SSL 笔记

SSL 协议 简述:

特点： 提供较高的安全性保证， 支持多种应用层协议

安全机制： 传输数据的机密性（对称秘钥），身份验证机制， 消息完整性验证

SSL 协议分层： 上层： SSL 握手协议 （ SSL handshake protocol ），SSLpassword变化协议（SSL change cipher spec protocol）和SSL警告协议（SSL alert protocol）

SSL 协议分层： 下层： SSL记录协议（SSL record protocol）

SSL 握手协议： 协商通信过程中使用的加密套件， 两种之间安全交换秘钥， 实现两者的身份认证

SSL 原理：

首先服务端必须有一个数字证书，当客户端连接到服务端时，会得到这个证书，然后客户端会判断这个证书是否是可信的，如果是，则交换信道加密密钥，进行通信。如果不信任这个证书，则连接失败。

> 证书的生成步骤 ：

```
keytool -genkey -v -alias demo-server -keyalg RSA -keystore ./server_ks -dname "CN=localhost,OU=cn,O=cn,L=cn,ST=cn,C=cn" -storepass server -keypass 123456
```

SSL 握手过程：

> 在server 和 client 之间协商会话参数 ，并且建立会话
> 会话主要参数 ：会话ID ，对方的证书 ，加密套件 ，主秘钥
> SSL 的三种不同握手 ： 仅仅验证server的SSL握手过程 ， 验证server和client的SSL握手过程，恢复原有会话的SSL握手过程

第一步：客户端发送ClientHello消息，发起SSL连接请求，告诉服务器自己支持的SSL选项（加密方式等）。 *** ClientHello, TLSv1

第二步：服务器响应请求，回复ServerHello消息，和客户端确认SSL加密方式：*** ServerHello, TLSv1

第三步：服务端向客户端发布自己的公钥。
第四步：客户端与服务端的协通沟通完毕，服务端发送ServerHelloDone消息：*** ServerHelloDone

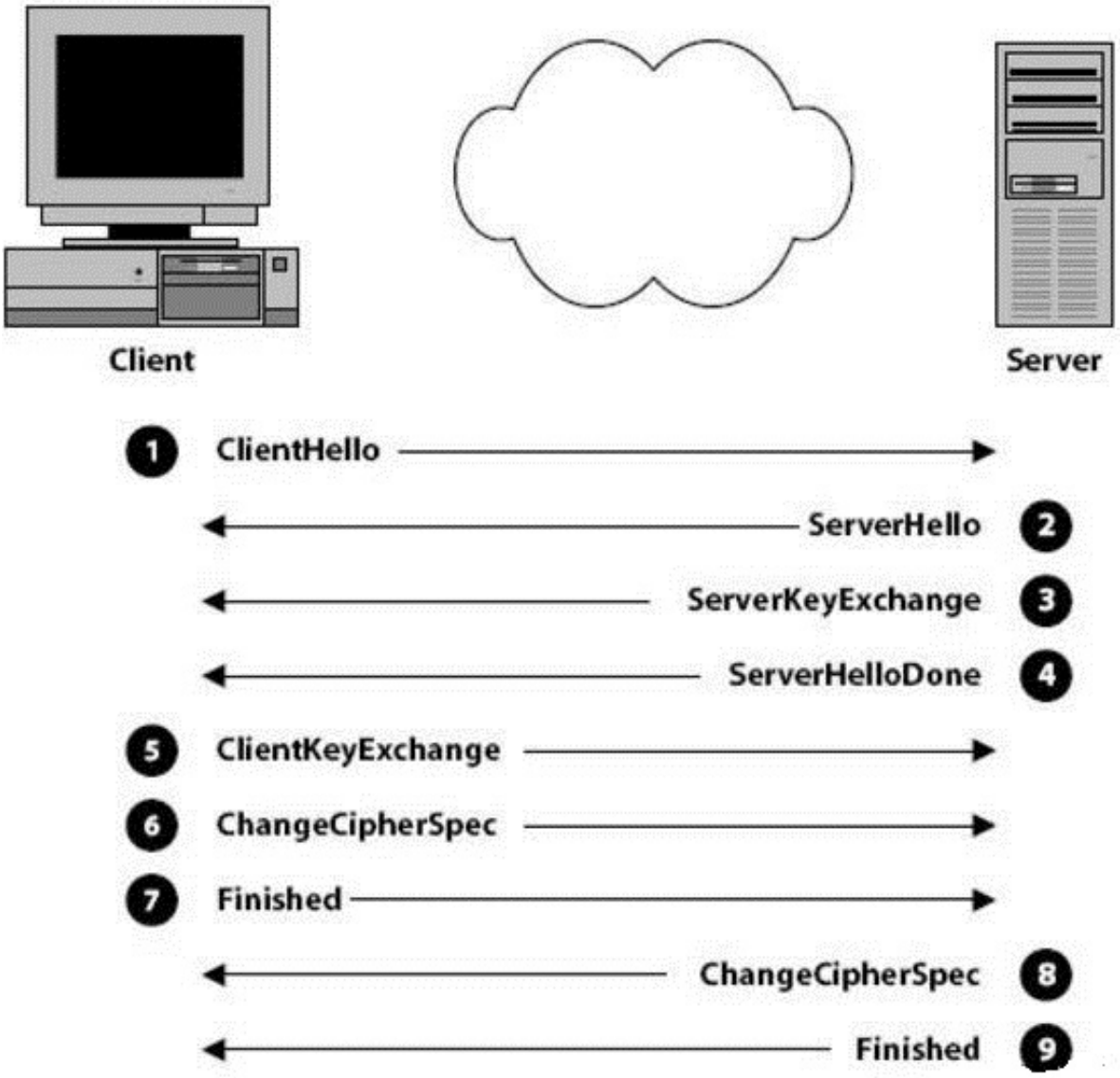
第五步：客户端使用服务端给予的公钥，创建会话用密钥（SSL证书认证完成后，为了提高性能，所有的信息交互就可能会使用对称加密算法），并通过ClientKeyExchange消息发给服务器：*** ClientKeyExchange, RSA PreMasterSecret, TLSv1

第六步： 客户端通知服务器改变加密算法，通过ChangeCipherSpec消息发给服务端：main, WRITE: TLSv1 Change Cipher Spec, length = 1

第七步： 客户端发送Finished消息，告知服务器请检查加密算法的变更请求：*** Finished

第八步：服务端确认算法变更，返回ChangeCipherSpec消息 : main, READ: TLSv1 Change Cipher Spec, length = 1

第九步：服务端发送Finished消息，加密算法生效：*** Finished



一个 SSL 的简单案例