原创 阳光之吻 2016-01-08 19:03:00 524 收藏 版权

分类专栏： Linux-open 文章标签： openssl

公钥与密钥应用的两种情形

- 用于数据加密
  - 两个人：Bob和Alice；Bob有自己的公钥和私钥，他把公钥公布给大家；当Alice给Bob发送数据时，她使用Bob的公钥加密这些数据；因为使用Bob的公钥加密的数据只有Bob的私钥能解密，所以Alice发送给Bob的数据只有Bob能解密并查看，其他人是不能解密的（除非他有Bob的私钥）。
- 用于认证
  - Bob和Alice通信，Bob如何向Alice证明自己就是Bob呢？Bob可以向Alice发一段用自己的私钥加密的内容，如果Alice可以使用Bob的公钥解密说明对方是Bob。
- 这两种情形有一个比较明显的问题：Alice怎么收到Bob公布的公钥？Alice怎么知道自己收到的公钥就是Bob的公钥？这个时候就需要第三方来认证了，那就是数字证书。

数字证书

- 上面提到的只是对公钥和私钥的简单说明，实际过程很复杂，所以后来才发展出了数字证书，数字证书就是用来数字证书发送方证明数字证书持有人的。以Bob和Alice为例，就是Bob向Alice证明自己就是Bob的。数字证书也是由公认的权威机构颁发的，而且这些机构会给自己生成一个数字证书，这些机构的数字证书被预制安装在操作系统中被用来对其他服务器发来的证书进行认证；
- 购买这些机构发行的数字证书价格不菲，我们能否自己私建证书对自己内部的主机进行认证呢？能！

私建数字证书

- 需要一台管理证书的服务器，比如我有一台centos7服务器；
  - 用到的程序：openssl；
  - 配置文件：

```
[root@mylinux7 pki]# ll /etc/pki/tls/openssl.cnf
-rw-r--r--. 1 root root 10923 Mar  5  2015 /etc/pki/tls/openssl.cnf
```

- 主目录结构：

```
[root@mylinux7 ~]# ll /etc/pki/CA/
    # /etc/pki/CA/ , Where everything is kept ;
total 24
drwxr-xr-x. 2 root root 4096 Mar  5  2015 certs
    # certs , Where the issued certs are kept ;
drwxr-xr-x. 2 root root 4096 Mar  5  2015 crl
    # crl ( 吊销证书列表 ) , Where the issued crl are kept ;
-rw-r--r--. 1 root root    3 Jan  4 18:49 crlnumber
    # crlnumber , the current crl number ;
-rw-r--r--. 1 root root    0 Jan  4 18:47 index.txt
    # index.txt , database index file ;
drwxr-xr-x. 2 root root 4096 Mar  5  2015 newcerts
```


分类专栏
linux command
Linux-DNS 1篇
Linux-open 1篇
phpmyadmin
wordpress 1篇
discuz 2篇
NFS 1篇

```
    # newcerts，default place for new certs；
drwx------. 2 root root 4096 Mar  5  2015 private
    # private，证书发现服务器本身私钥cakey.pem的存放目录；
-rw-r--r--. 1 root root    3 Jan  4 18:48 serial
    # serial，The current serial number；
注： crlnumber,index.txt,serial这三个文件需要新建（依据是配置文件）：
[root@mylinux7 ~]# cd /etc/pki/CA/
[root@mylinux7 CA]# touch index.txt
[root@mylinux7 CA]# echo 01 > serial
[root@mylinux7 CA]# echo 01 > crlnumber
```

- CA服务器自签证书过程（给自己发行证书）：

```
[root@mylinux7 CA]# (umask 077; openssl genrsa -out /etc/pki/CA/private/cakey.pem 2048)
    # 此语句是以077的umask生成一个cakey.pem私钥文件；
Generating RSA private key, 2048 bit long modulus
...............+++
.....................................................................+++
e is 65537 (0x10001)
[root@mylinux7 CA]# openssl req -new -x509 -key /etc/pki/CA/private/cakey.pem -days 7300 -out /etc
/pki/CA/cacert.pem
    # 可能您看到的是换行的，其实是一条语句；
    # openssl req 用于生成证书请求文件；
    # -new 生成新证书签署请求；
    # -x509 专用于CA生成自签证书；
    # -key 生成请求文件时用到的私钥文件；
    # days 证书的有效期限，以“天”为单位；
    # -out 证书的保存路径；
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CN
    # 国家名，两个字符；
State or Province Name (full name) []:Shanghai
    # 省名或州名；
Locality Name (eg, city) [Default City]:Shanghai
    # 城市名；
Organization Name (eg, company) [Default Company Ltd]:TestCompany
    # 公司名；
Organizational Unit Name (eg, section) []:web
    # 部门名称；
Common Name (eg, your name or your server's hostname) []:mylinux7
    # 你的名字或服务器名；
Email Address []:root@mylinux7
    # 你的Email地址；
[root@mylinux7 CA]# ll /etc/pki/CA/cacert.pem
-rw-r--r--. 1 root root 1411 Jan  5 04:48 /etc/pki/CA/cacert.pem
    # cacert.pem为CA的自签证书；
```

- 给其他主机发行证书
  - 我这里是给如下主机发行证书

```
[root@dns1 ~]# hostname
dns1.mysite.com
```

- 首先申请方服务器得生成一个私钥，并利用私钥生成一个请求文件：

```
[root@dns1 ~]# (umask 077; openssl genrsa -out /etc/httpd/ssl/httpd.key 2048)
    # 使用rsa算法生成一个私钥；
Generating RSA private key, 2048 bit long modulus
.....................+++
.........................................+++
e is 65537 (0x10001)
[root@dns1 ~]# openssl req -new -key /etc/httpd/ssl/httpd.key -days 365 -out /etc/httpd/ssl/httpd.csr
    # 使用刚生成的一个私钥再生成一个请求文件httpd.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CN
State or Province Name (full name) []:Shanghai
Locality Name (eg, city) [Default City]:Shanghai
Organization Name (eg, company) [Default Company Ltd]:TestCompany
Organizational Unit Name (eg, section) []:web
Common Name (eg, your name or your server's hostname) []:www
Email Address []:root@dns1.mysite.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@dns1 ~]# ll /etc/httpd/ssl/httpd.csr
-rw-r--r--. 1 root root 1054 Jan  8 20:41 /etc/httpd/ssl/httpd.csr
```

- 把文件通过某个方法传送（发送）给CA服务器
  - 由于是测试环境，我使用的是scp命令：

```
[root@dns1 ~]# scp /etc/httpd/ssl/httpd.csr root@192.168.1.105:/tmp/httpd.csr
The authenticity of host '192.168.1.105 (192.168.1.105)' can't be established.
RSA key fingerprint is 6c:3e:a2:06:52:e4:e4:b9:82:52:74:fc:0a:44:ea:6d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.105' (RSA) to the list of known hosts.
root@192.168.1.105's password:
httpd.csr                                     100% 1054     1.0KB/s   00:00
```

- 在CA服务器生成申请服务器的证书

```
[root@mylinux7 CA]# openssl ca -in /tmp/httpd.csr -out /etc/pki/CA/certs/httpd.crt -days 365
    # 使用openssl ca命令生成证书；
Using configuration from /etc/pki/tls/openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Jan  5 10:51:28 2016 GMT
            Not After : Jan  4 10:51:28 2017 GMT
        Subject:
```

```
            countryName               = CN
            stateOrProvinceName       = Shanghai
            organizationName          = TestCompany
            organizationalUnitName    = web
            commonName                = www
            emailAddress              = root@dns1.mysite.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                A4:CF:3A:18:D8:EE:08:54:11:18:DC:CD:A0:5B:17:F9:40:E1:8C:D4
            X509v3 Authority Key Identifier:
                keyid:DA:48:EB:1E:B2:36:DA:44:E7:3C:53:A9:47:62:D7:FD:5A:E4:D1:8D

Certificate is to be certified until Jan  4 10:51:28 2017 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[root@mylinux7 CA]# scp /etc/pki/CA/certs/httpd.crt root@192.168.1.108:/etc/httpd/ssl/httpd.crt
root@192.168.1.108's password:
httpd.crt                                                     100% 4606     4.5KB/s   00:00
    # 使用scp命令将证书传送回申请服务器；
```

- 可以发现CA服务器CA目录下的index.txt和serial文件内容已经更新，且在newcert目录下也生成了一个名字为01的证书；
- 在申请到证书的服务器上可以通过如下命令查看证书信息：

```
[root@dns1 ~]# openssl x509 -in /etc/httpd/ssl/httpd.crt -noout -serial -subject -text
    # 最后的-serial -subject -text三者可以根据需要任意出现；
```

- 吊销证书
  - 申请到证书的服务器应该首先使用上面提到的命令提取自己证书的serial和subject，并发送给CA服务器；
  - CA服务器收到serial和subject，与index.txt中的证书信息进行校验，通过则执行吊销：

```
[root@mylinux7 CA]# openssl ca -revoke /etc/pki/CA/newcerts/01.pem
    # 吊销证书命令“01”是serial；
Using configuration from /etc/pki/tls/openssl.cnf
Revoking Certificate 01.
Data Base Updated
You have new mail in /var/spool/mail/root
[root@mylinux7 CA]# openssl ca -gencrl -out myca.crl
    # 更新证书吊销列表；
Using configuration from /etc/pki/tls/openssl.cnf
```

–完–

Linux openssl 生成证书的详解 热门推荐 叶梦 4万+
目录 前言 1 概念 2 环境 3 创建根证书CA 4 颁发证书 4.1 在需要证书的服务器上，生成证书签署请求 4.2 在根证书服务器上，颁发证书 5 测试 5.1 读取te…

抢沙发
优质评论可以帮助作者获得更高权重
评论

linux下keytool生成证书_keytool命令 – 密钥和证书管理工具 10-24
-printcert打印证书内容 -printcertreq打印证书请求的内容 -printcrl打印CRL文件的内容 -storepasswd更改密钥库的存储口令 参考实例 生成服务器证书文件…

linux查看系统证书库,linux系统学习第八天-<<工程师技… 10-24
linux查看系统证书库,linux系统学习第八天-<<工程师技术>> 两台虚拟机,均修改防火器与主机名 虚拟机server0:# firewall-cmd --set-default-zone=trusted# …

linux查cer证书信息,openssl 查看证书 最新发布 weixin_28752743的博客 1606
查看证书# 查看KEY信息> openssl rsa -noout -text -in myserver.key# 查看CSR信息> openssl req -noout -text -in myserver.csr# 查看证书信息> openssl …

linux ca-certificates维护openssl证书 云行雨施 品物流形 1万+
SSL证书的维护由ca-certificates来提供支持 https://packages.debian.org/source/sid/ca-certificates Debian 软件包源码仓库(VCS: Git) https://anonscm.d…

Linux证书与CA简介_当世事再没完美,可远在岁月如歌中找你 10-24
Linux证书与CA简介 CA和证书 1 中间人攻击 Man-in-the-middle,简称为 MITM,中间人 以上的各种加密措施,前提条件都是【传输过程无任何问题】,实际上…

linux系统添加根证书 linux证书信任列表_lemonzone2010… 9-29
2.现有 证书twca.cer 需要添加到 linux 证书信任列表 相关证书转换参见:http://netkiller.github.io/cryptography/openssl/format.html #转换格式 .cer 到 .pem …

Linux证书访问 metpear的博客 471
工作需要用到多台Linux的机器，每次访问都需要输入密码。 使用证书登录，可以达到免密的效果。 配置步骤如下： 跳板机（操作的机子）： 为当前用户…

LINUX 证书导入 victorunique的专栏 6157
安装证书管理工具与Firefox不同，Chrome没有自己的证书管理，而是使用系统的证书管理。在Windows中，我们可以通过Internet选项来管理证书，添加…

Linux 部署CA数字证书服务_weixin_34261415的博客 10-24
Linux 部署CA数字证书服务 CA数字证书服务 CA Certificate Authority 数字证书授权中心 被通信双方信任的,独立的第三方机构 负责证书颁发,验证,撤销等…

Linux 搭建私有CA证书服务器之超详细版本_Harry_z666的… 8-21
Linux 搭建私有CA证书服务器之超详细版本 一、CA简介 CA是什么?CA是Certificate Authority的简写,从字面意思翻译过来是凭证管理中心,认证授权。它有…

Linux 添加证书 o_longzhong的专栏 1599
sudo cp path/to/goagent/local/your.crt /usr/share/ca-certificates/your.crt sudo chmod a+r /usr/share/ca-certificates/goagent.crt sudo dpkg-reconfigure …

linux下的证书安装 AndyMocan的博客 1万+
linux下的证书安装说明 拷贝证书到/usr/share/ca-certificates/下 cp CA.crt /usr/share/ca-certificates/x-net.crt 修改权限 chmod a+r /usr/share/ca-certificat…

Linux证书转换命令 培根芝士的专栏 654
PFK转JKS keytool -importkeystore -srckeystore ddd.pfx -srcstoretype PKCS12 -deststoretype JKS -destkeystore ddd.jks CRT+KEY转JKS pkcs12 -exp…

Linux服务器上如何给项目设置SSL证书 huangdj321的博客 3137
一、HTTPS和HTTP的区别 1、https协议需要到ca申请证书，一般免费证书较少，因而需要一定费用。 2、http是超文本传输协议，信息是明文传输，http…

linux 证书颁发的两种方法 weixin_33963189的博客 177
1 自签名的证书生成网站所使用的私钥openssl genrsa -out server.key 1024生成网站所使用的证书文件openssl req -new -x509 -key server.key -out serv…

Linux下如何安装 cer证书 fswhwd的博客 5865
Linux下如何安装 cer证书

Linux(CA申请数字证书过程) 李立衡 1536
1）在应用服务器上生成私钥 2）利用私钥生成证书请求文件，CSR文件 3）将CSR文件提交至CA 4）CA核实CSR 请求 5）CA签署数字证书 6）CA将签…

Linux 添加HTTPS证书 荧光之烛 9331
之前的文章是linux 做反向代理！ 现在继续添加证书。cd /etc/nginx/conf.d输入rz 回车上传证书文件 9358.com.crt 9358.com.key需要编辑两个文件 vi 9358…

Linux keytool命令密钥和证书管理工具,生成ssl证书 weixin_43484014的博客 210
Linux keytool命令密钥和证书管理工具,生成ssl证书 keytool -genkey -alias tomcat8 -keyalg RSA -keystore /opt/tomcat8/conf/.keystore -validity 36500 上…

linux中的用户管理、 用户认证信息、用户授权 橙汁Iter的博客 1032
一、用户管理 1.用户存在的意义安全，用户概念在系统中是安全机制的一部分，并且用来限制权力。 2.组存在的一意义 共享，开放权力（资源共享） 3.…

阳光之吻
码龄12年 暂无认证

15	33万+	137万+	3万+	
原创	周排名	总排名	访问	等级
496	11	12	0	26
积分	粉丝	获赞	评论	收藏

私信 关注

搜博主文章

热门文章

用c语言编写的可以计算+-*/的计算器 8674
Linux下的网络配置方法（一） 7534
Linux下的LVM管理命令 4560
Linux下btrfs子卷的挂载 2575
Linux下的网络配置方式(二) 2432

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

用c语言编写的可以计算+-*/的计算器

CenOS6.6下编译安装LAMP

使用虚拟主机配置phpmyadmin, wordpress, discuz

2016年 15篇

linux系统添加根证书 linux证书信任列表

lemonzone2010的专栏 3万+

linux访问https证书问题 linux系统添加根证书 linux证书信任列表