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

目　　次

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。