

 码龄14年  暂无认证

13

20万+

107万+

5万+



原创

周排名

总排名

访问

等级

702

14

2

7

11

积分

粉丝

获赞

评论

收藏







私信

关注

搜博主文章



热门文章

[翻译] (黑苹果)笔记本电脑原生电源管理指南 [Guide] Native Power Management for Laptops  11634

浏览器嵌入组件miniblink使用笔记  9198

ZTE V5 MAX (N958S)手动重新分区教程  5401

解决“可移动媒体不支持此操作”问题 (Solve The operation is not supported on removable media)  5190

等待JQuery异步全部完成执行语句(函数)  3748

最新评论

[翻译] (黑苹果)笔记本电脑原生电源管理...
Tisfy: 顶一个！

解决“可移动媒体不支持此操作”问题 (Sol...
ThursdayGame 回复 tomngx: 在 text 中：左
上角 打开--选择文件地方可以浏览，做复...

解决“可移动媒体不支持此操作”问题 (Sol...
tomngx 回复 ThursdayGame: 要用管理员权
限启动一个7-zip软件，在软件里面就可以...

解决“可移动媒体不支持此操作”问题 (Sol...
ThursdayGame: 挂载成功了 但是没有 访问
权限

解决“可移动媒体不支持此操作”问题 (Sol...
ThursdayGame: 挂载正确了 但是 没有访问
权限怎么办？

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

原创

tomngx

2019-04-15 19:29:38

 1131

 收藏 3

版权

分类专栏：

后端开发


OpenSSL

文章标签：

OpenSSL

证书

SubjectAltName

 后端开发

同时被 2 个专栏收录

0 订阅

2 篇文章

订阅专栏

首先, 在 <http://slproweb.com/products/Win32OpenSSL.html> 上下载已经编译好的OpenSSL库

然后通过如下步骤生成服务器证书：

1、生成根证书私钥：

```
openssl genrsa -out rootCA.key 4096
```

2、生成自签名根证书：

```
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.crt
```

3、生成server私钥：

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

4、根据subjectAltName.cnf生成server CSR:

```
openssl req -new -key server.key -out server.csr -config subjectAltName.cnf
```

5、查看生成的server CSR信息：

```
openssl req -noout -text -in server.csr
```








6、rootCA签署server CSR生成server CRT：

```
openssl x509 -req -days 500 -in server.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out server.crt -extensions req_ext -extfile subjectAltName.cnf
```

以下为subjectAltName.cnf文件内容，请根据实际情况对localhost.dev进行替换：

```
1 [ req ]
2 distinguished_name = req_distinguished_name
3 req_extensions     = req_ext
4
5 [ req_distinguished_name ]
6 countryName        = Country Name (2 letter code)
7 countryName_default = CN
8 stateOrProvinceName = State or Province Name (full name)
9 stateOrProvinceName_default = China
10 localityName       = Locality Name (eg, city)
11 localityName_default = Beijing
12 organizationName    = Organization Name (eg, company)
13 organizationName_default = localhost.dev
14 organizationalUnitName = Organizational Unit Name (eg, section)
15 organizationalUnitName_default = localhost.dev
16 commonName          = Common Name (e.g. server FQDN or YOUR name)
17 commonName_max       = 64
18 commonName_default   = localhost.dev
19
20 [ req_ext ]
21 subjectAltName = @alt_names
22
```

分类专栏

	前端开发	3篇
	VBScript	2篇
	Android	3篇
	c++	3篇
	后端开发	2篇
	Access	1篇
	Python	1篇
	SSL	1篇
	OpenSSL	1篇
	subjectAltName	
	系统	3篇
	黑苹果	2篇

最新文章

[翻译] (黑苹果)笔记本电脑原生电源管理指南
[Guide] Native Power Management for Laptops


[翻译] 禁用双GPU笔记本电脑的独显
Disabling discrete graphics in dual-GPU laptops

解决“可移动媒体不支持此操作”问题 (Solve The operation is not supported on removable media)

2019年	5篇	2018年	3篇
2017年	3篇	2016年	7篇
2009年	1篇		

```
23 [alt_names]
24 DNS.1 = localhost.dev
25 DNS.2 = *.localhost.dev
```

参考资料：
【HTTPS】使用OpenSSL生成带有SubjectAltName的自签名证书

 tomggx

关注

1

0

3





专栏目录

- openssl_certs：用于创建自签名CA证书和由CA签名的CN证书脚本-源码

02-16
- 使用openssl创建和管理证书脚本，让我们进行加密 1.使用HTTPS设置Jenkins并让我们加密证书 介绍 Let's Encrypt是由Internet Security Research Gro...
- 图书管理系统 (Java + Mysql) 我的第一个完全自己做的实训项目

01-04
- 图书管理系统 Java + MySQL 完整实训代码，MVC三层架构组织，包含所有用到的图片资源以及数据库文件，大三上学期实训，注释很详细，按照阿里巴...

 优质评论可以帮助作者获得更高权重

抢沙发

评论

基于OpenSSL自建CA和颁发SSL证书_Code Captain的专栏8-13

cd /etc/nginx/ssl# openssl genrsa -out nginx.key 2048 这里测试的时候CA中心与要申请证书的服务器是同一个。 1.5 为nginx生成证书签署请求 123456...

OPENSSL自建CA服务器自签证书服务器_松果177的博客7-27

自建CA服务器自签证书服务器 一、配置证书服务器模板 #修改openssl.cnf文件vi/etc/pki/tls/openssl.cnf#确保[req]下存在以下两行[req]distinguished_na...

用openssl自做CA自签发SSL证书swanabin的专栏9461

本人运行环境：openssl-1.0.1p，vs2010 首先运行CMD，跳转到..\openssl-1.0.1p\out32dll 目录下，比如我的: c:>cd c:\openssl-1.0.1p\out32dll c:\opens...

自做CA自签发SSL证书 httpsxinxintai的专栏4990

SSL Created Tuesday 16 October 2012 自做CA自签发SSL证书 http://www.csr.net/Notes/Apache-HTTPS-virtual-host.html http://wiki.cacert.org/VhostTa...

openssl私有CA实现及私有证书签署_donghaixiaolongwang...10-22

openssl私有CA实现及私有证书签署 当你用到私有CA自签证书的时候,那意味着你的数据需要加密了(在互联网上或者其他使用场景下传输数据)。 要想做...

OPENSSL生成SSL自签证书_心飞路漫的博客10-16

OPENSSL生成SSL自签证书 目前,有许多重要的公网可以访问的网站系统(如网银系统)都在使用自签SSL证书,即自建PKI系统颁发的SSL证书,而不是部署支...

OpenSSL生成自签名SSL证书过程heww的专栏263

windows下生成自证书https://my.oschina.net/fajar/blog/425478

建立自己的CA，签署自己的服务器证书，配置自己的https站点wqs1106的博客224

一、目标 从头开始配置一个自己的https站点，并让本机浏览器信任站点。 二、商用步骤 1. 创建自己的私钥 2. 创建CSR(Certificate Signing Request) 3. ...

openssl自签发https证书_小单的博客专栏8-13

服务端私钥与证书 openssl genrsa -out server.key 2048 openssl req -new -sha256 -key server.key -out server.csr -days 3650 -subj /C=CN/ST=JiangSu...

用openssl生成SSL使用的私钥和证书,并自己做CA签名_zxh...10-16

本文记叙的是一次基于SSL的socket通讯程序开发中,有关证书,签名,身份验证相关的步骤。 我们的场景下,socket服务端是java语言编写的,客户端是c语言...

openssl自签名CA证书huangbaoling66的博客342

原博客链接 本文非原创，系浏览各博客后结合自身使用的一个总结，方便回顾。 前情提要 通俗理解SSL/TLS协议区别与原理 数字签名是什么 什么是x509...

自定义ca，并使用该ca签署证书weixin_34006468的博客95

http协议是互联网应用中的主要协议，从诞生至今一直被广泛的使用，我们知道http协议是明文传输的，现在的互联网安全形势严峻，使用明文传输的http...

使用OpenSSL生成自签名SSL证书 热门推荐锐意工作室2万+

文章目录使用OpenSSL生成自签名SSL证书参考文档检查OpenSSL生成自签名的SSL证书和私钥第一步：生成私钥第二步：去除私钥中的密码第三步：生...

Ubuntu18.04 Openssl生成自签SSL证书 最新发布qq_40156159的博客960

Openssl生成自签SSL证书安装openssl生成证书 安装openssl 方法一 sudo apt-get install openssl sudo apt-get install libssl-dev 方法二 在openssl官网下...

CA证书自签详解z344945251的博客5897

原文链接：http://blog.csdn.net/liunian_siyou/article/details/53024407 首先需要安装openssl。 openssl的配置文件是openssl.cnf，我们一般就是用默认配...

openssl自签署证书 # openssl genrsa -des3 -out ca.key 10241.产生一个rsa加密算法生成的CA钥，设置私钥长度为1024字节，输入到ca.key文件中。Generating RSA privat...	独自陶醉 4902
使用Openssl生成自签证书 graph LR; S[开始] -- openssl genrsa --> A1[ca.key]; A1 -- openssl req --> B[ca.csr]; B -- openssl ca --> C[ca.cert]; C --> D;	罗小爬 2232
openssl生成SSL证书的流程 SSL证书通过在客户端浏览器和Web服务器之间建立一条SSL安全通道 (Secure socketlayer(SSL),SSL安全协议主要用来提供对用户和服务器的认证；对...	moonhillcity的博客 1万+
https ca 自签证书安装步骤 1. 生成自签证书 CA 服务器 (假设ip: 10.1.1.100) # redhat os cd /etc/pki/CA # s生成私钥不允许其他人访问, 使用077 umask 控制 (umask 077; openssl g...	王继超的专栏 4612
openssl 进行创建私有CA并自签，发证，吊销证书 一，创建私有CA (我使用的是192.168.10.2的服务器) 自签： openssl的配置文件： cat /etc/pki/tls/openssl.cnf dir = /etc/pki/CA 真正的工作目...	刘东义的博客 1644
基于OpenSSL自建CA和颁发SSL证书+nginx访问 关于SSL/TLS介绍见文章 SSL/TLS原理详解。关于证书授权中心CA以及数字证书等概念，请移步 OpenSSL 与 SSL 数字证书概念贴。 openssl是一个开...	ronon77的专栏 521
openssl生成https自签名证书 今天用openssl生成了下https的证书，总结下整个流程 1.设置openssl的环境变量， OPENSSL_CONF=openssl.cnf路径 2.将openssl配置文件中的 req_ext...	天道酬勤 6481
©2021 CSDN 皮肤主题: 大白 设计师:CSDN官方博客 返回首页	

