Free ASN.1:2008 compliance test suite

Yury Strozhevsky, http://www.strozhevsky.com

Free ASN.1:2008 compliance test suite, copyright (c) 2012 Yury Strozhevsky
www.strozhevsky.com

When you are working with ASN.1 data it is necessary to use an ASN.1 coder/decoder tool. Does not matter what it will be: ASN.1 compiler or a desktop application. You just need to be sure that all results from the tool you are using are absolutely correct. But from my own experience there is a situation when different tools can produce different results for standard ASN.1 encoded binary data. There are mistakes even in widely-spread ASN.1 applications which is the consequence from ASN.1 standard misunderstanding or problems during testing process.

In order to solve all the problems at once would be enough to make one thing: one "compliance test suite" for ASN.1 standard. But when have been digging into that I found there are no such "compliance suites", at least there are no free "compliance suites". By my info there are paid "compliance suites", but I have not found a free one. For the sake of helping all developers making free ASN.1 tools I would like to introduce truly free ASN.1:2008 compliance suite.

The aims of my compliance test suite are:

1. Provide tests set for all major ASN.1 types (in future I will cover all types);
2. Provide full set of uncommon situations during ASN.1 decoding/encoding;
3. Provide full set of error ASN.1 encoding and give an example how to handle it;
4. Provide an ability to everyone to participate in the compliance test suite development;

The compliance test suite consists of binary encoded ASN.1 BER files. In order to test any ASN.1 tool user must just decode the files with help from the tool and inspect the tool outcome. Expected outcome is described in my test suite, so user of the suite may easily check all differences between expected and tool outcome. Also I made a short description for each test from the suite - it will help an user of suite what they are testing. All the tests are valid ASN.1 BER encoded data and all the test data may exists in real life. Full archive with ASN.1 BER encoded tests (files "tc< number >.ber"), CompliXML files (files "transformed_< number >.xml", see bellow), iteratively encoded ASN.1 BER data (files "encoded_< number >.ber") and with full table of test's description (file "free_asn1_testsuite.pdf ") you can download by the link.

Initially when I had been creating the tests for the suite I used my previous experience and ASN.1 standard. But one question raised in my mind again and again - how to handle all the uncommon situation right and is it possible at all to handle it? In order to find an answers on the questions I made my own free ASN.1 BER encoder/decoder, which is 100% compliant to the test suite I am providing. All the source codes for the ASN.1 encoder/decoder (I named it COMPLI) you can use whatever you want (almost - the source code are under common BSD license). The COMPLI is only for testing purposes, also you can use the code as a source for templates for your own encoding/decoding tools.

At the beginning about some restrictions of the COMPLI:

1. Microsoft Window platform only;
2. Requires MSXML 6 installed;
3. The COMPLI is only for test purposes and also may be used as a source for templates of handling uncommon situations during encoding/decoding ASN.1 data;
4. There is no code optimization in COMPLI. I made it in order to provide better understanding of inside program structure;

Now about features of the COMPLI:

1. The program is a free ASN.1 BER encoder/decoder. Of course the COMPLI may encode/decoder DER and CER as well;
2. In addition COMPLI is working with BASE64-encoded BER data. Also I made my own XML format for detailed description of ASN.1 data - CompliXML (see bellow);
3. Encoding and decoding exist for all data types from latest ASN.1:2008;

4. Encoding and decoding are 100% matched all requirements of the test suite I made;
5. COMPLI is provided in source code under BSD license;
6. The code is C++ with object model programming;
7. The code of COMPLI was checked for bugs and memory leaks;
8. The code can be easily expanded;
9. The COMPLI has a batch mode of working - user may in one batch decode BER file and then encode the outcome in other format if it is needed. Configuration file for COMPLI is in XML format, XML schema for it can be downloaded via link;
10. The COMPLI has its special XML format named CompliXML. In the format all ASN.1 data types are described in each details, moreover the format provide ability to store warnings and errors from decoding/encoding process. XML schema for CompliXML can be downloaded via link;
11. The CompliXML format may be used as well as output, or input format. Hence COMPLI user may decode complex ASN.1 file, store outcome in CompliXML format, and the again encode it with help from COMPLI. User may also easily change a type in CompliXML file and then encode binary BER again (it may be necessary, for example, when user need to change BMP STRING ASN.1 type to PRINTABLE STRING type);

By developing of COMPLI I achieved the following aims:

1. Made free ASN.1 BER encoder/decoder;
2. Made a "test plant" for ASN.1 compliance suite I made;
3. Made a very detailed and flexible XML format describing ASN.1 data types;
4. Now it is possible to encode any ASN.1 BER binary files without any programming - you can only make a CompliXML file and encode it;
5. Made a source for templates of handling all uncommon situation of ASN.1 encoding/decoding;

The COMPLI is under development and I will expand functionality of the program. For the moment COMPLI can encode/decoder in and out of following formats:

1. BER (DER, CER);
2. BASE64-encoded BER (for example COMPLI is working with OpenSSL certificates);
3. CompliXML format;
4. XER will be added soon;

The test suite with test's description
All source codes for COMPLI
EXE file for COMPLI + all XSD schemas + COMPLI configuration file for the test suite