ICS 35.040
L 80
备案号:44627—2014

GM

中华人民共和国密码行业标准

GM/T 0026—2014

安全认证网关产品规范

Security authentication gateway product specification

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发布

中华人民共和国密码
行业标准
安全认证网关产品规范
GM/T 0026—2014
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.25 字数 34 千字
2014年5月第一版 2014年5月第一次印刷
*
书号:155066·2-27028 定价 27.00 元

GM/T 0026-2014

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 3
5　安全认证网关概述 …… 3
6　密码算法和密钥种类 …… 3
6.1　算法要求 …… 3
6.2　密钥种类 …… 4
7　安全认证网关产品要求 …… 4
7.1　产品功能要求 …… 4
7.2　产品性能参数 …… 6
7.3　安全性要求 …… 7
7.4　管理要求 …… 8
7.5　硬件要求 …… 10
7.6　过程保护 …… 11
8　安全认证网关产品检测 …… 11
8.1　产品功能检测 …… 11
8.2　产品性能检测 …… 13
8.3　安全管理检测 …… 13
8.4　硬件检测 …… 15
9　合格判定 …… 15

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由密码行业标准化技术委员会提出并归口。

本标准主要起草单位：上海格尔软件股份有限公司、无锡江南信息安全工程技术中心、上海市数字证书认证中心有限公司。

本标准主要起草人：谭武征、徐强、刘承、韩琳、刘欣。

引　言

本标准对安全认证网关产品的功能、性能和管理以及检测进行了规定，可用于指导安全认证网关产品的研制、检测、使用和管理。

本标准主要依据国家密码管理局制定的《IPSec VPN 技术规范》和《SSL VPN 技术规范》，按照我国相关密码政策和法规，结合我国实际应用需求及产品生产厂商的实际经验，对安全认证网关产品的使用、管理及合规性、某些功能项的实施和检测方法、性能测试方法提出了一些特别的规定。

安全认证网关产品规范

1 范围

本标准规定了安全认证网关产品的密码算法和密钥种类、功能要求、硬件要求、软件要求、安全性要求和检测要求等有关内容。

本标准适用于指导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

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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—2000 微型计算机通用规范

GB/T 15153.1—1998 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

GM/T 0005 随机性检测规范

GM/T 0014 数字证书认证系统密码协议规范

GM/T 0022 IPSec VPN 技术规范

GM/T 0024 SSL VPN 技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

密码算法 cryptographic algorithm

描述密码处理过程的运算规则。

3.2

带密钥的杂凑算法 keyed-hash message authentication code；HMAC

一种密码杂凑算法，密钥作为其输入参数参与运算。

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

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。

3.5

分组密码算法 block cipher algorithm

将输入数据划分成固定长度的分组进行加解密的一类对称密码算法。

3.6

密文分组链接工作模式　cipher block chaining operation mode;CBC

分组密码算法的一种工作模式,其特征是将当前的明文分组与前一密文分组进行异或运算后再进行加密得到当前的密文分组。

3.7

初始化向量/值　initialization vector/initialization value;IV

在密码变换中,为增加安全性或使密码设备同步而引入的用于数据变换的起始数据。

3.8

数据源鉴别　data origin authentication

对数据的来源或发送方进行鉴别。

3.9

数字证书　digital certificate

也称公钥证书,由证书认证机构(CA)签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书,按用途可分为签名证书和加密证书。

3.10

SSL 协议　secure socket layer protocol

一种传输层安全协议,用于构建客户端和服务端之间的安全通道。

3.11

认证头　authentication header;AH

属于 IPSec 的一种协议,用于提供 IP 数据包的数据完整性、数据源认证以及抗重放攻击的功能,但不提供数据机密性的功能。

3.12

封装安全载荷　encapsulating security payload;ESP

IPSec 的一种协议,用于提供 IP 数据包的机密性、数据完整性、对数据源认证以及抗重放攻击的功能。

3.13

虚拟专用网络　virtual private network;VPN

使用密码技术在通信网络中构建安全通道的技术。

3.14

安全报文　secure message

安全报文的目的是为了确保数据的机密性,完整性和对数据发送方的认证。通过报文认证码(MAC)来保障数据的完整性和对送方的认证,通过对数据的加密来保障数据的机密性。

3.15

SM1 算法　SM1 algorithm

一种分组密码算法,分组长度为 128 比特,密钥长度为 128 比特。

3.16

SM2 算法　SM2 algorithm

一种椭圆曲线公钥密码算法,其密钥长度为 256 比特。

3.17

SM3 算法　SM3 algorithm

一种密码杂凑算法,其输出为 256 比特。

3.18

SM4 算法　SM4 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

3.19

安全认证网关　security authentication gateway

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、访问控制和安全审计服务的产品。

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）

IPSec：IP 安全（Internet Protocol Security）

IV：初始化向量（Initialization Vector）

NAT：网络地址转换（Network Address Translation）

SSL：安全套接层协议（Secure Sockets Layer）

VPN：虚拟专用网络（Virtual Private Network）

5　安全认证网关概述

安全认证网关（Security Authentication Gateway）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、访问控制和安全审计服务的产品。安全认证网关与一般安全网关产品的主要区别在于安全认证网关采用了数字证书技术。安全认证网关产品的功能和检测中对网关的身份鉴别功能提出了要求。安全认证网关的部署模式分为物理串联和物理并联两种方式：

- 物理串联：指从物理网络拓扑上，用户必须经过网关才能访问到受保护的应用；
- 物理并联：指从物理网络拓扑上，用户可以不经过网关就访问到受保护的应用，可以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（比如通过来源 IP），以达到逻辑上串联的效果。

安全认证网关至少必须支持物理串联的部署模式。同时，考虑到实际情况的需要，安全认证网关可以在支持物理串联部署模式之外，支持物理并联部署方式，但必须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

安全认证网关使用国家密码管理主管部门批准的非对称密码算法、对称密码算法、密码杂凑算法和随机数生成算法。算法及使用方法如下：

- 非对称密码算法用于认证、数字签名和数字信封等；
- 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，算法的工作模式使用 CBC 模式，应符合 GB/T 17964 的要求；
- 密码杂凑算法用于对称密钥生成和完整性校验；

- 生成的随机数应能通过 GM/T 0005 规定的检测。

6.2 密钥种类

安全认证网关使用下列密钥：

- 设备密钥：非对称算法使用的公私钥对，用于实体验证、数字签名和数字信封等；
- 工作密钥：在密钥交换第一阶段得到的密钥，为对称算法使用于会话密钥交换过程的保护；
- 会话密钥：在密钥交换第二阶段得到的密钥，为对称算法使用于数据报文的加密和完整性保护。

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。

- 网关能对需要访问系统的相关用户进行增删改查；
- 网关能从其他身份管理系统(比如 CA，RA)同步证书用户的信息；
- 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

安全认证网关提供基于数字证书的方式来进行最终用户的身份鉴别。安全认证网关产品的身份鉴别应遵循 GB/T 15843.3。当安全认证网关使用代理模式时：

对于遵循 IPSec 协议的安全认证网关，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。

对于遵循 SSL 协议的安全认证网关，在每次 SSL 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)。

建议在外部环境支持的条件下，网关支持更为实时的证书状态验证方式，比如 OCSP 验证，或基于 CA 提供的其他接口进行实时证书状态验证。

7.1.3 应用管理

安全认证网关产品应可以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，应用地址按照类型不同可以分为三类：

- 网段：按照网络地址＋掩码进行标识，比如
  192.168.1.0/24；
- TCP/UDP 应用：按照协议(TCP/UDP)及端口号进行标识，比如
  tcp://192.168.3.6:25/
  或 udp://192.168.1.9:53/；
- WEB 应用：按照协议(HTTP/HTTPS)，域名，端口号和 WEB 路径进行标识，比如
  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，网关应可以对用户访问的应用的权限进行定义。

- 可以基于单个用户或用户组(角色)定义是否能访问某一应用；
- 访问权限的配置模式为白名单或黑名单方式；
- 如果采用了黑白名单混用的方式(比如用户在作为角色 A 能访问应用，但作为角色 B 时禁止访问应用)，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。

7.1.6 信息审计

安全认证网关产品应具有信息审计功能，能够对用户对系统的访问进行详细记录，记录信息包括：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

安全认证网关产品应具有随机数生成功能，其随机数应由多路硬件噪声源产生。

7.1.8 工作模式

遵循 IPSec 协议的安全认证网关产品的工作模式应遵循 GM/T 0022。遵循 SSL 协议的安全认证网关产品工作模式应遵循 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。

7.1.10 安全报文的传输

安全认证网关产品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。

对于遵循 IPSec 协议的安全认证网关，工作密钥的最大更新周期不大于 24 h，会话密钥的最大更新周期不大于 1 h。

对于遵循 SSL 协议的安全认证网关，在根据时间周期进行更新的情况下，客户端-服务端模式最长时间不超过 8 h，网关-网关模式最长时间不超过 1 h。

7.1.12 NAT 穿越

对于遵循 IPSec 协议的安全认证网关产品来说，NAT 穿越是必备检测。测试过程为：将待检测设备放在 NAT 下，与检测中心设备进行隧道测试，建立 ESP 协议的隧道模式的 IPSec VPN，测其功能是否完成。

7.1.13 抗重放攻击

利用测试设备或网络报文截获工具重放报文传输阶段的安全报文，在被测设备的内网口应不能检

测到重放的数据报文。

7.1.14 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以下条件之一：

- 是否已安装并启用反病毒软件；
- 是否已安装并启用个人防火墙；
- 是否已安装最新的操作系统安全补丁；
- 是否已为系统设置了登录口令。

7.2 产品性能参数

7.2.1 遵循 IPSec 协议的性能参数

7.2.1.1 加解密吞吐率

加解密吞吐率是指分别在 64 字节以太帧长和 1428(IPv4)/1408(IPv6)字节以太帧长时，IPSec VPN 网关产品在丢包率为 0 的条件下内网口上达到的双向数据最大流量。产品应满足用户网络环境对网络数据加解密吞吐性能的要求。

7.2.1.2 加解密时延

加解密时延是指分别在 64 字节以太帧长和 1428(IPv4)/1408(IPv6)字节以太帧长时，IPSec VPN 网关产品在丢包率为 0 的条件下，一个明文数据流经加密变为密文，再由密文解密还原为明文所消耗的平均时间。产品应满足用户网络环境对网络数据加解密时延性能的要求。

7.2.1.3 加解密丢包率

加解密丢包率是指分别在 64 字节以太帧长和 1428(IPv4)/1408(IPv6)字节以太帧长时，在 IPSec VPN 网关产品内网口处于线速情况下，单位时间内错误或丢失的数据包占总发数据包数量的百分比。产品应满足用户网络环境对网络数据加解密丢包率性能的要求。

7.2.1.4 每秒新建隧道数

每秒新建隧道数是指 IPSec VPN 网关产品在一秒钟的时间单位内能够新建立隧道数目的最大值。产品应满足用户网络环境对每秒新建隧道数性能的要求。

7.2.1.5 最大并发隧道数

最大并发隧道数是指 IPSec VPN 网关产品同时并存的隧道数目的最大值。产品应满足用户网络环境对最大并发隧道数性能的要求。

7.2.2 遵循 SSL 协议的性能参数

7.2.2.1 最大并发用户数

同时在线用户的最大数目，此指标反映产品能够同时提供服务的最大用户数量。

7.2.2.2 最大并发连接数

同时在线 SSL 连接的最大数目，此指标反映产品能够同时处理的最大 SSL 连接数量。

7.2.2.3 每秒新建连接数

每秒钟可以新建的最大 SSL 连接数目，此指标反映产品每秒能够接入新 SSL 连接的能力。

7.2.2.4 吞吐率

在丢包率为 0 的条件下，服务端产品在内网口上达到的双向数据最大流量。

7.3 安全性要求

7.3.1 密钥安全

7.3.1.1 设备密钥安全

设备签名密钥对由安全认证网关产品自身产生，其公钥应能被导出，由外部认证机构签发签名证书。

设备加密密钥对由外部密钥管理机构产生并由外部认证机构签发加密证书。加密密钥对的私钥保护方法见 GM/T 0014。

签名证书、加密证书和加密密钥对的私钥应能被导入安全认证网关产品中。

在安全认证网关产品中，设备密钥的私钥应有安全保护措施。

设备密钥应按设定的安全策略进行更新。

设备密钥可以安全形式进行备份，并在需要时能够恢复。

7.3.1.2 工作密钥安全

安全认证网关产品的工作密钥在密钥交换的第一阶段产生，工作密钥产生后应保存在易失性存储器中，达到其更新条件后应立即更换，在连接断开、设备断电时应销毁。

7.3.1.3 会话密钥安全

安全认证网关产品的会话密钥在密钥交换的第二阶段产生，产生后应保存在易失性存储器中，达到其更新条件后应立即更换，在连接断开、设备断电时应销毁。

7.3.2 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。

7.3.2.1 硬件安全

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。

所有密码运算应在独立的密码部件中进行。

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。遵循 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等安全措施。

7.3.2.2 软件安全

所有的安全协议及管理软件应实现源代码自主可控。

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。

任何操作指令及其任意组合，不能泄露密钥和敏感信息。

7.3.2.3 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，以保护完整性。

7.3.3 管理安全

7.3.3.1 分权管理

实现系统管理员、安全管理员、系统审计员分权管理。

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。

系统审计员负责对系统中的日志进行安全审计。

安全管理员负责业务配置、应用管理、授权管理等管理操作。

7.3.3.2 管理员登录安全

管理员采用数字证书认证，并通过加密通道对集中认证网关进行管理配置，管理员只能通过被授权的终端登录到集中认证网关进行相应的配置操作。

7.4 管理要求

7.4.1 管理方式

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、安全策略进行查询和监控，协议和接口应按照国家密码管理主管部门的要求进行管理。

a) 合规性验证

1) 对称算法验证

安全认证网关产品可提供远程调用接口接受国家密码管理主管部门对其 SM1 和 SM4 对称加密算法进行合规性验证。验证协议和接口应符合国家密码管理主管部门的要求。

2) 非对称算法验证

安全认证网关产品可提供远程调用接口接受国家密码管理主管部门对其 SM2 非对称加密算法合规性进行验证。验证协议和接口应符合国家密码管理主管部门的要求。

3) 杂凑算法验证

安全认证网关产品可提供远程调用接口接受国家密码管理主管部门对其 SM3 杂凑算法合规性进行验证。验证协议和接口应符合国家密码管理主管部门的要求。

4) 密钥随机性验证

安全认证网关产品可提供远程调用接口接受国家密码管理主管部门对其密钥随机性进行验证。验证协议和接口应符合国家密码管理主管部门的要求。

b) 远程参数配置

1) 安全策略配置

安全认证网关产品可提供协议和接口接受管理中心远程对其安全策略进行修改、添加、删除等操作。

2) 安全参数配置

安全认证网关产品可提供协议和接口接受管理中心远程对其安全参数进行配置。

3) 网络参数配置

安全认证网关产品可提供协议和接口接受管理中心远程对其网络配置参数进行设置。

4) 用户参数配置

当支持客户端模式时，安全认证网关产品可提供协议和接口接受管理中心远程对其用户信息进行设置，包括用户名和口令、用户配置信息（接入用 IP 地址、网关 IP 地址、DNS 服务器地址等）、用户有效期等，可对以上参数进行修改、添加、删除等操作。

5） 其他参数配置

安全认证网关产品可提供协议和接口接受管理中心远程对其其他功能模块的参数进行设置。

c） 远程监控

1） 参数查询

安全认证网关产品可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、用户参数等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

安全认证网关产品可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等系统资源的占有率）、系统信息（开机时间、运行时间、系统时间和设备名字及 IP 等）、网络流量、是否在线、隧道状态（建立时间、加密流量、有效期等）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

安全认证网关产品可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等操作。

4） 时间同步

安全认证网关产品可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：

- 操作行为，包括登录认证、参数配置、系统配置、策略配置、密钥管理等操作。
- 用户访问行为，包括用户、时间、访问资源、结果等。
- 安全事件，密钥交换成功及失败、密钥过期、隧道建立及删除等事件。
- 异常事件，解密失败、完整性校验失败、认证失败、非法访问等异常事件的统计。

7.4.2.2 管理员管理

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、备份和恢复等操作。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。

登录口令长度应不小于 8 个字符。

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，除必须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、管理员的产生等均应由用户完成。初始化数据中如含有私钥等敏感信息应提供安全 IC 卡或安全 Key 等硬件介质承载。

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，需要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。注册和监控过程应符合国家密码管理主管部门的要求。

7.4.2.3.3 设备自检

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。

应对密码运算部件等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。

应对存储的密钥等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。

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规定。

应对身份鉴别介质及其接口进行检查，确保其正常工作。

可对 CPU、内存、网络接口、非易失性存储介质等物理部件进行常规检查，确保各关键部件正常工作。

对算法正确性、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 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，可以通过 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经过国家密码管理主管部门审批的密码机或加密卡作为主要加密部件。

7.5.3 随机数发生器

随机数发生器采用国家密码管理主管部门批准的物理噪声源，应提供多路随机源，至少采用两个独立的物理噪声源芯片实现。

安全认证网关产品应提供随机数采集接口。随机数发生器应支持出厂检测、上电检测、使用检测三种检测方式：

a) 出厂检测：
   - 检测量：采集 50×10^6 比特随机数，分成 50 组，每组 10^6 比特；
   - 检测项目：依据 GM/T 0005 进行检测；
   - 检测通过标准：检测中如果有一项不通过检测标准，则告警检测不合格。
     允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

b) 上电检测：
   - 检测量：采集 20×10^6 比特随机数，分成 20 组，每组 10^6 比特；
   - 检测项目：依据 GM/T 0005 进行检测；
   - 检测通过标准：检测中如果有一项不通过检测标准，则告警检测不合格。

允许重复1次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

c) 使用检测：

1) 周期检测：

- 检测量：采集 4×10^5 比特随机数，分成20组，每组20000比特；
- 检测项目：对采集随机数按照GM/T 0005中除离散傅立叶检测、线性复杂度检测、通用统计检测外的12项项目检测；
- 检测通过标准：检测中如果有一项不通过检测标准，则告警检测不合格；
  允许重复1次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效；
- 检测周期：可配置，检测间隔最长不超过12 h。

2) 单次检测：

- 检测量：根据实际应用时每次所采随机数大小确定，但长度不应低于128比特，且已通过检测的未用序列可继续用；
- 检测项目：扑克检测。当样本长度小于320比特时，参数 $m=2$；
- 检测通过标准：检测中如果不通过检测标准，则告警检测不合格。
  允许重复1次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

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遵循GB/T 9813—2000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，见GB/T 15153.1—1998对电磁兼容性的要求。

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10000 h，平均可持续加密流量应不低于10000 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 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

8.1 产品功能检测

8.1.1 用户管理

对安全认证网关的用户进行修改、增删、查询用户证书信息、用户分组等操作，网关可以安全实现这些功能。

8.1.2 身份鉴别

按相应的数字证书技术规范进行协商，应能成功完成用户身份鉴别的过程。

8.1.3 应用管理

录入不同的应用信息，安全认证网关应可以对应用信息进行增删改查。

8.1.4 访问控制

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

8.1.5 单点登录

检测结果应符合 7.1.5 的要求。

8.1.6 信息审计

检测结果应符合 7.1.6 的要求。

8.1.7 随机数功能

按照 GM/T 0005 的要求提取样本，并按照该规范的相关要求进行检测，检测结果应合格。

8.1.8 工作模式

对于遵循 IPSec 协议的安全认证网关产品，将测试设备与被测设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；被测设备支持传输模式时，将测试设备与被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；将测试设备与被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。

对于遵循 SSL 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。

8.1.9 密钥交换

遵循 IPSec 协议的安全认证网关产品的密钥交换检测应按 GM/T 0022 进行；遵循 SSL 协议的安全认证网关产品的密钥交换检测应按 GM/T 0024 进行。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。

8.1.10 安全报文传输

对于遵循 IPSec 协议的安全认证网关产品，将测试设备与被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；将测试设备与被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。

对于遵循 SSL 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。

8.1.11 密钥更新

在被测设备上分别设定密钥的更新周期，当满足更新条件时，使用网络报文截获工具应能分别看到

相应的密钥的协商过程。

8.1.12 NAT 穿越

检测结果符合 7.1.12 的要求。

8.1.13 抗重放攻击

检测结果符合 7.1.13 的要求。

8.1.14 客户端主机安全检查

检测结果符合 7.1.14 的要求。

8.2 产品性能检测

8.2.1 遵循 IPSec 协议的安全认证网关产品

对于遵循 IPSec 协议的安全认证网关产品来说,需要检测的产品性能主要包括以下五个指标:

- 加解密吞吐率;
- 加解密时延;
- 加解密丢包率;
- 每秒新建隧道数;
- 最大并发隧道数。

8.2.2 遵循 SSL 协议的安全认证网关产品

对于遵循 SSL 协议的安全认证网关产品来说,产品的性能检测主要包括:

- 最大并发用户数;
- 最大并发连接数;
- 每秒新建连接数;
- 吞吐率。

8.3 安全管理检测

8.3.1 安全检测

8.3.1.1 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相应的产品规范要求。

8.3.1.2 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。

8.3.1.2.1 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要求。

8.3.1.2.2 软件安全

使用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。

8.3.1.2.3 客户端安全

检测结果应符合 7.3.2.3 的要求。

8.3.1.3 管理安全

8.3.1.3.1 分权管理

检测结果应符合 7.3.3.1 的要求。

8.3.1.3.2 管理员登录安全

检测结果应符合 7.3.3.2 的要求。

8.3.2 管理检测

8.3.2.1 日志管理安全

可以查看并导出日志记录。日志格式应符合国家密码管理主管部门的要求。

8.3.2.2 人员管理

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。

8.3.2.3 设备管理

8.3.2.3.1 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。

8.3.2.3.2 注册和监控

当系统有管理中心时,进行设备的注册、状态监控等管理操作。结果应符合相应产品规范的要求。

8.3.2.3.3 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。

8.3.2.4 远程管理

8.3.2.4.1 合规性验证

检测结果应符合 7.4.1a)的要求。

8.3.2.4.2 远程参数配置

检测结果应符合 7.4.1b)的要求。

8.3.2.4.3 远程监控

检测结果应符合 7.4.1c)的要求。

8.4 硬件检测

8.4.1 对外接口

检测结果应符合 7.5.1 的要求。

8.4.2 加密部件

检测结果应符合 7.5.2 的要求。

8.4.3 随机数发生器

检测结果应符合 7.5.3 的要求。

8.4.4 环境适应性

检测结果应符合 7.5.4 的要求。

8.4.5 电磁兼容性

检测结果应符合 7.5.5 的要求。

8.4.6 可靠性

检测结果应符合 7.5.6 的要求。

9 合格判定

符合本标准的安全认证网关产品判定为合格产品；

8.1 和 8.3(除 8.3.1.2)中的任意一项不合格，判定为产品不合格。