OpenSSL 专栏收录该内容

```c
#include <stdio.h>
#include <string.h>
#include <openssl/evp.h>
#include <openssl/x509.h>

void tSign()
{
    unsigned char sign_value[1024]; //保存签名值的数组
    int sign_len;       //签名值长度
 EVP_MD_CTX mdctx;      //摘要算法上下文变量
    char mess1[] = "xxh";       //待签名的消息
 RSA *rsa=NULL;         //RSA结构体变量
 EVP_PKEY *evpKey=NULL;      //EVP KEY结构体变量
    int i;

    printf("正在产生RSA密钥...");
 rsa = RSA_generate_key(1024,RSA_F4,NULL,NULL);//产生一个1024位的RSA密钥//printf ("bits: %d\n", BN_num_bits (rsa
    if(rsa == NULL)
    {
        printf("gen rsa err\n");
        return;
    }
    printf(" 成功.\n");
 evpKey = EVP_PKEY_new();//新建一个EVP_PKEY变量
    if(evpKey == NULL)
    {
        printf("EVP_PKEY_new err\n");
        RSA_free(rsa);
        return ;
    }
    if(EVP_PKEY_set1_RSA(evpKey,rsa) != 1)  //保存RSA结构体到EVP_PKEY结构体
    {
        printf("EVP_PKEY_set1_RSA err\n");
        RSA_free(rsa);
        EVP_PKEY_free(evpKey);
        return;
    }
    //以下是计算签名代码
    EVP_MD_CTX_init(&mdctx);//初始化摘要上下文
    if(!EVP_SignInit_ex(&mdctx, EVP_md5(), NULL))//签名初始化，设置摘要算法，本例为MD5
    {
        printf("err\n");
        EVP_PKEY_free(evpKey);
        RSA_free(rsa);
        return;
    }
    if(!EVP_SignUpdate(&mdctx, mess1, strlen(mess1)))//计算签名（摘要）Update
    {
        printf("err\n");
        EVP_PKEY_free(evpKey);
        RSA_free(rsa);
        return;
    }
    if(!EVP_SignFinal(&mdctx,sign_value,&sign_len,evpKey))  //签名输出
    {
        printf("err\n");
```

分类专栏 0 订阅 5 篇文章 订阅专栏

```
        EVP_PKEY_free(evpKey);
        RSA_free(rsa);
        return;
    }
    printf("消息\"%s\"的签名值是: \n",mess1);
    for(i = 0; i < sign_len; i++)
    {
        if(i%16==0)
            printf("\n%08xH: ",i);
        printf("%02x ", sign_value[i]);
    }
    printf("\n");
    EVP_MD_CTX_cleanup(&mdctx);

    printf("\n正在验证签名...\n");
    //以下是验证签名代码
    EVP_MD_CTX_init(&mdctx);//初始化摘要上下文
    if(!EVP_VerifyInit_ex(&mdctx, EVP_md5(), NULL))//验证初始化，设置摘要算法，一定要和签名一致。
    {
        printf("EVP_VerifyInit_ex err\n");
        EVP_PKEY_free(evpKey);
        RSA_free(rsa);
        return;
    }
    if(!EVP_VerifyUpdate(&mdctx, mess1, strlen(mess1)))//验证签名（摘要）Update
    {
        printf("err\n");
        EVP_PKEY_free(evpKey);
        RSA_free(rsa);
        return;
   }
    if(!EVP_VerifyFinal(&mdctx,sign_value,sign_len,evpKey))//验证签名
    {
        printf("verify err\n");
        EVP_PKEY_free(evpKey);
        RSA_free(rsa);
        return;
    }
    else
    {
        printf("验证签名正确.\n");
    }
    //释放内存
    EVP_PKEY_free(evpKey);
    RSA_free(rsa);
    EVP_MD_CTX_cleanup(&mdctx);
    return;
}
int main()
{
    OpenSSL_add_all_algorithms();
    tSign();
    return 0;
}
```

qq_37255824: 代码出现问题，无法运行。作者在吗 2年前 回复 •••

OpenSSL和Python实现RSA Key数字签名和验证_洛奇看世界 8-29
基于非对称算法的RSA Key主要有两个用途,数字签名和验证(私钥签名,公钥验证),以及非对称加解密(公钥加密,私钥解密)。本文提供一个基于OpenSSL命…

openssl 相关的rsa与sha1算法签名与验证_KuaiPengFei... 9-21
openssl是一个功能强大的工具包,它集成了众多密码算法及实用工具。我们即可以利用它提供的命令台工具生成密钥、证书来加密解密文件,也可以在利用…

openssl 非对称加密 RSA 加密解密以及签名验证签名 weixin_34008805的博客 104
1. 简介 openssl rsa.h 提供了密码学中公钥加密体系的一些接口， 本文主要讨论利用rsa.h接口开发以下功能 公钥私钥的生成 公钥加密，私钥…

基于openssl的RSA的加密,解密,签名和验证签名 09-20
基于openssl的RSA的加密,解密,签名和验证签名， RSR加密 RSA解密 openssl签名 openssl验签， 基于openssl的RSA的加密,解密,签名和验证签名

OpenSSL 摘要和签名验证指令dgst使用详解_sjrGCkym的博客 8-14
linuxidc@linuxidc:~/test$ openssl rsa -inRSA.pem -outpub.pem -pubout writing RSA key /*使用RSA公钥验证签名(verify参数),验证成功*/ linuxidc@linuxid…

使用OpenSSL做RSA签名验证 支付宝移动快捷支付 的服务... 8-19
由于第一次使用openssl做RSA验证签名,我们碰到了各种坑,为了避免其他项目也碰到类似问题,分享如下: 首先要说明的是RSA签名和签名验证的过程。 RS…

43万+ 周排名 | 72万+ 总排名 | 2万+ 访问 | 等级

linux c 使用openssl实现SHA1WithRSA实现，签名，验签 05-19
17 linux c 使用openssl实现SHA1WithRSA实现 6签名，验签 | 3 | 10

粉丝 | 获赞 | 评论 | 收藏

OpenSSL 命令详解（二）——摘要算法、签名、验签 热门推荐 scuyxi的专栏 1万+
本文主要介绍OpenSSL 摘要计算命令。 ref: http://blog.csdn.net/as3luyuan123/article/details/14046375用什么摘要算法指令代替时，默认使用该算法，…

openssl rsa加密签名_cheng0603的专栏 10-10
根据网上搜索及自己亲自代码调试,完成rsa加解密签名 1:输入命令,生成公钥和私钥(1024位) openssl genrsa -out prikey.pem 1024 openssl rsa -in privkey…

openssl_sign() 语法+RSA公私钥加密解密,非对称加密算法详解 或非与博客 1万+
其实有时候觉得写博客好烦，就个函数就开篇博客。很小的意见事情而已，知道的人看来多取一举，或者说没什么必要，浪费时间，不知道的人就会很郁…

openssl签名和验证 08-05
openssl签名和验证；openssl签名和验证；openssl签名和验证；

php openssl_sign() 语法+RSA公私钥加密解密,非对称加密算法详解 mengzuchao的专栏 1万+
其实有时候觉得写博客好烦，就个函数就开篇博客。很小的意见事情而已，知道的人看来多取一举，或者说没什么必要，浪费时间，不知道的人就会很郁…

openssl_基于EVP接口的RSA算法签名与验签 最新发布 Lee notes 319
#include <iostream> #include <openssl/rsa.h> #include <openssl/err.h> #include <openssl/evp.h> #include <openssl/pem.h> #ifdef _WIN32 #include <…

通过OpenSSL生成自签名证书，认识RSA算法 彼此当年少，莫负好时光 1389
前言 OpenSSL是一个安全套接字层密码库，囊括主要的密码算法、常用的密钥和证书封装管理功能及SSL协议，并提供丰富的应用程序供测试或其它目的…

openssl生成签名与验证签名 712
继上一篇RSA对传输信息进行加密解密，再写个生成签名和验证签名。 一般，安全考虑，比如接入支付平台时，请求方和接收方要互相验证是否…

(8) openssl rsautl（签名/验证签名/加解密文件）和openssl pkeyutl(文件的非对称加密)... weixin_30439131的博客 189
rsautl是rsa的工具，相当于rsa、dgst的部分功能集合，可用于生成数字签名、验证数字签名、加密和解密文件。 pkeyutl是非对称加密的通用工具，大体…

[crypto]-53-openssl命令行的使用（aes/rsa签名校验/rsa加密解密/hmac） 代码改变世界 2726
常用技巧 如何编写一个二进制规律性的文件, 比如你可以编写一个"0123456789abcdef"的文本文件，记得删除换行符然后用ultraedit打开，ctrl+H就可以看…

openssl rsa加密签名 zymx(u010820135)的专栏 3479
from http://blog.csdn.net/cheng0603/article/details/44491983 要使用rsa加密，本来准备在网上找rsa加密算法，但是找到的c源码都不太好用，后来搜索…

OpenSSL：基于RSA算法的签名和验证（原理+代码） 您的编程如已上线 5898
数字签名和验证（Digital signature and verification）数字签名主要用于验证被签数据在传输过程中是否被篡改 包含加密算法（encryption）和摘要算法…

如何使用OpenSSL创建自签名证书 p15097962069的博客 1619
我正在向嵌入式Linux设备添加HTTPS支持。 我尝试通过以下步骤生成自签名证书： openssl req -new > cert.csr openssl rsa -in privke

openssl自签名证书生成与单双向验证 gx_1983的专栏 1万+
什么加密,签名 下面这个博客解释的很好: https://www.cnblogs.com/f-ck-need-u/p/6089523.html 签名 在保证了数据的安全性后，还需要保证数据的完整性…

openssl sign 刚刚起步的菜鸟 4523
Step1：用openssl生成一对公钥/私钥rsa2048 openssl genrsa -des3 -out root.pem 2048 Step2： 签名openssl dgst -sign root.pem -sha256 -out sign.txt …

xxxa
码龄12年 暂无认证
1
原创
299
积分
私信 关注

搜博主文章

热门文章

OpenSSL EVP_des_ede3_cbc CBC方式的3个密钥的3DES算法 加密解密 9011
OpenSSL RSA 消息签名与验证 5484
RC5 分组密钥算法 C语言实现 4378
OpenSSL EVP_md5 消息摘要 2046
学生信息管理系统（c语言） 2001

最新评论

OpenSSL RSA 消息签名与验证
qq_37255824: 代码出现问题，无法运行。作者在吗
学生信息管理系统（c语言）
匿名用户: 不过有点小错误啊
学生信息管理系统（c语言）
匿名用户: [e03]

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

OpenSSL linux 证书操作
OpenSSL Base64编码与解码
OpenSSL EVP_md5 消息摘要

2014年 7篇　　2011年 1篇

2009年 1篇

xxxa

关注

2　1　5

专栏目录