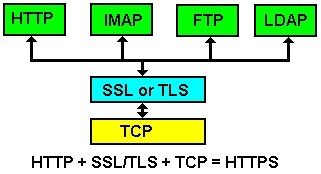
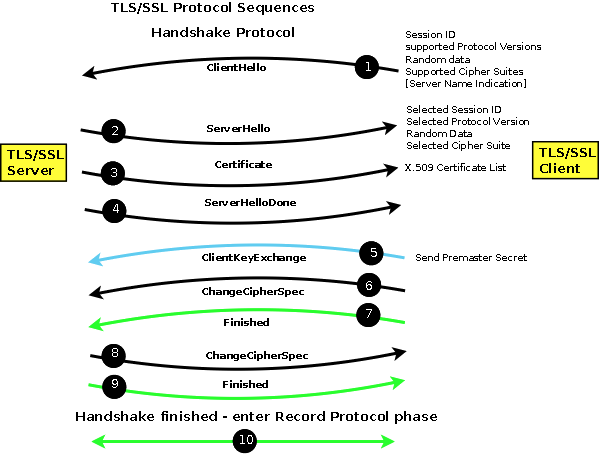
HTTPS是HTTP over SSL/TLS，HTTP是应用层协议，TCP是传输层协议，在应用层和传输层之间，增加了一个安全套接层SSL/TLS：



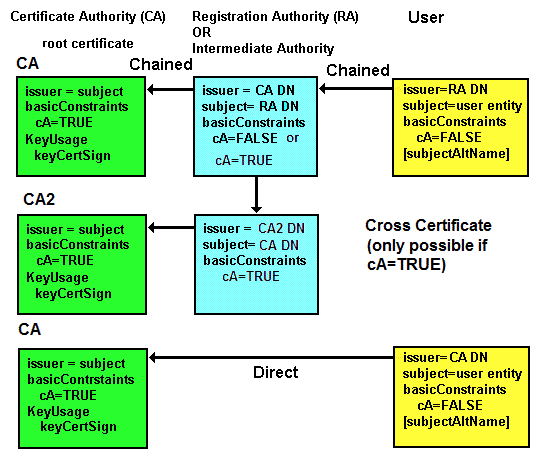
SSL/TLS层负责客户端和服务器之间的加解密算法协商、密钥交换、通信连接的建立，安全连接的建立过程如下所示：



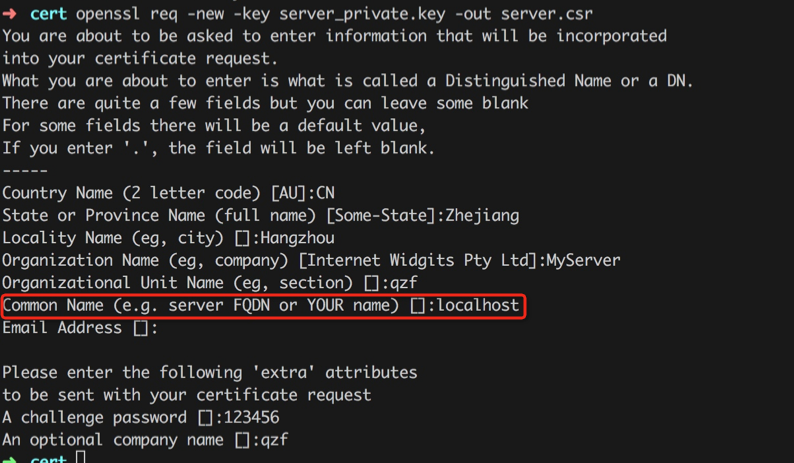
公钥基础设施（PKI）是一组由硬件、软件、参与者、管理政策与流程组成的基础架构，其目的在于创造、管理、分配、使用、存储以及撤销数字证书。公钥存储在数字证书中，标准的数字证书一般由可信数字证书认证机构(CA，根证书颁发机构)签发，此证书将用户的身份跟公钥链接在一起。CA必须保证其签发的每个证书的用户身份是唯一的。

链接关系（证书链）通过注册和发布过程创建，取决于担保级别，链接关系可能由CA的各种软件或在人为监督下完成。PKI的确定链接关系的这一角色称为注册管理中心（RA，也称中级证书颁发机构或者中间机构）。RA确保公钥和个人身份链接，可以防抵赖。如果没有RA，CA的Root 证书遭到破坏或者泄露，由此CA颁发的其他证书就全部失去了安全性，所以现在主流的商业数字证书机构CA一般都是提供三级证书，Root 证书签发中级RA证书，由RA证书签发用户使用的证书。

X509证书链，左边的是CA根证书，中间的是RA中间机构，右边的是用户



**2.2 自有数字证书的生成**  
  
HTTPS网站所用的证书可向可信CA机构申请，不过这一类基本上都是商业机构，申请证书需要缴费，一般是按年缴费，费用因为CA机构的不同而不同。如果只是APP与后台服务器进行HTTPS通信，可以使用openssl工具生成自签发的数字证书，可以节约费用，不过得妥善保护好证书私钥，不能泄露或者丢失。HTTPS通信所用的数字证书格式为X.509。  
  
自签发数字证书步骤如下：   
  
**Step1 生成自己的CA根证书**  
  
生成CA私钥文件ca.key：  
openssl genrsa -out ca.key 1024  
  
生成X.509证书签名请求文件ca.csr：  
openssl req -new -key ca\_private.key -out ca.csr   
  
在生成ca.csr的过程中，会让输入一些组织信息等。  
  
生成X.509格式的CA根证书ca\_public.crt（公钥证书）：  
openssl x509 -req -in ca.csr -signkey ca\_private.key -out ca\_public.crt  
  
**Step2 生成服务端证书**  
  
先生成服务器私钥文件server\_private.key：  
openssl genrsa -out server\_private.key 1024  
  
根据服务器私钥生成服务器公钥文件server\_public.pem：  
openssl rsa -in server\_private.key -pubout -out server\_public.pem  
  
服务器端需要向CA机构申请签名证书，在申请签名证书之前依然是创建自己的证书签名请求文件server.csr：  
openssl req -new -key server\_prviate.key -out server.csr



对于用于HTTPS的CSR，Common Name必须和网站域名一致，以便之后进行Host Name校验。

服务器端用server.csr文件向CA申请证书，签名过程需要CA的公钥证书和私钥参与，最终颁发一个带有CA签名的服务器端证书server.crt：

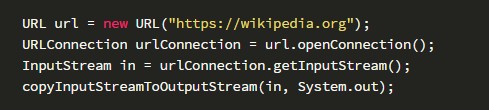
openssl x509 -req -CA ca\_public.crt -CAkey ca\_private.key -CAcreateserial -in server.csr -out server.crt

如果服务器端还想校验客户端的证书，可以按生成服务器端证书的形式来生成客户端证书。

使用openssl查看证书信息：

openssl x509 -in server.crt -text –noout

**2.3 使用HttpsURLConnection进行HTTPS通信**  
  
Android官网给出了使用HttpsURLConnection API访问HTTPS的网站示例：



此方法的特点：  
  
· 由Android系统校验服务端数字证书的合法性，用可信CA签发的数字证书的网站才可以正常访问，私有CA签发的数字证书的网站无法访问。  
  
· 不能抵御在用户设备上安装证书（将中间人服务器的证书放到设备的信任列表中）进行中间人攻击，做此类攻击的一般是为了分析应用和服务器的交互协议，找应用和服务器的其他漏洞。  
  
· 如果网站没有启用SSL site wide（use HTTPS only）或HSTS(HTTP Strict Transport Security)则无法抵御SSL Strip（HTTPS降级为HTTP）攻击，局域网攻击，如针对免费WiFi。  
  
如果要使用私有CA签发的证书，必须重写校验证书链TrustManager中的方法，否则的话会出现javax.net.ssl.SSLHandshakeException: java.security.cert.CertPathValidatorException: Trust anchor for certification path not found。但是在重写TrustManger中的checkServerTrusted()很多开发者什么也没有做，会导致证书弱校验（没有真正校验证书）。