ASN.1: A Powerful Schema Notation for XML

Olivier DUBUISSON
ITU-T Q.12/17 (ASN.1) Rapporteur
Leader of the ITU-T ASN.1 Project
Olivier.Dubuisson@francetelecom.com
http://asn1.elibel.tm.fr
http://www.itu.int/itu-t/asn1/
Overview

▶ ASN.1 is a *schema* for encoded values:
  - Type definitions are based on the ITU-T Rec. X.680-series notation
  - Types describe the expected general structure of values
  - Each built-in type defines a class of distinct values
  - Constraints restrict a class and the validity of values

▶ Encoded values are binary or text:
  - Binary encodings based on ITU-T Rec. X.690 (BER, DER), X.691 (PER) or X.692 (ECN)
  - Text encoded as plain or markup values:
    -ASN.1 Value Notation: ITU-T Rec. X.680
    -XML Encoding Rules (XER, CXER): ITU-T Rec. X.693
    -XER Encoding Notation (XCN): ITU-T Rec. X.693 Amd. 1 (*draft*)
XML notation for ASN.1 values

AnyName ::= SEQUENCE {
    givenName     VisibleString,
    initial       VisibleString (SIZE (1)) OPTIONAL,
    familyName    VisibleString }

ChildInformation ::= SET {
    name          AnyName,
    dateOfBirth   INTEGER (1..MAX) } -- YYYYMMDD

hubert ::= <AnyName>
    <givenName> Hubert </givenName>
    <initial> L </initial>
    <familyName> Owen </familyName>
</AnyName>

lee ::= <ChildInformation>
    <name>
        <givenName> Lee </givenName>
        <familyName> Owen </familyName>
    </name>
    <dateOfBirth> 19501003 </dateOfBirth>
</ChildInformation>
As a rule...

Whenever possible, the identifier name is used as the default markup tag. Otherwise, the user defined type name is used:

```plaintext
Employee ::= SEQUENCE {
  -- type
  number INTEGER(0..MAX), -- identifier
  dateOfHire Date } -- identifier

<Employee>
  <number> 51 </number>
  <dateOfHire> 19710917 </dateOfHire>
</Employee>
```

But this can be changed with help of an XCN (XER Control Notation) module:

```plaintext
MyColoring XCN-DEFINITIONS ::= BEGIN
  PROCESS MyModule
    NAME Employee AS UNCAPITALIZED;
END
```

France Télécom R&D
XER benefits (1)

- The ASN.1 module is the Schema to validate data
- A single schema for all values:
  - Eliminates multiple schema mappings
  - ASN.1 is a mature, stable schema for XML markup
- Exploits the very real advantages of both techniques (win-win solution):
  1. Allows a closer integration of XML schema specification languages and of traditional tools for protocol implementation
  2. Displays (BER- or PER-encoded) ASN.1-data in an XML-browser
  3. ASN.1 applications can send and receive XML values
  4. Efficient (BER, PER, ECN) encoding for transmission:
     - XML has no associated encoding that is very efficient and error-proof
       (Binary XML: not so efficient, jeopardized evolution, interoperability problems)
  5. Canonical (DER, CXER) encoding for secure messages (encryption, digital signatures...):
     - XML doesn’t support an easy-to-use canonical encoding
- More information: http://asn1.elibel.tm.fr/xml
XER benefits (2)

ASN.1/XML Application

XML (+ XSL) HTML

Browser Application

Plain text

Compact binary encoding (PER, ECN)

Wireless Application

SDF Application
Using ASN.1 as a schema notation for XML (1)

Compare:

```asn1
LineItem ::= SEQUENCE {
  part-no    INTEGER,
  quantity   INTEGER }
```

with:

```xml
<xsd:complexType name="lineItem">
  <xsd:sequence>
    <xsd:element name="part-no" type="xsd:number"/>
    <xsd:element name="quantity" type="xsd:number"/>
  </xsd:sequence>
</xsd:complexType>
```

All information such as data types used, optional fields, and constraints must be carried in the schema in the transfer (as in XML) or understood one time only (as in ASN.1) and assumed for all subsequent transfers.

France Télécom R&D
Using ASN.1 as a schema notation for XML (2)

- ASN.1 provides a reliable and easy way to manage extensibility (the need for version 1 systems to be able to interwork with yet-to-be-defined version 2 systems) and versioning of schemas. This is done with help of extensibility markers “...” and version brackets “[[ ]]”: LineItem ::= SEQUENCE {
  part-no    INTEGER,
  quantity   INTEGER, -- version 0
  ...,
  [[1: code  NumericString,
     price REAL ]]  -- added in version 1 --}

- Including extensibility in version 0 of the ASN.1 schema allows an application (using any version of the ASN.1 schema) to communicate with another application (based on any other version of the ASN.1 schema). An XML Schema would reject an extended XML document while the ASN.1 schema would accept it.

- The exception handling “!” can also be specified in the ASN.1 schema, so that decoders can report when they receive unexpected data

France Télécom R&D
Using ASN.1 as a binary encoding for XML (1)

- No tree information is stored in the binary encoding.
- If a binary encoding was pointless, why would have areas like MPEG7 or WAP created their proprietary solution?
- On average the compression rate is better than tools like zip (see http://lists.xml.org/archives/xml-dev/200107/msg01248.html).
- High-throughput transaction processing systems, low-bandwidth communications and low-power processors with small memory are not generally places where complex compression algorithms are worthwhile.
- The application is not slowed down because there is no need to build a dictionary on the fly (the encoder&decoder have been generated once for all).
- Some people say that the major drawback is that a binary encoding is not readable (unless it is converted back to XML markup), however this is not necessary for many applications where most messages are never read by humans.
Using ASN.1 as a binary encoding for XML (2)

AnyName ::= SEQUENCE {
  givenName     VisibleString,
  initial       VisibleString (SIZE (1)) OPTIONAL,
  familyName    VisibleString }

hubert ::= <AnyName>
  <givenName> Hubert </givenName>
  <initial> L </initial>
  <familyName> Owen </familyName>
</AnyName>

- This value encodes in 19 bytes with BER, 14 bytes with PER.
- Using XML markup requires 96 bytes (85 bytes just for tags).
XER Control Notation (XCN)

Also called “coloring” (ITU-T Rec. X.693 Amd. 1, draft)

Overlook of the syntax:
MyColoringModule XCN-DEFINITIONS ::= 
BEGIN 
PROCESS MyASN1Module
  NAME ALL AS UNCAPITALIZED
  NAME ALL AS PREFIX “xyz”
  NAME Type1.field1 AS “fred”
  ATTRIBUTE attr1, attr2 IN Type2
  LIST Type3.seqOfInteger -- space-separated list
  TEXT Bool, Enum, BitString, Integer -- instead of <true/>...
  NAMESPACE Type4 AS “http://www.w3.org/2001/XMLSchema-instance”
    PREFIX “xsi”
    -- other properties available... --;
END

Tool vendors are free to define tool-specific directives (comments such as --<UNCAPITALIZED>--) that the tool could use to generate the XCN module

France Télécom R&D
ASN.1 encoding for XML documents

- Automatic translation (mapping) of XML Schemas into ASN.1 modules
- Compact (PER, ECN) or canonical (DER) encodings then available for data initially described in XML
- ITU-T Rec. X.694 | ISO/IEC 8825-5 (under work)
- Example of potential application domains:
  - WML (Wireless Markup Language)
  - HDML (Handheld Device Markup Language)
  - SyncML (Synchronization Markup Language)
  - VoiceXML
  - tML (telecommunications Markup Language)
  - …

- More information: [http://asn1.elibel.tm.fr/xml/#schema-mapping](http://asn1.elibel.tm.fr/xml/#schema-mapping)

France Télécom R&D
In a nutshell

- ASN.1 + XCN is as powerful and expressive as XSD (XML Schema Definition), but less verbose and much more readable.
- ASN.1 is a mature schema notation for XML. No schema mapping is needed.
- ASN.1/XER offers efficient binary encodings together with XML (+ XSL) display (or transfer if needed).
- There is a canonical variant of XER for secured transactions called CXER.
- ASN.1/XER should be in the picture for high-throughput transaction processing systems, low-bandwith communications and low-power processors with small memory where compression (zipping) cannot be the answer.
- An XER-decoder is just another name for an XML parser.
- ASN.1/XER tools are available ([http://asn1.elibel.tm.fr/links/#xml](http://asn1.elibel.tm.fr/links/#xml)).
Group says ASN.1 can field XML, save bandwidth (in EE Times, Aug. 9, 2001)

“As digital communications spreads from cell phones to wireless personal organizers and XML-powered informations appliances, [ASN.1] claims to have the interoperability ‘Rosetta stone’ in place.”

ASN.1 Markup Language (in The XML Cover Pages, Aug. 8, 2001)

“Work is also underway to allow messages described using XML to be converted to ASN.1, thereby circumventing the verbosity of XML encodings and allowing them to be encoded very compactly.”

ASN.1 and XML Messaging (in Dr. Dobb’s Journal, Jul. 17, 2001)

“It makes it possible for XML to go places that right now it just cannot go. Specifically, [the ASN.1 group] expects that cellphones, PDAs, and other constrained devices will want to use ASN.1 to transform XML messages into a bandwith-friendly for transmission.”

France Télécom R&D
Press releases (2)

  
  “The encodings created [...] will be specified in accordance with the ASN.1 schema definitions published in ANS X9.84:2000 ‘Biometrics Information Management and Security for The Financial Services Industry’.”

- Other press releases
Set of ASN.1 standards

**Candidate for withdraw in 2002:**

  *Not free*


**In-force:**

  *Free: [http://www.itu.int/itu-t/studygroups/com17/languages/](http://www.itu.int/itu-t/studygroups/com17/languages/)*

**The 2002 edition includes XML and will be approved Summer 2002:**
- Draft texts: [ftp://ties.itu.int](ftp://ties.itu.int) - login: asn1 - password: notation1

France Télécom R&D
For more information

- **ASN.1 website:** [http://asn1.elibel.tm.fr](http://asn1.elibel.tm.fr)
- **Presentation of ASN.1:**
- **Standards download:**
  [http://www.itu.int/itu-t/studygroups/com17/languages/](http://www.itu.int/itu-t/studygroups/com17/languages/)

- **ASN.1 - Communication Between Heterogeneous Systems**
  (Olivier Dubuisson, Morgan Kaufmann, 2001)

- **ASN.1 Complete**
  (John Larmouth, Morgan Kaufmann, 2000)
  free download: [http://www.oss.com/asn1/larmouth.html](http://www.oss.com/asn1/larmouth.html)
Some free tools

- OSS Nokalva syntax and semantics checker:

- France Telecom syntax checker and pretty-printer:
  - [http://asn1.elibel.tm.fr/asnp](http://asn1.elibel.tm.fr/asnp)

- XML Encoding Rules tools:
  - [http://asn1.elibel.tm.fr/links/#xml](http://asn1.elibel.tm.fr/links/#xml)

- Other tools:
  - [http://asn1.elibel.tm.fr/links/#tools](http://asn1.elibel.tm.fr/links/#tools)

- ITU-T ASN.1 module database:
  - [http://www.itu.int/itu-t/asn1/database](http://www.itu.int/itu-t/asn1/database)

- Object identifier (OID) repository:
  - [http://asn1.elibel.tm.fr/oid](http://asn1.elibel.tm.fr/oid)
ITU-T ASN.1 Project

- Promote ASN.1 to all ITU-T study groups and also to other standardization organizations (ISO, ETSI, ECMA, W3C, IETF…)
- Help users understand and write ASN.1 specifications
- Provide tools and ensure quality of the specifications to be published
- First actions:
  - Free ASN.1 module database: [http://www.itu.int/itu-t/asn1/database](http://www.itu.int/itu-t/asn1/database)
  - Object identifier (OID) repository: [http://asn1.elibel.tm.fr/oid](http://asn1.elibel.tm.fr/oid)
- Website: [http://www.itu.int/itu-t/asn1](http://www.itu.int/itu-t/asn1)

France Télécom R&D
ASN.1 Consortium

- Share resources and information
- Promote ASN.1 (towards newspaper and journals, companies, universities…)
- No standardization work

Three forums:
- Industry forum
- Standardization forum
- Academic forum

Website: [http://www asn1 org](http://www.asn1.org)