开发的，已广泛应用于万维网上客户端和服务器间的认证及加密通信。

- http://www.netscape.com/eng/ssl3/draft302.txt
  "The SSL Protocol Version 3.0"（"SSL 协议版本 3.0"）是网景公司 1996 年的 SSL 规范。

- http://developer.netscape.com/tech/security/ssl/howitworks.html
  "How SSL Works"（"SSL 是如何工作的"）是网景公司对密钥加密技术的介绍。

- http://www.openssl.org
  OpenSSL 项目是一个合作开发项目，目的是开发一个强壮的、全功能的、商业级开源工具集，以实现安全套接字层（SSL v2/v3）和传输层安全（TLS v1）协议以及强大的通用密码库。这个项目由全世界范围内的志愿者社区管理，那些志愿者通过因特网进行交流、制定计划、开发 OpenSSL 工具集并撰写相关文档。OpenSSL 基于 Eric A. Young 和 Tim J. Hudson 开发的优秀 SSLeay 库。OpenSSL 工具集有一个 Apache 风格的许可证，这基本上就意味着只要遵循一些基本的许可条件，就可免费获得并将其用于商业或非商业目的。

14.10.3 公开密钥基础设施

- http://www.ietf.org/html.charters/pkix-charter.html
  IETF PKIX 工作组组建于 1995 年，目的是开发一些因特网标准，支持基于
337 X.509 的公开密钥基础设施。这是对此小组活动很好的总结。

- http://www.ietf.org/rfc/rfc2459.txt
  RFC 2459，"Internet X.509 Public Key Infrastructure Certificate and CRL Profile"（"因特网 X.509 公开密钥基础设施证书及 CRL 概述"），详细介绍了 X.509 v3 数字证书。

14.10.4 数字密码

- *Applied Cryptography*[14]（《应用密码学》）
  Bruce Schneier 著，John Wiley & Sons 公司出版。这是为实现者编写的经典密码学书籍。

- *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*[15]（《密码故事——人类智力的另类较量》）
  Simon Singh 著，Anchor Books 公司出版。这是一本有趣的密码学入门书籍。它
338 不是为技术专家编写的，而是一本生动的密码学历史读物。

注 14：本书中文版由机械工业出版社出版。（编者注）
注 15：本书中文版由海南出版社出版。（编者注）