

Parser for Certificates

Term project

Gajdár Michal, 373872

Kollár Roman, 396030

Parser is based on ASN.1 grammar according to RFC 5280. ASN.1 stands for Abstract Syntax Notation 1. It is notation for describing abstract types and values. It is independent on HW or operating system. It defines different types. Simple as INTEGER, BIT STRING; structured types as SEQUENCE, SET and OID types (Object Identifier) - Sequence of integer components that identify an object.

DER (Distinguished Encoding Rules) is encoding rule consists of TLV values.

The program does not parse whole certificate, but just some (most) fields of it.

The restrictions are on some fields of certificate:

```
Time ::= CHOICE {  
    utcTime          UTCTime,  
    generalTime      GeneralizedTime }  
AlgorithmIdentifier ::= SEQUENCE {  
    algorithm          OBJECT IDENTIFIER,  
    parameters        ANY DEFINED BY algorithm OPTIONAL }  
Extension ::= SEQUENCE {  
    extnID            OBJECT IDENTIFIER,  
    critical          BOOLEAN DEFAULT FALSE,  
    extnValue         OCTET STRING }
```

The DirectoryString, id-ce-authorityKeyIdentifier, AuthorityKeyIdentifier, KeyIdentifier, id-ce-keyUsage, KeyUsage, id-ce-basicConstraints and BasicConstraints are also not supported by the parser.

RESULTS:

It was implemented in C language. Code consists almost 1 000 lines.

DIFICULTIES: To understand how Object Identifier is encoded.

TEST DATA: We tested on Facebook and Duolingo certificates.