ICS 35.040
L 80
备案号:44625—2014

GM

中华人民共和国密码行业标准

GM/T 0024—2014

SSL VPN 技术规范

SSL VPN 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、华为技术有限公司、深圳市深信服电子科技有限公司、深圳市奥联科技有限公司、网御神州科技（北京）有限公司、成都卫士通信息产业股份有限公司、北京东方华盾信息技术有限公司、中国国际电子商务有限公司、联想网御科技（北京）有限公司、上海安达通信息安全有限公司、无锡江南信息安全工程技术中心、北京天融信网络安全技术有限公司。

本标准主要起草人：刘平、谭武征、黄敏、曾建发、但波、刘建锋、罗俊、李志超、李飞伯、何致宇、陈凯、朱正超、倪永年、韩琳。

引　言

本标准的协议内容参照传输层安全协议(RFC4346 TLS1.1),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践经验,在 TLS1.1 的握手协议中增加了 ECC、IBC 的认证模式和密钥交换模式,取消了 DH 密钥交换方式,修改了密码套件的定义。另外,在本标准中还增加了网关-网关协议。

SSL VPN 技术规范

1 范围

本标准对 SSL VPN 的技术协议、产品的功能、性能和管理以及检测进行了规定。

本标准适用于 SSL VPN 产品的研制，也可用于指导 SSL VPN 产品的检测、管理和使用。

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。

GM/T 0005 随机性检测规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0010 SM2 密码算法加密签名消息语法规范

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

3 术语和定义

下列术语和定义适用于本文件。

3.1

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。

3.2

IBC 算法 identity based cryptography algorithm

IBC 算法又称为标识密码算法，是一种能以任意标识作为公钥，不需要使用数字证书证明公钥的非对称密码算法。

3.3

IBC 标识 IBC identity

IBC 标识是表示实体身份或属性的字符串。

3.4

IBC 公共参数 IBC public parameter

IBC 公共参数包含了 IBC 密钥管理中心的名称、运算曲线、标识编码方式和密钥生成算法等公开参数信息，这些信息用于将实体标识转换为公开密钥。

3.5

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作数据变换的起始数据。