ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38636—2020

信息安全技术　传输层密码协议(TLCP)

Information security technology—Transport layer cryptography protocol(TLCP)

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:山东得安信息技术有限公司、格尔软件股份有限公司、北京信安世纪科技有限公司、成都卫士通信息产业股份有限公司、长春吉大正元信息技术股份有限公司、北京握奇智能科技有限公司、北京三未信安科技发展有限公司、北京海泰方圆科技有限公司、国家密码管理局商用密码检测中心、北京江南天安科技有限公司、中金金融认证中心有限公司、北京天融信网络安全技术有限公司。

本标准主要起草人:郑强、马洪富、汪宗斌、罗俊、赵丽丽、张立廷、汪雪林、田敏求、张岳公、蒋红宇、吕春梅、李国、孙圣男、雷晓锋。

信息安全技术　传输层密码协议(TLCP)

1　范围

本标准规定了传输层密码协议,包括记录层协议、握手协议族和密钥计算。

本标准适用于传输层密码协议相关产品(如 SSL VPN 网关、浏览器等)的研制,也可用于指导传输层密码协议相关产品的检测、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。

GB/T 20518　信息安全技术　公钥基础设施　数字证书格式规范

GB/T 35275　信息安全技术　SM2 密码算法加密签名消息语法规范

GB/T 35276　信息安全技术　SM2 密码算法使用规范

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

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。

注: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

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

表示实体身份或属性的字符串。

3.4

IBC 公共参数　IBC public parameter

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。

注:参数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。

4　符号和缩略语

4.1　符号

下列符号适用于本文件。