环境

CA认证中心服务端：xuegod63.cn IP：192.168.1.63

          客户端：xuegod64.cn IP：192.168.1.64

CA认证中心简述

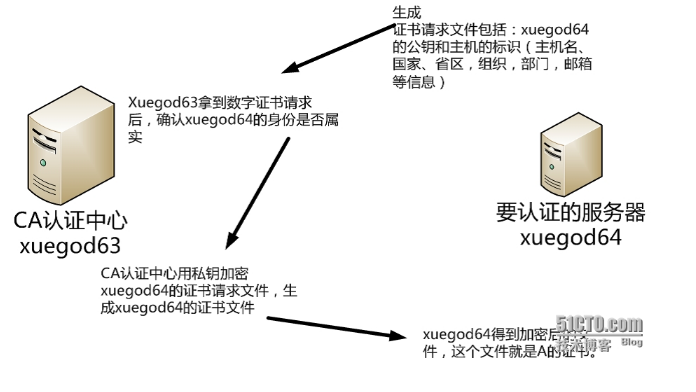
 CA ：CertificateAuthority的缩写，通常翻译成认证权威或者认证中心，主要用途是为用户发放数字证书。

功能：证书发放、证书更新、证书撤销和证书验证。

作用：身份认证，数据的不可否认性

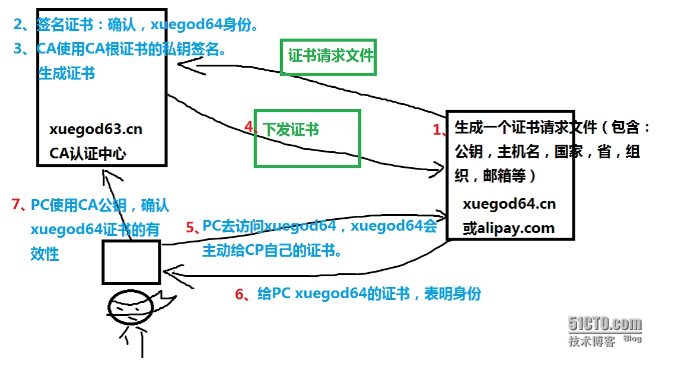
端口：443

过程：



证书请求文件:CSR是Cerificate 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的私钥签名就生成了证书文件，也就是颁发给用户的证书。

用户使用CA证书确认服务器身份过程：



一：搭建CA认证中心

配置一个自己的CA认证中心

|  |
| --- |
| [root@xuegod63 CA]# vim /etc/pki/tls/openssl.cnf  改： 172 #basicConstraints=CA:FALSE  为：172 basicConstraints=CA:TRUE #让自己成为CA认证中心 |

配置认证中心，生成私钥与根证书

|  |
| --- |
| [root@xuegod63 CA]# /etc/pki/tls/misc/CA -h #查看帮助  usage: /etc/pki/tls/misc/CA -newcert|-newreq|-newreq-nodes|-newca|-sign|-verify  [root@xuegod63 ~]# /etc/pki/tls/misc/CA -newca  #配置一个新的CA认证中心  CA certificate filename (or enter to create) #直接回车  Making CA certificate ...  Generating a 2048 bit RSA private key  ....................+++  ..........................................................................+++  writing new private key to '/etc/pki/CA/private/./cakey.pem'  Enter PEM pass phrase:123456 # 输入密码，保护私钥  Verifying - Enter PEM pass phrase:123456 #再次输入密码  -----  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 aDN.  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  #国家地区  State or Province Name (full name) []:beijing  #城市  Locality Name (eg, city) [Default City]:haidian  #当地名称  Organization Name (eg, company) [Default Company Ltd]: xuegod #组织名称  Organizational Unit Name (eg, section) []:IT  #组织部门名称  Common Name (eg, your name or your server's hostname) []:xuegod63.cn #通用名称（例如，您的姓名或您的服务器的主机名）,随便写  Email Address []:1@163.com  #邮箱  Please enter the following 'extra' attributes  to be sent with your certificate request #添加一个“额外”的属性，让客户端发送CA证书,请求文件时，要输入的密  A challenge password []: #直接加车  An optional company name []:#直接加车  Using configuration from /etc/pki/tls/openssl.cnf #CA服务器的配置文件。上面修改的内容会添加到这个配置文件中  Enter pass phrase **for** /etc/pki/CA/private/./cakey.pem: 123456 #输入刚才保护CA密钥的密码  Check that the request matches the signature  Signature ok  Certificate Details:  Serial Number:  c9:16:bb:49:48:20:ed:16  Validity  Not Before: Dec 20 12:00:19 2014 GMT  Not After : Dec 19 12:00:19 2017 GMT  Subject（主题）:  countryName = CN  stateOrProvinceName = beijing  organizationName = xuegod  organizationalUnitName = IT  commonName = shenjianming  emailAddress = 1@163.com  X509v3 extensions:  X509v3 Subject Key Identifier:  BF:E3:16:CC:EB:42:BD:6D:56:8E:A4:21:70:E6:72:40:0C:77:C0:C0  X509v3 Authority Key Identifier:  keyid:BF:E3:16:CC:EB:42:BD:6D:56:8E:A4:21:70:E6:72:40:0C:77:C0:C0  X509v3 Basic Constraints:  CA:TRUE  Certificate is to be certified **until** Dec 19 12:00:19 2017 GMT (1095 days)  Write out database with 1 new entries  Data Base  Updated |

#这里了配置CA认证中心，在里面就生成了CA认证根证书的私钥，在配置完结束之后，就会生成一个根证书，这个根证书中有这证书的 公钥

注：到此CA认证中心就搭建好了。

查看生成的CA根证书：

|  |
| --- |
| [root@xuegod63 CA]#vim /etc/pki/CA/cacert.pem #存在CA认证下的根证书，这里面包含了根证书的公钥。  Certificate:  Data:  Version: 3 (0x2)  Serial Number:  c0:1d:ed:ba:fc:7e:b4:40  Signature Algorithm: sha1WithRSAEncryption  Issuer:C=CN, ST=beijing, O=xuegod, OU=IT, CN=shenjianming/emailAddress=1@1  63.com #CA 机构信息  Validity  Not Before: May 9 11:54:20 2015 GMT  Not After : May 8 11:54:20 2018 GMT  Subject: C=CN, ST=beijing, O=xuegod, OU=IT,CN=shenjianming/emailAddress=1@  163.com  SubjectPublic Key Info: #CA认证中心公钥信息  Public Key Algorithm: rsaEncryption  Public-Key: (2048 bit)  Modulus: |

#这里查看根证书的中，我们可以看到里面存在着根证书的公钥。

查看根证书的私钥

|  |
| --- |
| [root@xuegod63 CA]# vim /etc/pki/CA/private/cakey.pem #存在CA认证下根证书的私钥  （cakey.pem）。  -----BEGIN ENCRYPTED PRIVATE KEY-----  MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI2JxR6+eEWI0CAggA  MBQGCCqGSIb3DQMHBAjjVO7+mmTUuwSCBMil6B4xGLDfbskPQd++sEtyMtV8Y62l  GztBjiSSNCE0amDVvhi5hG5dZpq9i/ik1Jh31DQ6siet10vm7/EZC4KSqagDsi66 |

二：使用证书搭建https

1、安装：httpd

|  |
| --- |
| [root@xuegod64 ~]# yum install httpd  [root@xuegod64 ~]# vim /etc/httpd/conf/httpd.conf  改：#ServerName www.example.com:80  为：ServerName 192.168.1.64:80  [root@xuegod64 ~]# service httpd restart |

2、xuegod64生成证书请求文件

|  |
| --- |
| [root@xuegod64 ~]# openssl genrsa -h #查看帮助  usage:genrsa [args] [numbits]   -des           encrypt the generated key with DES **in** cbc mode   -des3          encrypt the generated key with DES **in** ede cbc mode (168 bit key)   -idea          encrypt the generated key with IDEA **in** cbc mode   -seed                   encrypt PEM output with cbcseed   -aes128, -aes192, -aes256                   encrypt PEM output with cbcaes   -camellia128, -camellia192, -camellia256                   encrypt PEM output with cbccamellia   -out file      output the key to 'file   -passout arg   output file pass phrase source   -f4            use F4 (0x10001) **for** the E value   -3             use 3 **for** the E value   -engine e      use engine e, possibly a hardware device.   -rand file:file:...                   load the file (or the files inthe directory) into                   the random number generator |

2.1：生一个私钥密钥：

|  |
| --- |
| [root@xuegod64 ~]# openssl genrsa -des3 -out /etc/httpd/conf.d/server.key  Generating RSA private key, 512 bit long modulus  .....++++++++++++  ..............................++++++++++++  e is 65537 (0x10001)  Enter pass phrase **for** /etc/httpd/conf.d/server.key:123456 #输入保护私钥的密码  Verifying - Enter pass phrase **for** /etc/httpd/conf.d/server.key: 123456    [root@xuegod64 ~]# cat /etc/httpd/conf.d/server.key #查看一下私钥  -----BEGIN RSA PRIVATE KEY----- #  Proc-Type: 4,ENCRYPTED  DEK-Info: DES-EDE3-CBC,D1CCE8B91BCAD4F4 #进行了二次加密    TlIQpxnrXh9WgLpqfqvKymsCdDDYUjvGyc2C9FOdZtEo+4B2toHGRKjyCyyRcWb7  PV9AJU5FsGyMDVDnOvTcBjYy5MPFhSPUpJ7Y5WeQBWZ6cn5Yh5OtVqQh5EyIxhVJ  j1m6XOrcAVpgRDOfyH68r+mipmse95kiBAjxh2gm5OzLLJt27dFZ5XRmd7oXys0q  V1SFftuN7M7DEx6Qzsut/C4teAZ64Bx3kM1RlXjAESixZUmrPyB/l12rVxd/kMQT  h2gvHM40mn52iNddaXQu8EeKy9CzJUpou85154v7tlqftJ98Hg9oFxebhIhS/16f: |

2.2：生成请求文件

|  |
| --- |
| [root@xuegod64 ~]# openssl req -new -key /etc/httpd/conf.d/server.key-out /server.csr #注意后期添加的国家，省，组织等信息要和CA保持一致  Enter pass phrase **for** /etc/httpd/conf.d/server.key:123456 #输入私钥的密码  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 aDN.  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) []:beijing  Locality Name (eg, city) [Default City]:haidian  Organization Name (eg, company) [Default Company Ltd]:xuegod  Organizational Unit Name (eg, section) []:IT  Common Name (eg, your name or your server's hostname) []:xuegod64.cn  #这里要求输入的CommonName必须不通过浏览器访问您网站的 URL 完全相同，否则用户会发现您服务器证书的通用名不站点的名字丌匹配，用户就会怀疑您的证书的真实性。可以使域名也可以使IP地址。  Email Address []:1@163.com  Please enter the following 'extra' attributes  to be sent with your certificate request  A challenge password []: #不输密码直接回车  An optional company name []: |

3：将证书请求文件发给CA服务器：

|  |
| --- |
| [root@xuegod64 ~]# scp /server.csr 192.168.1.63:/tmp/  The authenticity of host '192.168.1.63 (192.168.1.63)' can't beestablished.  RSA key fingerprint is f5:49:15:f3:62:37:05:0c:d5:15:ca:18:ea:c3:df:13.  Are you sure you want to **continue** connecting (yes/no)? yes  Warning: Permanently added '192.168.1.63' (RSA) to the list of knownhosts.  root@192.168.1.63's password:123456  server.csr                                    100%  688    0.7KB/s   00:00 |

4：CA认证中心进行CA签名

|  |
| --- |
| [root@xuegod63 CA]# openssl ca -h  #查看CA认证中心的帮助内容  [root@xuegod63~]# openssl ca -keyfile /etc/pki/CA/private/cakey.pem -cert /etc/pki/CA/cacert.pem-in /tmp/server.csr -out /server.crt  Using configuration from /etc/pki/tls/openssl.cnf  Enter pass phrase **for** /etc/pki/CA/private/cakey.pem:123456  Check that the request matches the signature  Signature ok  Certificate Details:  Serial Number:  ce:60:e0:a3:fe:ee:88:09  Validity  Not Before: Dec 21 14:25:53 2014 GMT  Not After : Dec 21 14:25:53 2015 GMT  Subject:  countryName = CN  stateOrProvinceName = beijing  organizationName = xuegod  organizationalUnitName = IT  commonName = xuegod64.cn  emailAddress = 1@163.com  X509v3 extensions:  X509v3 Basic Constraints:  CA:TRUE  Netscape Comment:  OpenSSL Generated Certificate  X509v3 Subject Key Identifier:  1B:30:0B:28:4A:31:EA:FC:05:7D:54:A3:87:A0:6E:BE:F8:D6:3C:F8  X509v3 Authority Key Identifier:  keyid:6D:0F:0C:C5:96:32:A8:8B:D3:FF:36:39:5B:14:5B:9B:31:12:4A:C3  Certificate is to be certified **until** Dec 21 14:25:53 2015 GMT (365 days) #证书有效期是365天。证书进行认证，直到12月21日十四时25分53秒格林尼治标准时间2015年（365天）  Sign the certificate? [y/n]:y #注册证书  1 out of 1 certificate requests certified, commit? [y/n]y #确认  Write out database with 1 new entries  Data Base Updated  将证书复制到xuegod64  [root@xuegod63 CA]# scp /server.crt 192.168.1.64:/ |

#这里的认证中心进行的签名是用自己的私钥进行签名，

5：CA认证中心进行颁发证书

|  |
| --- |
| [root@xuegod63 ~]# scp /server.csr 192.168.1.64:/  The authenticity of host '192.168.1.64 (192.168.1.64)' can't beestablished.  RSA key fingerprint is f5:49:15:f3:62:37:05:0c:d5:15:ca:18:ea:c3:df:13.  Are you sure you want to **continue** connecting (yes/no)? yes  Warning: Permanently added '192.168.1.64' (RSA) to the list of knownhosts.  root@192.168.1.64's password: 123456  server.csr                                    100%  688    0.7KB/s   00:00 |

#这里再颁发之前，CA认证中心会使用自己的公钥进行加密

三：使用证书实现https

SSL：(Secure Socket Layer)安全套接字层，通过一种机制在互联网上提供密钥传输。其主要目标是保证两个应用间通信数据的保密性和可靠性,可在服务器端和用户端同时支持的一种加密**[算法](http://lib.csdn.net/base/datastructure" \o "算法与数据结构知识库" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)**。目前主流版本SSLV2、SSLV3(常用）。

SSL四次握手安全传输：

加密协议： SSL 3.0 或 TLS 1.0

C -------------------------------------------------> S 1. 请求一个安全的会话，协商**[算法](http://lib.csdn.net/base/datastructure" \o "算法与数据结构知识库" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)**

C <------------------------------------------------- S 2. 将自己Server端的证书给客户端，证书中包括了64自己的公钥。

C -------------------------------------------------> S 3. 客户端用浏览中存放CA的根证书检测xuegod64证书，如果对，使用CA根证书中的公钥解密。得到xuegod64的公钥； 然后生成一把对称的加密密钥,用xuegod64的公钥加密这个密钥发给xuegod64。 后期使用对称密钥加密数据

C <------------------------------------------------> S

4. xuegod64使用私钥解密，得到对称的加密密钥然后，使用对称加密密钥来进行安全快速传输数据

1：配置HTTPSweb服务器： xuegod64

安装复制并查看

|  |
| --- |
| [root@xuegod64 ~]# yum install mod\_ssl -y 安装：SSL模块  [root@xuegod64 ~]# cp /server.crt /etc/httpd/conf.d/ #复制证书  [root@xuegod64 ~]# cat /server.crt  ertificate:      Data:          Version: 3 (0x2)          Serial Number:              96:db:28:b4:8b:a7:fb:bc      Signature Algorithm: sha1WithRSAEncryption          Issuer: C=CN, ST=beijing, O=xuegod,OU=IT, 颁发者是63-  CN=xuegod63.cn/emailAddress=1@163.cn          Validity              Not Before: Nov  3 11:12:34 2015 GMT              Not After : Nov  2 11:12:34 2016 GMT          Subject: C=CN, ST=beijing, O=xuegod,OU=IT, CN=xuegod63.cn/emailAddress=1@163.cn请求的是64，这里我没有修改          Subject Public Key Info:这里可以看出，证书中用了公钥加密              Public Key Algorithm: rsaEncryption                  Public-Key: (1024 bit)                  Modulus:  [root@xuegod64 ~]# ls /etc/httpd/conf.d/server.key #查看私钥  /etc/httpd/conf.d/server.key  [root@xuegod64 ~]# vim /etc/httpd/conf.d/ssl.conf  104 # certificate can be generated using the genkey(1) command.  改：  105 SSLCertificateFile /etc/pki/tls/certs/localhost.crt  为：  SSLCertificateFile /etc/httpd/conf.d/server.crt  106 #SSLCertificateFile /etc/pki/tls/certs/localhost.crt  107  108 # Server Private Key:  109 # If the key is not combined with the certificate, use this  110 # directive to point at the key file. Keep in mind that if  111 # you've both a RSA and a DSA private key you can configure  112 # both in parallel (to also allow the use of DSA ciphers, etc.)  改：113 SSLCertificateKeyFile /etc/pki/tls/private/localhost.key  为：  SSLCertificateKeyFile /etc/httpd/conf.d/server.key  114 #SSLCertificateKeyFile /etc/pki/tls/private/localhost.key |

启劢服务:

|  |
| --- |
| [root@xuegod64 ~]# service httpd restart  Stopping httpd: [ OK ]  Starting httpd: Apache/2.2.15 mod\_ssl/2.2.15 (Pass Phrase Dialog)  Some of your private key files are encrypted **for** security reasons.  In order to read them you have to provide the pass phrases.  Server bt-199-034.bta.net.cn:443 (RSA)  Enter pass phrase:123456 #保护私钥密码  OK: Pass Phrase Dialog successful.  [ OK ] |

**[测试](http://lib.csdn.net/base/softwaretest" \o "软件测试知识库" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)**：

|  |
| --- |
| 查看端口：  [root@xuegod64 ~]# netstat -antup | grep 443 #发现找丌到  访问： https://192.168.1.64/ 后  再查看：  [root@xuegod64 ~]# netstat -antup | grep 443  tcp 0 0 :::443 :::\* LISTEN 5138/httpd  只有调用一下https，才会开启。 像 ftp ：20传输数据， 21 监听服务，传输命令。 没有数据传输时，看不到20端口。 修改物理机：C:\Windows\System32\drivers\etc\hosts   添加：  192.168.1.64  xuegod64.cn |

2：查看证书安装证书

