

ICS 35.040  
A 90

# GA

## 中华人民共和国公共安全行业标准

GA/T 686—2007

GA/T 686—2007

### 信息安全技术 虚拟专用网安全技术要求

Information security technology—  
Technical requirements of virtual private network security

中华人民共和国公共安全  
行业标准  
信息安全技术  
虚拟专用网安全技术要求  
GA/T 686—2007

\*

中国标准出版社出版发行  
北京复兴门外三里河北街16号  
邮政编码:100045

网址 [www.spc.net.cn](http://www.spc.net.cn)  
电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷  
各地新华书店经销

\*

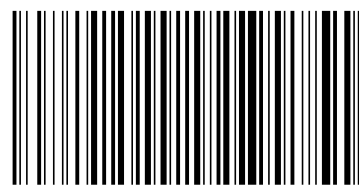
开本 880×1230 1/16 印张 2.75 字数 75 千字  
2007年8月第一版 2007年8月第一次印刷

\*

书号:155066·2-17984 定价 30.00 元

如有印装差错 由本社发行中心调换  
版权专有 侵权必究

举报电话:(010)68533533



GA/T 686—2007

2007-03-20 发布

2007-05-01 实施

中华人民共和国公安部 发布

全策略,并提供所要求的附加服务。VPN 中,VPN 安全设施是一个物理上分散、逻辑上统一的分布式 VPN 安全设施。

#### A.5 关于密码技术

密码技术是 VPN 安全保护的关键技术。在不同安全保护等级中所采用的不同安全策略,应选取不同配置的密码技术作为构成 VPN 安全保护的重要机制,或将密码技术与系统安全技术相结合,组成统一的安全机制。利用密码功能可提供的以下支持:标识与鉴别、抗抵赖、数据加密保护、数据的完整性保护等。若采用 PKI 技术,则应参照相应 PKI 的技术要求实施。各个安全等级密码技术的具体配置由国家密码主管部门决定。本标准对于密码的应用不作详细的要求。

## 目 次

前言 .....	V
引言 .....	VI
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语、定义和缩略语 .....	1
4 VPN 的一般说明 .....	2
4.1 概述 .....	2
4.2 安全环境 .....	2
4.2.1 安全威胁 .....	2
4.2.2 安全应用假设 .....	3
5 安全功能技术要求 .....	3
5.1 标识和鉴别 .....	3
5.1.1 用户标识 .....	3
5.1.2 用户鉴别 .....	3
5.1.3 鉴别失败处理 .....	4
5.1.4 用户-主体绑定 .....	4
5.2 安全审计 .....	4
5.2.1 安全审计的响应 .....	4
5.2.2 安全审计数据产生 .....	4
5.2.3 安全审计分析 .....	5
5.2.4 安全审计查阅 .....	5
5.2.5 安全审计事件存储 .....	5
5.2.6 网络环境安全审计与评估 .....	5
5.3 通信抗抵赖 .....	6
5.3.1 抗原发抵赖 .....	6
5.3.2 抗接收抵赖 .....	6
5.4 标记 .....	6
5.5 自主访问控制 .....	7
5.6 强制访问控制 .....	7
5.7 用户数据存储保护 .....	7
5.8 用户数据传输保护 .....	7
5.8.1 VPN 内数据传输保护 .....	7
5.8.2 VPN 向公用网络输出数据的保护 .....	7
5.8.3 公用网络向 VPN 输入数据的保护 .....	8
5.9 用户数据完整性保护 .....	8
5.9.1 存储数据的完整性 .....	8
5.9.2 传输数据的完整性 .....	8
5.9.3 处理数据的完整性 .....	8

5.10	剩余信息保护	8
5.11	隐蔽信道分析	8
5.11.1	一般性的隐蔽信道分析	8
5.11.2	系统化的隐蔽信道分析	9
5.11.3	彻底化的隐蔽信道分析	9
5.12	可信路径	9
5.13	密码支持	9
6	安全保证技术要求	9
6.1	VPN 安全功能自身安全保护	9
6.1.1	安全运行测试	9
6.1.2	失败保护	9
6.1.3	输出 VPN 安全功能数据的可用性	9
6.1.4	输出 VPN 安全功能数据的保密性	10
6.1.5	输出 VPN 安全功能数据的完整性	10
6.1.6	VPN 内 VPN 安全功能数据传输	10
6.1.7	物理安全保护	10
6.1.8	可信恢复	10
6.1.9	重放检测	11
6.1.10	参照仲裁	11
6.1.11	域分离	11
6.1.12	状态同步协议	11
6.1.13	时间戳	11
6.1.14	数据一致性	11
6.1.15	安全功能检测	11
6.1.16	资源利用	11
6.1.17	VPN 安全设施访问控制	12
6.1.18	可信路径/信道	12
6.2	VPN 设计和实现	13
6.2.1	配置管理	13
6.2.2	分发和操作	14
6.2.3	开发	14
6.2.4	指导性文档	16
6.2.5	生命周期支持	16
6.2.6	测试	17
6.2.7	脆弱性评定	18
6.3	VPN 安全设施安全管理	19
6.3.1	功能管理	19
6.3.2	安全属性的管理	19
6.3.3	VPN 安全功能数据的管理	19
6.3.4	安全角色管理	19
6.3.5	时限授权	20
6.3.6	撤销	20
7	VPN 安全保护等级划分要求	20

表 A.2 (续)

保证要求分类	保证要求详细分类	第一级	第二级	第三级	第四级	第五级
VPN 安全功能自身安全保护	参照仲裁			+	+	+
	域分离			+	++	+++
	状态同步协议			+	++	+++
	时间戳	+	+	+	+	+
	数据一致性			+	+	+
	安全功能检测	+	+	++	++	++
	可信路径/信道				+	+
资源利用	故障容错	+	+	++	++	++
	服务优先级	+	+	++	++	++
	资源分配	+	+	++	++	++
VPN 安全设施访问控制	+	++	+++	+++	+++	
VPN 安全设施设计和实现	配置管理	+	++	+++	++++	+++++
	分发和操作	+	++	+++	++++	+++++
	开发	+	++	+++	++++	+++++
	指导性文档	+	++	++	++	++
	生命周期支持	+	++	+++	++++	+++++
	测试	+	++	+++	++++	+++++
VPN 安全设施安全管理	脆弱性评定		+	++	++++	+++++
	功能管理	+	+	+	+	+
	安全属性的管理			+	+	+
	VPN 安全功能数据的管理			+	++	++
	安全管理角色	+	++	+++	+++	+++
	时限授权			+	+	+
	撤销			+	+	+

### A.3 关于 VPN 中的主体与客体

在 VPN 中,每一个实体成分都应是主体或客体,或既是主体又是客体。主体是一个主动的实体,它包括用户、用户组、终端、主机或一个应用。系统中最原始的主体应是用户(包括一般用户、系统管理员、系统安全员、系统审计员等)。每个进入系统的用户应是唯一标识的,并经过鉴别确定为真实的。

### A.4 关于 VPN 中的安全设施、安全功能和安全功能策略

在 VPN 中,VPN 安全设施(可信计算基)是构成一个安全的 VPN 的所有安全保护装置的组合体。一个 VPN 安全设施可以包含多个 TSF(VPN 安全设施安全功能模块),每个 TSF 是一个或多个 VPN 安全功能策略的实现。TSP(VPN 安全设施安全功能策略)是这些 VPN 安全功能策略的总称,构成一个安全域,以防止不可信主体的干扰和篡改。实现 TSF(VPN 安全设施安全功能策略)有两种方法,一种是设置前端过滤器,另一种是设置访问监督器。两者都是在一定硬件基础上通过软件实现确定的安