SSL

1.SSL(Secure Sockets Layer [安全套接层](http://baike.baidu.com/view/525499.htm" \t "http://baike.baidu.com/_blank)),及其继任者[传输层安全](http://baike.baidu.com/view/831898.htm" \t "http://baike.baidu.com/_blank)（Transport Layer Security，TLS）是为[网络通信](http://baike.baidu.com/view/538641.htm" \t "http://baike.baidu.com/_blank)提供安全及[数据完整性](http://baike.baidu.com/view/702953.htm" \t "http://baike.baidu.com/_blank)的一种安全协议。TLS与SSL在[传输层](http://baike.baidu.com/view/239605.htm" \t "http://baike.baidu.com/_blank)对网络连接进行加密。当前版本为3.0。它已被广泛地用于[Web浏览器](http://baike.baidu.com/view/206703.htm" \t "http://baike.baidu.com/_blank)与服务器之间的[身份认证](http://baike.baidu.com/view/1014826.htm" \t "http://baike.baidu.com/_blank)和加密数据传输。

1. SSL协议可分为两层：

SSL记录协议（SSL Record Protocol）：它建立在可靠的[传输协议](http://baike.baidu.com/view/441895.htm" \t "http://baike.baidu.com/_blank)（如TCP）之上，为高层协议提供[数据封装](http://baike.baidu.com/view/262940.htm" \t "http://baike.baidu.com/_blank)、压缩、加密等基本功能的支持。

SSL[握手协议](http://baike.baidu.com/view/1712962.htm" \t "http://baike.baidu.com/_blank)（SSL Handshake Protocol）：它建立在SSL记录协议之上，用于在实际的数据传输开始前，通讯双方进行[身份认证](http://baike.baidu.com/view/1014826.htm" \t "http://baike.baidu.com/_blank)、协商[加密算法](http://baike.baidu.com/view/155969.htm" \t "http://baike.baidu.com/_blank)、交换加密[密钥](http://baike.baidu.com/view/934.htm" \t "http://baike.baidu.com/_blank)等。

(1)握手协议

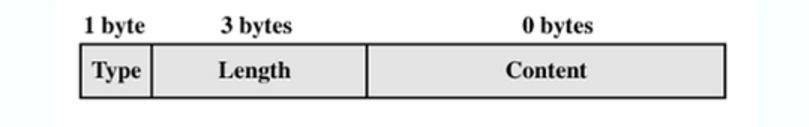
握手协议是客户机和服务器用SSL连接通信时使用的第一个子协议，握手协议包括客户机与服务器之间的一系列消息。SSL中最复杂的协议就是握手协议。该协议允许服务器和客户机相互验证，协商加密和MAC算法以及保密密钥，用来保护在SSL记录中发送的数据。握手协议是在应用程序的数据传输之前使用的。

　　每个握手协议包含以下3个字段

　　（1）Type：表示10种消息类型之一

　　（2）Length：表示消息长度字节数

　　（3）Content：与消息相关的参数



(2)握手协议的4个阶段

第一阶段启动逻辑连接，建立这个连接的安全能力。首先客户机向服务器发出client hello消息并等待服务器响应，随后服务器向客户机返回server hello消息，对client hello消息中的信息进行确认。

第二阶段，服务器是本阶段所有消息的唯一发送方，客户机是所有消息的唯一接收方。该阶段分为4步：

　　（a）证书：服务器将数字证书和到根CA整个链发给客户端，使客户端能用服务器证书中的服务器公钥认证服务器。

　　（b）服务器密钥交换（可选）：这里视密钥交换算法而定

　　（c）证书请求：服务端可能会要求客户自身进行验证。

　　（d）服务器握手完成：第二阶段的结束，第三阶段开始的信号

第三阶段，客户机是本阶段所有消息的唯一发送方，服务器是所有消息的唯一接收方。该阶段分为3步：

　　（a）证书（可选）：为了对服务器证明自身，客户要发送一个证书信息，这是可选的，在IIS中可以配置强制客户端证书认证。

　　（b）客户机密钥交换（Pre-master-secret）：这里客户端将预备主密钥发送给服务端，注意这里会使用服务端的公钥进行加密。

（c）证书验证（可选），对预备秘密和随机数进行签名，证明拥有（a）证书的公钥。

第四阶段，客户端发起使服务器结束。该阶段分为4步，前2个消息来自客户机，后2个消息来自服务器。

　(2)、记录协议

记录协议在客户机和服务器握手成功后使用，即客户机和服务器鉴别对方和确定安全信息交换使用的算法后，进入SSL记录协议，记录协议向SSL连接提供两个服务：

　 （1）保密性：使用握手协议定义的秘密密钥实现

　　（2）完整性：握手协议定义了MAC，用于保证消息完整性