

# Parsing certificates in DER format

Roman Kollar, Michal Gajdar

November 12, 2015

# Table of contents

Description

Implementation

# ASN.1

- ▶ ASN.1 = Abstract Syntax Notation One
- ▶ notation standard
- ▶ representing, encoding, transmitting..
- ▶ example:  
Foo ::= SEQUENCE {  
    number INTEGER,  
    text IA5String  
}

# DER

- ▶ subset of BER (= Basic Encoding Rules)
  - ▶ TLV format
- ▶ DER = Distinguished Encoding Rules
- ▶ described with ASN.1
- ▶ exactly one way to encode an ASN.1 value
- ▶ used for X.509 certificates

- ▶ subset of the standard implemented in C
- ▶ without public key parsing
- ▶ for each ASN.1 type check\* function