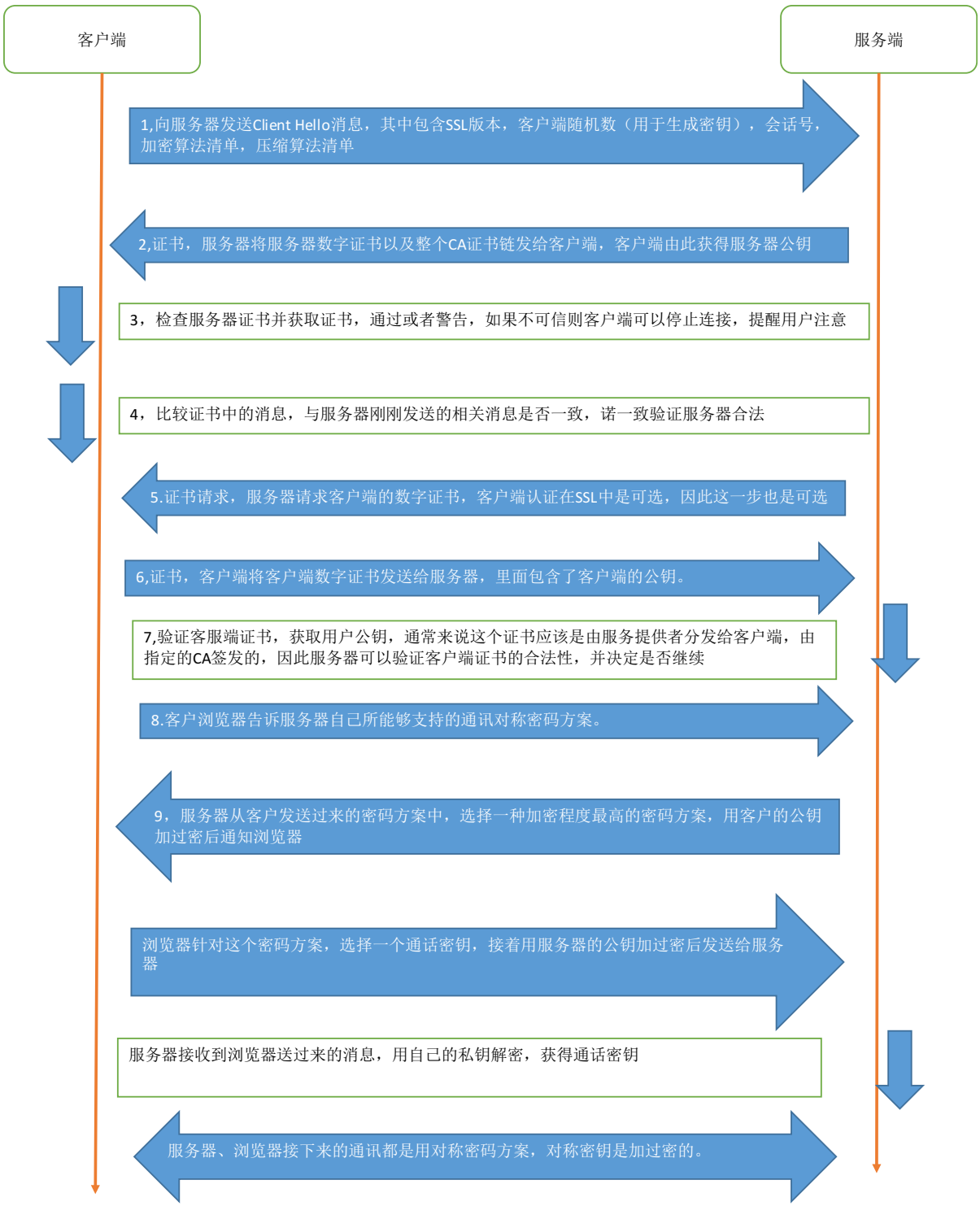
客户端
服务端
1,向服务器发送Client Hello消息，其中包含SSL版本，客户端随机数（用于生成密钥），会话号，加密算法清单，压缩算法清单
2,证书，服务器将服务器数字证书以及整个CA证书链发给客户端，客户端由此获得服务器公钥
3，检查服务器证书并获取证书，通过或者警告，如果不可信则客户端可以停止连接，提醒用户注意
4，比较证书中的消息，与服务器刚刚发送的相关消息是否一致，诺一致验证服务器合法
5.证书请求，服务器请求客户端的数字证书，客户端认证在SSL中是可选，因此这一步也是可选
6,证书，客户端将客户端数字证书发送给服务器，里面包含了客户端的公钥。
7,验证客服端证书，获取用户公钥，通常来说这个证书应该是由服务提供者分发给客户端，由指定的CA签发的，因此服务器可以验证客户端证书的合法性，并决定是否继续
8.客户浏览器告诉服务器自己所能够支持的通讯对称密码方案。
9，服务器从客户发送过来的密码方案中，选择一种加密程度最高的密码方案，用客户的公钥加过密后通知浏览器
浏览器针对这个密码方案，选择一个通话密钥，接着用服务器的公钥加过密后发送给服务器
服务器接收到浏览器送过来的消息，用自己的私钥解密，获得通话密钥
服务器、浏览器接下来的通讯都是用对称密码方案，对称密钥是加过密的。