1.简要介绍

SSL是安全套接层(secure sockets layer)，而TLS是SSL的继任者，叫传输层安全(transport layer security)。

是为网络通信提供安全及数据完整性的一种安全协议。TLS与SSL在传输层对网络连接进行加密。

比如如HTTP协议是明文传输，加上SSL层之后，就有了雅称HTTPS。它的发展依次经历了下面几个时期:

SSL1.0: 已废除

SSL2.0: RFC6176,已废除

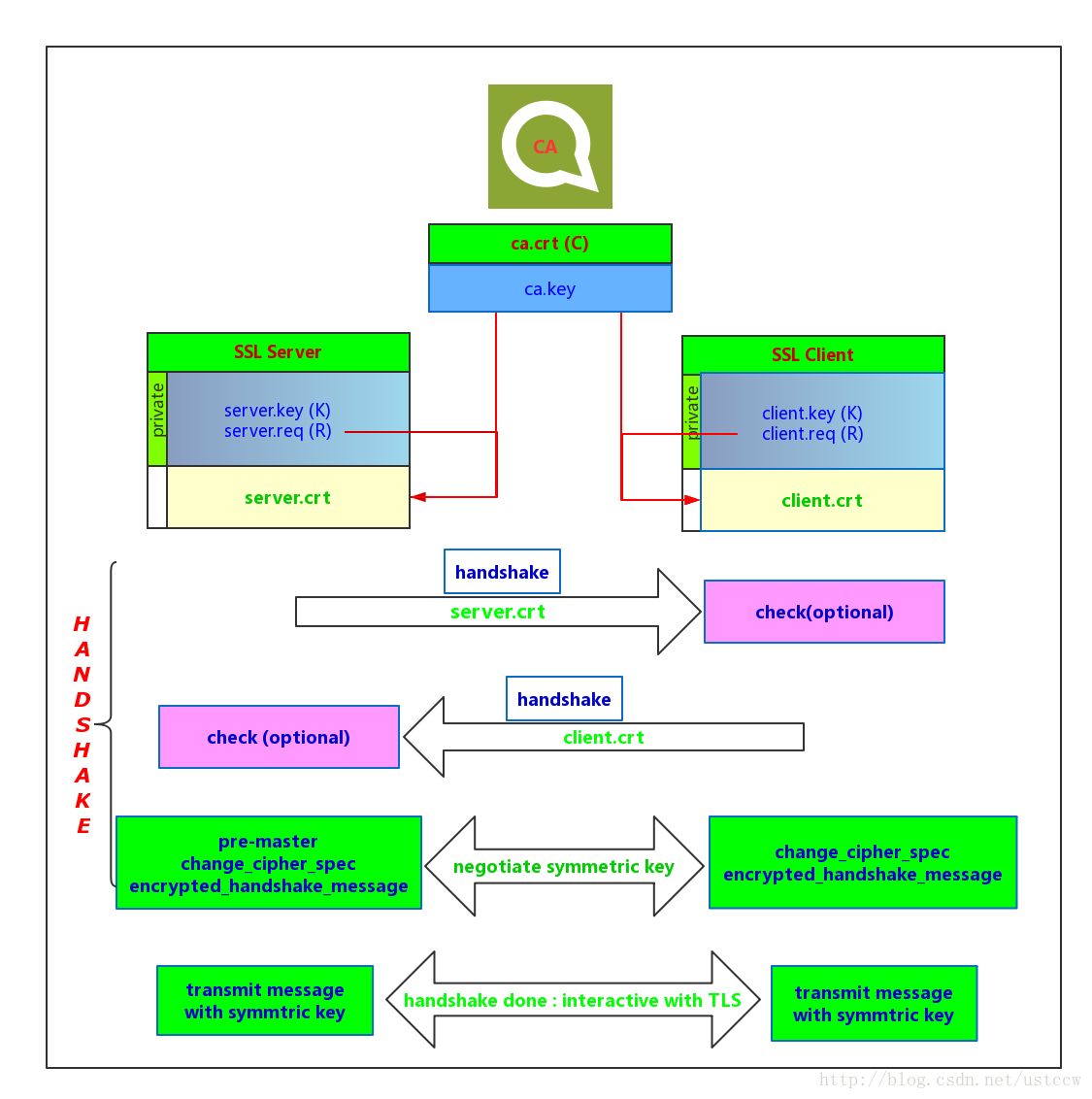
SSL3.0: RFC6101,基本废除

TLS1.0: RFC2246,目前大都采用此种方式

TLS1.1: RFC4346

TLS1.2: RFC5246,没有广泛使用

TLS1.3: RFC 8446,于2018年8月发表



CA: 证书授权中心( certificate authority)。 它呢，类似于国家出入境管理处一样，给别人颁发护照；也类似于国家工商管理局一样，给公司企业颁发营业执照。

它有两大主要性质：

1.CA本身是受信任的 // 国际认可的

2.给他受信任的申请对象颁发证书 // 和办理护照一样，要确定你的合法身份，你不能是犯罪分子或造反派。当然，你需要被收保护费，同时，CA可以随时吊销你的证书。

证书长啥样？其实你的电脑中有一堆CA证书。你可以看一看嘛：

1）360浏览器: 选项/设置-> 高级设置 -> 隐私于安全 -> 管理 HTTPS/SSL 证书 -> 证书颁发机构

2）火狐浏览器: 首选项 -> 高级 -> 证书 -> 查看证书 -> 证书机构

3）chrome浏览器: 设置 -> 高级 -> 管理证书 -> 授权中心

4）ubuntu: /etc/ssl/certs

这些都是 CA 的证书！

CA 的证书 ca.crt 和 SSL Server的证书 server.crt 是什么关系呢？

1.SSL Server 自己生成一个私钥/公钥对。server.key/server.pub // 私钥加密，公钥解密！

2.server.pub 生成一个请求文件 server.req. 请求文件中包含有 server 的一些信息，如域名/申请者/公钥等。

3.server 将请求文件 server.req 递交给 CA，CA验明正身后，将用 ca.key和请求文件加密生成 server.crt

4.由于 ca.key 和 ca.crt 是一对, 于是 ca.crt 可以解密 server.crt.

5.在实际应用中：如果 SSL Client 想要校验 SSL server.那么 SSL server 必须要将他的证书 server.crt 传给 client.然后 client 用 ca.crt 去校验server.crt 的合法性。如果是一个钓鱼网站，那么CA是不会给他颁发合法server.crt证书的，这样client 用ca.crt去校验，就会失败。比如浏览器作为一个 client,你想访问合法的淘宝网站https://www.taobao.com,结果不慎访问到 https://wwww.jiataobao.com ,那么浏览器将会检验到这个假淘宝钓鱼网站的非法性，提醒用户不要继续访问！这样就可以保证了client的所有https访问都是安全的。