ASN.1 Serialization for oneM2M Introduction

Andreas Kraft, Deutsche Telekom

Introduction

Abstract Syntax Notation One

Description language to define data structures.

Serialization is defined in a platform and transport technology independet way.

Distinguish between:

ASN.1 Description

Human & machine readable data structure specification. X.208/X.680

ASN.1 Encoding Rules

Serialization of data and data structures. X.209/X.680

Encoding Rules

Basic Encoding Rules (BER)
The encoding of data generally follows the TLV[1] principle and consists of four components:

- Identifier octets / Type
- Length octets
- Contents octets (optional, depends on type)
- End-of-contents octets (optional, only used when length is "indefinite")

Distinguished Encoding Rules (DER)
Based on and backward compatible to BER, but no encoding ambiguities.

Packed Encoding Rules (PER)
Much more compact encoding. Uses the ASN.1 structure, defined data type boundaries & length, bit-aligned encodings etc. to represent the data units using the minimum number of bits.

[1] Tag, Length, Value

Data Types

Simple Types	Structured Types	Other Types
BIT STRING - arbitrary string of bits	SEQUENCE - ordered collection of 1..n types	CHOICE - union of 1..n alternatives
IA5String - arbitrary string of IA5 (ASCII) characters	SEQUENCE OF - ordered collection of 0..n occurrences of a given type	ANY - arbitrary value of an arbitrary type
INTEGER - arbitrary integer	SET - unordered collection of 1..n types	
NULL - null value	SET OF - unordered collection of 0..n occurrences of a given type	
OBJECT IDENTIFIER - object identifier, which is a sequence of integer components that identify an object		
OCTET STRING - arbitrary string of octets (eight-bit values)		
PrintableString - arbitrary string of printable characters.		
UTCTime - "coordinated universal time" or Greenwich Mean Time (GMT) value		
BOOLEAN - boolean value		
REAL - float value		
UTF8String - variable width character encoding		

...

Encoding - Identifier Octets

Octet 1								Octet 2 onwards							
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1
Tag class		P/C	Tag number (0–30)					N/A							
			31					More	Tag number						

Class	Value	Description
Universal	0	The type is native to ASN.1
Application	1	The type is only valid for one specific application
Context-specific	2	Meaning of this type depends on the context (such as within a sequence, set or choice)
Private	3	Defined in private specifications

P/C	Value	Description
Primitive (P)	0	The contents octets directly encode the element value.
Constructed (C)	1	The contents octets contain 0, 1, or more element encodings.

Source https://en.wikipedia.org/wiki/X.690

Encoding - Length Octets

First length octet

Form	Bits							
	8	7	6	5	4	3	2	1
Definite, short	0	Length (0–127)						
Indefinite	1	0						
Definite, long	1	Number of following octets (1–126)						
Reserved	1	127						

Long form example, length 435

Octet 1								Octet 2								Octet 3							
1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	1	1
Long form	2 length octets							435 content octets															

For indefinite length, two **End-of-contents octets** are appended to indicate the end of the structure encoding : **0x00 0x00**

Source https://en.wikipedia.org/wiki/X.690

Example - Encoding

From X.500: A name is a sequence of X.500 relative distinguished names (RDNs).
As ASN.1 description and in DER encoding.

```
Name ::= SEQUENCE OF RelativeDistinguishedName
RelativeDistinguishedName ::= SET OF AttributeTypeValue
AttributeTypeValue ::= SEQUENCE {
  type         OBJECT IDENTIFIER,
  value        ANY
}
```

```
1.     30 23                                  ; SEQUENCE (0x23 Bytes)
2.     |  |  31 0f                               ; SET (0xf Bytes)
3.     |  |  |  30 0d                               ; SEQUENCE (0xd Bytes)
4.     |  |  |     06 03                               ; OBJECT_ID (0x3 Bytes)
5.     |  |  |     |  55 04 03                            ; 2.5.4.3 Common Name (CN)
6.     |  |  |     13 06                               ; PRINTABLE_STRING (0x6 Bytes)
7.     |  |  |        54 65 73 74 43 4e                     ; "TestCN"
8.     |  |  31 10                               ; SET (0x10 Bytes)
9.     |  |     30 0e                               ; SEQUENCE (0xe Bytes)
10.    |  |        06 03                               ; OBJECT_ID (0x3 Bytes)
11.    |  |        |  55 04 0a                            ; 2.5.4.10 Organization (O)
12.    |  |        13 07                               ; PRINTABLE_STRING (0x7 Bytes)
13.    |  |           54 65 73 74 4f 72 67                  ; "TestOrg"
```

Source: https://docs.microsoft.com/en-us/windows/win32/seccertenroll/about-introduction-to-asn-1-syntax-and-encoding

Example - oneM2M

Possible ASN.1 description of oneM2M Battery resource.

```
Battery ::= SEQUENCE {
  mgmtResource          MgmtResource,
  batteryLevel          INTEGER (0..4294967295),
  batteryStatus         BatteryStatus,
  choice            [0] IMPLICIT CHOICE {
                          childResource     [0] IMPLICIT ChildResourceRef,
                          subscription      [1] IMPLICIT SEQUENCE OF Subscription
                        } OPTIONAL
}

BatteryStatus       ::= INTEGER

MgmtResource        ::= [...]
ChildResourceRef    ::= [...]
Subscription        ::= [...]
```

Helpful Links

Playground
https://asn1.io/asn1playground/

Tutorial
https://www.obj-sys.com/asn1tutorial/asn1only.html

Layman's Guide
http://luca.ntop.org/Teaching/Appunti/asn1.html

ASN.1 Complete (PDF)
https://www.oss.com/asn1/resources/books-whitepapers-pubs/larmouth-asn1-book.pdf

ITU-T - SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS, OSI networking and system aspects – Abstract Syntax Notation One (ASN.1)
https://www.itu.int/ITU-T/studygroups/com17/languages/X.691-0207.pdf