

基于 IP 地址的 HTTPS 证书 白皮书

Copyright © 2023 All rights reserved

版本记录

版本	日期	描述

内容

1.0	背景介绍	5
2.0	配置方法	6
2.1	服务端配置	6
2.2	浏览器所在机器配置	8

1.0 背景介绍

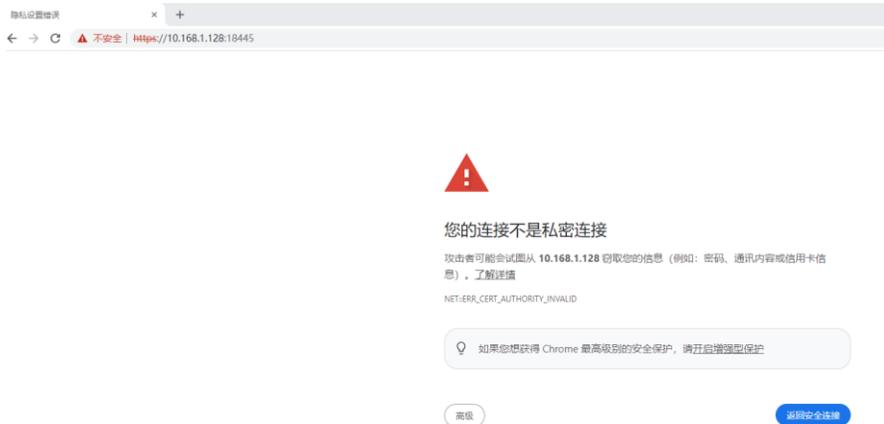
如果让浏览器信任某个 HTTPS 服务(以下称服务), 服务使用证书必须在浏览器信任的证书链上, 一般证书需要购买, 证书绑定域名, 类似下图中的:



但是如果服务在内网, 无法使用域名, 能否根据 IP 地址让浏览器信任服务, 答案是可以的, 但是需要所有的浏览器所在的电脑手工导入根证书, 所有的客户端都使用一个根证书, 分发起来也比较方便。如下以 Chrome 为例。如果有多台服务, 只需要在每台服务端生成证书, 根证书保持不变。

2.0 配置方法

配置前如果访问服务，需要手工信任，如下图所示：



配置后如果访问服务，服务已经变成可信任服务，如下图所示：



2.1 服务端配置

2.1.1 生成证书

假设服务 IP 地址是 10.168.1.128。进入到服务根目录，windows 需要开启 cmd.exe

执行 genca.bat 10.168.1.128 (Linux 是 ./genca.sh) 参考下图, 密码请输入 1234:

```
C:\xdev\share\release\r16\h5s-r16.8.1023.23-win64-release>genca.bat 10.168.1.128
C:\xdev\share\release\r16\h5s-r16.8.1023.23-win64-release>REM mkdir certificate
C:\xdev\share\release\r16\h5s-r16.8.1023.23-win64-release>if "10.168.1.128" == "" GOTO BLANK
C:\xdev\share\release\r16\h5s-r16.8.1023.23-win64-release>set IPADDR=10.168.1.128
C:\xdev\share\release\r16\h5s-r16.8.1023.23-win64-release>set OPENSSL_CONF=openssl.cnf
C:\xdev\share\release\r16\h5s-r16.8.1023.23-win64-release>del certificate\ca*
C:\xdev\share\release\r16\h5s-r16.8.1023.23-win64-release>REM using "1234" for every password
Generating RSA private key, 2048 bit long modulus (2 primes)
.....++++
.....++++
e is 65537 (0x010001)
Ignoring -days, not generating a certificate
Signature ok
subject=C = CN, ST = Shanghai, O = linkingvision, CN = 10.168.1.128
Getting CA Private Key
Enter pass phrase for certificate\rootCA.key:
已复制 1 个文件。

[user@localhost h5s-r16.8.1023.23-linux-x86_64-64bit]$ ./genca.sh 10.168.1.128
IP is 10.168.1.128
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Signature ok
subject=/C=CN/ST=Shanghai/O=linkingvision/CN=10.168.1.128
Getting CA Private Key
Enter pass phrase for certificate/rootCA.key:
[user@localhost h5s-r16.8.1023.23-linux-x86_64-64bit]$
```

2.1.2 应用证书

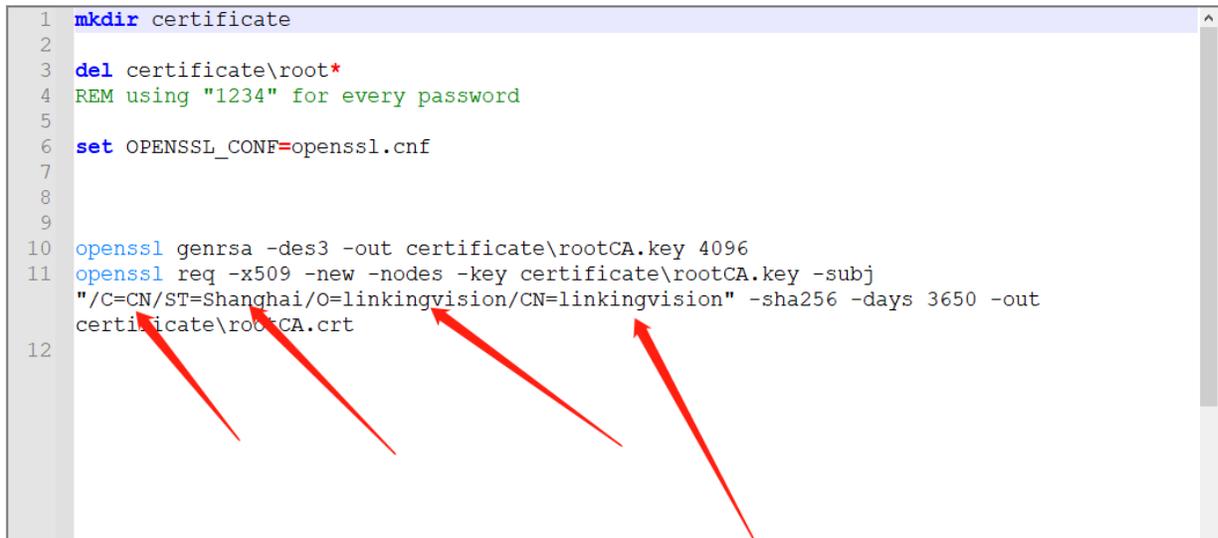
上一步生成的新证书在 certificate 下, 文件名为 ca.pem, Linux 和 windows 上文件结构相同, 参考下图:

ca.crt	2023/10/24 12:08	安全证书	2 KB
ca.csr	2023/10/24 12:08	CSR 文件	1 KB
ca.key	2023/10/24 12:08	KEY 文件	2 KB
ca.pem	2023/10/24 12:08	PEM 文件	4 KB
cluster.pem	2022/7/4 17:14	PEM 文件	4 KB
rootCA.crt	2022/7/4 17:05	安全证书	2 KB
rootCA.key	2022/7/4 17:05	KEY 文件	4 KB
rootCA.srl	2023/10/24 12:08	SRL 文件	1 KB
server.pem	2023/10/24 12:11	PEM 文件	4 KB

然后把 server.pem 删除, 把 ca.pem 重新命名为 server.pem, 然后重新启动服务。服务重启后会应用新的证书。

同时把 rootCA.crt 文件拷出来，分发给需要访问服务的 Chrome 所在的电脑，根证书是固定的。可以应用多台服务。如果需要修改根证书信息，可以修改 genrootca.bat (genrootca.sh)，并产生新的根证书，一个项目里面建议所有服务共享一个根证书，这样分发根证书比较方便，如果根证书变更的话，所有的服务证书都需要重做，因为服务证书是使用根证书签发的。

```
1 mkdir certificate
2
3 del certificate\root*
4 REM using "1234" for every password
5
6 set OPENSSSL_CONF=openssl.cnf
7
8
9
10 openssl genrsa -des3 -out certificate\rootCA.key 4096
11 openssl req -x509 -new -nodes -key certificate\rootCA.key -subj
    "/C=CN/ST=Shanghai/O=linkingvision/CN=linkingvision" -sha256 -days 3650 -out
    certificate\rootCA.crt
12
```



2.2 浏览器所在机器配置

2.2.1 导入根证书

把从服务拷出来的 rootCA.crt 双击打开，根据如下截图操作：

常规 详细信息 证书路径

 证书信息

此 CA 根目录证书不受信任。要启用信任，请将该证书安装到“受信任的根证书颁发机构”存储区。

颁发给: linkingvision

颁发者: linkingvision

有效期从 2022/7/4 到 2032/7/1

安装证书(I)...

颁发者说明(S)

确定

欢迎使用证书导入向导

该向导可帮助你将证书、证书信任列表和证书吊销列表从磁盘复制到证书存储。

由证书颁发机构颁发的证书是对你身份的确信，它包含用来保护数据或建立安全网络连接的信息。证书存储是保存证书的系统区域。

存储位置

- 当前用户(C)
- 本地计算机(L)

单击“下一步”继续



 下一步(N)

证书存储

证书存储是保存证书的

Windows 可以自动选

根据证书类型,

将所有的证书都

证书存储:

选择证书存储

选择要使用的证书存储(C)。

- 个人
- 受信任的根证书颁发机构
- 企业信任
- 中间证书颁发机构
- 受信任的发布者
- 不信任的证书
- 第三方根证书颁发机构

显示物理存储区(S)

确定 取消

...)

下一步(N) 取消



最后显示导入成功，导入成功后服务已经变成可信任服务。