

 加密算法与证书 专栏收录该内容

OpenSSL

数字签名与验证

<https://liumiaocn.blog.csdn.net>

这篇文章将通过一个具体的例子来说明使用OpenSSL数字签名与验证的过程。

场景：

liumiao有一封写给Michael的信（txt文件），他把内容和一个签名文件放在一起寄给Machael，签名文件用于说明这个文件是liumiao提供的。

写信&对信的内容进行签名

事前准备

准备名为messages的文件，其中保存着liumiao写给Michael的内容。

```
1 [root@liumiaocn ~]# mkdir sign
2 [root@liumiaocn ~]# cd sign
3 [root@liumiaocn sign]# echo -n "Hello ,this is greetings from liumiao" >messages
4 [root@liumiaocn sign]# cat messages
5 Hello ,this is greetings from liumiao[root@liumiaocn sign]#
6 [root@liumiaocn sign]#
```

生成签名用的私钥

因为需要使用私钥进行签名，所以这里首先生成一个私钥文件

```
1 [root@liumiaocn sign]# ls
2 messages
3 [root@liumiaocn sign]# openssl genrsa -out rsa_key.private
4 Generating RSA private key, 2048 bit long modulus (2 primes)
5 ..+++++
```

生成签名用的私钥

使用私钥文件对messages文件进行签名

验证签名

验证方式1: 使用私钥来验证签名文件

验证方式2: 使用公钥来验证签名

分类专栏

订阅专栏

```
6 .....+++++
7 e is 65537 (0x010001)
8 [root@liumiaocn sign]# ls
9 messages rsa_key.private
10 [root@liumiaocn sign]#
```

使用私钥文件对messages文件进行签名

使用刚刚生成的私钥文件使用md5算法对messages文件进行签名,签名后生成一个名为messages.sign的签名文件

```
1 [root@liumiaocn sign]# openssl dgst -md5 -out messages.sign -sign rsa_key.private messages
2 [root@liumiaocn sign]# ls
3 messages messages.sign rsa_key.private
4 [root@liumiaocn sign]#
```

验证签名

验证方式1: 使用私钥来验证签名文件

Michael收到信和签名文件之后,如果Michael也有私钥的话,可以使用私钥来验证签名文件,执行示例如下所示:

```
1 [root@liumiaocn sign]# openssl dgst -md5 -prverify rsa_key.private -signature messages.sign messages
2 Verified OK
3 [root@liumiaocn sign]#
```

验证方式2: 使用公钥来验证签名

由于私钥的特殊性,注定不能得到广泛传播,而从私钥中生成的公钥进行签名的验证更加符合实际的使用情况。首先从私钥生成一个公钥:

```
1 [root@liumiaocn sign]# openssl rsa -pubout -in rsa_key.private -out rsa_key.public
2 writing RSA key
3 [root@liumiaocn sign]# ls
4 messages messages.sign rsa_key.private rsa_key.public
5 [root@liumiaocn sign]# cat rsa_key.public
6 -----BEGIN PUBLIC KEY-----
7 MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6XPTRGxvZK3RYgVjJ4XV
8 W8P00AJUJsoEmdrV0/WG5nuKtbDtyInNAjwN0saHi+3CAWr2A9u8k6j3Mopag1Pw
9 Sh8SDhmE3y1bI1xL/5x4pm0+ZVtfa0ReyyNOX4IQUSYJe6IyS29y/5eMc970gmig
10 7VMgfr1KpV4oR4b5bmWxbNIOK0RoorbhmtmLt+SPwuq05EWJlwC6AT4p1JB1B8xB
11 pfjz2dRRL4u16SxPfZeID6xDMIq14KBgCNVv9FdSw+6KSsWY3lj7n0GeoqJ3eW02
12 aD40wnezDLXounaNngDu62AItVdoog1U1BNCqvYfpCEownrW1LRBh8hp016xf3PI
13 9QIDAQAB
14 -----END PUBLIC KEY-----
15 [root@liumiaocn sign]#
```

Michael获得此公钥则是比较简单和正常的事情,然后结合messages文件和签名文件即可进行签名的验证了,执行示例如下所示

```
1 [root@liumiaocn sign]# openssl dgst -md5 -verify rsa_key.public -signature messages.sign messages
2 Verified OK
3 [root@liumiaocn sign]#
```

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;



森叔 1 专家
码龄5年 暂无认证

1348

原创



优质评论可以帮助作者获得更高权重

3852

周排名

ytfdfiw: 不错, 感谢分享。 7 月前 回复

2万+

总排名

667万+

访问



等级



7万+
积分

私信 关注

搜博主文章

淼叔的知行合一 

新书：企业级DevOps技术与工具实战

本书全面介绍DevOps的核心理念和实践，讲述了企业级DevOps落地实施的流程体系，为读者提供了系统化的企业级DevOps实施指南。

Breakdown



企业级
DevOps
技术与工具实战

刘刚 张英梅 编著

中国工信出版集团
电子工业出版社

<http://www.eelink.com.cn>

热门文章

Docker CE 还是 Docker EE 76904

Kubernetes之kubectl常用命令使用指南:1: 创建和删除 71815

Robot Framework基础入门: (1): 简介 67224








2018年DevOps最新现状研究报告解读 52516

LDAP基础: 6: 使用ldapsearch进行数据查询 44778

最新评论 

GitLab: 使用用户名/密码创建Access Tok...
 李广元: 1997: 请问您是怎么解决GitLab接口的
 的跨域问题的？
 Chrome下可用的Kubernetes Dashbo...
 李昊轩的博客: 写的真好, 同学欢迎来到我的博
 客看看哦
 CodeBlocks : 1: 在MacOS上安装2.0.3
 瑞朗: 大神们，大一新生电脑小白，谁可以
 教教我啊，好像哪一步都不会 🤔
 Linux基础: timedatectl命令使用介绍
 Java法师: synchronized好像是在联网的
 情况下自动同步的，所以你联网了就是y...
 Vmware添加磁盘的方法：扩展磁盘
 ...等... : 超有用 按照步骤直接OK👍

您愿意向朋友推荐“博客详情页”吗？

1万+	2032	929	3878
粉丝	获赞	评论	收藏
<div>tx100800: 谢谢 2 年前 回复 ...</div> <div>        </div>			
<div>一枚快乐的野指针~: 好 2 年前 回复 ...</div>			

OpenSSL学习之使用个人信息数字证书(PFX)进行签名和验... 10-6

最近需要用到数字签名的相关技术,但是网络上对这方面的文章说的含糊,所以自己把这段时间在学习OpenSSL过程中得到心得发表出来,供大家讨论,欢迎大...

用openssl生成SSL使用的私钥和证书,并自己做CA签名_zzh... 10-16

本文记叙的是一次基于SSL的socket通讯程序开发中,有关证书,签名,身份验证相关的步骤。我们的场景下,socket服务端是java语言编写的,客户端是c语言...

openssl生成签名与验证签名 716

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...

用openssl命令制作生成证书和自签名
用openssl命令制作生成证书和自签名

openssl证书请求和自签名_侯海云 9-15

libssl:加密模块应用库,实现了ssl及tls,包nssOpenSSL命令:两种运行模式:交互模式和批处理模式 openssl version:查看OpenSSL程序版本号 标准命令:enc(...

使用openssl生成自签名证书以及nginx ssl双向验证_weix... 10-2

三、自签名生成的csr文件必须要经过CA签名才能形成自己的证书,我们可以通过第三方权威认证机构进行签名,但是这个需要收费,我们制作自签名根证书...

利用OpenSSL制作自签名证书 Geoffrey's Blog 5194

利用OpenSSL制作自签名证书在apache或者nginx启用HTTPS后，需要加密证书才能正常工作。我们现在可以利用OpenSSL工具简单快速的创建一个自签...

[\[OpenSSL\]原获得文件签名](#)
Jacky_Dai的专栏 218

测试数据链接: [url]<http://jacky-dai.iteye.com/admin/blogs/1743774>[url] [code="c++"] #include #include #pragma comment(lib, "libcrypto32.lib") void Reve...

调用OpenSSL实现数字签名功能例程(一)_lee353086的专栏 8-19

```
#include<openssl/ssl.h> #pragma comment(lib,"libeay32.lib") #pragma comment(lib,"ssleay32.lib") /* PKCS7Sign.cpp Auth:Kagula 功能:调用OpenSSL实...
```

使用OpenSSL创建自签名SSL证书_lordwish的专栏 9-15

基于这两条考虑,考虑使用开源组件OpenSSL创建自签名SSL证书。自己发给自己的证书,可不就想怎么改就怎么改。 2. OpenSSL创建自签名证书过程 2.1...

OpenSSL 签名需要的文件

使用 Openssl 验证自签名证书

4. 使用server证书请求文件通过CA生成自签名证书 [openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key 5. 验证server证书](#) [qouxiu@qouxiu...](#) 10-22

Open SSL 常用函数——签名与验证_zqt520的专栏_open ssl 9-16

Open SSL 常用函数——签名与验证 OpenSSL 中的验证是先对原始数据计算摘要,再对摘要进行私钥加密,验证的过程是对原始消息计算摘要,解密验证值,和...

OpenSSL: 基于RSA算法的签名和验证 (原理+代码) 您的编程已上线 5919

数字签名和验证 (Digital signature and verification) 数字签名主要用干验证被篡改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 (hashing)

OpenSSL 命令详解 (二) ——摘要算法、签名、验签 热门推荐 scuyxi 的专栏 1万+

使用Openssl 验证自签名证书_kmyhy的专栏_openssl 验证... 9-2

Python中多个数组行合并及列合并的方法总结 最新发布 12-24

采用numpy中函数将两个矩阵或数组合并成一个数组：import numpy as np 数组 a = [[1 2 3] [4 5 6]] b = [[1 1 1] [2 2 2]] 数组纵向合并 1) c = np.vstack((

基于OpenSSL库的ECDSA签名与验证,附代码和文档

PHP合并两个或多个数组的方法 10-17

linux下利用/proc进行进程树的打印

在Linux下利用C语言实现的链接库的打印，主要通过打印下的目录中的链接文件，获取status中的链接信息内容，然后利用速记实现链接库的打印

实验：openssl 签名和验证

htttcooL123的博客 81

强烈不推荐不推荐一般般推荐强烈推荐

最新文章

ng-alain新版尝试

zsh下brew安装

Mac基础：启用root

2021年 3篇

2020年 363篇

2019年 475篇

2018年 199篇

2017年 142篇

2016年 168篇

记住：Data +public key = encryption -----> private key =DE encryption Data +private key = sign-----> public key =verify ----->...

OpenSSL RSA 消息签名与验证

xxh 5498

#include #include #include #include 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; ...

openssl rsa公钥验签名

dingzhaoyan的博客 3762

场景：只有公钥字符串(base64编码),需验证签名。环境：c++ + openssl step1 从内存读取公钥 static RSA* GetPublicKeyRSA(string strPublicKey) { int ...

OpenSSL命令行工具验证数字签名

人生如棋 8657

一、发送方A：生成私钥：OpenSSL> genrsa -passout pass:123456 -out apri.pem 1024生成公钥：OpenSSL> rsa -passin pass:123456 -pubout -in apr...

©2021 CSDN 皮肤主题: 数字20 设计师:CSDN官方博客 返回首页

淼叔

关注

1

3

12





专栏目录

联网举报中心 家长监护 Chrome商店下载 ©1999-2021北京创新乐知网络技术有限公司 版权与免责声明 版权申诉 出版物