原创 henter 于 2014-10-13 10:13:35 发布 3015 收藏 版权
分类专栏： OpenSSL ASN.1编码 文章标签： openssl C语言

OpenSSL 同时被 2 个专栏收录 19 订阅 33 篇文章 订阅专栏

分类专栏
屏幕录制 1篇
虚拟机 2篇
Kali 4篇
MIRACL 4篇
OpenSSL 33篇
XML 6篇
VC 14篇
GCC 6篇
C语言 13篇
linux 15篇
密码学与信息安全 18篇
ASN.1编码 12篇
Python 2篇
vim 1篇
C# 7篇
杂文 4篇
html 1篇
字符编码 2篇
COM 1篇
文件格式 2篇
随机性检测 3篇
WebSocket 6篇
操作系统 1篇

OID(Object Identifier) denotes an object.
Examples:

OID   object

1.3.14.3.2.26   SHA-1
2.16.840.1.101.3.4.2.1   SHA-256
1.2.840.113549.1.7.2   PKCS-7 signedData

In OpenSSL no functions are directly provided to compute the OID ASN.1 encode. At lease two methods can be taken into account.

1. Create a temporary object by invoking function OBJ_create(), then encode it by invoking function i2d_ASN1_OBJECT().
Implementation (Not recommended)

```
/**************************************************
* Author: HAN Wei
* Author's blog: http://blog.csdn.net/henter/
* Date: Oct 11th, 2014
* Description: implement the OID ASN.1 encode function
**************************************************/

#include <stdio.h>
#include <openssl/objects.h>
#include <openssl/asn1.h>

int Asn1EncodeOid(char *oid,
                  unsigned char *encode,
                  int *encode_len)
{
  int new_nid, byte_len;
  ASN1_OBJECT *obj;
  unsigned char *tmp_pointer;

  new_nid = OBJ_create(oid, "oid example", "Object Identifier Example");
  obj = OBJ_nid2obj(new_nid);

  if (!encode)
  {
    byte_len = i2d_ASN1_OBJECT(obj, NULL);
    if (byte_len <= 0)
    {
#ifdef _DEBUG
      printf("get ASN.1 encode byte length failed at %s, line %d!\n", __FILE__, __LINE__);
#endif
      OBJ_cleanup();
      return (-1);
    }
    else
    {
   *encode_len = byte_len;
      OBJ_cleanup();
      return 0;
    }
  }
  else
  {
    tmp_pointer = encode;
    byte_len = i2d_ASN1_OBJECT(obj, &tmp_pointer);
    if (byte_len <= 0)
    {
#ifdef _DEBUG
      printf("ASN.1 encode OID failed at %s, line %d!\n", __FILE__, __LINE__);
#endif
      OBJ_cleanup();
      return (-1);
    }
    else
    {
      *encode_len = byte_len;
      OBJ_cleanup();
      return 0;
    }
  }
}
```

This is not a good implementation. OBJ_cleanup() will free all dynamically created object, so this function must be used carefully. Especially when multiple threads are running, the fact that one thread invokes OBJ_cleanup() may run the risk of cleaning object created by other threads. The consequence is unpredictable.

2. Compute OID payload part ASN.1 encode by invoking function a2d_ASN1_OBJECT() firstly, compute the OID encode by invoking function i2d_ASN1_OBJECT() next.

A complete Implementation (recommended)

Header file:

```
/**************************************************
* File name: oid_encode.h
* Author: HAN Wei
* Author's blog: http://blog.csdn.net/henter/
* Date: Oct 11th, 2014
* Description: declare the OID ASN.1 encode function
**************************************************/

#ifndef HEADER_OID_ASN1_ENCODE_H
  #define HEADER_OID_ASN1_ENCODE_H

#ifdef  __cplusplus
extern "C" {
#endif
```

Function implementation file:

```
/**************************************************
* File name: oid_encode.c
* Author: HAN Wei
* Author's blog: http://blog.csdn.net/henter/
* Date: Oct 11th, 2014
* Description: implement the OID ASN.1 encode function
**************************************************/

#include <stdio.h>
#include <openssl/objects.h>
#include <openssl/asn1.h>

int Asn1EncodeOid(char *oid,
                  unsigned char *encode,
                  int *encode_len)
{
  int payload_len, total_len;
  ASN1_OBJECT obj;
  unsigned char *tmp_pointer, *payload_encode;

// get payload ASN.1 encode
  payload_len = a2d_ASN1_OBJECT(NULL, 0, oid, -1);
  if (payload_len <= 0)
  {
#ifdef _DEBUG
    printf("get ASN.1 encode byte length failed at %s, line %d!\n", __FILE__, __LINE__);
#endif
    return (-1);
  }
  if ( !(payload_encode=(unsigned char *)malloc(payload_len)) )
  {
#ifdef _DEBUG
    printf("invoke malloc() function failed at %s, line %d!\n", __FILE__, __LINE__);
#endif
    return (-1);
  }
  payload_len = a2d_ASN1_OBJECT(payload_encode, payload_len, oid, -1);
  if (payload_len <= 0)
  {
#ifdef _DEBUG
    printf("ASN.1 encode payload failed at %s, line %d!\n", __FILE__, __LINE__);
#endif
```

```c
    free(payload_encode);
    return (-1);
  }

// get the whole OID ASN.1 encode
  obj.data = payload_encode;
  obj.length = payload_len;
  if (!encode)
  {
    total_len = i2d_ASN1_OBJECT(&obj, NULL);
    if (total_len <= 0)
    {
#ifdef _DEBUG
      printf("get ASN.1 encode byte length failed at %s, line %d!\n", __FILE__, __LINE__);
#endif
      free(payload_encode);
      return (-1);
    }
    else
    {
      *encode_len = total_len;
      free(payload_encode);
      return 0;
    }
  }
  else
  {
    tmp_pointer = encode;
    total_len = i2d_ASN1_OBJECT(&obj, &tmp_pointer);
    if (total_len <= 0)
    {
#ifdef _DEBUG
      printf("ASN.1 encode OID failed at %s, line %d!\n", __FILE__, __LINE__);
#endif
      free(payload_encode);
      return (-1);
    }
    else
    {
      *encode_len = total_len;
      free(payload_encode);
      return 0;
    }
  }
}
```

A demo program file:

```c
/**************************************************
* File name: test.c
* Author: HAN Wei
* Author's blog: http://blog.csdn.net/henter/
* Date: Oct 11th, 2014
* Description: this program demonstrates how to invoke
    the OID ASN.1 encode function
**************************************************/

#include "oid_encode.h"
#include <stdio.h>
#include <stdlib.h>
int main(void)
{
  char oid[128]="2.16.840.1.101.3.4.2.1";  /* SHA-256 OID */
  unsigned char *buffer;
  int buffer_len, i;

  if ( Asn1EncodeOid(oid, NULL, &buffer_len) )
  {
    printf("error detected!\n");
#if defined(_WIN32) || defined(_WIN64)
    system("pause");
#endif
    return (-1);
  }
  printf("OID ASN.1 encode length is %d bytes.\n", buffer_len);

  if ( !(buffer = (unsigned char *)malloc(buffer_len)) )
  {
    printf("invoke malloc() function failed!\n");
#if defined(_WIN32) || defined(_WIN64)
    system("pause");
#endif
    return (-1);
  }

  if ( Asn1EncodeOid(oid, buffer, &buffer_len) )
  {
    printf("error detected!\n");
    free(buffer);
#if defined(_WIN32) || defined(_WIN64)
    system("pause");
#endif
    return (-1);
  }
  printf("OID ASN.1 encode:\n");
  for (i=0; i<buffer_len; i++)
    printf("0x%x  ", buffer[i]);
  printf("\n");

  free(buffer);
#if defined(_WIN32) || defined(_WIN64)
  system("pause");
#endif
  return 0;
}
```

ASN.1 encode of SHA-256 is obtained from the demo: 0x6 0x9 0x60 0x86 0x48 0x1 0x65 0x3 0x4 0x2 0x1
This is a better implementation.

对象标识符(OBJECT IDENTIFIER, OID) 的编码规则 cat_lover的专栏 8939
对象标识符(OBJECT IDENTIFIER, OID) 的编码规则 对象标识符类型　　对象标识符(OBJECT IDENTIFIER, OID)类型用层次的形式来表示标准规范．标…

ASN.1 -- 编码规则 mao834099514的博客 5202
3.2CER与DER CER与DER（Canonical and Distinguished Encoding Rules） 3.2.1更多限制规则的需求 在X.400和X.500中应用接力传递消息，会使用到…

ASN.1入门（超详细） 笑不语的博客 1万+
ASN.1简介 ASN.1(Abstract Syntax Notation dotone),抽象语法标记1。是定义抽象数据类型形式的标准，描绘了与任何表示数据的编码技术无关的通用数…

13.openssl编程——ASN1库 艾小小雨的博客 1287
13.1 ASN1简介 ANS.1(Abstract Syntax Notation One, X.208)，是一套灵活的标记语言，他允许定义多种数据类型，从integer、bit string、一类的简单类…

安全不安全002：C#实现RSA算法加密解密 杨友山 5643
通过前面的文章我们学会了如何生成公钥和私钥，详见这篇文章：https://blog.csdn.net/yysyangyangyangshan/article/details/80368397。那么，我们来…

RSA非对称加密算法在C#中的实现（.NET/C#实现RSA非对称加密算法） 最新发布 风生晚凉的博客 1239
using Cari.Safety.SSO.Interface; using System; using Org.BouncyCastle.Asn1; using Org.BouncyCastle.Asn1.Pkcs; using Org.BouncyCastle.Asn1.X50…

C# 与JAVA 的RSA 加密解密交互，互通，C#使用BouncyCastle来实现私钥加密，公钥解密的方法... weixin_30564785的博客 508
因为C#的RSA加密解密只有公钥加密，私钥解密，没有私钥加密，公钥解密。在网上查了很久也没有很好的实现。BouncyCastle的文档少之又少。很多人…

ASN1标准对OID的编码 Netfilter 6697

asn1对OID的编码有一些规定，形如a.b.c.d.e的OID被编码的时候，完全可以按照der的编码规则将整个oid的类型设定为object，然后将每一个点分…

ASN.1笔记——基本类型详述 sever2012的专栏 1万+
<!-- p {margin-bottom:0.21cm} --> ASN.1笔记——2 一.ASN.1基本类型 基本类型汇总表 类型 UNIVERSALTag 取值 BOOLEAN 1 TRUE，FALSE NULL 5 N…

ASN.1笔记——语法规则与类型概述 热门推荐 sever2012的专栏 3万+
<!-- p {margin-bottom:0.21cm} h2 {margin-bottom:0.21cm} h2.western {font-family:"DejaVu Sans",sans-serif; font-size:14pt; font-style:italic} h2.cjk {font…

SNMP--Windows API--AsnObjectIdentifier Coperator 1107
原文来自MSDN Library for Visual Studio 2008 SP1，翻译部分仅为个人观点，想要看更多信息请看MSDN，如有版权问题请联系QQ 643166601，邮件64…

ASN1对象与OID之间转换的函数 weixin_34209851的博客 779
ASN1对象与OID之间转换的函数,经常会用到. Name OBJ_nid2obj, OBJ_nid2ln, OBJ_nid2sn, OBJ_obj2nid, OBJ_txt2nid, OBJ_ln2nid, OBJ_sn2nid, OBJ_…

SNMP++ 04-SNMP中OBJECT IDENTIFIER的BER编码与解码及一些思考 woquhan的博客 3483
阅读完本文你可以学到：（1）SNMP 中OBJECT IDENTIFIER的 BER 编码与解码代码实现。（2）在学习OBJECT IDENTIFIER 编解码过程中的一些思考…

未知类型ASN.1编码的解析 爱java的小蓝的博客 1758
最近一直在研究BC中的ASN1组装和解析，从BC开源项目中中拿出给如下一段ASN1编码，在不知道组合以及对象情况时，如何解析呢？ private byte[] un…

使用asn1tools进行asn1编解码 dianjie9145的博客 2521
最近在做3GPP的编解码，发现有两个第三方库比较好用。一个是ASN1C(c语言编译环境)，一个是python第三方库asn1tools。这里介绍下asn1tools的使…

ASN.1概述及数据类型详解 工作日志 2万+
1.ASN.1概述　抽象语法表示（标记）ASN.1（Abstract Syntax Notation One ）一种数据定义语言，描述了对数据进行表示、编码、传输和解码的数据格…

ASN.1探索 - 2 基础知识（2）（转） weixin_34202952的博客 182
转自： http://wmfbravo.blog.163.com/ 感谢： wmfbravo 2 基础知识 & 注释： 本章的内容主要翻译自《ASN.1 Communication between Heterogeneous S…

热门文章

在 Win7 下安装 KB4512506 补丁报告 0x80092004 错误的解决办法 21653

使用 OpenSSL 时一定要注意不同版本之间的差异 20876

ThinkPad T450 笔记本电脑 Fn + F8 组合键失效后开启无线网络的办法 13359

基于OpenSSL 1.1.1版实现的SM2加密与解密C程序 12370

基于OpenSSL 1.1.1版实现的SM2签名与验签C程序 12166

最新评论

将Kali Linux安装到优盘并实现文件的持…
henter: 在制作启动U盘完成之后，使用U盘引导计算机启动时，会出现一个菜单，一…

将Kali Linux安装到优盘并实现文件的持…
henter: 您好！如果有技术问题欢迎留言交流。

将Kali Linux安装到优盘并实现文件的持…
诗Spanx: 大佬您好

将Kali Linux安装到优盘并实现文件的持…
m0_73352021: 操作完了 还是保存不了

介绍一种门限SM2密码方案
henter: 计算s2时是需要做模n运算的，谢谢指出！

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

适用于Windows平台的录屏软件Captura简介

在Oracle VirtualBox中导入Kali Linux官方制作的虚拟机

将Kali Linux安装到优盘并实现文件的持久存储(3)

2022年 5篇　2021年 4篇
2020年 8篇　2019年 23篇
2018年 27篇　2017年 23篇