Tipuri de date ASN.1

Tip de date	Categorie	Valoare	Semnificaţie
BOOLEAN	Primitive	0x01	Boolean: true/false
INTEGER	Primitive	0x02	Număr unsigned/signed
BIT STRING	Primitive	0x03	Vector de biţi
OCTET STRING	Primitive	0x04	Vector de bytes
NULL	Primitive	0x05	Valoare NULL
OBJECT IDENTIFIER	Primitive	0x06	Identificator: număr universal şi unic, algoritm, structură de date, obiect etc.
PrintableString	Primitive	0x13	Vector de caractere
T61String	Primitive	0x14	Vector de caractere T.61 (8 biţi)
IA5String	Primitive	0x16	Vector de caractere IA5 (ASCII)
UTCTime	Primitive	0x17	Greenwich Mean Time (GMT)
SEQUENCE	Build	0x30	Colecţie ordonată formată din unul sau mai multe tipuri de date
SEQUENCE OF	Build	0x10	Colecţie ordonată formată din zero sau mai multe tipuri de date
SET	Build	0x31	Colecţie neordonată formată din unul sau mai multe tipuri de date
SET OF	Build	0x11	Colecţie neordonată formată din zero sau mai multe tipuri de date

Structură certificat **SampleCert.cer**

Tag	Length	Value	ASN 1 Notation	Comments
30	82 02 12		SEQUENCE {	0x30: ASN 1 header, SEQUENCE (nivel 1) complexă 0x82: indicator pentru considerarea următorilor 2 bytes ca lungime 0x0212: lungime secvenţă 530 bytes
30	82 01 7B		SEQUENCE {	0x30: SEQUENCE (nivel 2) 0x82: indicator pentru considerarea următorilor 2 bytes ca lungime 0x017B: lungime 379 bytes; to be signed parts begin here
A0	03		[0] {	0x0A: tip enumerativ 0x03: lungime tip 3 bytes 0x02 0x01 0x02: conţinut tip
02	01	02	INTEGER 2 }	0x02: Atribut INTEGER (versiune) 0x01: lungime 1 byte 0x02: valoare atribut: versiune 3 pentru X 509 (se pleacă de la 0)
02	01	01	INTEGER 1	0x02: Atribut INTEGER (Serial Number) 0x01: lungime 1 byte 0x01: valoare atribut: SN 1
30	0D		SEQUENCE {	0x30: SEQUENCE (nivel 3) deschisă

				0x0D: lungime 13 bytes
06	09	2A 86 48 86-F7 0D 01 01 05	OBJECT IDENTIFIER rsaWithSha1 (1 2 840 113549 1 1 5)	0x06: OBJECT IDENTIFIER 0x09: lungime 9 bytes Identificator algoritm de semnare - sha1RSA = sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha1-with-rsa-signature(5)} For 840 from the OID the formula is 0x06*128 + 0x48 (form 0x86 0x48)= 768 + 72 = 840 0x06*2^14 + 0x77*2^7 + 0x0d*2^0 = 6*16384 + 119*128 + 13*1 = 98304 + 15232 + 13 = 113549
05	00		NULL }	0x05: NULL 0x00: lungime 0 bytes; SEQUENCE (nivel 3) este închisă
30	4F		SEQUENCE {	0x30: SEQUENCE (nivel 3) deschisă 0x4F: lungime SEQUENCE 79 bytes
31	0B		SET {	0x31: SET deschis 0x0B: lungime 11 bytes
30	09		SEQUENCE {	0x30: SEQUENCE (nivel 4) deschisă 0x09: lungime 9 bytes
06	03	55 04 06	OBJECT IDENTIFIER countryName (2 5 4 6)	0x06: OBJECT IDENTIFIER 0x03: lungime 3 bytes: 0x550406: countryName {joint-iso-itu-t(2) ds(5) attributeType(4) countryName(6)}
13	02	52 4F	PrintableString 'RO'	0x13: PrintableString 0x02: lungime 2 bytes 0x524F: valoare countryName = 'RO'
			} }	Închidere SET şi SEQUENCE (nivel 4)
31	0C		SET {	0x31: SET deschis 0x0C: lungime 12 bytes
30	0A		SEQUENCE {	0x30: SEQUENCE (nivel 4) deschis 0x0A: lungime secvenţă: 10 bytes
06	03	55 04 0A	OBJECT IDENTIFIER organizationName	0x06: OBJECT IDENTIFIER 0x03: lungime 3 bytes 0x55040A regulă formare organizationName
13	03	41 53 45	PrintableString ’ASE'	0x13: PrintableString 0x03: lungime 3 bytes 0x415345 organizationName = 'ASE' pentru organizaţia emitentă
			} }	Închidere SEQUENCE (nivel 4) (10 Bytes), închidere SET

31	1C		SET {	0x31: SET deschis 0x1C: lungime 28 bytes
30	1A		SEQUENCE {	0x30: SEQUENCE (nivel 4) deschis 0x1A: lungime 26 bytes
06	03	55 04 0B	OBJECT IDENTIFIER organizationUnitName	0x06: OBJECT IDENTIFIER 0x03: lungime 3 bytes 0x55040B regulă formare pentru organizationUnitName
13	13	49 54 43 20 53 65 63 75 72 69 74 79 20 4D 61 73 74 65 72	PrintableString 'ITC Security Master'	0x13: PrintableString 0x13: lungime 19 bytes 0x495443205365637572697479204D617746572: valoare 'ITC Security Master'
			} }	Închidere SEQUENCE (nivel 4), închidere SET
31	14		SET {	0x31: SET deschis 0x14: lungime 20 bytes
30	12		SEQUENCE {	0x30: SEQUENCE (nivel 4) deschis 0x12: lungime 18 bytes
06	03	55 04 03	OBJECT IDENTIFIER commonName	0x06: OBJECT IDENTIFIER 0x03: lungime 3 bytes 0x550403 regulă formare pentru commonName
13	0B	4D 61 72 69 75 73 20 50 6F 70 61	PrintableString 'Marius Popa'	0x13: PrintableString 0x0B: lungime 11 bytes 0x4D617269757320506F7061: valoare 'Marius Popa'
			} } }	Închidere SEQUENCE (nivel 4), închidere SET, închidere SEQUENCE (nivel 3)
30	1E		SEQUENCE {	0x30: SEQUENCE (nivel 3) deschis 0x1E: lungime 30 bytes
17	0D	31 31 31 32 31 36 30 39 32 38 35 38 5A	UTCTime '111216092858Z'	0x17: UTCTime 0x0D: lungime 13 bytes 0x313131323136303932383538 5A: valoare conform format YYMMDDHHmmSS, 16 Decembrie 2011, 09:28:58
17	0D	31 31 31 32 32 32 30 39 32 38 35 38 5A	UTCTime '111222092858Z'	0x17: UTCTime 0x0D: lungime 13 bytes 0x313131323232303932383538 5A: valoare conform format YYMMDDHHmmSS format, 22 Decembrie 2011, 09:28:58
			}	Închidere SEQUENCE (nivel 3)
30	4F		SEQUENCE {	0x30: SEQUENCE (nivel 3) deschisă 0x4F: lungime SEQUENCE 79 bytes
31	0B		SET {	0x31: SET deschis 0x0B: lungime 11 bytes
30	09		SEQUENCE {	0x30: SEQUENCE (nivel 4) deschisă 0x09: lungime 9 bytes
06	03	55 04 06	OBJECT IDENTIFIER	0x06: OBJECT IDENTIFIER 0x03: lungime 3 bytes:

			countryNam e (2 5 4 6)	0x550406: countryName {joint-iso-itu-t(2) ds(5) attributeType(4) countryName(6)}
13	02	52 4F	PrintableStri ng 'RO'	0x13: PrintableString 0x02: lungime 2 bytes 0x524F: valoare countryName = 'RO'
			} }	Închidere SET şi SEQUENCE (nivel4)
31	0C		SET {	0x31: SET deschis 0x0C: lungime 12 bytes
30	0A		SEQUENCE {	0x30: SEQUENCE (nivel 4) deschis 0x0A: lungime secvenţă: 10 bytes
06	03	55 04 0A	OBJECT IDENTIFIER commonNa me	0x06: OBJECT IDENTIFIER 0x03: lungime 3 bytes 0x55040A regulă formare commonName
13	03	41 53 45	PrintableStri ng ’ASE'	0x13: PrintableString 0x03: lungime 3 bytes 0x415345 commonName = 'ASE' pentru organizaţia emitentă
			} }	Închidere SEQUENCE (nivel 4) (10 Bytes), închidere SET
31	1C		SET {	0x31: SET deschis 0x1C: lungime 28 bytes
30	1A		SEQUENCE {	0x30: SEQUENCE (nivel 4) deschis 0x1A: lungime 26 bytes
06	03	55 04 0B	OBJECT IDENTIFIER organization UnitName	0x06: OBJECT IDENTIFIER 0x03: lungime 3 bytes 0x55040B regulă formare pentru organizationUnitName
13	13	49 54 43 20 53 65 63 75 72 69 74 79 20 4D 61 73 74 65 72	PrintableStri ng ’ITC Security Master'	0x13: PrintableString 0x13: lungime 19 bytes 0x49544320536563757269747920 4D617346572: valoare ’ITC Security Master'
			} }	Închidere SEQUENCE (nivel 4), închidere SET
31	14		SET {	0x31: SET deschis 0x14: lungime 20 bytes
30	12		SEQUENCE {	0x30: SEQUENCE (nivel 4) deschis 0x12: lungime 18 bytes
06	03	55 04 03	OBJECT IDENTIFIER commonNa me	0x06: OBJECT IDENTIFIER 0x03: lungime 3 bytes 0x550403 regulă formare pentru commonName
13	0B	4D 61 72 69 75 73 20 50 6F 70 61	PrintableStri ng ’Marius Popa'	0x13: PrintableString 0x0B: lungime 11 bytes 0x4D617269757320506F7061: valoare ’Marius Popa’
			} } }	Închidere SEQUENCE (nivel 4), închidere SET, închidere SEQUENCE (nivel 3)

30	81 9F		SEQUENCE {	0x30: SEQUENCE (nivel 3) 0x81: indicator pentru considerarea următorului byte ca lungime (cel mai semnificativ bit din lungime este setat) 0x9F: lungime 159 bytes
30	0D		SEQUENCE {	0x30: SEQUENCE (nivel 4) 0x0D: lungime 13 bytes
06	09	2A 86 48 86 F7 0D 01 01 01	OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)	0x06: OBJECT IDENTIFIER 0x09: lungime 9 bytes 0x2A864886F70D010101: rsaEncryption ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
05	00		NULL }	0x05: Element NULL 0x00: lungime 0 bytes
			}	Închidere SEQUENCE (nivel 4)
03	81 8D	00 30 81 89 02 81 81 00 F5 70 CA D3 C8 1A 54 89 81 82 D1 B1 85 EC 21 A9 B0 8E 61 20 73 10 7B 7D 84 A9 88 9D 50 90 D8 D1 37 D3 4B B7 99 C1 9C EB CD6E BA A2 2E D2 F9 46 29 86 B3 67 DC 84 B0 E4 97 E2 88 F0 C2 84 89 F4 E3 81 1B 9C 0E 47 9B 34 64 9E 5B 8C 3F D2 39 53 46 D1 C5 24 9F DB 11 79 FE F3 46 5E 78 81 F9 7F F5 D8 90 EA A8 BA 18 30 30 B9 5F D4 B5 5C 14 3E 57 58 A5 72 F4 2A D3 55 97 EB D1 86 69 CA CC 63 02 03 00 FF FF	BIT STRING 0 unused bits, encapsulates {	0x03: BIT STRING (cheie public RSA) 0x81: indicator pentru considerarea următorului byte ca lungime (cel mai semnificativ bit din lungime este setat) 0x8D: lungime 141 bytes 0x30: al 2-lea byte - SEQUENCE

			} }	Închidere SEQUENCE (nivel 3) şi SEQUENCE (nivel 2)
30	0D		SEQUENCE {	0x30: SEQUENCE deschis (nivel 2) 0x0D: lungime 13 bytes
06	09	2A 86 48 86 F7 0d 01 01 05	OBJECT IDENTIFIER rsaWithSha1 (1 2 840 113549 1 1 5)	0x06: OBJECT IDENTIFIER 0x09: lungime 9 bytes 0x2a 86 48 86 f7 0d 01 01 05: identificato algoritm semnătură sha1RSA = sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha1-with-rsa-signature(5)}
05	00		NULL }	0x05: Element NULL 0x00: lungime 0 bytes
			}	Închidere SEQUENCE (nivel 2)
03	81 81	00 E5 F3 74 09 C6 53 A0 F8 EE 10 EF EA 47 1D 9C 65 20 16 9B BE CA A7 C8 76 50 83 20 58 25 71 1C 2E B8 03 7D BB 9D F8 CE 56 3C DF 1E 2C 73 50 28 C4 2C E0 33 E6 69 C4 CA F0 4C 63 5D EE 95 FC E7 76 E5 70 6D CC 92 DD BC C2 92 0A 39 CE 91 4D 37 8E C7 A3 F2 CB 32 C0 89 2D 09 8E 0C 07 F5 7E 3E 22 54 2B 89 8B 20 D4 FC FB 80 E7 2D 83 45 53 13 35 5A A9 C9 65 15 2A 69 B4 5E 34 87 6D 5A F0 7F 74	BIT STRING 0 unused bits, encapsulates {	0x03: BIT STRING (semnătură digitală Autoritate de Certificare) 0x81: indicator pentru considerarea următorului byte ca lungime (cel mai semnificativ bit din lungime este setat) 0x81: lungime 129 bytes
			}	Închidere SEQUENCE (nivel 1)

Sintaxa ASN.1 pentru certificat self-signed

SEQUENCE{

```
SEQUENCE{
        [0]{
                INTEGER 2
        }
INTEGER 1
SEQUENCE {
        OBJECT IDENTIFIER
                rsaWithSha1
        NULL
}
SEQUENCE{
        SET {
                SEQUENCE {
                        OBJECT IDENTIFIER
                                countryName
                                PrintableString ‘RO’
                }
        }
        SET {
                SEQUENCE {
                        OBJECT IDENTIFIER
                                organizationName
                                PrintableString ‘ASE’
                }
        }
        SET {
                SEQUENCE {
                        OBJECT IDENTIFIER
                                organizationUnitName
                                PrintableString ‘ITC Security Master’
                }
        }
        SET {
                SEQUENCE {
                        OBJECT IDENTIFIER
                                commonName
                                PrintableString ‘Marius Popa’
                }
        }
}
SEQUENCE {
   UTCTime ‘111216092858Z’
   UTCTime ‘111222092858Z’
 }
SEQUENCE{
        SET {
                SEQUENCE {
                        OBJECT IDENTIFIER
                                countryName
                                PrintableString ‘RO’
                }
        }
        SET {
                SEQUENCE {
                        OBJECT IDENTIFIER
                                organizationName
```

PrintableString ‘ASE’
}
}
SET {
SEQUENCE {
OBJECT IDENTIFIER
organizationUnitName
PrintableString ‘ITC Security Master’
}
}
SET {
SEQUENCE {
OBJECT IDENTIFIER
commonName
PrintableString ‘Marius Popa’
}
}
}

SEQUENCE {
SEQUENCE {
OBJECT IDENTIFIER rsaEncryption
NULL
}
BIT STRING 0 unused bits, encapsulates {**//cheie publică**}
SEQUENCE {
OBJECT IDENTIFIER rsaWithSha1 (1.2.840.113549.1.1.5)
NULL
}
BIT STRING 0 unused bits, encapsulates {**//semnătură AC**}
}
}