ASN.1 notes

Frank Braun

2019-06-05

Abstract Syntax Notation One (ASN.1) allows defining data structures that can be serialized and deserialized in a cross-platform way.

Basic Encoding Rules (BER) specify a self-describing and self-delimiting format for encoding ASN.1 data structures.

Distinguished Encoding Rules (DER) is a restricted variant of BER thas is unequivocal.

DER is a *tag-length-value* (TLV) encoding:

- tag (two forms):
  - *low-tag-number form*: One octet. Bits 8 and 7 specify the class, bit 6 has value 0 indicating that the encoding is primitive, and bits 5-1 give the tag number.
  - *high-tag-number form*: Two or more octets. First octet is as in low-tag-number form, except that bits 5-1 all have value 1 Second and following octets give the tag number, base 128, most significant digit first, with as few digits as possible, and with the bit 8 of each octet except the last set to 1. If bit 6 has value 1, it indicates that the encoding is constructed.
- length (two forms):
  - *Short form*: One octet. Bit 8 has value 0 and bits 7-1 give the length.
  - *Long form*: Two to 127 octets. Bit 8 of first octet has value 1 and bits 7-1 give the number of additional length octets. Second and following octets give the length, base 256, most significant digit first.
- value: actual value as byte array of defined length.

Class encodings:

```
universal:        bit 8 is 0, bit 7 is 0
application:      bit 8 is 0, bit 7 is 1
context-specific: bit 8 is 1, bit 7 is 0
private:          bit 8 is 1, bit 7 is 1
```

References

- Go asn1 package[1]
- A Layman's Guide to a Subset of ASN.1, BER, and DER[2]

[1] https://golang.org/pkg/encoding/asn1/
[2] http://luca.ntop.org/Teaching/Appunti/asn1.html