
OpenSSL - asn1parse

Parser les structures ASN.1, ou extraire les données ASN.1

OPTIONS

- inform DER|PEM** Format d'entrée (DER : binaire, PEM : base64)
- in filename** Fichier d'entrée
- out filename** Fichier de sortie où placer les données DER.
- noout** Ne sort pas la version parsée du fichier en entrée
- offset number** Commence à parser à l'offset spécifié
- length number** Nombre d'octets à parser
- i** Indenter la sortie en accord avec le "depth" des structures
- oid filename** Un fichier contenant un OID additionnel.
- stdparse offset** Parse le contenu des octets de l'objet ASN.1 en commençant à l'offset spécifié. Peut être spécifié plusieurs fois.
- genstr string, -genconf file** Génère des données encodée basé sur la chaîne ou le fichier spécifié en utilisant le format ASN1_generate_nconf

SORTIE

La sortie contient des lignes de ce type :

```
0:d=0 hl=4 l= 681 prim : SEQUENCE
.....
229:d=3 hl=3 l= 141 prim : BIT STRING
373:d=2 hl=3 l= 162 cons : cont [ 3 ]
376:d=3 hl=3 l= 159 cons : SEQUENCE
379:d=4 hl=2 l= 29 cons : SEQUENCE
381:d=5 hl=2 l= 3 prim : OBJECT
```

Chaque ligne commence avec un offset décimal. **d=xx** spécifie la profondeur courante. **hl=XX** donne la longueur d'en-tête du type courant. **l=XX** donne la longueur du contenu.

Exemples

parser un fichier

```
openssl asn1parse -in file.pem
```

parser un fichier DER

```
openssl asn1parse -inform DER -in file.der
```

générer un UTF8String simple

```
openssl asn1parse -genstr 'UTF8 :Hello World'
```

Générer un UTF8String, ne pas parser la sortie

```
openssl asn1parse -genstr 'UTF8 :Hello World' -noout -out utf8.der
```

générer en utilisant un fichier de configuration

openssl asn1parse -genconf asn1.cnf -noout -out asn1.der

exemple de fichier de configuration

asn1=SEQUENCE :seq_sect

[seq_sect]

field1=BOOL :TRUE

field2=EXP :0, UTF8some random string