

View ASN.1 structure of a file:

**unber csca.der**

```
<C O="0" T="[UNIVERSAL 16]" TL="4" V="1266" A="SEQUENCE">
  <C O="4" T="[UNIVERSAL 16]" TL="4" V="806" A="SEQUENCE">
    <C O="8" T="[0]" TL="2" V="3">
      <P O="10" T="[UNIVERSAL 2]" TL="2" V="1" A="INTEGER" F>2</P>
    </C O="13" T="[0]" L="5">
      <P O="13" T="[UNIVERSAL 2]" TL="2" V="1" A="INTEGER" F>1</P>
    <C O="16" T="[UNIVERSAL 16]" TL="2" V="65" A="SEQUENCE">
      <P O="18" T="[UNIVERSAL 6]" TL="2" V="9" A="OBJECT IDENTIFIER"
F>1.2.840.113549.1.1.10</P>
      <C O="29" T="[UNIVERSAL 16]" TL="2" V="52" A="SEQUENCE">
        <C O="31" T="[0]" TL="2" V="15">
```

....

See the content of a certificate:

**openssl x509 -text -noout -inform DER -in csca.der**

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: 1.2.840.113549.1.1.10

Issuer: C=CZ, O=Czech Republic, OU=Ministry of Interior, CN=CSCA\_CZ

Validity

Not Before: Jul 24 00:00:00 2006 GMT

Not After : Oct 24 23:59:59 2021 GMT

Subject: C=CZ, O=Czech Republic, OU=Ministry of Interior, CN=CSCA\_CZ

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (3072 bit)

Modulus (3072 bit):

Convert certificate from DER to PEM:

**openssl x509 -out csca.pem -inform DER -in csca.der**

Prepare the C and H files for the ASN.1 structures:  
**asn1c -fnative-types sod.asn1**

Compiled AlgorithmIdentifier.c  
Compiled AlgorithmIdentifier.h  
Compiled LDSSecurityObjectVersion.c  
Compiled LDSSecurityObjectVersion.h  
Compiled DigestAlgorithmIdentifier.c  
Compiled DigestAlgorithmIdentifier.h  
Compiled LDSSecurityObject.c  
Compiled LDSSecurityObject.h  
Compiled DataGroupHash.c  
Compiled DataGroupHash.h  
Compiled DataGroupNumber.c  
Compiled DataGroupNumber.h  
Symlinked /usr/local/share/asn1c/ANY.h -> ANY.h  
Symlinked /usr/local/share/asn1c/ANY.c -> ANY.c  
Symlinked /usr/local/share/asn1c/INTEGER.h -> INTEGER.h  
Symlinked /usr/local/share/asn1c/NativeEnumerated.h -> NativeEnumerated.h  
Symlinked /usr/local/share/asn1c/INTEGER.c -> INTEGER.c  
...

Compile a sample DER-XML converter:  
**gcc \*.c -o LDSview -I. -DPDU=LDSSecurityObject**

rm converter-sample.c  
cp ? sod\_sample.c

Compile a sample application:  
**gcc \*.c -o LDStest -I.**

**Assignment: Modify the sample program displaying the LDS Security object to include verification of the hash of the datagroup (based on the files read from an ePassport). To test your application use the Sample\_Data provided. [10 points]**