ISO/IEC JTC1/SGFS N1373

ISO/IEC JTC 1/SC 21 N

DATE: 22 May 1996

Original format Word 6.0

ISO/IEC JTC 1/SC 21

Open Systems Interconnection, Data Management and

Open Distributed Processing

Secretariat: U.S.A. (ANSI)

TITLE: Liaison statement - Progress on ASN.1 at Kansas City

SOURCE: ISO/IEC JTC 1/SC 21/WG 8/Presentation and ASN.1 Rapporteur Group

PROJECT:

STATUS: Rapporteur Group output

ACTION: Per SC21 Kansas resolution, this document is forwarded to ITU-T SG 7, SC6, SC18, SC22, SC24, SC27, SC29, SGFS, TC46, TC 184/SC5, Internet Society for information and comment.

DISTRIBUTION: P and L Members
Mr. P. Bartoli, Chmn JTC 1/21
Convener and Secretariat, JTC 1/21/8
Prof. J. Larmouth, Rapporteur for Presentation & ASN.1
Mr. B. Scott, Project Editor
Mr. H. Zhao, ITU-T SG 7

Address Reply to:
Secretariat ISO/IEC JTC 1/SC 21 - American National Standards Institute, 11 West 42nd Street, New York, NY 10036
Telephone: 212-642-4935; Facsimile: 212-398-0023; e-mail: jshildne@ansi.org or jshildneck@attmail.com

To: ISO ITU-T and known users of ASN.1

From: SC21 WG8 ASN.1 Rapporteur Group

Date: 23 May 1996

Progress on ASN.1 at Kansas City meeting

> **NOTE** — Most of the actions and recommendations listed below from the Kansas City meeting of the ASN.1 Rapporteur Group are subject to approval by ITU-T SG7.

1—Run-time parameters

The work on run-time parameters to enable further optimisation of the PER encodings is being issued for PDAM ballot out of Kansas City, and is expected to progress to DIS at the next annual meeting of SC21.

A number of groups have expressed a need for this function, and it would now be appropriate to use it in working drafts.

No major changes were made to the earlier draft.

This work enables parameters to be associated with any type, with their values passed with the encoding of the type in an instance of communication. Syntactically, the parameters are specified immediately in front of the type specification with the same syntax as is used for defining normal dummy parameters, they can then be passed as actual parameters to a parameterised type,, or used directly in constraints. When used in constraints, the PEr visibility of those constraints is not affected, and their use will produce much more compact encodings in cases where direct application of PER without their use would lead to repetitive transmission of the same variable information.

The purpose is to provide efficient transmission of tabular and other material. For full details and examples, see the CD text.

2—Formal model

The formal model work is also being issued for PDAM ballot out of Kansas City. This is unlikely to affect most people writing ASN.1, as the formal restrictions have general been drafted to provide maximum freedom to the ASN.1 user.

The document is mainly of interest to those writing ASN.1 support tools, removing ambiguities in the base text about what is legal ASN.1 in some abstruse cases.

3—Global parameters

In contrast to run-time parameters, the ASN.1 group has had no input from users of ASN.1 confirming their need for this feature, and in the interests of simplicity and readability for naive readers, it was agreed to abandon this work and to delete the sub-project.

4—Relaxation of rules on extensibility

A number of groups have made representations and liaison statements concerning their desire to be able to insert extension additions for sequence and set at a point in the root sequence or set other than at the end. (The only place currently permitted.)

The following agreements have been made, and are being balloted as a Draft Technical Corrigendum from the Kansas City meeting:

- There will be only ONE insertion point allowed for extension additions to any given SEQUENCE or SET, but this can be at any place within the SEQUENCE or SET.

- If there is a single ellipsis (...), then the insertion point is at the end. (This is all that is currently allowed).

- If there are a pair of ellipses, these mark the start and end of the insertion point. (If the second of the pair is at the end of the SEQUENCE or SET, this is redundant, but is permitted).

- For SEQUENCE, the actual transmission of the extension additions will occur at the point in the sequence where they have been inserted. For SET, the normal rules apply in BER, but for PER they are always transmitted at the end.

- For the purposes of automatic tagging, the extension additions are treated as if they were inserted at the end, not matter where in practice they are inserted.

- To mend an extensibility bug, it has been necessary to impose the following rule: if automatic tagging is in use, and the root does not contain an element which is textually tagged, then no element added as an extension addition can be textually tagged.

- It is also now permitted to group together a number of extensions inside a "version bracket". The version bracket starts with a pair of adjacent opening square brackets ([[) before the first extension addition of the version and ends with a pair of closing square braces (]]) before the comma or closing curly brace following the last extension addition of that version. Use of version brackets is not mandatory, but is recommended. In the case of PER, their use produces significant improvements in the size of the encoding (a single length field for the entire set of additions, rather than one for each addition).

Assuming that the Draft Technical Corrigendum ballot is one of approval, ASN.1 users can take advantage of these features immediately.

5—ASN.1 1990

The retention of ASN.1 1990 for a further year has been re-affirmed, but the ASN.1 group is recommending that it should be withdrawn on 31 August 1997.

6—Bug in EMBEDDED PDV and CHARACTER STRING encoding

Over the last three months there has been considerable discussion about a number of problems with these encodings due to interaction of the chaining technique used to reduce verbosity with particular implementation architectures, with the sorting of SET OF, and most seriously with the presence of these types in extension additions.

Solving these problems has unavoidably necessitated a change that affects the bits on the line for EMBEDDED PDV and CHARACTER STRING (for both BER and PER), and has removed the optimisation provided by the chaining mechanism.

A Draft Technical Corrigendum is being ballotted out of Kansas City, and should be available as a fully approved Technical Corrigendum by the middle of the summer. Where possible, it is recommended that specifications using these types and referring to ASN.1 (1994) should include a note drawing implementors attention to this technical corrigendum.

7—UTCTime in the year 2000

Concern has been expressed about the possible effects in the year 2000 of implementations of standards using UTCTime, as it only records the last two digits of the year.

The Directories group is recommending that for the purpose of sorting in an application, all UTCTime dates should be interpreted as in the range 1950 to 2050.

> **NOTE** — This in no way affects the rule in CER, DER, and canonical PER for sorting elements of a SET-OF, the sort in this case being based on the octets produced by an encoding, not on the semantics of UTCTime.)

The ASN.1 group is taking no action in the ASN.1 specification, but other groups using UTCTime may wish to consider whether they need to take any action. It may be desirable also to consider an eventual transition to GeneralizedTime where possible, as this carries a full four digits for the year.

8—UTCTime in DER and CER

The specification of a canonical encoding of UTCTime in DER and CER was overlooked. That specification (based on the specification for GeneralizedTime) is being ballotted as a Draft Technical Corrigendum out of Kansas City.

9—ASN.1/C++ API

Users of ASN.1 may wish to be aware that X/Open have now got a complete draft going through the approval process for an "ASN.1 API in C++". This consists of an extensive set of class and method specifications for a standardised mapping of ASN.1 into C++, and should in due course ensure that implementations of ASN.1-defined protocols are independent of the particular tool vendor chosen to provide their C++ mappings and their encode/decode routines. X/Open are being encouraged to submit this as a PAS for rapid processing to an ISO Standard, to ensure that any future changes to ASN.1 take account of and are incorporated in this API.

23 May 1996