https双向认证 本地创建自定义证书 nginx配置https双向认证

前言

本篇博文将为你解答这些问题：

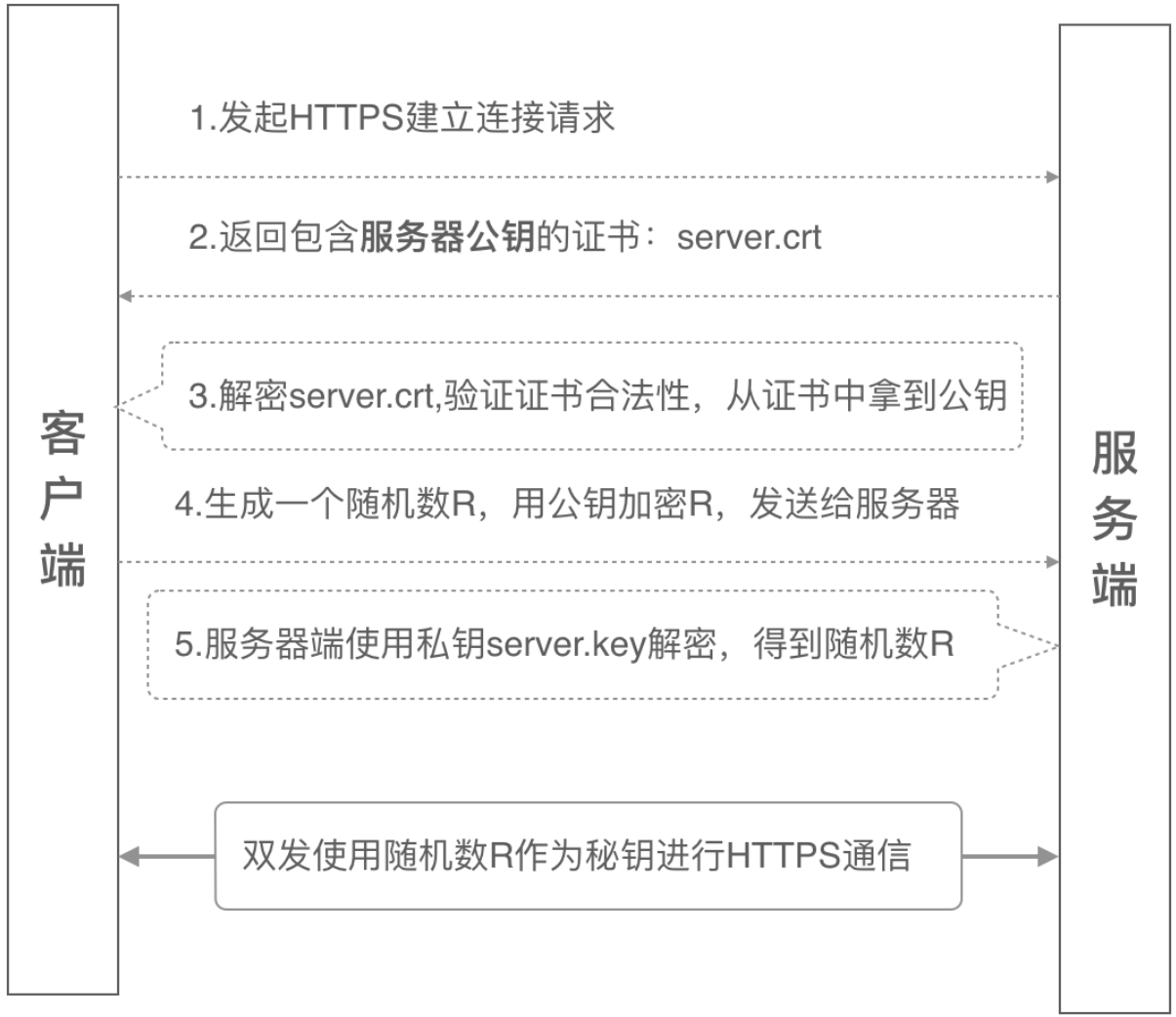
1. https单相认证和双向认证的讲解
2. https证书获取途径：腾讯云、阿里云、自签名证书
3. nginx如何配置https双向认证?
4. 如何验证https双向认证?
5. uni-app 配置 https 自签名客户端证书
6. mac如何安装客户端证书
7. chrome浏览器访问自签名证书地址显示【您的连接不是私密连接】解决办法

如果有什么不懂，可以留言沟通

正文

1. https单相认证和双向认证的讲解

单向认证流程

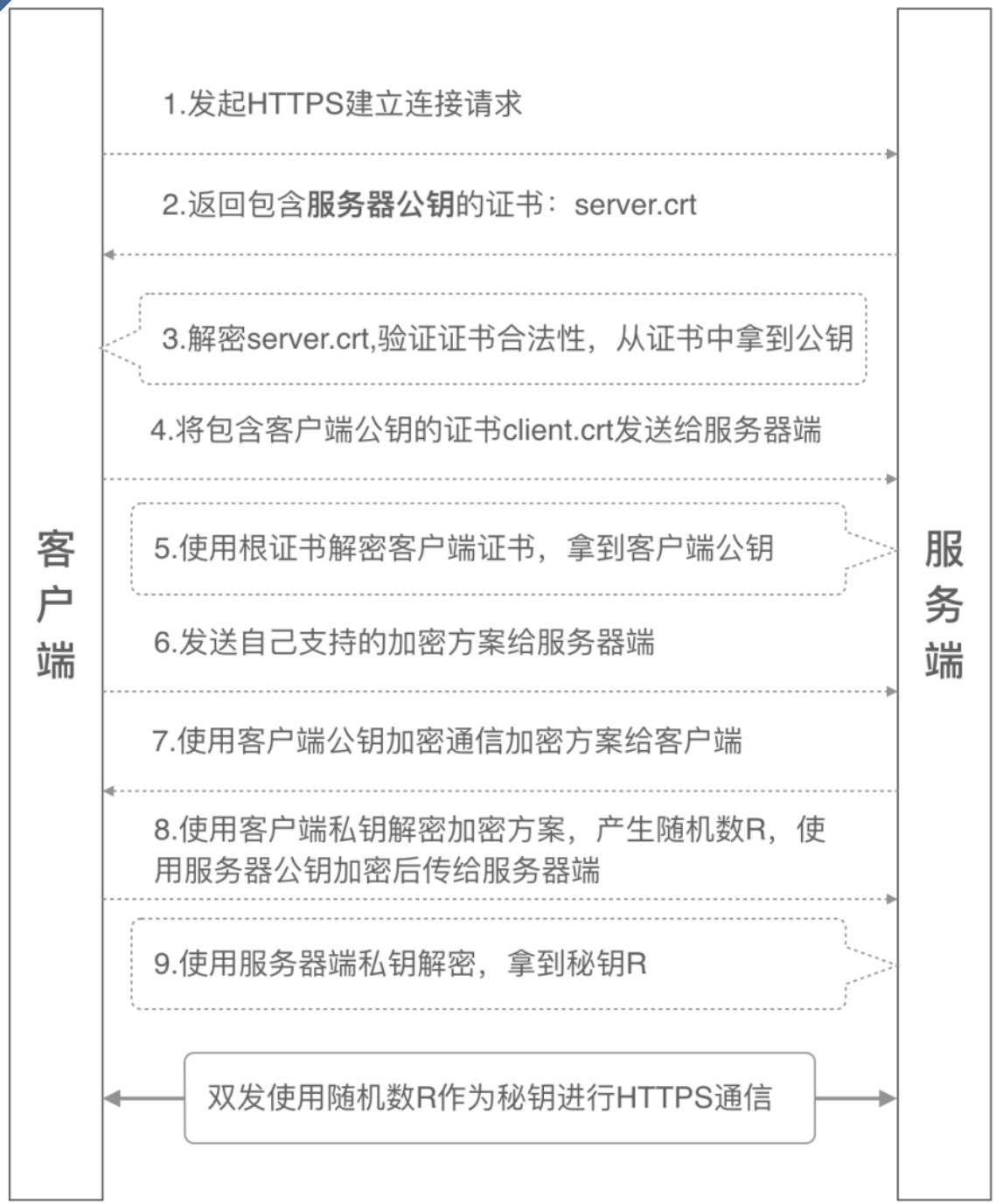


服务器
证书：
秘钥：

1. 客户端发起建立HTTPS连接请求，将SSL协议版本的信息发送给服务器端；
2. 服务器端将本机的公钥证书（server.crt）发送给客户端；

3. 客户端读取公钥证书（server.crt），取出了服务端公钥；
4. 客户端生成一个随机数（密钥R），用刚才得到的服务器公钥去加密这个随机数形成密文，发送给服务端；
5. 服务端用自己的私钥（server.key）去解密这个密文，得到了密钥R
6. 服务端和客户端在后续通讯过程中就使用这个密钥R进行通信了。

双向认证流程



服务器端
证书：server.crt
秘钥：server.key
根证书：root.crt

客户端
证书：client.crt
秘钥：client.key
或者包含证书和秘

1. 客户端发起建立HTTPS连接请求，将SSL协议版本的信息发送给服务端；
2. 服务器端将本机的公钥证书（server.crt）发送给客户端；
3. 客户端读取公钥证书（server.crt），取出了服务端公钥；
4. 客户端将客户端公钥证书（client.crt）发送给服务器端；
5. 服务器端使用根证书（root.crt）解密客户端公钥证书，拿到客户端公钥；
6. 客户端发送自己支持的加密方案给服务器端；
7. 服务器端根据自己和客户端的能力，选择一个双方都能接受的加密方案，使用客户端的公钥加密8. 后发送给
8. 客户端使用自己的私钥解密加密方案，生成一个随机数R，使用服务器公钥加密后传给服务器端；
9. 服务端用自己的私钥去解密这个密文，得到了密钥R
10. 服务端和客户端在后续通讯过程中就使用这个密钥R进行通信了。

整个双向认证的流程需要六个证书文件：

1. 服务器端公钥证书：server.crt
2. 服务器端私钥文件：server.key
3. 根证书：root.crt
4. 客户端公钥证书：client.crt
5. 客户端私钥文件：client.key
6. 客户端集成证书（包括公钥和私钥，用于浏览器访问场景）：client.p12

2. https证书获取途径：腾讯云、阿里云、自签名证书

如果你只需要单向认证，在腾讯云的 【SSL证书】这个产品下，即可申请到免费的单域名证书。也可以再阿里云平
用安全）】这个产品下申请免费的单域名证书。

需要双向认证，有两种办法：

1. 购买正规厂商出售的证书，不过价格相对比较高昂。
2. 使用自签名证书，自己在本地用开源工具 openssl 生成所需要的6个证书文件

使用 openssl 工具生成证书文件

> openssl安装请自行搜索

1. 生成自签名根证书
    1. 创建根证书

```
openssl genrsa -out root.key 1024
```

    2. 创建根证书请求文件

```
openssl req -new -out root.csr -key root.key
```

这里有许多参数需要填写，请自行填写： A challenge password 密码可以不设置

```
Country Name (2 letter code) [XX]:cn
State or Province Name (full name) []:bj
Locality Name (eg, city) [Default City]:bj
Organization Name (eg, company) [Default Company Ltd]:shuiche
Organizational Unit Name (eg, section) []:test
Common Name (eg, your name or your servers hostname) []:root
Email Address []:a.alibaba.com
A challenge password []:
An optional company name []:
```

3. 创建根证书

```
openssl x509 -req -in root.csr -out root.crt -signkey root.key -CAcreateserial
```

2. 生成服务端证书

1. 生成服务器端证书私钥

```
openssl genrsa -out server.key 1024
```

2. 生成服务器证书请求文件

```
openssl req -new -out server.csr -key server.key
```

这里有许多参数需要填写

```
Country Name (2 letter code) [XX]:cn
State or Province Name (full name) []:bj
Locality Name (eg, city) [Default City]:bj
Organization Name (eg, company) [Default Company Ltd]:shuiche
Organizational Unit Name (eg, section) []:test
Common Name (eg, your name or your servers hostname) []:root
Email Address []:a.alibaba.com
A challenge password []:
An optional company name []:
```

3. 生成服务器端公钥证书

```
openssl x509 -req -in server.csr -out server.crt -signkey server.key -CA root.c
root.key -CAcreateserial -days 3650
```

些教程里生成的是 .pem 格式的公钥证书，.pem 和 .crt 其实是一样的。都代表公钥证书

经过上面的三个命令，我们得到：

server.key：服务器端的密钥文件

server.crt：有效期十年的服务器端公钥证书，使用根证书和服务器端私钥文件一起生成

3. 生成客户端证书

1. 生成客户端证书密钥：

```
openssl genrsa -out client.key 1024
```

2. 生成服务器证书请求文件

```
openssl req -new -out client.csr -key client.key
```

这里有许多参数需要填写

```
Country Name (2 letter code) [XX]:cn
State or Province Name (full name) []:bj
Locality Name (eg, city) [Default City]:bj
Organization Name (eg, company) [Default Company Ltd]:shuiche
Organizational Unit Name (eg, section) []:test
Common Name (eg, your name or your servers hostname) []:root
Email Address []:a.alibaba.com
A challenge password []:
An optional company name []:
```

3. 生客户端证书

```
openssl x509 -req -in client.csr -out client.crt -signkey client.key -CA root.c
root.key -CAcreateserial -days 3650
```

4. 生客户端p12格式证书， **需要输入一个密码**，选一个好记的，比如123456

> 密码一定要记牢，安装客户端证书时需要填写的

```
openssl pkcs12 -export -clcerts -in client.crt -inkey client.key -out client.p1
```

经过上面的四个命令，我们得到：

client.key：客户端的私钥文件

client.crt：有效期十年的客户端证书

client.p12： 证书文件包含客户端的公钥和私钥，主要用来给浏览器访问使用（uniapp再配置双向认证时也需要）

3. nginx如何配置双向认证

直接上配置文件：

```
server {
    listen       443 ssl; # 开启ssl
    server_name  www.******.com; # 域名或者本机ip 【自行修改成你的值】
    ssl_certificate      /usr/local/webserver/nginx/conf/cert/server.crt; # 服务端证书
    ssl_certificate_key  /usr/local/webserver/nginx/conf/cert/server.key; # 服务端私钥

    ssl_session_cache    shared:SSL:1m; # 配置共享会话缓存大小
    ssl_session_timeout  5m; # session有效期5分钟
    ssl_protocols  SSLv2 SSLv3 TLSv1 TLSv1.1 TLSv1.2; #启用指定的协议
    ssl_ciphers  ALL:!DH:!EXPORT:!RC4:+HIGH:+MEDIUM:-LOW:!aNULL:!eNULL; #加密算法
```

```
    ssl_prefer_server_ciphers  on; # 优先采取服务器算法
    ssl_verify_client on;# 开启客户端证书校验
    ssl_client_certificate  /usr/local/webserver/nginx/conf/cert/ca.crt; # CA证书用于
性
    ssl_verify_depth 6; # 校验深度
    ssl_trusted_certificate /usr/local/webserver/nginx/conf/cert/ca.crt; # 将CA证书设
    # 减少点击劫持
    add_header  X-Frame-Options DENY;
    # 禁止服务器自动解析资源类型
    add_header  X-Content-Type-Options  nosniff;
    # 防止XSS攻击
    add_header  X-Xss-Protection 1;

    location / {
      # start  防止跨域问题
      add_header Access-Control-Allow-Origin *;
      add_header Access-Control-Allow-Methods 'GET, POST, OPTIONS';
      add_header Access-Control-Allow-Headers 'DNT,X-Mx-ReqToken,Keep-Alive,User-Ager
With,If-Modified-Since,Cache-Control,Content-Type,Authorization';

      if ($request_method = 'OPTIONS') {
          return 204;
      }
      # end
      root   /home/ljcw/micro/;
      index  index.html index.htm;
       try_files $uri $uri/ /index.html;
    }
}

```

4. 如何验证https双向认证?

1. 携带客服端证书访问:

```
#--cert 指定客户端公钥证书的路径
#--key 指定客户端私钥文件的路径
#-k 使用本参数不校验证书的合法性，因为我们用的是自签名证书
#-v 可以使用 -v 来观察具体的SSL握手过程
curl --cert ./client2.crt --key ./client2.key https://integration-fred2.fredhuang.c
```

2. 不携带客户端证书访问

```
curl https://integration-fred2.fredhuang.com -k
```

5. uni-app 配置 https 自签名客户端证书

1. 调用 uni.configMTLS 函数。查看文档 https://uniapp.dcloud.net.cn/api/request/request.html#configmtls

uni.configMTLS 直接在 App.vue 的 onLaunch 中调用一次即可

2. 正常使用 uni.request 就可以了

```
uni.configMTLS({
        certificates: [{
        host: 'www.test.com',  // 换成你证书设定的域名（也就是https请求的域名）
        client: '/static/client.p12',
        clientPassword: '123456',
        server: ['/static/server.pem']
    }],
    complete (res) {
        console.log('res', res)
    }
```

如果报错这个

```
"errMsg": "request:fail abort statusCode:-1 Hostname www.unihttps.com not verified:\n certificate: sha256/4clBWyy+2BlD/ME12B4hlRVEefrl5X0nL0/3DGlSfKA=\n DN: CN=www.unihttps.com\n subjectAltNames: []"
```

问题所在：server证书没有配置-SAN参数，参考这个 使用openssl生成SAN证书

6. mac如何安装客户端证书

直接双击 client.p12 文件，按提示操作

既可以在：mac的【钥匙串访问】这个app里面找到，然后在证书文件右键，选择永久信任证书即可

7. chrome浏览器访问自签名证书地址显示【您的连接不是私密连接】解决办法

解决办法：

在当前页面用键盘输入 thisisunsafe ，不是在地址栏输入，就直接敲键盘就行了，页面即会自动刷新进入网页。

后记

参考文章：

Chrome 您的连接不是私密连接解决办法https://zhuanlan.zhihu.com/p/341857389

SSL 双向认证的一个小问题https://maoxian.de/2016/02/1370.html

阿里云 HTTPS双向认证（Mutual TLS authentication)(https://help.aliyun.com/document_detail/160093.html

SSL 客户端验证https://graycarl.me/2016/09/27/ssl-client-side-authentication.html

nginx配置https双向认证https://juejin.cn/post/6909621056848265230

uni.request接口https://uniapp.dcloud.net.cn/api/request/request.html#configmtls

关于uniapp双向认证https的经验分享 https://ask.dcloud.net.cn/article/39567

作者：水车
出处：https://www.cnblogs.com/shuiche/p/16655444.html

分类：水车--网络协议

« 上一篇： gin nginx 获取不到真实ip 一直是127.0.0.1 c.ClientIP()获取不到真实ip
» 下一篇： 卸载阿里云云盾(安骑士)(Agent)

posted @ 2022-09-04 17:38 水车 阅读(2078)