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

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

2007-03-20 发布　　2007-05-01 实施

中华人民共和国公安部　　发布

GA/T 686—2007

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
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

GA/T 686-2007

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

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	+	++	+++	++++	++++
	脆弱性评定		+	++	++++	++++
VPN 安全设施安全管理	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