# 1,如何使用OpenSSL生成一个自签名

使用HTTP（超文本传输）协议访问互联网上的数据是没有经过加密的。也就是说，任何人都可以通过适当的工具拦截或者监听到在网络上传输的数据流。但是有时候，我们需要在网络上传输一些安全性或者私秘性的数据，譬如：包含信用卡及商品信息的电子订单。这个时候，如果仍然使用HTTP协议，势必会面临非常大的风险！相信没有人能接受自己的信用卡号在互联网上裸奔。

HTTPS（超文本传输安全）协议无疑可以有效的解决这一问题。所谓HTTPS，其实就是HTTP和SSL/TLS的组合，用以提供加密通讯及对网络服务器的身份鉴定。HTTPS的主要思想是在不安全的网络上创建一安全信道，防止黑客的窃听和攻击。

SSL（安全套接层）可以用来对Web服务器和客户端之间的数据流进行加密。

SSL利用非对称密码技术进行数据加密。加密过程中使用到两个秘钥：一个公钥和一个与之对应的私钥。使用公钥加密的数据，只能用与之对应的私钥解密；而使用私钥加密的数据，也只能用与之对应的公钥解密。因此，如果在网络上传输的消息或数据流是被服务器的私钥加密的，则只能使用与其对应的公钥解密，从而可以保证客户端与与服务器之间的数据安全。

所谓数字证书:是一种用于电脑的身份识别机制，由数字证书颁发机构（CA）对使用私钥创建的签名请求文件做的签名（盖章），表示CA结构对证书持有者的认可，数字证书具有一下优点:

* 提高用户的可信度
* 数字证书中的公钥，能够与服务端的私钥配对使用，实现数据传输过程中的加密情况，
* 在认证使用者身份期间，使用者的敏感个人数据并不会被传输至证书持有者的网络系统上。

X.509证书包含三个文件:key,csr,crt

Key 是服务器上的私钥文件，用于对发送给客户端数据的加密，以及对从客户端接收到数据的解密。

Csr是证书签名请求文件，用于提交给证书颁发机构（CA）对证书签名

Crt是证书颁发机构签名后的证书或者是开发者自签名的证书，包含证书持有人的信息，

持有人的公钥，以及签署者的签名等信息

步骤:

1. 生成私钥

使用openssl 工具生成一个RSA私钥

openssl genrsa -des3 -out server.key 2048

Des3 算法 2048 位强度 server.key 是秘钥文件

1. 生成csr (证书签名请求)

Openssl req -new -key server.key -out server.csr

1. 删除私钥密码

在第1步创建私钥的过程中，由于必须要指定一个密码。而这个密码会带来一个副作用，那就是在每次Apache启动Web服务器时，都会要求输入密码，这显然非常不方便。要删除私钥中的密码，操作如下：

cp server.key server.key.org

openssl rsa -in server.key.org -out server.key

1. 生成自签名证书

如果你不想花钱让CA签名，或者只是测试SSL的具体实现。那么，现在便可以着手生成一个自签名的证书了。

需要注意的是，在使用自签名的临时证书时，浏览器会提示证书的颁发机构是未知的。

openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

说明：crt上有证书持有人的信息，持有人的公钥，以及签署者的签名等信息。当用户安装了证书之后，便意味着信任了这份证书，同时拥有了其中的公钥。证书上会说明用途，例如服务器认证，客户端认证，或者签署其他证书。当系统收到一份新的证书的时候，证书会说明，是由谁签署的。如果这个签署者确实可以签署其他证书，并且收到证书上的签名和签署者的公钥可以对上的时候，系统就自动信任新的证书。

# 2, nginx 配置https

1, 检查nginx 是否安装http\_ssl\_module

Nginx –V 如果出现configure arguments: --with-http\_ssl\_module则已经安装

2， nginx 配置

Server {

Listen 443 ssl;

Server\_name localhost;

Keepalive\_timeout 100;

Ssl\_session\_cache shared:SSL:10m;

Ssl\_session\_timeout 10m;

Ssl\_certificate /etc/nginx/cert/server.crt;

Ssl\_certificate\_key /etc/nginx/cert/server.key;

Index index.html index.htm;

Location / {

Root /opt/app/code;

}

}

3， 检查nginx 配置文件语法

Nginx –t

重载nignx

Nginx –s reload