

原创

Mlib

2018-11-01 14:12:51

9784

收藏 5

版权


分类专栏：

Web

文章标签：

HTTPS

TLS



Web 专栏收录该内容

操作步骤

首先新建一个配置文件 `ssl.conf` 如下：

```
1 [ req ]
2 default_bits = 4096
3 distinguished_name = req_distinguished_name
4 req_extensions = req_ext
5
6 [ req_distinguished_name ]
7 countryName = Country Name (2 letter code)
8 countryName_default = GB
9 stateOrProvinceName = State or Province Name (full name)
10 stateOrProvinceName_default = England
11 localityName = Locality Name (eg, city)
12 localityName_default = Brighton
13 organizationName = Organization Name (eg, company)
14 organizationName_default = Hallmarkdesign
15 organizationalUnitName = Organizational Unit Name (eg, section)
16 organizationalUnitName_default = IT
17 commonName = Common Name (e.g. server FQDN or YOUR name)
18 commonName_max = 64
19 commonName_default = localhost
20
21 [ req_ext ]
22 subjectAltName = @alt_names
23
24 [alt_names]
25 IP.1 = 192.168.1.8
26 DNS.1 = your-website.dev
27 DNS.2 = another-website.dev
```

1. 生成私钥

```
1 openssl genrsa -out private.key 4096
```

2. 生成证书请求文件（CSR）

CSR是Certificate Signing Request的英文缩写，即证书请求文件，也就是证书申请者在申请数字证书时由CSP(加密服务提供者)在生成私钥的同时也生成证书请求文件，证书申请者只要把CSR文件提交给证书颁发机构后，证书颁发机构使用其根证书私钥签名就生成了证书公钥文件，也就是颁发给用户的证书。

```
1 openssl req -new -sha256 \
2     -out private.csr \
3     -key private.key \
4     -config ssl.conf
```

这里会要求输入一系列参数，可以不填直接回车。

可以使用下面的命令是查看证书内容：

```
1 openssl req -text -noout -in private.csr
```

分类专栏

0 订阅

9 篇文章

订阅专栏

应该可以看到：

X509v3 Subject Alternative Name: DNS:my-project.site and Signature Algorithm: sha256WithRSAEncryption

3. 生成证书

然后生成证书命令如下：

```
1 openssl x509 -req \  
2     -days 3650 \  
3     -in private.csr \  
4     -signkey private.key \  
5     -out private.crt \  
6     -extensions req_ext \  
7     -extfile ssl.conf
```

参考资料

- Generate ssl certificates with Subject Alt Names on OSX

2万+	88万+	94万+	
周排名	总排名	访问	等级
certify:使用"subjectAltName"扩展名创建自签名证书-源码	使用"subjectAltName"扩展名创建自签名证书-源码	244	06-19
228证明 Certify 使用"subjectAltName"扩展名创建自签名 X.509 SSL/TLS 证书。介绍 首先要做的事情是：如果您想要在面向公众的 https 网站上使用 SSL/...	508自签名 X.509 SSL/TLS 证书。介绍 首先要做的事情是：如果您想要在面向公众的 https 网站上使用 SSL/...	332	
粉丝	获赞	评论	收藏
OpenSSL自签发配置有多域名或ip地址的证书 热门推荐			山鬼谣的专栏 2万+
环境翻译加实践概述HTTPS服务是工作在SSL/TLS上的HTTP。首先简单区分一下HTTPS，SSL，TLS，OpenSSL这四者的关系：SSL：(Secure Soc...			



优质评论可以帮助作者获得更高权重

抢沙发

评论

OpenSSL自签CA证书签署服务器SSL证书完整流程_tomggx的...	8-20
参考资料:【HTTPS】使用OpenSSL生成带有SubjectAltName的自签名证书	
openssl 自签名证书生成_Yuri's FarmLand	8-14
openssl 自签名证书生成 local3.cnf [dn] CN= xkyy.com [req] distinguished_name = dn [EXT] subjectAltName= @alt_names keyUsage=digitalSignature e...	
如何使用OpenSSL生成带有SubjectAltName的自签名证书？	Crystal360的博文 7881
我试图生成一个自签名证书与OpenSSL with SubjectAltName in.While我生成证书的csr，我的猜测是我必须使用OpenSSL x509的v3扩展。我在用：open...	
介绍一下 X.509 数字证书中的扩展项 subjectAltName	henter的专栏 8507
在 RFC 5280 《Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile》中定义了 X.509 公钥数字证书和证书...	
【SSL】关于自签名类型_michaelwoshi的博文	10-13
# openssl x509 -nout -text -in harbor.crt 私有CA签名证书的issuer和Subject是不同的。 四、数字证书(Certificate) 在HTTPS的传输过程中有一个非常关...	
openssl 自签证书_lingqiao023的博文	8-13
[req_ext] subjectAltName = @alt_names [alt_names] DNS.1 = minikube.com DNS.2 = *.minikube.com DNS.3 = localhost IP = 127.0.0.1 EOF \$ openssl ...	
openssl证书添加多个IP	林三的专栏 1万+
前文http://blog.csdn.net/linsanhua/article/details/16878817 描述了基于 OpenSSL 的 CA 建立及证书签发过程。 这里描述怎么利用subjectAltName添加ip...	
输出每个数字对应的拼音	Joway 1万+
【描述】输入一个整数，输出每个数字对应的拼音。当整数为负数时，先输出“fu”字。十个数字对应的拼音如下： 0: ling 1: yi 2: er 3: san 4: si 5: wu 6: liu...	
使用pyopenssl提取证书中的subjectAltName	村中少年的专栏 1774
本文介绍一下如何通过Python的pyopenssl模块解析证书的subjectAltName	
Windows 下使用 OpenSSL 命令行创建包含 subjectAltName 扩展项的数字证书	henter的专栏 2433
1. CA 的基本原理简介（了解相关背景知识的读者请跳过这一部分）我们回想一下在生活中，两个以前从未谋面的人如何核实对方的身份。由于每一个公...	
使用 OpenSSL 制作一个包含 SAN (Subject Alternative Name) 的证书	weixin_34387468的博文 4881
为什么80%的码农都做不了架构师？>>> ...	
OpenSSL创建带SAN扩展的证书并进行CA自签	liwei2633的专栏 1万+
什么是 SANSAN(Subject Alternative Name) 是 SSL 标准 x509 中定义的一个扩展。使用了 SAN 字段的 SSL 证书，可以扩展此证书支持的域名，使得一个...	
OpenSSL生成v3证书方法及配置文件	weixin_34066347的博文 968
场景：业务需要生成v3版的证书，而一般使用OpenSSL生成证书时都是v1版的，不带扩展属性。方法：在使用CA证书进行签署证书时加入-extfile和-exten...	



Mlib

码龄8年



暂无认证

102

原创

7406

积分



私信

关注

搜博主文章



热门文章

【算法】大数乘法问题及其高效算法 79211

"二分查找"算法的时间复杂度 63386

【算法】如何判断链表有环 51073

【面试题】N级台阶（比如100级），每次可走1步或者2步，求总共有多少种走法？ 50261

【Android】技术调研：用代码模拟屏幕点击、触摸事件 35678

最新评论

【算法】如何判断链表有环
辛梓Paula: 对的，我觉得答主这里有点小问题。

【面试题】N级台阶（比如100级），每...
zaccur: [code=python] def sum_stairs_dy namic__(num: int): methods = [0, 1, 2, 3]...

【算法】大数乘法问题及其高效算法
叶臻铭: 写得非常好，解答了我大部分的疑问。不过还有个问题，JAVA好像是转换差...

【Java】Thread类中的join()方法原理

六骑六贵: 太强啦

八大排序算法总结与java实现
mianmianjun: 博主，你的希尔排序为啥内部是个冒泡。。。。

您愿意向朋友推荐“博客详情页”吗？

强烈不推荐不推荐一般般推荐强烈推荐

最新文章

为什么说TCP是面向流的协议？而UDP是面向数据报的协议？

【Java】反编译Mac版Charles，修改一些功能

【Android】移动端接入Cronet实践

2019年6篇

2018年16篇

2017年38篇

2016年42篇

2015年15篇

2014年2篇

2013年2篇

使用openssl生成自签证书使项目支持https

使用openssl生成自签证书使项目支持https生成CA证书创建私钥opensslgenrsa-outca-key.pem1024创建证书请求opensslreq-new-outca.csr-key...

weixin_41774732的博客107

SSL证书生成全过程

建立私有CA签发证书。

F2004的专栏8691

通过OpenSSL创建自签名证书在Flask实现HTTPS

最新发布

子燕若水的博客140

Generate a private keyopensslgenrsa-des3-outserver.key1024Generate a CSRopensslreq-new-keyserver.key-outserver.csrRemove Passphr...

解决自签名证书在Chrome上的“不是私密连接问题”

Newpyer的博客2万+

有时候需要在局域网上访问IP地址，但是由于操作系统或者浏览器的原因(苹果，小程序不允许在app中访问http接口)，会弹出警告，如下: 此问题可用o...

OpenSSL生成https服务器端数字证书

技不如人2379

1. 下载安装OpenSSL 可以从OpenSSL官网下载源码编译，也可以直接下载安装文件，地址：http://download.csdn.net/download/nicholas_lin/10169024 ...

OpenSSL 生成自签名证书 (Self-signed SSL certificate)【转】

我的地盘6694

OpenSSL生成自签证书

©2021 CSDN 皮肤主题: 编程工作室 设计师:CSDN官方博客 返回首页

Mlib

关注

4

0

5

专栏目录

联网举报中心 家长监护 Chrome商店下载 ©1999-2021北京创新乐知网络技术有限公司 版权与免责声明 版权申诉 出版...