ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0024—2023
代替 GM/T 0024—2014

SSL VPN 技术规范

SSL VPN specification

2023-12-04 发布　　2024-06-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GM/T 0024—2014《SSL VPN技术规范》，与GM/T 0024—2014相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了GB/T 36624—2018（见5.1.2）、GB/T 25069（见第2章）、GM/T 0081—2020（见6.4.5.3和6.4.5.4）、GM/T 0090—2020（见6.4.5.3）和GM/Z 4001（见第2章）；

b) 删除了术语“数字证书”（见2014年版的3.1）、“初始化向量/值”（见2014年版的3.5）、“SSL协议”（见2014年版的3.6）、“载荷”（见2014年版的3.7）、“会话”（见2014年版的3.8）、“SM1算法”（见2014年版的3.9）、“SM2算法”（见2014年版的3.10）、“SM3算法”（见2014年版的3.11）、“SM4算法”（见2014年版的3.12）、“SM9算法”（见2014年版的3.13）、“椭圆曲线密码算法”（见2014年版的3.14）、“RSA算法”（见2014年版的3.15）、“证书认证机构”（见2014年版的3.16）和“密钥管理中心”（见2014年版的3.17）；

c) 增加了缩略语“AEAD”“ADD”“GCM”“HMAC”“IV”和“TLCP”（见4.2）；

d) 删除了SHA-1算法及SM1算法的介绍（见2014年版的5.1.2和5.1.3），增加了GCM加密模式（见5.1.2）；

e) 更改了客户端密钥中的签名密钥由对应的客户端密码模块产生（例如智能密码钥匙）（见5.2.6，2014年版的5.2.3）；

f) 增加了密码杂凑算法的描述（见5.1.3）；

g) 增加了对版本号值的定义[见6.3.3.2b)]；

h) 增加了fixed_iv_length固定的初始向量长度（见6.3.2）；

i) 增加了客户端写初始向量client write iv和服务端写初始向量server write iv（见6.3.2）；

j) 增加了“带关联数据的可鉴别的加密（AEAD）的数据处理”（见6.3.3.4.4）

k) 更改了表2“密码套件列表”（见表2，2014年版的表2）；

l) 增加了是否需要扩展的选择和extensions的描述（见6.4.5.2.1和6.4.5.2.2）；

m) 增加了“Hello消息扩展字段”（见6.4.5.2.3）；

n) 更改了certificate_types中的一个枚举类型[见6.4.5.5a)，2014年版的6.4.4.4a)]

o) 增加了client_write_IV[SecurityParameters.fixed_iv_length]和server_write_IV[Secu rityParameters.fixed_iv_length]（见6.5.2）；

p) 更改了Client Key Exchange消息中的PKCS#1版本为2.1（见6.4.5.8，2014年版的6.4.4.7）；

q) 更改了Certificate Verify消息中的opaque sha1_hash[20]（见6.4.5.9，2014年版的6.4.4.8）；

r) 增加了Client Hello消息的扩展字段client_id（见6.4.5.2.3）；

s) 增加了Server Certificate消息中ibc_parameter字段的内容定义（见6.4.5.3）；

t) 更改了Server Key Exchange消息signed_params中，当密钥交换算法为IBC时的内容定义（见6.4.5.4，2014年版的6.4.4.3）；

u) 删除了“身份鉴别”（见2014年版的7.1.5）；

v) 更改了报文流量为“必备”功能（见7.1.6，2014年版的7.1.7）；

w) 删除了“客户端主机安全检查”（见2014年版的7.1.8）；

x) 更改了“服务端密钥”的描述（见7.3.1.1，2014年版的7.3.1.1.1）；

y) 更改了“SSL”名称为“TLCP”(见 7.2.1 和 7.2.2,2014 年版的 7.2.2 和 7.2.3);

z) 增加了“实例释放”时应销毁(见 7.3.1.1);

aa) 更改了“硬件安全”的标题和内容(见 7.3.1.3,2014 年版的 7.3.1.2.1);

bb) 增加了“扩展字段说明”(见附录 A)。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位:格尔软件股份有限公司,北京信安世纪科技股份有限公司、蚂蚁科技集团股份有限公司、飞天诚信股份有限公司、山东渔翁信息技术股份有限公司、山东得安信息技术有限公司、北京天威诚信电子商务服务有限公司、广东省电子商务认证有限公司、北京国脉信安科技有限公司、智巡密码(上海)检测技术有限公司、天融信科技股份有限公司、山东大学、华为技术有限公司、阿里云计算有限公司、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、中电科网络安全科技股份有限公司、无锡江南信息安全工程技术中心、长春吉大正元信息技术股份有限公司、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。

本文件主要起草人:刘平、郑强、汪宗斌、杨洋、李延昭、谭武征、黄敏、朱鹏飞、罗俊、王鹏、胡金山、赵敏、梁宁宁、药乐、韩玮、安高峰、孔凡玉、曾建发、但波、韩琳。

本文件所代替文件的历次版本发布情况为:

——2014 年首次发布为 GM/T 0024—2014;

——本次为第一次修订。

SSL VPN 技术规范

1 范围

本文件规定了 SSL VPN 的技术协议、产品功能要求、产品性能参数和安全管理要求。

本文件适用于 SSL VPN 产品的研制，也适用于指导 SSL VPN 产品的检测、管理和使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 25069 信息安全技术 术语

GB/T 36624—2018 信息技术 安全技术 可鉴别的加密机制

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 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0081—2020 SM9 密码算法加密签名消息语法规范

GM/T 0090—2020 标识密码应用标识格式规范

GM/Z 4001 密码术语

3 术语和定义

GB/T 25069 和 GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

IBC 算法 identity based cryptography algorithm

基于用户/实体唯一性身份标识和系统主密钥而生成用户密钥的密码机制。

3.2

IBC 标识 IBC identity

由实体无法否认的信息组成，可唯一确定一个实体的身份。

注：如实体的可识别名称、电子邮箱、身份证号、电话号码、街道地址等。

3.3

IBC 公共参数 IBC public parameter

为 IBC 系统的用户提供包括密码算法参数、系统策略和用户标识变化等相关公开信息的服务。

4 符号和缩略语

4.1 符号

下列符号适用于本文件。