ICS 35.040
L 80
备案号:44626—2014

GM

中华人民共和国密码行业标准

GM/T 0025—2014

SSL VPN 网关产品规范

SSL VPN 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
SSL VPN 网关产品规范
GM/T 0025—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　字数 24 千字
2014 年 5 月第一版　2014 年 5 月第一次印刷
*
书号:155066·2-27027　定价 18.00 元

GM/T 0025-2014

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语、定义和缩略语 …… 1
3.1　术语和定义 …… 1
3.2　缩略语 …… 2
4　密码算法和密钥种类 …… 2
4.1　算法要求 …… 2
4.2　密钥种类 …… 3
5　SSL VPN 网关产品要求 …… 3
5.1　产品功能要求 …… 3
5.2　产品性能参数 …… 4
5.3　安全性要求 …… 5
5.4　管理要求 …… 6
5.5　过程保护 …… 8
5.6　参数可配置能力要求 …… 8
6　SSL VPN 网关产品检测 …… 8
6.1　产品功能检测 …… 8
6.2　产品性能检测 …… 9
6.3　安全性检测 …… 10
6.4　安全管理检测 …… 10
7　合格判定 …… 11

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、山东得安计算机技术有限公司、成都卫士通信息产业股份有限公司、上海市数字证书认证中心有限公司、兴唐通信科技有限公司、北京数字认证股份有限公司。

本标准主要起草人：谭武征、孔凡玉、李元正、刘承、李述胜、王妮娜、韩琳。

引　言

本标准主要依据国家密码管理局制定的《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 SSL VPN 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。

SSL VPN 网关产品规范

1 范围

本标准规定了 SSL VPN 网关产品的功能要求、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 SSL VPN 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 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 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0024 SSL VPN 技术规范

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

密码算法 cryptographic algorithm

描述密码处理过程的运算规则。

3.1.2

密码杂凑算法 cryptographic 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。

3.1.3

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。

3.1.4

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。

3.1.5

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。

3.1.6

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。

3.1.7

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。

3.1.8

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。

3.1.9

SSL 协议　secure sockets layer protocol;SSL

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。

3.1.10

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。

3.1.11

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。

3.2　缩略语

下列缩略语适用于本文件。

CBC:密码分组链接(Cipher Block Chaining)

IV:初始化向量(Initialization Vector)

SSL:安全套接层协议(Secure Sockets Layer)

VPN:虚拟专用网络(Virtual Private Network)

4　密码算法和密钥种类

4.1　算法要求

SSL VPN 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,见 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 的检测。

4.2 密钥种类

4.2.1 服务端密钥

服务端密钥为非对称密码算法的密钥对，包括签名密钥对和加密密钥对，其中签名密钥对由 VPN 自身密码模块产生，加密密钥对应通过 CA 认证中心向 KMC 申请。用于握手过程中服务端身份鉴别和预主密钥的协商。

4.2.2 客户端密钥

客户端密钥为非对称密码算法的密钥对，包括签名密钥对和加密密钥对，其中签名密钥对由 VPN 自身密码模块产生，加密密钥对应通过 CA 认证中心向 KMC 申请。用于握手过程中客户端身份鉴别和预主密钥的协商。

4.2.3 预主密钥

预主密钥(pre_master_secret)是双方协商生成的密钥素材，用于生成主密钥。

4.2.4 主密钥

主密钥(master_secret)由预主密钥、客户端随机数、服务端随机数、常量字符串，经计算生成的密钥素材，用于生成工作密钥。

4.2.5 工作密钥

工作密钥包括数据加密密钥和校验密钥。其中数据加密密钥用于数据的加密和解密，校验密钥用于数据的完整性计算和校验。在本标准中，发送方使用的工作密钥称为写密钥，接收方使用的工作密钥称为读密钥。

5 SSL VPN 网关产品要求

5.1 产品功能要求

5.1.1 随机数生成

SSL VPN 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。

5.1.2 工作模式

SSL VPN 网关产品工作模式分为客户端-服务端模式和网关-网关模式两种。其中客户端-服务端模式是必备模式，网关-网关模式是可选模式。

5.1.3 密钥交换

SSL VPN 网关产品应具有密钥交换功能，通过协商产生工作密钥。

密钥交换应按照 GM/T 0024 的要求进行。

5.1.4 安全报文传输

SSL VPN 网关产品具有安全报文传输功能，保证数据的安全传输。

安全报文传输应按照 GM/T 0024 的要求进行。

5.1.5 身份鉴别

SSL VPN 网关产品应具有实体鉴别的功能，鉴别方式采用数字证书。数字证书格式应满足GM/T 0015的要求。服务端的鉴别是必备功能，客户端的鉴别是可选功能，应支持基于数字证书(RSA或 SM2)或者基于标识算法的监别机制。任何一种鉴别方式都需要保证鉴别的完整性和有效性。

5.1.6 访问控制

SSL VPN 网关产品应具有细粒度的访问控制功能，基于用户或用户组对资源进行有效控制。其中对网络访问至少应控制到 IP 地址、端口和协议，对 Web 资源的访问至少应控制到 URL，并能根据访问时间进行控制。

5.1.7 密钥更新

SSL VPN 网关产品应具有根据时间周期或报文流量进行工作密钥更新的功能。其中，根据时间周期进行更新为必备功能，根据报文流量进行更新为可选功能。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。

5.1.8 信息审计

SSL VPN 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、访问资源、上传流量、下载流量、访问结果、错误原因。

5.1.9 信息传递

SSL VPN 网关应具有信息传递功能，用户访问 HTTP 应用时，系统在完成相应的身份监别后，把验证结果、用户的基本信息插入到 HTTP 请求中传送给后台的应用系统，应用系统通过标准的 HTTP 操作即可获取信息，并基于该信息作相应的访问控制以及进行相应的业务审计。获取的信息包括：用户 IP 地址，用户证书的关键信息。

5.1.10 客户端主机安全检查

SSL VPN 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 SSL VPN。

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。

5.2 产品性能参数

5.2.1 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。

5.2.2 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。

5.2.3 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。

5.2.4 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。

5.3 安全性要求

5.3.1 密钥安全

5.3.1.1 服务器端密钥

服务端签名密钥对由 SSL VPN 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。

服务端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 SSL VPN 网关产品中。

在 SSL VPN 网关产品中，服务端密钥的私钥应有安全保护措施。

服务端密钥应按设定的安全策略进行更新。

服务端密钥可以安全形式进行备份，并在需要时能够恢复。

5.3.1.2 工作密钥

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。

5.3.1.3 会话密钥

会话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。

5.3.2 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。

5.3.2.1 硬件安全

SSL VPN 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。

5.3.2.2 软件安全

所有的安全协议及管理软件应自主实现源代码完全可控。

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。

5.3.2.3 客户端安全

SSL VPN 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。

5.3.3 管理安全

5.3.3.1 分权管理

管理员包括系统管理员、安全管理员、审计管理员三类，这三类管理员对系统进行分权管理。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。

5.3.3.2 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 SSL VPN 网关进行管理配置，管理员只能通过被授权的终端登录到 SSL VPN 网关进行相应的配置操作。

5.4 管理要求

5.4.1 日志管理

SSL VPN 网关产品应提供日志记录、查看和导出功能。SSL VPN 网关产品的客户端不要求日志管理。

日志内容包括：

- 管理员操作行为，包括用户管理、登录认证、系统配置、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；
- 异常事件，包括认证失败、非法访问等异常事件的记录。

日志格式要包括事件发生的日期和时间、主体身份和事件内容。

5.4.2 管理员管理

SSL VPN 服务端产品应设置管理员，进行系统配置、密钥生成、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。

5.4.3 设备管理

5.4.3.1 设备初始化

SSL VPN 网关产品的初始化，除必须由厂商进行的操作外，系统配置、密钥的生成和管理、管理员的产生等均应由用户完成。

5.4.3.2 设备自检

SSL VPN 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、非对称和杂凑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。

5.4.4 硬件要求

5.4.4.1 对外接口

SSL VPN 网关产品应分别具有工作网口和管理接口。其中管理接口应包括本地维护接口和远程管理接口，可以采用网口或串口通信；工作网口应至少具备两个，分别为内网接口和外网接口。

5.4.4.2 加密部件

SSL VPN 网关产品应采用经过国家密码管理主管部门审批的加密芯片或加密卡作为主要加密部件。

5.4.4.3 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。

SSL VPN 网关产品应提供随机数采集接口。随机数发生器能通过送样检测、出厂检测、上电检测和使用检测四个不同应用阶段的随机数检测：

a) 送样检测：

依据 GM/T 0005 进行随机数检测。

b) 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。

c) 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。

d) 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 随机性检测规范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。

5.4.4.4 环境适应性

SSL VPN 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。

5.4.4.5 电磁兼容性

SSL VPN 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。

5.4.4.6 可靠性

SSL VPN 网关产品的平均无故障工作时间应不低于 10000 h。

5.5 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。

5.6 参数可配置能力要求

SSL VPN 网关产品可支持对设备的相关参数进行配置，包括网络接口的 MTU（最大传输单元）、MAC 地址、速度（自适应或者固定速率）、双工/半双工、是否开启流控等。

6 SSL VPN 网关产品检测

6.1 产品功能检测

6.1.1 工作模式

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。检测结果应符合 5.1.1 的要求。

6.1.2 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，检测结果应符合 5.1.1 的要求。

6.1.3 密钥交换

密钥交换协议应按照 GM/T 0024 的要求进行。检测结果应符合 5.1.3 的要求。

6.1.4 安全报文传输

安全报文封装协议应按照 GM/T 0024 的要求进行。检测结果应符合 5.1.4 的要求。

6.1.5 身份鉴别

身份鉴别应按照 GM/T 0024 的要求进行。检测结果应符合 5.1.5 的要求。

6.1.6 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 5.1.6 的要求。

6.1.7 密钥更新

密钥更新应按照 GM/T 0024 的要求进行。检测结果应符合 5.1.7 的要求。

6.1.8 信息审计

用户通过访问后,系统应能对用户访问信息进行记录。检测结果应符合 5.1.8 的要求。

6.1.9 信息传递

用户通过 SSL VPN 访问 HTTP 应用时,应用系统可以从 HTTP 请求信息中获取用户信息。检测结果应符合 5.1.9 的要求。

6.2 产品性能检测

6.2.1 最大并发用户数

最大并发用户数是指在同一时刻能够与服务器进行交互的在线用户的最大数量。这些用户的最大特征是和服务器产生了交互,这种交互既可以是单向的传输数据,也可以是双向的传送数据。在检测平台模拟多个客户端行为,与服务端建立 SSL 会话,在这个会话上,从内网服务器下载 512 字节页面的数据,并在内网服务器上设置页面延迟,以保证在整个负载增加的过程中每一个会话均被保持且有数据通过。然后,不断增加客户端,并重复此过程,取负载稳定期的平均并发会话数作为测试结果。

6.2.2 最大并发连接数

最大并发连接数是指在同一时刻能够与服务器进行交互的连接的最大数量。在检测平台模拟多个客户端行为,与服务端进行 SSL 连接并保持,然后不断增加客户端,并重复此过程,直到无法建立并保持连接为止。取已经接入的 SSL 连接数目为测试结果。

6.2.3 每秒新建连接数

在检测平台模拟多个客户端行为,并发与服务端建立 SSL 会话。重复此过程一段时间,取每秒建立 SSL 会话数目的平均值作为测试结果。

6.2.4 吞吐率

在检测平台模拟多个客户端行为,与服务端建立 SSL 会话。在这个会话上,从内网服务器下载 1MB 数据,重复以上步骤,直到每个用户成功下载 20MB 大小的数据。然后向内网服务器上传 1MB 数据,重复以上步骤,直到每个用户成功上传 20MB 大小的数据。取内网服务器收发数据的平均速率作为

测试结果。

6.3 安全性检测

6.3.1 密钥安全

6.3.1.1 服务端密钥

检测结果应符合5.3.1.1的要求。

6.3.1.2 工作密钥

检测结果应符合5.3.1.2的要求。

6.3.2 配置数据安全

检测结果应符合5.3.2的要求。

6.3.2.1 硬件安全

检测结果应符合5.3.2.1的要求。

6.3.2.2 软件安全

检测结果应符合5.3.2.2的要求。

6.3.2.3 客户端安全

检测结果应符合5.3.2.3的要求。

6.3.3 管理安全

6.3.3.1 分权管理

检测结果应符合5.3.3.1的要求。

6.3.3.2 管理员登录安全

检测结果应符合5.3.3.2的要求。

6.4 安全管理检测

6.4.1 日志管理

检测结果应符合5.4.1的要求。

6.4.2 管理员管理

检测结果应符合5.4.2的要求。

6.4.3 设备管理

6.4.3.1 设备初始化

检测结果应符合5.4.3.1的要求。

6.4.3.2 设备自检

检测结果应符合5.4.3.2的要求。

6.4.4 硬件要求

6.4.4.1 对外接口

检测结果应符合5.4.4.1的要求。

6.4.4.2 加密部件

检测结果应符合5.4.4.2的要求。

6.4.4.3 随机数发生器

检测结果应符合5.4.4.3的要求。

6.4.4.4 环境适应性

检测结果应符合5.4.4.4的要求。

6.4.4.5 电磁兼容性

检测结果应符合5.4.4.5的要求。

6.4.4.6 可靠性

检测结果应符合5.4.4.6的要求。

7 合格判定

本标准中,6.1、6.3(除6.3.2)和6.4中的任意一项不合格,判定为产品不合格。