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 și
			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	Colecție ordonată formată din unul
			sau mai multe tipuri de date
SEQUENCE OF	Build	0x10	Colecție ordonată formată din zero
			sau mai multe tipuri de date
SET	Build	0x31	Colecție neordonată formată din
			unul sau mai multe tipuri de date
SET OF	Build	0x11	Colecție neordonată formată din
			zero sau mai multe tipuri de date

Structură certificat SampleCert.cer

Tag	Length	Value	ASN 1	Comments
			Notation	
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	OBJECT	0x06: OBJECT IDENTIFIER
		86-F7 0D 01	IDENTIFIER	0x09: lungime 9 bytes
		01 05	rsaWithSha1	
		02.00	(1 2 840	Identificator algoritm de semnare -
			113549 1 1	sha1RSA = sha-1WithRSAEncryption
			5)	Sharkov Sha Ittiento Line yption
			3,	OBJECT IDENTIFIER ::= {iso(1) member-
				body(2) us(840) rsadsi(113549) pkcs(1)
				pkcs-1(1) sha1-with-rsa-signature(5)}
				pres 1(1) shall with 13a signature(5))
				For 840 from the OID the formula is
				0x06*128 + 0x48 (form 0x86 0x48)= 768 +
				72 = 840
				72 - 040
				0x06*2^14 + 0x77*2^7 + 0x0d*2^0 =
				6*16384 + 119*128 + 13*1 = 98304 +
				15232 + 13 = 113549
				15252 + 15 - 115549
05	00		NULL	0x05: NULL
			}	0x00: lungime 0 bytes;
			,	SEQUENCE (nivel 3) este închisă
30	4F		SEQUENCE {	0x30: SEQUENCE (nivel 3) deschisă
30	"		32021102 (0x4F: lungime SEQUENCE 79 bytes
31	ОВ		SET {	0x31: SET deschis
01	05		02. (0x0B: lungime 11 bytes
30	09		SEQUENCE {	0x30: SEQUENCE (nivel 4) deschisă
			(0x09: lungime 9 bytes
06	03	55 04 06	OBJECT	0x06: OBJECT IDENTIFIER
			IDENTIFIER	0x03: lungime 3 bytes:
			countryNam	0x550406: countryName {joint-iso-itu-t(2)
			e (2 5 4 6)	ds(5) attributeType(4) countryName(6)}
13	02	52 4F	PrintableStri	0x13: PrintableString
			ng 'RO'	0x02: lungime 2 bytes
				0x524F: valoare countryName = 'RO'
			}	Închidere SET și SEQUENCE (nivel 4)
			;	, ===== (,
31	0C		SET {	0x31: SET deschis
-				0x0C: lungime 12 bytes
30	0A		SEQUENCE {	0x30: SEQUENCE (nivel 4) deschis
				0x0A: lungime secvență: 10 bytes
06	03	55 04 0A	OBJECT	0x06: OBJECT IDENTIFIER
			IDENTIFIER	0x03: lungime 3 bytes
			organization	0x55040A regulă formare
			Name	organizationName
13	03	41 53 45	PrintableStri	0x13: PrintableString
	"	1 - 23 .3	ng 'ASE'	0x03: lungime 3 bytes
			1.0 1.02	0x415345 organizationName = 'ASE' pentru
				organizația emitentă
			}	Închidere SEQUENCE (nivel 4) (10 Bytes),
			}	inchidere SET
			J	mondere of i

31	1C		SET {	0x31: SET deschis
			(0x1C: lungime 28 bytes
30	1A		SEQUENCE {	0x30: SEQUENCE (nivel 4) deschis
			0 0 0 0 0 0 0 0	0x1A: lungime 26 bytes
06	03	55 04 0B	OBJECT	0x06: OBJECT IDENTIFIER
			IDENTIFIER	0x03: lungime 3 bytes
			organization	0x55040B regulă formare pentru
			UnitName	organizationUnitName
13	13	49 54 43 20	PrintableStri	0x13: PrintableString
		53 65 63 75	ng 'ITC	0x13: lungime 19 bytes
		72 69 74 79	Security	0x495443205365637572697479204D6177
		20 4D 61 73	Master [']	46572: valoare 'ITC Security Master'
		74 65 72		
			}	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	0x06: OBJECT IDENTIFIER
			IDENTIFIER	0x03: lungime 3 bytes
			commonNa	0x550403 regulă formare pentru
			me	commonName
13	OB	4D 61 72 69	PrintableStri	0x13: PrintableString
		75 73 20 50	ng 'Marius	0x0B: lungime 11 bytes
		6F 70 61	Popa'	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	UTCTime	0x17: UTCTime
		31 36 30 39	'11121609285	0x0D: lungime 13 bytes
		32 38 35 38	8Z'	0x3131313231363039323835385A: valoare
		5A		conform format YYMMDDHHmmSS, 16 Decembrie 2011, 09:28:58
17	0D	31 31 31 32	UTCTime	0x17: UTCTime
17	OD	32 32 30 39	'11122209285	0x0D: lungime 13 bytes
		32 38 35 38	8Z'	0x3131313232323039323835385A: valoare
		5A		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	OB		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	0x06: OBJECT IDENTIFIER
			IDENTIFIER	0x03: lungime 3 bytes:

			countryNam	0x550406: countryName {joint-iso-itu-t(2)
			e (2 5 4 6)	ds(5) attributeType(4) countryName(6)}
13	02	52 4F	PrintableStri	0x13: PrintableString
13	02	32 41	ng 'RO'	0x02: lungime 2 bytes
			ing ito	0x524F: valoare countryName = 'RO'
			}	Închidere SET și SEQUENCE (nivel4)
			}	memacre ser gr sequence (mver4)
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	0x06: OBJECT IDENTIFIER
			IDENTIFIER	0x03: lungime 3 bytes
			commonNa	0x55040A regulă formare commonName
			me	
13	03	41 53 45	PrintableStri	0x13: PrintableString
			ng 'ASE'	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	0x06: OBJECT IDENTIFIER
			IDENTIFIER	0x03: lungime 3 bytes
			organization	0x55040B regulă formare pentru
			UnitName	organizationUnitName
13	13	49 54 43 20	PrintableStri	0x13: PrintableString
		53 65 63 75	ng 'ITC	0x13: lungime 19 bytes
		72 69 74 79	Security	0x495443205365637572697479204D6177
		20 4D 61 73	Master'	46572: valoare 'ITC Security Master'
		74 65 72	1	Înskidana CEOUENCE (nivel 4) înskidana
			}	Închidere SEQUENCE (nivel 4), închidere SET
31	14		SET {	0x31: SET deschis
31	14		JLI (0x14: lungime 20 bytes
30	12		SEQUENCE {	0x30: SEQUENCE (nivel 4) deschis
30	12		JEQUEINCE (0x12: lungime 18 bytes
06	03	55 04 03	OBJECT	0x06: OBJECT IDENTIFIER
		33 04 03	IDENTIFIER	0x03: lungime 3 bytes
			commonNa	0x550403 regulă formare pentru
			me	commonName
13	OB	4D 61 72 69	PrintableStri	0x13: PrintableString
-		75 73 20 50	ng 'Marius	0x0B: lungime 11 bytes
		6F 70 61	Popa'	0x4D617269757320506F7061: valoare
			- 1	'Marius Popa'
			}	Închidere SEQUENCE (nivel 4), închidere
			}	SET, închidere SEQUENCE (nivel 3)
			}	
<u> </u>	1	I .	1 -	II.

SEQUENCE	30	81 9F	T	SEUTIENCE (Ov20: SECHENCE (sixel 2)
SEQUENCE Ox30: SEQUENCE (invel 4)	30	81 9F		SEQUENCE {	
SEQUENCE SEQUENCE Semificativ bit din lungime este setat)					<u> </u>
SEQUENCE 0x9F: lungime 159 bytes					
SEQUENCE Ox30: SEQUENCE (nivel 4)					
Ox00: lungime 13 bytes Ox00: lungime 13 bytes					·
06	30	0D		SEQUENCE {	. ,
F7 0D 01 01 O1 01 01 01 01 01 01 01 01 01 01 01 01 01					
01	06	09			
12 840					,
113549 1 1 1) pkcs(1) pkcs-1(1) rsaEncryption(1)			01		
NULL NOXO: Element NULL NOXO: Ungime 0 bytes				,	
Section Sect				113549 1 1 1)	pkcs(1) pkcs-1(1) rsaEncryption(1)}
Section Sect	05	00		NULL	0x05: Flement NULL
Standard				}	
03 81 8D 00 30 81 89 02 81 81 00 00 30 81 89 02 81 81 00 00 81 81 00 00 81 81 00 00 81 81 00 00 81 81 00 00 81 81 00 00 81 1 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 0x30: al 2-lea byte -				}	
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 D8 11 79 FE F3 46 5E 78 81 F9 7F F5 D8 90 EA A8 BA 18 30 30 89 5F D4 B5 5C 14 3E 57 58 A5 72 F4 2A D3 55 97 EB D1 86 66 9C AC CC 63 02 30 00 FF	03	81 8D	00 30 81 89	BIT STRING 0	, ,
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 80 E4 97 E2 88 F0 C2 84 89 F4 E3 81 1B 9C 0E 47 9B 34 66 9E 5B 8C 3F D2 39 53 46 D1 C5 24 9F DB 11 79 EE F3 46 5E 78 81 F9 7F F5 D8 90 EA A8 BA 18 30 30 89 5F D4 B5 5C 14 3E 57 58 A5 72 F4 2A D3 55 97 EB D1 86 69 CA CC 63 02 30 00 FF					
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 94 55 B 8C 3F D2 39 53 46 D1 C5 24 9F D8 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				encapsulates {	•
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 48 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 D8 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					, , ,
85 EC 21 A9 B0 8E 61 20 73 10 7B 7D 84 A9 88 9D 50 90 D8 D1 37 D3 48 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					
B0 8E 61 20 73 10 78 7D 84 A9 88 9D 50 90 BD 11 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 18 9C 0E 47 98 34 64 9E 58 8C 3F D2 39 53 46 D1 CS 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					
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 CC 2 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					
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					
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					
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					
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					
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					
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					
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					
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					
97 E2 88 F0 C2 84 89 F4 E3 81 1B 9C OE 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 O2 03 00 FF					
C2 84 89 F4 E3 81 1B 9C OE 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 O2 03 00 FF					
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					
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					
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					
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					
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					
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					
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					
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					
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					
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					
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					
B5 5C 14 3E 57 58 A5 72 F4 2A D3 55 97 EB D1 86 69 CA CC 63 02 03 00 FF					
57 58 A5 72 F4 2A D3 55 97 EB D1 86 69 CA CC 63 02 03 00 FF					
F4 2A D3 55 97 EB D1 86 69 CA CC 63 02 03 00 FF					
97 EB D1 86 69 CA CC 63 02 03 00 FF					
69 CA CC 63 02 03 00 FF					
02 03 00 FF			97 EB D1 86		
			69 CA CC 63		
FF			02 03 00 FF		
			FF		

			}	Închidere SEQUENCE (nivel 3) și SEQUENCE
			}	(nivel 2)
30	0D		SEQUENCE {	0x30: SEQUENCE deschis (nivel 2)
				0x0D: lungime 13 bytes
06	09	2A 86 48 86	OBJECT	0x06: OBJECT IDENTIFIER
		F7 Od 01 01	IDENTIFIER	0x09: lungime 9 bytes
		05	rsaWithSha1	0x2a 86 48 86 f7 0d 01 01 05: identificato
			(1 2 840 113549 1 1 5)	algoritm semnătură sha1RSA = sha-
			113343 1 1 3)	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	BIT STRING 0	0x03: BIT STRING (semnătură digitală
		09 C6 53 A0	unused bits,	Autoritate de Certificare)
		F8 EE 10 EF	encapsulates {	0x81: indicator pentru considerarea
		EA 47 1D 9C		următorului byte ca lungime (cel mai
		65 20 16 9B		semnificativ bit din lungime este setat)
		BE CA A7 C8		0x81: lungime 129 bytes
		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		
			}	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}
         }
}
```