ICS 35.020
L 80

中华人民共和国国家标准

GB/T 28457—2012

SSL 协议应用测试规范

Testing specification for applications of SSL protocol

2012-06-29 发布　　2012-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国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。

本标准的起草单位:信息工程大学信息工程学院。

本标准的主要起草人:颜学雄、王清贤、曾勇军、刘琰、耿俊燕、尹中旭。

引　言

目前，市场上 SSL 协议应用相关产品比较多，为了保证相关产品的质量，需对其进行测试。为统一产品的开发方、第三方授权测试认证单位和产品用户方对 SSL 协议应用相关产品的测试活动，并便于实现测试结果的相互认可和可重复性，特制定本标准。本标准规范了 SSL 协议应用相关产品的测试内容和基本测试过程。

为消除自然语言描述带来的二义性，本标准以有限状态自动机理论为基础，建立了 SSL 协议规范的形式化模型，并由此模型生成 SSL 协议应用的功能测试规范。相应的形式化模型见附录 A。

目前，还没有标准化的 SSL 协议应用测试工具。本标准没有规范具体的测试工具和测试环境，但为了规范测试人员的测试活动，本标准给出了测试指南，旨在规范测试基本步骤和关键要点，测试人员可以在此基础上，选择相关的辅助工具，产生具体的测试用例，并进行测试。

SSL 协议应用测试规范

1 范围

本标准规定了 SSL 协议应用的测试内容和基本测试步骤。

本标准适用于 SSL 协议应用的开发单位、第三方授权测试认证机构、用户等对 SSL 协议应用的测试。

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 5271.8—2001 信息技术 词汇 第 8 部分：安全

GB/T 17178.1—1997 信息技术 开放系统互连 一致性测试方法和框架 第 1 部分：基本概念

3 术语和定义

GB/T 5271.8 界定的以及下列术语和定义适用于本文件。

3.1

SSL 协议 Secure Sockets Layer Protocol

一种应用于传输层的安全协议，用于构建客户端和服务器之间的安全通道，它提供保密性、完整性和可选的身份鉴别等安全功能。

3.2

SSL 协议应用 application of the SSL protocol

按照 SSL 协议规范标准实现的产品或功能模块。

3.3

客户端 client

主动发出 SSL 协议连接请求的通信方。

3.4

服务器 server

接收 SSL 协议连接请求的通信方。

3.5

功能测试 function testing

测试 SSL 协议应用的基本功能，包括基本连通测试、安全功能测试和行为测试。

3.6

性能测试 performance testing

测试在不同的网络负载情况下 SSL 协议应用的性能参数。

3.7

互操作性测试 interoperability testing

测试不同 SSL 协议应用之间的互操作能力。