管理

7.4.2.3.1 设备初始化

安全认证网关产品的初始化，除应由厂商进行的操作外，系统配置、参数的配置、安全策略的配置、密钥的生成和管理、管理员的产生均应由用户完成。初始化数据中如含有私钥敏感信息应提供安全IC卡或安全Key承载。

7.4.2.3.2 注册和监控

安全认证网关产品进行远程管理时，应具有向管理中心进行注册的功能，同时接受管理中心对其运行状态的实时监控管理。

7.4.2.3.3 设备自检

设备自检的要求如下。

a) 安全认证网关产品在开机、管理接口收到管理指令时应进行自检。
b) 应对密码运算部件关键部件进行正确性检查。应确保密码运算部件正常工作，设备所采用的各种密码算法：包括对称、杂凑和非对称算法的正确性在设备自检时应得到验证。
c) 应对存储的密钥敏感信息进行完整性检查。应确保设备密钥得到安全保护，工作密钥和会话密钥不存放在非易失性存储介质中。
d) 应对硬件随机数产生部件进行检查，应确保硬件随机数产生部件正常工作，随机数产生质量符合GM/T 0005的规定。
e) 应对身份鉴别介质及其接口进行检查，确保其正常工作。
f) 应对随机数发生器进行检查，应符合GM/T 0062的E类。
g) 应对CPU、内存、网络接口、非易失性存储介质物理部件进行常规检查，确保各关键部件正常工作。
h) 算法正确性、密钥完整性、随机数可靠性检测为必选项，硬件功能模块、软件功能模块正确性

检测为可选项。在检查不通过时应报警并停止工作。

7.5 产品硬件要求

7.5.1 对外接口

安全认证网关产品应至少具备两个工作网口，分别为内网接口和外网接口。还应提供一个管理接口，通过 TCP/IP 网络或串行接口与管理设备连接。

7.5.2 加密部件

安全认证网关产品应采用通过商用密码检测认证的密码模块或安全芯片作为密码部件实现密码运算和密钥管理。

7.5.3 随机数发生器

安全认证网关采用的随机数发生器应通过商用密码检测认证，生成的随机数应由多路硬件随机源产生并符合 GM/T 0005 的要求，至少采用两个独立的物理噪声源芯片实现。

7.5.4 环境适应性

安全认证网关产品的工作环境应根据实际需要符合 GB/T 9813.3 中关于“气候环境适应性”的规定要求。

7.5.5 电磁兼容性

安全认证网关产品应满足一定条件下的电磁兼容等级，产品应符合 GB/T 15153.1 中指标和严酷等级要求。

7.5.6 可靠性

安全认证网关服务器端的平均无故障工作时间应不低于 10 000 h，平均可持续加密流量应不低于 10 000 Gb。

安全认证网关客户端产品平均无故障工作时间应不低于 100 h，平均可持续加密流量应不低于 100 Gb，一般故障可在重启后恢复正常。

7.6 产品过程保护

设置必要保护措施，保障产品在运输和安装过程中的安全，不被嵌入恶意信息。

8 安全认证网关产品检测要求

8.1 检测说明

检测要求规定了安全认证网关的通用检测内容和方法。检测应包括外观和结构检查、提交文档的检查、功能检测、性能检测、安全管理检测和硬件检测。

8.2 外观和结构的检查

根据产品的物理参数，对被检测设备的外观、尺寸、内部部件及附件进行检查。

8.3 提交文档的检查

被检测设备研制单位应按照具备资质的商用密码检测、认证机构的检测要求提交相关文档资料，作为安全认证网关的检测认证依据。

8.4 产品功能检测

8.4.1 用户管理

网关可以实现对安全认证网关的用户进行修改、增删、查询用户证书信息、用户分组操作。检测结果应符合 7.1.1 的要求。

8.4.2 身份鉴别

以管理员身份登录被检测设备，被检测设备应对管理员身份进行实体鉴别，鉴别方式应符合 GB/T 15843.3 的要求。检测结果应符合 7.1.2 的要求。

8.4.3 访问控制

从客户端访问服务端保护的内网服务器，应只能访问到相应的授权资源。检测结果应符合 7.1.4 的要求。

8.4.4 单点登录

用户只通过一次身份鉴别过程能访问同一台安全认证网关保护的多个应用。检测结果应符合 7.1.5 的要求。

8.4.5 应用管理

录入不同的应用信息，安全认证网关应对应用信息进行增删改查。检测结果应符合 7.1.3 的要求。

8.4.6 信息审计

通过安全认证网关能够查询到用户对系统的访问进行的详细记录。 检测结果应符合 7.1.6 的要求。

8.4.7 随机数功能

随机数检测应符合 GM/T 0005 和 GM/T 0062 E 类产品的要求。检测结果应符合 7.1.7 的要求。

8.4.8 工作模式

对于符合 IPSec 协议的安全认证网关产品，将检测设备与被检测社备均设置为隧道模式，应能成功完成密钥交换，建立 IPSec 隧道进行通信；被检测设备支持传输模式时，将检测设备与被检测设备均设置为传输模式，应能成功完成密钥交换，进行通信；将检测设备与被检测设备一方设置为隧道模式，另一方设置为传输模式，密钥交换应失败，无法建立 IPSec 隧道进行通信。

对于符合 TLCP 协议的安全认证网关产品，在客户端－服务端工作模式下，客户端应能通过服务端访问到受保护的内网服务器；在网关－网关工作模式下，一个网关保护的客户主机应能访问到另一个网关保护的内网服务器。

检测结果应符合 7.1.8 的要求。

8.4.9 密钥交换

符合 IPSec 协议的安全认证网关产品的密钥交换协议检测应符合 GM/T 0022;符合 TLCP 协议的安全认证网关产品的密钥交换协议检测应符合 GM/T 0024。对密钥交换过程进行网络数据截获,其过程应能正确进行加解密通信。检测结果应符合 7.1.9 的要求。

8.4.10 安全报文的传输

对于符合 IPSec 协议的安全认证网关产品,将检测设备与被检测设备的安全报文封装协议均配置为 ESP 协议,对通信的报文进行网络数据截获,其封装格式应符合 GM/T 0022 的要求,应能正确进行加解密通信;将检测设备与被检测设备的安全报文封装协议均配置为 AH 协议嵌套 ESP 协议,对通信的报文进行网络数据截获,其封装格式应符合相应技术规范的要求,应能正确进行加解密通信。

对于符合 TLCP 协议的安全认证网关产品,安全报文封装协议应符合 GM/T 0024 的要求。

检测结果应符合 7.1.10 的要求。

8.4.11 密钥更新

在检测设备和被检测设备上按照相同参数设定工作密钥和会话密钥的更新周期,应能成功完成密钥的更新。对于符合 IPSec 协议的安全认证网关产品,当满足密钥更新条件时,使用网络报文截获工具应能分别看到相应的第一阶段和第二阶段的密钥交换过程;对于符合 TLCP 协议的安全认证网关产品,使用网络报文截获工具应能分别看到工作密钥的交换过程。检测结果应符合 7.1.11 的要求。

8.4.12 NAT穿越

应符合 GM/T 0023 中 NAT 穿越的检测要求。检测结果应符合 7.1.12 的要求。

8.4.13 抗重放攻击

利用检测设备或网络报文截获工具重放报文传输阶段的安全报文,在被检测设备的内网口应不能检测到重放的数据报文。检测结果应符合 7.1.13 的要求。

8.4.14 包过滤

在被检测设备上分别配置不同五元组对应 IPSec 策略的处理选择为丢弃、明文转发或密文转发(使用 IPSec 处理),利用检测设备在被检测设备的内网口发送前述不同五元组的数据报文,在被检测设备的外网口应不能检测到设定为丢弃的数据报文、应检测到设定为明文转发的数据报文明文、应检测到设定为密文转发的数据报文密文。检测结果应符合 7.1.14 的要求。

8.4.15 客户端主机安全检查

客户端在连接服务端时,应根据服务端下发的客户端安全策略检查用户操作系统的安全性。检测结果应符合 7.1.15 的要求。

8.5 产品性能检测

8.5.1 符合IPSec协议的安全认证网关产品

对于符合 IPSec 协议的安全认证网关产品,应符合 GM/T 0023 中产品的性能检测。检测结果应符合 7.2.1 的要求。

8.5.2 符合TLCP协议的安全认证网关产品

对于符合 TLCP 协议的安全认证网关产品，应符合 GM/T 0024 中产品的性能检测。检测结果应符合 7.2.2 的要求。

8.6 安全管理检测

8.6.1 安全检测

8.6.1.1 密钥安全

对密钥进行管理以确保密钥安全。在被测设备的管理界面上进行设备密钥的产生或导入、备份和恢复以及更新操作。密钥的检测结果应符合 7.3.1 的要求。

8.6.1.2 配置数据安全

所有的配置数据应保证其在设备中的完整性、可靠性。应有管理界面对配置数据进行配置和管理，管理员进入管理界面应通过身份鉴别。检测结果应符合 7.3.2.1 的要求。

8.6.1.3 敏感参数配置安全

对被检测设备的包括密钥在内的敏感安全参数进行生成、建立、输入、输出、存储和置零操作。检测结果应符合 7.3.2.2 的要求。

8.6.1.4 硬件安全

审查厂商提供的设计文档和厂商提交的产品安全性承诺，应符合相应产品规范的要求。检测结果应符合 7.3.2.3 的要求。

8.6.1.5 软件安全

使用漏洞扫描工具探测系统的端口和服务，并审查厂商提供的设计文档和厂商提交的产品安全性承诺，应符合相应产品规范的要求。检测结果应符合 7.3.2.4 的要求。

8.6.1.6 客户端安全

安全认证网关的客户端产品应能通过数字签名等技术进行完整性的自校验功能。检测结果应符合 7.3.2.5 的要求。

8.6.1.7 管理安全

8.6.1.7.1 分权管理

系统管理员、安全管理员、系统审计员应具备各自的分权管理职责。检测结果应符合 7.3.3.1 的要求。

8.6.1.7.2 管理员登录安全

管理员应能通过基于数字证书技术的身份鉴别，并通过加密通道对安全认证网关进行管理配置，管理员应能通过被授权的终端登录到安全认证网关进行相应的配置操作。检测结果应符合 7.3.3.2 的要求。

8.6.2 管理检测

8.6.2.1 日志管理

可以查看并导出日志记录。日志格式应符合相关产品规范的要求。检测结果应符合 7.4.2.1 的要求。

8.6.2.2 管理员管理

用非法的身份或错误的口令登录，系统应拒绝；当连续重试次数到达系统设定的限制值时系统应锁定；用合法的身份和正确口令登录，应能进入管理界面，进行相应的管理操作。检测结果应符合 7.4.2.2 的要求。

8.6.2.3 设备管理

8.6.2.3.1 设备初始化

对设备进行初始化操作，结果应符合相应产品规范的要求。检测结果应符合 7.4.2.3.1 的要求。

8.6.2.3.2 注册和监控

当系统有管理中心时，进行设备的注册、状态监控管理操作，对于异常操作（例如，中断网络连接或停止密码部件工作），被检测设备应发出告警。检测结果应符合 7.4.2.3.2 的要求。

8.6.2.3.3 设备自检

对设备进行自检操作，产品检测结果应符合相应产品规范的要求。检测结果应符合 7.4.2.3.3 的要求。

8.6.2.4 远程管理

8.6.2.4.1 合规性验证

使用被检测设备提供的接口，对被检测设备对称算法、非对称算法、杂凑算法实现的合规性以及密钥随机性进行验证。检测结果应符合 7.4.1 a)的要求。

8.6.2.4.2 远程参数配置

使用被检测设备提供的接口，对被检测设备进行安全策略、安全参数、网络参数、用户参数的添加、删除、修改、查询操作，并对重要配置数据进行完整性检查和备份恢复操作，可配置项的数量应不少于设备正常工作所必需的配置项。检测结果应符合 7.4.1 b)的要求。

8.6.2.4.3 远程监控

使用被检测设备提供的接口，对被检测设备进行参数查询、状态检测、远程控制和时间同步的操作。检测结果应符合 7.4.1 c)的要求。

8.7 硬件检测

8.7.1 外部接口

对被检测设备的外部接口进行检查，检查结果应符合 7.5.1 的要求。

8.7.2 密码部件

对被检测设备的密码部件进行检查，检查结果应符合 7.5.2 的要求。

8.7.3 随机数发生器

对被检测设备的随机数发生器进行检查，检查结果应符合 7.5.3 的要求。

8.7.4 其他硬件

对被检测设备的环境适应性、电磁兼容性和可靠性进行检查，检查结果应符合 7.5.4～7.5.6 的要求。

9 判定规则

8.4、8.6(除 8.6.1.2)和 8.7(除 8.7.4)中的任意一项不合格，判定为产品密码检测不合格。