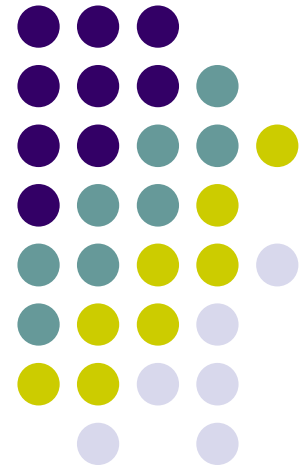


# ASN.1:

# Introduction

Zdeněk Říha





# ASN.1

- Abstract Syntax Notation 1
- notation for describing abstract types and values
- Defined in ITU-T X.680 ... X.695
- Used in many file formats, including crypto
  - Public keys, private keys
  - Certificate requests, certificates
  - Digital signatures, padding, encrypted files



# ASN.1

- Allows format/storage/transmission of data
  - Compatible among many applications
  - Not dependent on HW platform
    - E.g. little/big endian
  - Not dependent on operating system
- Simple & Structured types
- Multiple encoding rules (methods)

# ASN.1 – Types



Type	Tag number (decimal)	Tag number (hexadecimal)
INTEGER	2	02
BIT STRING	3	03
OCTET STRING	4	04
NULL	5	05
OBJECT IDENTIFIER	6	06
SEQUENCE and SEQUENCE OF	16	10
SET and SET OF	17	11
PrintableString	19	13
IA5String	22	16
UTCTime	23	17



# ASN.1 – simple types

- Integer
  - signed integer (there's no unsigned integer)
- Bit string
  - The number of bits does not have to be a multiple of 8
- Octet string
  - an arbitrary string of octets
- NULL
  - No data (used in parameters)
- PrintableString, IA5String, UTF8String, ...
  - Strings – the sets of characters are various
- UTCTime
  - Time



# ASN.1 – OID type

- Object identifier (OID)
  - Sequence of integer components that identify an object
  - Assigned in a hierarchical way
- Example
  - sha-1WithRSAEncryption = 1.2.840.113549.1.1.5
  - iso(1) member-body(2)  
us(840) rsadsi(113549)  
pkcs(1) pkcs-1(1) 5
    - [1.2.840.113549.1.1](#) - PKCS-1
    - [1.2.840.113549.1](#) - PKCS
    - [1.2.840.113549](#) - RSADSI
    - [1.2.840](#) - USA
    - [1.2](#) - ISO member body
    - [1](#) - ISO assigned OIDs
    - [Top of OID tree](#)



# ASN.1 – structured types

- SEQUENCE
  - an ordered collection of one or more types
- SEQUENCE OF
  - an ordered collection of zero or more occurrences of a given type
- SET
  - an unordered collection of one or more types
- SET OF
  - an unordered collection of zero or more occurrences of a given type



# ASN.1 Encoding Rules

- XML – oriented formats
  - XER (XML Encoding Rules)
- Byte-oriented formats
  - BER (Basic Encoding Rules)
  - CER (Canonical Encoding Rules) – subset of BER
  - **DER (Distinguished Encoding Rules) – subset of BER**
    - **Used for crypto files**
- Bit-oriented formats
  - PER (Packed Encoding Rules)
- Verbose, human readable formats
  - GSER (Generic String Encoding Rules)





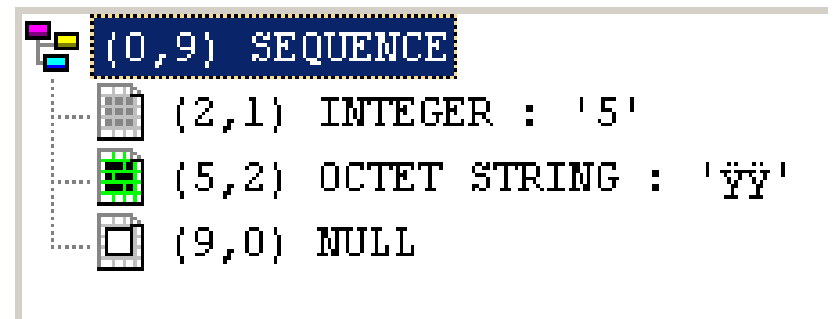
# BER encoding

- TLV – Tag Length Value
  - All the data is encoded using a simple TLV format
  - Tag – what kind of data it is
  - Length – the length of the data
  - Value – the data itself
- Example
  - 02 01 05 [hexadecimal values]
    - Tag – Integer
    - Length of data – 1 byte
    - Data: (positive integer) 5



# Nested data

- SEQUENCE is similar to struct/record
- 30 09 02 01 05 04 02 FF FF 05 00
  - 30 09 – sequence of length 9 bytes
  - 02 01 05 – integer 5
  - 04 02 FF FF – octet string FF FF
  - 05 00 – NULL (no data)





# BER tags

- Tag encoding



- Class

Class	Bit 8	Bit 7
universal	0	0
application	0	1
context-specific	1	0
private	1	1

- Tag number

- Bits 1-5
- If all bits are 1 then the tag continues in the following byte(s)



# BER length

- `length >=0 && length <= 127`
  - The length is coded directly
    - E.g. '05'
- Otherwise the bit 8 is set, bits 1-7 code the number of bytes that specify the length
  - E.g. 255 -> '81' 'FF'
  - E.g. 256 -> '82' '01' '00' or also '83' '00' '01' '00'
    - BER x DER
- '80' is “indefinite” length
  - Not allowed in DER



# BER value

- The data itself
- Dependent on data type
  - Integer: signed – e.g. 128 -> '00 80'
  - Octet string: directly the data
  - Bit string: number of unused bits + padded bit string to a multiple of 8 bits (padding is at the end)
  - UTCTime: string of one of the forms

*YYMMDDhhmmZ*

*YYMMDDhhmm+hh'mm'*

*YYMMDDhhmm-hh'mm'*

*YYMMDDhhmmssZ*

*YYMMDDhhmmss+hh'mm'*

*YYMMDDhhmmss-hh'mm'*





# DER vs. PEM

- PEM
  - Privacy Enhanced Mail
- PEM as such not used, but formats still used
- Textual formats
  - Practical for transport channels where full 8bit data can be damaged
- PEM is base64 coded DER enveloped with
  - -----BEGIN **SOMETHING**-----
  - -----END **SOMETHING**-----
  - Where **SOMETHING** is CERTIFICATE/PKCS7/KEY...

# Sample PEM file







# ASN.1 viewers

- Unber (part of asn1c)
- Openssl asn1parse
- ASN.1 Editor
- ...

# OpenSSL asn1parse

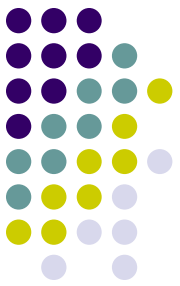


```
C:\WINDOWS\system32\cmd.exe
C:\Program Files\OpenSSL\bin>openssl.exe asn1parse -inform DER -in CZE_CSCA_2009
0113.der
0:d=0  hl=4  l=1266 cons: SEQUENCE
4:d=1  hl=4  l= 806 cons: SEQUENCE
8:d=2  hl=2  l=   3 cons: cont [ 0 ]
10:d=3  hl=2  l=   1 prim: INTEGER           :02
13:d=2  hl=2  l=   1 prim: INTEGER           :3A
16:d=2  hl=2  l=  65 cons: SEQUENCE
18:d=3  hl=2  l=   9 prim: OBJECT             :1.2.840.113549.1.1.10
29:d=3  hl=2  l=  52 cons: SEQUENCE
31:d=4  hl=2  l=  15 cons: cont [ 0 ]
33:d=5  hl=2  l=  13 cons: SEQUENCE
35:d=6  hl=2  l=   9 prim: OBJECT             :sha256
46:d=6  hl=2  l=   0 prim: NULL
48:d=4  hl=2  l=  28 cons: cont [ 1 ]
50:d=5  hl=2  l=  26 cons: SEQUENCE
52:d=6  hl=2  l=   9 prim: OBJECT             :1.2.840.113549.1.1.8
63:d=6  hl=2  l=  13 cons: SEQUENCE
65:d=7  hl=2  l=   9 prim: OBJECT             :sha256
76:d=7  hl=2  l=   0 prim: NULL
78:d=4  hl=2  l=   3 cons: cont [ 2 ]
80:d=5  hl=2  l=   1 prim: INTEGER           :20
83:d=2  hl=2  l=  87 cons: SEQUENCE
85:d=3  hl=2  l=  11 cons: SET
87:d=4  hl=2  l=   9 cons: SEQUENCE
89:d=5  hl=2  l=   3 prim: OBJECT             :countryName
94:d=5  hl=2  l=   2 prim: PRINTABLESTRING   :CZ
98:d=3  hl=2  l=  23 cons: SET
100:d=4  hl=2  l=  21 cons: SEQUENCE
102:d=5  hl=2  l=   3 prim: OBJECT             :organizationName
107:d=5  hl=2  l=  14 prim: PRINTABLESTRING   :Czech Republic
123:d=3  hl=2  l=  29 cons: SET
125:d=4  hl=2  l=  27 cons: SEQUENCE
127:d=5  hl=2  l=   3 prim: OBJECT             :organizationalUnitName
132:d=5  hl=2  l=  20 prim: PRINTABLESTRING   :Ministry of Interior
154:d=3  hl=2  l=  16 cons: SET
156:d=4  hl=2  l=  14 cons: SEQUENCE
158:d=5  hl=2  l=   3 prim: OBJECT             :commonName
163:d=5  hl=2  l=   7 prim: T61STRING           :CSCA_CZ
172:d=2  hl=2  l=  30 cons: SEQUENCE
174:d=3  hl=2  l=  13 prim: UTCTIME             :090113000000Z
189:d=3  hl=2  l=  13 prim: UTCTIME             :240413000000Z
204:d=2  hl=2  l=  87 cons: SEQUENCE
206:d=3  hl=2  l=  11 cons: SET
208:d=4  hl=2  l=   9 cons: SEQUENCE
210:d=5  hl=2  l=   3 prim: OBJECT             :countryName
215:d=5  hl=2  l=   2 prim: PRINTABLESTRING   :CZ
219:d=3  hl=2  l=  23 cons: SET
221:d=4  hl=2  l=  21 cons: SEQUENCE
223:d=5  hl=2  l=   3 prim: OBJECT             :organizationName
228:d=5  hl=2  l=  14 prim: PRINTABLESTRING   :Czech Republic
244:d=3  hl=2  l=  29 cons: SET
246:d=4  hl=2  l=  27 cons: SEQUENCE
```



anxur.fi.muni.cz - PuTTY

```
labak:~$ unber /usr/share/doc/dirmngr-1.0.3/examples/extra-certs/bnetza-10r-ocsp-2.crt
<C 0="0" T="[UNIVERSAL 16]" TL="4" V="952" A="SEQUENCE">
  <C 0="4" T="[UNIVERSAL 16]" TL="4" V="804" A="SEQUENCE">
    <C 0="8" T="[0]" TL="2" V="3">
      <P 0="10" T="[UNIVERSAL 2]" TL="2" V="1" A="INTEGER" F>2</P>
    </C 0="13" T="[0]" L="5">
      <P 0="13" T="[UNIVERSAL 2]" TL="2" V="1" A="INTEGER" F>53</P>
    <C 0="16" T="[UNIVERSAL 16]" TL="2" V="10" A="SEQUENCE">
      <P 0="18" T="[UNIVERSAL 6]" TL="2" V="6" A="OBJECT IDENTIFIER" F>1.3.36.3.3.1.2</P>
      <P 0="26" T="[UNIVERSAL 5]" TL="2" V="0" A="NULL"></P>
    </C 0="28" T="[UNIVERSAL 16]" A="SEQUENCE" L="12">
      <C 0="28" T="[UNIVERSAL 16]" TL="2" V="63" A="SEQUENCE">
        <C 0="30" T="[UNIVERSAL 17]" TL="2" V="11" A="SET">
          <C 0="32" T="[UNIVERSAL 16]" TL="2" V="9" A="SEQUENCE">
            <P 0="34" T="[UNIVERSAL 6]" TL="2" V="3" A="OBJECT IDENTIFIER" F>2.5.4.6</P>
            <P 0="39" T="[UNIVERSAL 19]" TL="2" V="2" A="PrintableString">DE</P>
          </C 0="43" T="[UNIVERSAL 16]" A="SEQUENCE" L="11">
            </C 0="43" T="[UNIVERSAL 17]" A="SET" L="13">
              <C 0="43" T="[UNIVERSAL 17]" TL="2" V="26" A="SET">
                <C 0="45" T="[UNIVERSAL 16]" TL="2" V="24" A="SEQUENCE">
                  <P 0="47" T="[UNIVERSAL 6]" TL="2" V="3" A="OBJECT IDENTIFIER" F>2.5.4.10</P>
                  <P 0="52" T="[UNIVERSAL 12]" TL="2" V="17" A="UTF8String">Bundesnetzagentur</P>
                </C 0="71" T="[UNIVERSAL 16]" A="SEQUENCE" L="26">
                  </C 0="71" T="[UNIVERSAL 17]" A="SET" L="28">
                    <C 0="71" T="[UNIVERSAL 17]" TL="2" V="20" A="SET">
                      <C 0="73" T="[UNIVERSAL 16]" TL="2" V="18" A="SEQUENCE">
                        <P 0="75" T="[UNIVERSAL 6]" TL="2" V="3" A="OBJECT IDENTIFIER" F>2.5.4.3</P>
                        <P 0="80" T="[UNIVERSAL 12]" TL="2" V="11" A="UTF8String">10R-CA 1:PN</P>
                      </C 0="93" T="[UNIVERSAL 16]" A="SEQUENCE" L="20">
                        </C 0="93" T="[UNIVERSAL 17]" A="SET" L="22">
                          </C 0="93" T="[UNIVERSAL 16]" A="SEQUENCE" L="65">
                            <C 0="93" T="[UNIVERSAL 16]" TL="2" V="30" A="SEQUENCE">
                              <P 0="95" T="[UNIVERSAL 23]" TL="2" V="13" A="UTCTime">0508040827092</P>
                              <P 0="110" T="[UNIVERSAL 23]" TL="2" V="13" A="UTCTime">0712310823492</P>
                            </C 0="125" T="[UNIVERSAL 16]" A="SEQUENCE" L="32">
                              <C 0="125" T="[UNIVERSAL 16]" TL="2" V="65" A="SEQUENCE">
                                <C 0="127" T="[UNIVERSAL 17]" TL="2" V="11" A="SET">
                                  <C 0="129" T="[UNIVERSAL 16]" TL="2" V="9" A="SEQUENCE">
                                    <P 0="131" T="[UNIVERSAL 6]" TL="2" V="3" A="OBJECT IDENTIFIER" F>2.5.4.6</P>
                                    <P 0="136" T="[UNIVERSAL 19]" TL="2" V="2" A="PrintableString">DE</P>
                                  </C 0="140" T="[UNIVERSAL 16]" A="SEQUENCE" L="11">
                                    </C 0="140" T="[UNIVERSAL 17]" A="SET" L="13">
                                      <C 0="140" T="[UNIVERSAL 17]" TL="2" V="26" A="SET">
                                        <C 0="142" T="[UNIVERSAL 16]" TL="2" V="24" A="SEQUENCE">
                                          <P 0="144" T="[UNIVERSAL 6]" TL="2" V="3" A="OBJECT IDENTIFIER" F>2.5.4.10</P>
                                          <P 0="149" T="[UNIVERSAL 12]" TL="2" V="17" A="UTF8String">Bundesnetzagentur</P>
                                        </C 0="168" T="[UNIVERSAL 16]" A="SEQUENCE" L="26">
```



# Manual viewing/processing

```
cze_csca_20060724.cer (~\Plocha\PKI) - GVIM3
Soubor  Úpravy  Nástroje  Syntaxe  Buffery  Okna  Nápověda

00000000: 3082 04f2 3082 0326 a003 0201 0202 0101  8...8...&.....
00000010: 3041 0609 2a86 4886 f70d 0101 0a30 34a0  0A...*.H.....04.
00000020: 0f30 0d06 0960 8648 0165 0304 0201 0500  .8...`.H.e.....
00000030: a11c 301a 0609 2a86 4886 f70d 0101 0830  ..8...*.H.....8
00000040: 0d06 0960 8648 0165 0304 0201 0500 a203  ...`.H.e.....
00000050: 0201 2030 5731 0b30 0906 0355 0406 1302  .. 0W1.8...U....
00000060: 435a 3117 3015 0603 5504 0a13 0e43 7a65  CZ1.8...U....Cze
00000070: 6368 2052 6570 7562 6c69 6331 1d30 1b06  ch Republic1.8..
00000080: 0355 040b 1314 4d69 6e69 7374 7279 206f  .U....Ministry o
00000090: 6620 496e 7465 7269 6f72 3110 300e 0603  f Interior1.8...
000000a0: 5504 0314 0743 5343 415f 435a 301e 170d  U....CSCA_CZ0...
000000b0: 3036 3037 3234 3030 3030 3030 5a17 0d32  06072400000002..2
000000c0: 3131 3032 3432 3335 3935 395a 3057 310b  1102423595920W1.
000000d0: 3009 0603 5504 0613 0243 5a31 1730 1506  8...U....CZ1.8..
000000e0: 0355 040a 130e 437a 6563 6820 5265 7075  .U....Czech Repu
000000f0: 626c 6963 311d 301b 0603 5504 0b13 144d  blic1.8...U....M
00000100: 696e 6973 7472 7920 6f66 2049 6e74 6572  inistry of Inter
00000110: 696f 7231 1030 0e06 0355 0403 1407 4353  ior1.8...U....CS
00000120: 4341 5f43 5a30 8201 a230 0d06 092a 8648  CA_CZ0...8...*.H
00000130: 86f7 0d01 0101 0500 0382 018f 0030 8201  .....8..
00000140: 8a02 8201 8100 af51 99ea a824 c5f8 b0b5  .....Q...$.
00000150: 6aa5 4b32 852c 8a0b cd84 e72a 59f2 aef9  j.K2.,.....*Y...
00000160: 71b2 e0db d2dc 97b4 2c80 a045 97bd 0372  q.....,E...r
00000170: 149d fe4d d00a c337 78dd 989a d7d6 e834  ...H...7x.....4

Počet filtrovaných řádků: 7                                1,1          Začátek
```

- 30 82 04 f2
  - SEQUENCE
  - length 1266B
- 30 82 03 26
  - SEQUENCE
  - length 806B
- A0 03
  - CONTEXT SPECIFIC 0
  - Length 3B
- 02 01 02
  - INTEGER: 2

# ASN.1 Editor

 CSCA\_CZE.crt



ASN.1 Editor - Opening File: CZE\_CSCA\_20090113.der

File View Tools Help

(0,1266) SEQUENCE

- (4,806) SEQUENCE
  - (8,3) CONTEXT SPECIFIC (0)
    - (13,1) INTEGER : '58'
    - (16,65) SEQUENCE
      - (83,87) SEQUENCE
        - (85,11) SET
          - (87,9) SEQUENCE
            - (89,3) OBJECT IDENTIFIER : countryName : '2.5.4.6'
            - (94,2) PRINTABLE STRING : 'CZ'
          - (98,23) SET
            - (100,21) SEQUENCE
              - (102,3) OBJECT IDENTIFIER : organizationName : '2.5.4.10'
              - (107,14) PRINTABLE STRING : 'Czech Republic'
            - (123,29) SET
              - (125,27) SEQUENCE
                - (127,3) OBJECT IDENTIFIER : organizationalUnitName : '2.5.4.11'
                - (132,20) PRINTABLE STRING : 'Ministry of Interior'
              - (154,16) SET
                - (156,14) SEQUENCE
                  - (158,3) OBJECT IDENTIFIER : commonName : '2.5.4.3'
                  - (163,7) T61 STRING : 'CSCA\_CZ'
      - (172,30) SEQUENCE
      - (204,87) SEQUENCE
      - (293,418) SEQUENCE
      - (715,97) CONTEXT SPECIFIC (3)
    - (814,65) SEQUENCE
      - (881,385) BIT STRING UnusedBits: 0 : '1B4BF9165526F44B40EA408AE79327AA67687EFEAFA2333DD2248FBFAFA836DA7DE9FE1771FA7C6994CD02347EDDB842A'

File Name: C:\Documents and Settings\Administrator\Plocha\PKI\CZE\_CSCA\_20090113.der Size: 1270 (bytes)

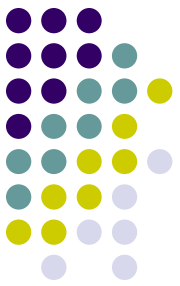


- To understand the structure (what is the meaning of particular fields) we need ASN.1 grammar

```

TBSCertList ::= SEQUENCE {
    version                Version OPTIONAL,
                        -- if present, MUST be v2
    signature              AlgorithmIdentifier,
    issuer                 Name,
    thisUpdate             Time,
    nextUpdate             Time OPTIONAL,
    revokedCertificates    SEQUENCE OF SEQUENCE {
        userCertificate    CertificateSerialNumber,
        revocationDate     Time,
        crlEntryExtensions Extensions OPTIONAL
                        -- if present, MUST be v2
    } OPTIONAL,
    crlExtensions         [0] EXPLICIT Extensions OPTIONAL
                        -- if present, MUST be v2
}

```



# ASN.1 – RSA keys

```
RSAPublicKey ::= SEQUENCE {  
    modulus          INTEGER,  -- n  
    publicExponent   INTEGER   -- e  
}  
  
--  
-- Representation of RSA private key with information for the CRT algorithm.  
--  
RSAPrivateKey ::= SEQUENCE {  
    version          Version,  
    modulus          INTEGER,  -- n  
    publicExponent   INTEGER,  -- e  
    privateExponent  INTEGER,  -- d  
    prime1           INTEGER,  -- p  
    prime2           INTEGER,  -- q  
    exponent1        INTEGER,  -- d mod (p-1)  
    exponent2        INTEGER,  -- d mod (q-1)  
    coefficient       INTEGER,  -- (inverse of q) mod p  
    otherPrimeInfos   OtherPrimeInfos OPTIONAL  
}
```

 RSA.key

Source:  
PKCS#1