Openssl验证证书的有效性

时间 2015-02-27
栏目 SSL

好久没写博客了，直接上代码

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <openssl/x509.h>
#include <openssl/x509_vfy.h>
int LoadCert(unsigned char * szFilePath, unsigned char *pbCert, int size)
{
 int len = 0;
 if(szFilePath == NULL || pbCert == NULL || size < 128)
        {
    return -1;
        }
 FILE *fp = fopen(szFilePath, "rb");
 if ( NULL == fp)
        {
    return -2;
        }

 len = fread(pbCert, 1, size, fp);
 fclose(fp);
 return len;
}

int VerifyCert(unsigned char *pbCaCert, int nCaLen, unsigned char *pbCert, int nCertLen, unsigned char *pbCN, int size)
{
 int rv = -1;
 if(pbCaCert == NULL || nCaLen < 128 || pbCert == NULL || nCertLen < 128)
        {
    return rv;
        }

 X509 *ca = NULL;
 X509 *cert = NULL;

 X509_STORE *caStore = NULL;
 X509_STORE_CTX *ctx = NULL;
 X509_NAME *subject = NULL;

 OpenSSL_add_all_algorithms();

 caStore = X509_STORE_new();
 ctx = X509_STORE_CTX_new();

 ca = d2i_X509(NULL, ( const unsigned char **)&pbCaCert, nCaLen);
 if(ca == NULL)
        {
    return -2;
        }

 rv = X509_STORE_add_cert(caStore, ca);
 if ( rv != 1 )
        {
    rv = -3;
  goto EXIT_VERIFY;
```

```
        }

 cert = d2i_X509(NULL, ( const unsigned char **)&pbCert, nCertLen);
 if(cert == NULL)
        {
     r v    =    - 4 ;
   g o t o   E X I T _ V E R I F Y ;
        }

 rv = X509_STORE_CTX_init(ctx, caStore, cert, NULL);
 if ( rv != 1 )
        {
     r v    =    - 5 ;
   g o t o   E X I T _ V E R I F Y ;
        }

 rv = X509_verify_cert(ctx);
 if ( rv != 1 )
        {
  fprintf(stderr, "X509_verify_cert fail, rv = %d, error id = %d, %s\n",
  rv, ctx->error, X509_verify_cert_error_string(ctx->error));
   rv = (rv == 0 ? 1 : rv);
   g o t o   E X I T _ V E R I F Y ;
        }
 subject = X509_get_subject_name(cert);
 if(subject)
        {
  X509_NAME_get_text_by_NID(subject, NID_commonName, pbCN, size);
        }
 rv = (rv == 1 ? 0 : rv);

EXIT_VERIFY:
 if(cert) X509_free(cert);
 if(ca) X509_free(ca);
 if(caStore) X509_STORE_free(caStore);
 i f ( c t x )
        {
  X509_STORE_CTX_cleanup(ctx);
  X509_STORE_CTX_free(ctx);
        }

 return rv;
}

int main(void)
{
 int rv = 0;
 int i = 0;
 int caLen = 0;
 int certLen =0;
 unsigned char cn[255] = {0};
 unsigned char cert[4096] = {0};
 unsigned char ca[4096] = {0};

 caLen = LoadCert("ca.cer", ca, 4096);
 certLen = LoadCert("Jinhill.cer", cert, 4096);
 rv = VerifyCert(ca, caLen, cert, certLen, cn, 255);
 printf("rv=%d, cn=%s\n", rv, cn);
 return 0;

}
```

相关文章

- 1. 数字证书的有效性验证
- 2. Openssl 对x509证书有效性进行验证
- 3. openssl的证书链验证
- 4. openssl verify 验证证书
- 5. OPENSSL X509证书验证
- 6. 邮箱有效性验证
- 7. textbox有效性验证
- 8. 表单有效性验证
- 9. 验证身份证有效性：
- 10. openssl自建CA证书(亲验证)
- 更多相关文章...

每日一句

每一个你不满意的现在，都有一个你没有努力的曾经。

最新文章

- 1. 2019 10 23专业英语-王菲
- 2. CSP-S 代码基本框架
- 3. GIL全局解释器锁死锁递归锁信号量
- 4. 进程队列补充、socket实现服务器并发、线程完结
- 5. appium环境搭建步骤
- 6. day39
- 7. esp8266 第二章 如何通过Makefile 重写esp工程结构
- 8. 【LeetCode】加油站
- 9. Shell编程

本站公众号

欢迎关注本站公众号,获取更多程序园信息

相关文章

- 1. 数字证书的有效性验证
- 2. Openssl 对x509证书有效性进行验证
- 3. openssl的证书链验证
- 4. openssl verify 验证证书
- 5. OPENSSL X509证书验证
- 6. 邮箱有效性验证
- 7. textbox有效性验证
- 8. 表单有效性验证
- 9. 验证身份证有效性：
- 10. openssl自建CA证书(亲验证)

>>更多相关文章<<