Registration Authorities for OID components

Prof John Larmouth

Larmouth Training & Protocol Design Services Ltd

ISO & ITU-T Rapporteur for ASN.1

j.larmouth@salford.ac.uk

Note, for best viewing, this presentation needs the Dom Casual, Brush Script, and Tw Cen MT fonts to be on your machine.

ASN.1 consortium

Protocols need to carry names!

- **Generic carrier protocols need names for their contents**

- **Directory (X.500) protocols need names for things they are trying to access**

- **E-mail (X.400) protocols need names for originator and recipient names**

ASN.1 consortium

Historical contributions to the naming problem

- One of the first attempts at a naming standard for data communication was X.121, used in X.25.

- 32-bit Ethernet name allocation was another important piece of standardisation.

- Network Service Access Point addresses in OSI (NSAP addresses) made an important contribution.

- ASN.1 definition of the Object Identifier Tree in about 1986 was a seminal contribution.

- UUID naming mechanisms developed in the 1990s introduced new concepts to naming.

ASN.1 consortium

Hierarchical v Central

- **I'm the Registration Authority, and that's it (the Monolithic Approach).**

- **I will do my bit, you can add to it (the Hierarchical Approach).**

- **Let's use as much as possible of existing naming (the Pragmatic Approach).**

- **Marriages, marriages, marriages.**

- **For example, ISO Biometrics work uses a centralised registration authority (Monolithic Approach), but has an Annex that formally defines its allocations as part of an ASN.1 OID (Hierachical Approach)**

ASN.1 consortium

Character versus binary naming

- Character versus binary protocols remains an area of contention – preferred naming often follows this decision.

- Current work on "Fast Web Services" in ITU-T can be stated as "binary encodings for Web Services exchanges"

- Fast Web Services may or may not gain acceptance against XML (character-based) encodings for Web Services, but it is a fight worth fighting! **Please fight!**

- Historically, ITU-T (CCITT before it) has backed both binary *and* character-based naming horses.

ASN.1 consortium

ASN.1 grasped the nettle

- **The easy bit:**
  - Combine the Hierarchical Approach and the Pragmatic approach
- **The hard bit:**
  - Long character strings versus obscure binary representations
- **A lot of blood was spilled in 1985.**
- **Went for binary!!!! (In the encoding, characters in the value notation – see later)**
- **OIDs are essentially binary encodings.**
- **Even when sent with XML they are things like 0.2.693.57. etc – encoded in characters, but it is still binary!**

ASN.1 consortium

Notation for OID values – human-readable

- **Early notation for OID values (allocations) looked like:**

   {iso standard 8571 *etc*}

- **SNMP started the rot: use simply a character representation of the encoding: 1.0.8571.*etc* for human consumption.**

- **The change from "ccitt" to "itu-t" in "joint-iso-ccitt" also caused problems.**

- **The numeric form is now accepted as valid notation.**

- **Names are now regarded as not normative.**

ASN.1 **consortium**

X.400 and X.500

- X.500 went for what became called "long-names" – character-based.

- X.400 used both forms! (Differed a bit in the 1984 vs. 1988 versions)

- Major fight on introduction of "short-names" into X.500 around 1988ish

- Accepted, but never really took off or implemented. Today, X.500 distinguished names are not considered "long" – compared, for example with Certificate Revocation Lists (CRLs).

ASN.1 consortium

Navigating the tree

- **X.500 also added the concept that a sub-arc might be identified by a pair of values (for example, organisational unit and location), rather than just by a single value.**

- **This is the principal difference (apart from character v binary representation) between the X.500 use of the RH-name tree concept and the ASN.1 use of the RH-name tree concept for the Object Identifier tree.**

ASN.1 **consortium**

Moving to the Web

- **Publication of naming allocations on the Web is increasingly common but adds cost for an RA.**

- **The ITU-T OID description database is an excellent example, with over 50,000 entries.**

- **OID repository: http://oid.elibel.tm.fr**

- **Automatic allocations (possibly using Fast Web Services protocols) reduces the cost of running an RA.**

- **First done by IANA for ASN.1 OID components for SNMP.**

ASN.1 consortium

ASN.1 Project and ITU-T support

- We live in interesting times!

- An immense amount done already on the module database and the OID registry.

- Suggestions for automatic machine access to ASN.1 modules from the database – Sun Microsystems involvement, tool vendor agreement to provide clients.

- Suggestions for automatic registration of UUID values for an OID component (see later).

ASN.1 consortium

Enough of history and futures – what of the NOW?

- **The revised X.660 and X.670 series Recommendations are just that – revisions.**

- **Incorporate amendments, update tables and lists, and improve editorial clarity.**

- **Don't bother to read them!**

ASN.1 consortium

What are these Recommendations?
(Yuck, he's getting serious – time to walk out to my main meeting!)

- Sorry folks, but one slide per Recommendation (could just be two or three for some!).

- I owe that to the authors that spent a lot of time on the original work.

- Walk out if you like, but this is the guts of the presentation.

ASN.1 consortium

General contents

- **(Sometimes) provides information on Registration Hierarchical name trees.**

- **Usually specifies procedures for the operation of a Registration Authority.**

- **Mainly defines procedures for allocation under a specific ASN.1 Object Identifier arc.**

- **Revision makes no real technical changes – incorporates amendments, changes CCITT to ITU-T, clarifies, etc.**

- **Makes UPU legitimate!**

ASN.1 consortium

X.660 (ISO/IEC 9834-1)

- **Title:** INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – PROCEDURES FOR THE OPERATION OF OSI REGISTRATION AUTHORITIES: GENERAL PROCEDURES

- **A bad title!** Still not quite settled!

- **This describes the RH-Name tree, and specifies general procedures for registration authorities in this area.**

- **These procedures are referenced from other parts of the series.**

ASN.1 consortium

No X.661 (ISO/IEC 9834-2)

- **FTAM Document type registration.**

- **Many registrations within the ISO profiles work.**

- **ISO work never supported by ITU-T.**

- **Will not be revised, and not of interest.**

ASN.1 consortium

X.662 (ISO/IEC 9834-3)

- **Title:** INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – PROCEDURES FOR THE OPERATION OF OSI REGISTRATION AUTHORITIES: REGISTRATION OF ASN.1 OBJECT IDENTIFIER ARCS FOR JOINT ISO AND ITU-T WORK

- **This is an important Recommendation**

- **Provides the Registration of areas of joint work with ITU-T and ISO.**

- **About 25 current allocations.**

- **ANSI remains the Registration Authority.**

- **Simple resolution from SG17 and SC6.**

ASN.1 consortium

No X.663 (ISO/IEC 9834-4)

- **VT profile registration.**

- **Many registrations within the ISO profiles work.**

- **ISO work never supported by ITU-T.**

- **Will not be revised, and not of interest.**

ASN.1 consortium

No X.664 (ISO/IEC 9834-5)

- **VT control object registration.**

- **Many registrations within the ISO profiles work.**

- **ISO work never supported by ITU-T.**

- **Will not be revised, and not of interest.**

ASN.1 consortium

X.665 (ISO/IEC 9834-6)

- **Title:** INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – PROCEDURES FOR THE OPERATION OF OSI REGISTRATION AUTHORITIES: APPLICATION PROCESSES AND APPLICATION ENTITIES

- **Joint with ISO.**

- **Will be formally revised, but defunct and not of interest.**

ASN.1 consortium

X.666 (ISO/IEC 9834-7)

- **Title:** INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – PROCEDURES FOR THE OPERATION OF OSI REGISTRATION AUTHORITIES: JOINT ISO AND ITU-T REGISTRATION OF INTERNATIONAL ORGANIZATIONS

- **This is one of two Recommendations for registration of International Organizations (see X.669 later).**

- **Registers international organisations under the ASN.1 joint ITU-T and ISO "international-organisation" arcs, but also defines X.500 and X.400 naming of International Organisations**

- **For X.400 it defines the PRMD and ADMD concepts.**

ASN.1 consortium

X.667 (ISO/IEC 9834-8)

- **Title:** INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – PROCEDURES FOR THE OPERATION OF OSI REGISTRATION AUTHORITIES: GENERATION AND REGISTRATION OF UNIVERSALLY UNIQUE IDENTIFIERS (UUIDS)

- This is an important new Recommendation, for approval at the March 2004 meeting of SG17.

- The history of UUID (GUID) work is worth several slides on its own!

- It involves Microsoft, IETF Draft RFCs and the Open Group.

ASN.1 consortium

Wow! A second slide!

- **UUIDs are extremely widely used, but with no standard specifying them!**

- **They are used in Bluetooth specifications and in ISO/IEC/JTC1/SC37 BioAPI and CBEFF specifications (probably many others).**

- **References in the ISO work rely on this Recommendation | International Standard**

ASN.1 consortium

And a third!

- **UUIDs are quite big – 16 octets.**

- **They can be self-allocated on a transient basis that guarantees uniqueness up to AD 3400, with allocations of up to 10 million per second.**

- **They can also be allocated for permanent identification.**

- **Registration is not required, but reduces probable uniqueness from 99% certain to 100% certain.**

- **Can be used as ASN.1 OID components.**

ASN.1 consortium

Not X.668 (Not ISO/IEC 9834-9)

- **The one that got away.**

- **Proposed as the RA Standard for Biometric Registration.**

- **X.600 series had a lot to offer, and much text from that series is being used.**

- **But decided to proceed with pure ISO/SC37 Standard, as a second part of CBEFF.**

- **Pity, but we tried!**

ASN.1 consortium

X.669

- **Title:** INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – PROCEDURES FOR THE OPERATION OF OSI REGISTRATION AUTHORITIES: ITU-T REGISTRATION OF INTERNATIONAL ORGANIZATIONS REGISTRATION

- This is one of two Recommendations for registration of International Organizations.

- This registers under the ITU-T arc to ITU-T Members.

- The other (X.666) registers organisations under the joint ISO/ITU-T arc.

- For totally historical reasons, this is quite different from X.666 text. X.666 is probably the more important and better text.

ASN.1 consortium

X.670

- **Title:** PROCEDURES FOR REGISTRATION AGENTS OPERATING ON BEHALF OF ORGANIZATIONS TO REGISTER ORGANIZATION NAMES SUBORDINATE TO COUNTRY NAMES.

- **This is a Recommendation for software to register International Organizations under multiple countries (see X.671).**

- **It is believed that neither this Recommendation nor X.671 has been implemented, and revision is a formality to ensure coherence of the series.**

ASN.1 consortium

X.671

- **Title:** PROCEDURES FOR A REGISTRATION AUTHORITY OPERATING ON BEHALF OF COUNTRIES TO REGISTER ORGANIZATION NAMES SUBORDINATE TO COUNTRY NAMES.

- **This is a Recommendation for the operation of a Registration Authority in a country to register International Organization names under that country name (see also X.670).**

- **It is believed that neither this Recommendation nor X.670 has been implemented, and revision is a formality to ensure coherence of the series.**

ASN.1 consortium

If you have lasted this far, you have been very patient

Good-bye!

The End

ASN.1 consortium