

openssl ans.1编码规则分析及证书密钥编码方式

1 数据编码格式

openssl的数据编码规则是基于asn.1的，asn.1是什么？先上高大上的解释

ASN.1(Abstract Syntax Notation One), 是一种结构化的描述语言，包括两部分,数据描述语言和数据编码规则，数据描述语言标准：语言标准允许用户自定义的基本数据类型，并可以通过简单的数据类型组成更复杂的数据类型。数据编码规则：这些编码方法规定了将数字对象转换成应用程序能够处理、保存、传输的二进制形式的一组规则。标准ASN.1编码规则有规范编码规则（CER，Canonical Encoding Rules）、唯一编码规则（DER，Distinguished Encoding Rules）、压缩编码规则（PER，Packed Encoding Rules）和XML编码规则（XER，XML Encoding Rules）。

没看懂？好吧，我也没看懂。经过搜索无数资料后，现把自己的理解说一下，有不对的地方请大牛指正

我们知道在计算机语言中有很多的数据结构，有列表、集合、数组等等。但对应用程序特别是网络来说，这些数据结构都是二进制的数

据流，那么如何把这些不同的数据结构变成数据流，又能让其他应用能够识别呢。这就需要有一个标准，也就是我们说的asn.1，大家都遵守这个标准，自然可以和平共处。OK，这个标准到底是什么玩意？

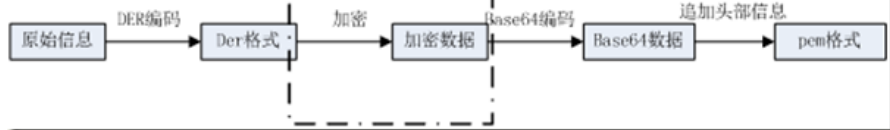
这个问题一会再来回答。现在我们想想如何把一个二叉树中的数据以流的形式发出去，对于整型、字符串这些基本类型我们可以直接塞进数据流里，但对于这种复杂的结构，这种方法就不显示了，怎么办？我们引入一个数字对象的概念，把这些数据结构转化成一个数字对象，怎么转？这就用到了asn.1标准的第一部分--数据描述语言标准，这个标准定义了一些基本的数据类型，如果我们使用到复杂的数据结构，asn.1还允许通过简单数据类型组成复杂的数据类型(x.509)。

数字对象已经建立的，怎么把这个数据对象变成二进制流呢，这就需要用到asn.1的第二部分--编码规则，编码方法规定了将数字对象转换成应用程序能够处理、保存、传输的二进制形式的一组规则。

现在可以回答上面这个问题了，简单来说这个标准就是规定了把数据转化成数据对象，又规定数据对象编码为二进制流的方法。

openssl使用的是asn.1的der编码规则，保证每个asn.1对象使用der编码的出的二进制编码是唯一的。

openssl使用pem作为基本的文件编码格式，pem和der是什么关系，如下图所示，几种加密环节是可选的



从本质上来说，openssl是pem编码就是在der编码的技术上进行Base64编码，然后添加一些头尾信息组成，可以通过openssl指令对der和pem进行格式转换

2 证书编码格式

常见的证书编码格式有三种X.509证书，PKCS#12证书PKCS#7证书。

X.509证书：最常用的证书格式，它仅包含了公钥信息而没有私钥信息，一个openssl签发经过PEM编码的X.509证书看起来如下

```
-----BEGIN CERTIFICATE-----
XXX
-----END CERTIFICATE-----
```

中间部分就是经过PEM编码的X509证书。除了上述形式的头尾格式，还可能出现以下两种不同的标识符

```
-----BEGIN X.509 CERTIFICATE-----
XXX
-----END X.509 CERTIFICATE-----
或者
-----BEGIN TRUSTED CERTIFICATE-----
-----END TRUSTED CERTIFICATE-----
```

X.509证书文件的后缀名经常是der,cer或者crt。openssl的指令x509提供了对X.509证书进行格式转换的方法。

访问人数：

UV

访问总量：

PV

昵称：Gordon0918

园龄：6年8个月

粉丝：21

关注：1

+加关注

< 2020年4月 >						
日	一	二	三	四	五	六
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

搜索

常用链接

[我的随笔](#)

[我的评论](#)

[我的参与](#)

[最新评论](#)

[我的标签](#)

我的标签

[android\(6\)](#)

[逆向\(4\)](#)

[Hook\(2\)](#)

[ida\(2\)](#)

[genrsa\(2\)](#)

[RSA\(2\)](#)

[smali\(2\)](#)

[so\(1\)](#)

[sphinx\(1\)](#)

[substrate\(1\)](#)

[更多](#)

随笔分类

[android\(6\)](#)

[android安全\(11\)](#)

[C/C++\(2\)](#)

[git\(1\)](#)

[Linux\(3\)](#)

[openssl\(8\)](#)

[Scrapy\(2\)](#)

[Windows\(1\)](#)

[渗透测试](#)

[协议\(2\)](#)

PKCS#12证书: PKCS12证书可以包含一个或者多个证书, 并且还可以包含证书对应的私钥。openssl的pkcs12指令可以将X.509格式的证书和私钥封装成PKCS#12格式的证书, 也可以将PKCS#12证书转换成X.509证书

PKCS#12证书的后缀名通常是p12或者pdx

PKCS#7证书: PKCS#7可以封装一个或者多个X.509证书或者PKCS#6证书, 并且可以包含CRL信息。PKCS#7证书中也不包含私钥信息。openssl提供了crl2pkcs7和pkcs7两个指令来生成和处理PKCS#7文件, 可以使用他们在X.509证书和PKCS#7证书之间进行转换和处理

PKCS#7证书的后缀名是p7b

3 密钥编码

openssl有多种形式的密钥, openssl提供PEM和DER两种编码方式对这些密钥进行编码, 并提供相关指令可以使用用户在这两种格式之间进行转换

openssl密钥大致可以分为两种, 一种是可以公开的, 例如公钥, 一种是不能公开的, 比对私钥。反映在编码上, 有的密钥需要加密, 有的密钥就不需要加密。一个经过加密的PEM编码密钥文件会在PEM文件中增加一些头信息, 表明密钥的加密状态, 加密算法及初始化向量等信息

openssl指令提供了对密钥加密的功能, 并提供了多种可选的对称加密算法, 比如DES和DES3。当对密钥进行加密的时候通常需要用户输入口令, 这里的口令并非直接用来作为加密的密钥, 而是根据这个口令使用一系列HASH操作来生成一个用户加密密钥数据的密钥。当读取这类密钥的时候, 同样需要输入同样的口令。

分类: [openssl](#)



 [Gordon0918](#)
[关注 - 1](#)
[粉丝 - 21](#)

[+加关注](#)

« 上一篇: [Https协议简析及中间人攻击原理](#)

» 下一篇: [Linux UGO和ACL权限管理](#)

0

0

posted @ 2016-03-11 10:06 [Gordon0918](#) 阅读(3410) 评论(0) 编辑 收藏

[刷新评论](#) [刷新页面](#) [返回顶部](#)

注册用户登录后才能发表评论, 请 [登录](#) 或 [注册](#), [访问](#) 网站首页。

【推荐】超50万行VC++源码: 大型组态工控、电力仿真CAD与GIS源码库

【推荐】腾讯云产品限时秒杀, 爆款1核2G云服务器99元/年!

相关博文:

- [使用 openssl 生成证书](#)
- [数字证书常见格式整理](#)
- [\(备忘\)openssl的证书格式转换](#)
- [使用openssl进行证书格式转换](#)
- [证书格式简介及不同格式之间的转换方式](#)
- » [更多推荐...](#)

最新 IT 新闻:

- [量子计算公司D-Wave宣布向任何COVID-19病毒研究者提供量子计算云服务](#)
- [《动物森友会》爆红背后, 任天堂是这么「利用」人性的](#)
- [招募波音前高管担任负责人 亚马逊拟扩大无人机送货业务](#)
- [Mozilla正着手将Android上的Firefox Beta迁移到Fenix引擎](#)
- [SpaceX公布Starship手册 介绍它如何取代航天飞机并提供舒适旅途](#)
- » [更多新闻...](#)

随笔档案

2017年12月(1)
2017年4月(6)
2017年3月(4)
2016年6月(4)
2016年5月(1)
2016年4月(5)
2016年3月(6)
2016年1月(5)
2015年7月(1)
2015年1月(3)
2014年7月(1)

最新评论

1. [Re:openssl 对称加密算法enc命令详解](#)
fedora 29 x86 workstation OpenSSL
1.1.1d FIPS 10 Sep 2019 没有 aes-256-gcm. openssl enc -ciphers 何解...
--NickD
2. [Re:openssl 对称加密算法enc命令详解](#)
-pass env:passwd 的passwd的前面不需要加\$?
--creazyloser
3. [Re:Android AccessibilityService\(辅助服务\) 使用示例](#)
他是返回的整个activity 的view , 所以会包含三个Fragment 的
--伍歌歌
4. [Re:PPTP协议握手流程分析](#)
大佬 自己能用软件模拟vpn 并建立通道 进行数据传输吗
--54辉哥
5. [Re:Https协议简析及中间人攻击原理](#)
写的不错
--aqu415

阅读排行榜

1. [openssl 对称加密算法enc命令详解\(25871\)](#)
2. [openssl 证书请求和自签名命令req详解\(23150\)](#)
3. [如何把java代码转换成smali代码\(20906\)](#)
4. [openssl 非对称加密算法RSA命令详解\(18578\)](#)
5. [openssl 摘要和签名验证指令dgst使用详解\(18021\)](#)

评论排行榜

1. [如何把java代码转换成smali代码\(4\)](#)
2. [android调试系列--使用ida pro调试原生程序\(3\)](#)
3. [openssl 对称加密算法enc命令详解\(2\)](#)
4. [openssl 非对称加密算法RSA命令详解\(1\)](#)
5. [openssl 非对称加密算法DSA命令详解\(1\)](#)

推荐排行榜

1. [openssl 证书请求和自签名命令req详解\(5\)](#)
2. [Android调试系列一使用android studio调试smali代码\(3\)](#)
3. [openssl 非对称加密算法RSA命令详解\(2\)](#)
4. [openssl CA服务器模拟指令CA详解\(1\)](#)
5. [Https协议简析及中间人攻击原理\(1\)](#)