```
#include <iostream>
#include <openssl/x509v3.h>
#include <openssl/pem.h>

using namespace std;

#define USER_CERT "用户证书路径"            // 这里保存的是pem格式证书
#define CA_CERT "根证书路径"


int main()
{
 SSLeay_add_all_algorithms();

 X509_STORE_CTX *ctx = NULL;         // 证书存储区句柄
 X509_STORE *pCaCertStore = NULL;    // 证书存储区
  X509 *pCert = NULL;                // X509 证书结构体，保存用户证书
  X509 *pCaCert = NULL;              // X509 证书结构体，保存根证书
  X509_CRL *Crl = NULL;              // X509_CRL 结构体，保存CRL
  STACK_OF(X509) *CertStack = NULL;

 BIO * pbio = NULL;

 pbio = BIO_new_file(USER_CERT,"r");
 pCert = PEM_read_bio_X509(pbio,NULL,NULL,NULL);
 if(pCert == NULL)
 {
  cout<<"读取用户证书失败！"<<endl;
  return -1;
 }
 BIO_free(pbio);
 pbio = NULL;

 pbio = BIO_new_file(CA_CERT,"r");
 pCaCert = PEM_read_bio_X509(pbio,NULL,NULL,NULL);
 BIO_free(pbio);
 pbio = NULL;
 if(pCaCert == NULL)
 {
  cout<<"打开根证书失败"<<endl;
  return -1;
 }

    pCaCertStore = X509_STORE_new();    // 新建X509 证书存储区

    X509_STORE_add_cert(pCaCertStore,pCaCert);    // 添加根证书到证书存储区

   // 设置检查CRL 标志位，如果设置此标志位，则检查CRL ，否则不检查CRL 。

 // 读取CRL文件
    Crl = PEM_read_bio_X509_CRL(pbio,NULL,NULL,NULL);
```

最新文章

SNMPv3原理-SNMPv3协议框架

H3C SNMPv3 配置

SNMPv3的加密和认证过程

2017年 56篇　2016年 80篇
2015年 51篇　2014年 78篇
2013年 61篇　2012年 47篇
2011年 111篇　2010年 48篇
2009年 24篇　2008年 15篇
2007年 27篇

```
  if (Crl==NULL)
{
      X509_free(pCaCert);
 cout<<"读取吊销列表文件失败"<<endl;
     return -1 ;
  }
BIO_free(pbio);
pbio = NULL;

   X509_STORE_set_flags(pCaCertStore,X509_V_FLAG_CRL_CHECK);

   X509_STORE_add_crl(pCaCertStore,Crl);   // 添加CRL 到证书存储区

   ctx = X509_STORE_CTX_new();   // 新建证书存储区句柄

   int ret = X509_STORE_CTX_init(ctx,pCaCertStore,pCert,CertStack);   // 初始化根证书存储区、用户证书1

   if (ret != 1)
   {
     cout<<"X509_STORE_CTX_init err"<<endl;

     X509_free(pCert);
     X509_free(pCaCert);
     X509_STORE_CTX_cleanup(ctx);
     X509_STORE_CTX_free(ctx);
     X509_STORE_free(pCaCertStore);
    return -1 ;
   }
   // 验证用户证书
   ret = X509_verify_cert(ctx);
   if (ret != 1)
   {
     cout<<"verify cer err.error="<<ctx->error<<"info:"<<X509_verify_cert_error_string(ctx->error)<<endl;
   }

   // 释放内存
   X509_free(pCert);
   X509_free(pCaCert);
   X509_STORE_CTX_cleanup(ctx);
   X509_STORE_CTX_free(ctx);
   X509_STORE_free(pCaCertStore);

 cout<<"OK!"<<endl;

 return 0;
}
```

lang_f: 看到了，是自己看代码不认真了，抱歉 4 年前 回复 •••

lang_f: 验证前一定需要添加crl吗 Crl = PEM_read_bio_X509_CRL(pbio,NULL,NULL,NULL); if (Crl==NULL) { X509_free(pCaCert); cout<<"读取吊销列表文件失败"<<endl; return -1 ; } BIO_free(pbio); pbio = NULL; X509_STORE_set_flags(pCaCertStore,X509_V_FLAG_CRL_CHECK); X509_STORE_add_crl(pCaCertStore,Crl); 这段代码之前说可以设置不检查crl，怎么设置，是指X509_STORE_add_crl(pCaCertStore,Crl); 可以不用写吗？ 4 年前 回复 •••

lang_f: 验证前一定需要添加crl吗 Crl = PEM_read_bio_X509_CRL(pbio,NULL,NULL,NULL); if (Crl==NULL) { X509_free(pCaCert); cout<<"读取吊销列表文件失败"<<endl; return -1 ; } BIO_free(pbio); pbio = NULL; X509_STORE_set_flags(pCaCertStore,X509_V_FLAG_CRL_CHECK); X509_STORE_add_crl(pCaCertStore,Crl); 这段代码之前说可以设置不检查crl，怎么设置，是指X509_STORE_add_crl(pCaCertStore,Crl); 可以不用写吗？ 4 年前 回复 •••

qq_38188155 回复： 这个一定要设置吗 7 月前 回复 •••

openssl创建根证书并用根证书创建子证书_weixin_342199... 9-23
// 生成p12证书 openssl pkcs12 -export -in child.cer -inkey child.key -password pass:111111-out child.p12 // 然后使用上面1、2命令创建server.csr、serv…

利用openssl 库制作证书以及验证_悠悠茹的小窝 10-24
openssl req -new -x509 -key cakey.key -out cacert.pem -days 1234 这个命令将用上面生成的密钥cakey.pem生成一个数字证书cacert.pem 用户证书: op…

openssl 验证证书是否是某个CA证书签发 crazy Crypto 2898
int VerifyCertByIssuer(X509 *cert, X509 *issuer) { int res = 0; EVP_PKEY *pubkey = 0; if (X509_check_issued(issuer, cert) != X509_V_OK) { goto end; }…

openssl命令操作证书链实例 09-06
提供实际操作的示例，演示linux下用openssl提供的命令，生成多级证书，并验证各级证书的合法性。

OpenSSL生成CA证书及终端用户证书_weixin_30849591的博客 10-24
openssl req \ -new \ -sha256 \ -outserver.csr\ -keyserver.key\ -configserver.conf 配置文件中已经有默认值了,shell交互时一路回车就行。 2.4 用CA证书…

CA根证书和服务器、客户端证书制作及使用说明文档（node.js和java代码验证）.docx 09-07
本文实现了OpenSSL的CA跟证书的制作、服务器和客户端证书的制作，并使用node.js实现了服务器和客户端代码，也实现了java代码，同时验证了SSL/T…

在openssl中对SM2的公私钥进行加解密的验证 热门推荐 dong_beijing的博客 1万+
在上一篇文章中《通过openssl生成sm2的公私钥的方法》介绍了如何在openssl系统中生成公私钥对，如何对生成的公私钥对进行验证呢？ 在ecparam.c…

SM2算法第四篇：基于Openssl实现SM2秘钥协商协议 刘兵马俑的博客 6844
这篇博客的背景和目的： 背景：前几篇博客已经搞清楚了，SM2椭圆曲线公钥加密算法是什么，以及如何实现。另外，已经从网上吓到了实现SM2的C语…

从零开始学React Native之数据持久化存储 wang_gwei的博客 822
数据持久化就是指应用程序将某些数据存储在手机存储空间中。 AsyncStorage API RN框架为开发者提供了 AsyncStorage API，开发者可以利用它将任意…

SM2国密算法证书解析 sunboy2718的专栏 8677
一、数字证书的组成 1）证书数据结构 数字证书使用ASN.1编码，证书文件以二进制或Base64格式存放，数据格式使用TLV（Tag Length Value）形式，T…

用openssl验证证书和私钥是否有效 wqs1106的博客 1万+
1.openssl s_server -msg -verify -tls1_2 -state -cert cert.cer -key ..\privkey -accept 18444 使用上面的命令开启一个ssl测试服务器 2.openssl s_client -ms…

OPENSSL X509证书验证 在线笔记 5503
步骤： 1）初始化环境 a.新建证书存储区X509_STORE_new() b.新建证书校验上下文X509_STORE_CTX_new() 2）导入根证书 a.读取CA证书，从DER…

OpenSSL生成根证书CA及签发子证书 lipviolet的博客 2351
系统：CentOS7 32位 目标：使用OpenSSL生成一个CA根证书，并用这个根证书颁发两个子证书server和client。 先确保系统中安装了OpenSSL，若没安…

利用openssl工具生成根证书及颁发子证书 错位竞争，单点突破。 1万+
参考自：http://zhtx168.blog.163.com/blog/static/416015482008125032 48/ 使用openssl工具来生证书过程如下: 一）首先创建CA根证书 1) 生成RSA priv…

使用OpenSSL工具构建自签名根证书、服务器证书和客户证书，搭建双向认证服务... Stay Hungry, Stay Foolish 214
Linux下的shelle脚本（注意最后一行keytool命令位于$JAVA_HOME/bin下）： md ca md client md server md jks openssl genrsa -out ca/ca-key.pem 204…

openssl验证证书常用命令 Qinng的博客 1243
输出x509证书信息 openssl x509 -noout -text -in ca.pem 结果如下 Certificate: Data: Version: 3 (0x2) Serial Number: 5f:11:aa:b3:70:18:fd:89:b0:25:7a:9…

x509证书验证示例 chuicao4350的博客 1万+
openssl实现了标准的x509v3数字证书，其源码在crypto/x509和crypto/x509v3中。其中x509目录实现了数字证书以及证书申请相关的各种函数，包括了X5…

wzsy
码龄17年 暂无认证

19	42万+	117万+	116万+	
原创	周排名	总排名	访问	等级
1万+	138	65	67	249
积分	粉丝	获赞	评论	收藏

私信 关注

搜博主文章

热门文章

最新评论

x86保护模式的几点思考——IRQ、中断…
lunat:c: 图床挂了，求求不要复制粘贴了好吗

pxe-mof exiting intel pxe rom operating s…
Tisfy: 十分完美，正如：看雪飞、苹底芦梢

，未如鬓白。

PUTTY无法远程连接服务器故障解决

m0_56158060: 我也想问一下大佬怎么查看sshd_config配置信息？

openssl 用根证书验证一个用户证书

qq_38188155: 这个一定要设置吗

使用 Windows Vista 的凭据提供程序创造…

walker2928: 博主，您好，我已经在GetSerialization中调用了相关usbkey的验证密码...

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

x509证书验证 269

X509_verify_cert函数负责用来验证证书的有效性，函数原型如下int X509_verify_cert(X509_STORE_CTX *ctx)，验证成功返回1，失败返回其他值，失败…

openssl采用sm2进行自签名的方法 dong_beijing的博客 1万+

自签名有两种方法: 1 用自己会话生成的私钥,来签发自己的csr生成证书，也可以直接生成私钥和证书 2 自己做一个CA. 1,2的差别在于私钥的生成和存活的…

openssl SM2签名密钥生成 qq_16613311的博客 627

密钥生成流程,pkcs#8格式私钥pem文件： 1 生成sm2私钥: openssl ecparam -genkey -name SM2 -out sm2PriKey.pem 2 sm2私钥导出公钥: openssl ec -i…

我的总结之nginx https的配置 自己生成ssl证书 curl命令总结 https工作原理 find命令 PolarSSL http协议总结 json ur… xu_ya_fei的专栏 5847

鉴于公司的业务需要需要，我需要对nginx的ssl模块研究一下，顺便记录一下研究过程。 首先需要将ssl模块配置跑通（前提是要已经with了该模块，可用/d…