Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14045
Date:	2009-07-28
Replaces:	
Document Type:	National Body Contribution
Document Title:	NB of UK's comments on 6N13999 Revised text of ISO/IEC 16512-2 FPDAM 1
Document Source:	NB of UK
Project Number:	
Document Status:	See also the revised document produced by NB of UK in 6N14046.
Action ID:	FYI
Due Date:	
No. of Pages:	6

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

UK review of the revised ISO/IEC 16512-2/FPDAM 1 text

1. General comments

The UK National Body of SC 6 supports the extensive improvements made to the original ISO/IEC 16512-2/FPDAM 1 text and welcomes the opportunity review the output text for consistency and editorial corrections as recorded in the SC 6 Tokyo resolution 6.7.8. At the request of the Project Editor we have based our comments on an updated draft (containing modifications agreed in the Tokyo meeting that were not included in N 13999) and not on the output document circulated for review.

Detailed comments are contained in Sections 2 – 4 of this document.

Section 2 of this review contains a UK response to proposed Disposition of Comments document in SC 6 N 14041 containing points that require further consideration. A major point concerns the UK ballot comment GB 12. The Project Editor's answers to two of the questions that were raised in this comment has led us to the conclusion that Table 18, SEC_NAME codes, in clause 12 is not required. These codes are not used elsewhere in the Amendment and that removal of this table will have no technical effect. Several consequent modifications will require to be made, however. Once the decision has been made there should be no difficulty in implementing these corrections. Other comments in Section 2 deal with the UK comments GB 13, 14 and 29.

Section 3 contains two proposed changes that were not contained in the original UK comments. One proposes a new sub-clause stating that the hexadecimal notation used in clause 11 (Message formats) and clause 12 (Parameters) should be introduced by a statement early on in the Amendment. This completes the specification rather than adding any technical change. The other change proposes deletion of the informative Annex F which has been overtaken by events.

Section 4 deals with general considerations related the consistency of the message format specifications. This is essential as it is necessary for a common understanding between the message originators and recipients if the protocol is to work properly. It will also sharpen up the specification. Consistency of figures is also required. This section also covers improvement of the English language usage in the specification and correction editorial and typographical errors.

The Appendix to these comments contains a mark-up text of the Amendment incorporating all the changes (apart from consistency of figures) raised above.

The UK notes that the Amendment is expected to subject to the ITU_T Alternative Approval Process from the ITU-T SC 11 meeting in Argentina, September 2009. We consider that all the above comments can be resolved at the SC 6/WG 7 meeting held in conjunction with the SG 11 meeting.

2. UK RESPONSE TO THE DISPOSITION OF COMMENTS ON ISO/IEC 16512-2/FPDAM 1 IN SC 6 N 14014

2.1 GB 12. SEC_NAME attributes

Table 12; Sub-clause 11.2.5.3, Table 18 and subsequent table numbers.

Comment GB 12 contained a number of questions relating to attributes in the SECAGREQ, SECLIST and SECAGANS messages, including items a) and b):

a) The values of the SEC_NAME attributes are the same as for the GK_NAME attributes but with the addition of the MEM_AUTH attribute. Is the choice of the MEM_AUTH required in this list of values? The use of MEM_AUTH is a mandatory part of secure RMCP-2 and it does not fit easily with the PREFER options of the SEC_NAME attributes.

   NOTE – This action will remove the anomaly that MEM_AUTH is coded 0x07 in the SEC_NAME and 0x01 in AUTH_NAME.

b) If MEM_AUTH is removed from the SEC_NAME values, could the SEC_NAME attribute be renamed as the GK_NAME attribute (the range of values will the same)? In this case, Table 18 could be removed from clause 12 and reference made to Table 23 [The Table numbers have been changed to those in the output text from the Tokyo meeting].

The response to these questions (which were related to the SECAGREQ message) in N 14014 agreed that MEM_AUTH was mandatory and that the PREFER parameter in the SEC_NAME control in the SECAGREQ message was not appropriate for the MEM_AUTH attribute. The response also stated that if MEM_AUTH was removed from the SEC_NAME attributes, the change of attribute name from SEC_NAME to GK_NAME would improve the consistency of the specification. No changes, however, have been made to the specification of the SEC_NAME specification in the review text for the SECAGREQ message in N 13999.

Table 12, Multicast security policy, contains a line item for SEC_NAME but there is no equivalent control in the SECLIST message, nor is there any specific mention of the use SEC_NAME (other than in Table 12) in clause 10, Protocol operation. The equivalent GK_NAME mechanism is mentioned in 10.2.4, Secure tree join, however. Consequently, we consider that the SEC_NAME line item could be removed from Table 12 without affecting the technical content of the Amendment.

We propose that the following changes be made to Amendment 1:

1. Delete SEC_NAME form Table 12.

2. Rename the SEC_MECH_CAPAB control in 11.2.5.3 (and also in Figure 110 and Table 16) to read GK_MECH_CAPAB control, and the SEC_NAME parameter to read GK_NAME parameter.

3. Delete Table 18, SEC_NAME codes. The codes in Table 18 are still retained in Tables 23 and 25 (GK_NAME codes and AUTH_NAME code).

4. Renumber all the subsequent tables following Table 18.

5. Change the references to the current tables 19 – 28 to tables 18 – 27 to align with the changes in item 4.

Comment GB 12 was part of the UK's vote of disapproval on ISO/IEC 16512-2/FPDAM 1 and **adoption of these changes will convert our vote to one of approval**.

2.2 Comment GB 14. AUTH_ATTRIBUTE code

Table 24. Meaning column.

We consider that our proposed wording (in the UK ballot response) for the Meaning column is a more definitive explanation of the AUTH_ATTRIBUTE and should replace the current wording.

Delete: 'Membership describes its authority is checked and defines its mechanism.'
Insert: 'Membership of the session is authenticated using the Membership Authentication procedure defined in Annex E'

2.3 Comment GB 14. AUTH_ATTRIBUTE code
Note to Table 24.

The following note to Table 24 (without the words 'in future revisions') was originally attached to Table 10 (now Table 12), 'Multicast security policy' in an interim draft of 2 June 2009:

> NOTE – If other authentication mechanisms could be applied on defined AUTH_ATTRIBUTE such as message, source or user, then the corresponding authentication mechanism will be defined as a new code by SM in future revisions.

A UK email response sent to the Tokyo meeting on 3 June 2009 stated

> The MEM_AUTH mechanism and the membership attribute form an important mandatory part of the specification. We cannot approve the note to Table 10 that indicates that the Session Manager can include codes for alternative types of authentication and authentication mechanisms.
> We would be willing to insert a note stating that further code values for AUTH_ATTRIBUTE and AUTH_NAME may be considered for inclusion in future revisions of the standard.

It is undesirable that a note should indicate that the Session Manager may be able to override the mandatory features of the standard. Any future changes can only be added by SC 6 and SG 11 in a future revision (corrigendum, amendment or new edition) of the standard. We are unwilling to accept any further comment to the current Table 24 than:

> 'NOTE – Further code values for AUTH_ATTRIBUTE and AUTH_NAME may be considered for inclusion in future revisions of the standard'

Even this wording means that there is a possibility that Annex E may be downgraded from a mandatory to an optional procedure, or even withdrawn. We would prefer to see this note deleted altogether.

2.4 GB 13. AUTH_NAME code
Table 25

We understand from N 14014 that our proposal to change the reference from 'See Annex E' to 'The procedure defined in Annex E' had been accepted. Rationale: The proposed wording will reference a normative annex to the standard and will be in closer alignment to similar references to ISO/IEC standards and IETF RFCs.

Replace the existing wording with the UK proposal in GB 13.

2.5 GB 29. Access control for RMAs
Sub-clause 10.1.5

1) DMAs are established prior to the subscription of RMAs and at this stage the SM will not have an ACL. Figure 96 indicates a random time before the creation of the ACL. Should 10.1.5 indicate that the DMA cannot request an ACL until after the session has been opened to RMAs?

2) We welcome the secretariat observation in N 14014 that the modified information is sent to DMA through HRSREQ and HRSANS messages periodically.

3) Is the rejection of an RMA that is not listed in the ACL an optional action for the DMA, or should it be mandatory? If the latter action is correct, the text should read 'A DMA shall reject an RMA ….'.

We propose the following replacement text:

> The SM creates an access control list (ACL) containing hashed MAID and HASHED_AUTH for each authenticated RMA in the current session. Figure 96 illustrates the ACL procedure. After the session has been opened to RMAs, a DMA may request an ACL from the SM using an HRSREQ message encrypted by Ks. The SM responds with an HRSANS message encrypted by Ks which contains the ACL. A DMA may update its ACL information through the periodic exchange of HRSREQ and HRSANS messages with the SM.

A DMA shall reject a request from an RMA to join the group if the ACL list does not contain the information for that RMA.

The sentence 'The DMA may have ACL of all the RMAs in the RMCP-2 session or of some of the RMAs in its own MM group' has not been included as its intention is not clear. Our proposed rewording above implies that the DMA retains and updates its own ACL information as received from the SM.

3. ADDITIONAL COMMENTS NOT RAISED IN THE UK BALLOT COMMENTS ON FPDAM 1

3.1 Hexadecimal notation

The hexadecimal notation is used throughout clauses 11 and 12 without any explanation. We propose that a new sub-clause is added to 9.1., Conventions, stating that these values are expressed in hexadecimal notation:

9.1.2 Hexadecimal notation

Code values for message parameters in clause 11 (Format of secure RMCP-2 messages) and clause 12 (Parameters) are expressed in hexadecimal notation, e.g 0x14 for 20 in decimal notation.

3.2 Annex F. Key management

Annex F is an informative annex has been present in the draft amendment for a very long time. Its terminology is not consistent with the definition of groups and regions in 9.5 and, although it states that three new keys are newly created, it only describes two keys – Ks and Kg. Presumably Kc is the third key and this is managed by the SMA.

The specification of keys in the main body of the amendment has undergone considerable redrafting since Annex F was added and it is doubtful whether this annex adds anything to the specification of the keys in the normative text. We consider that any attempt to improve Annex F would be a waste of time and that this annex should be deleted from Amendment 1.

4. COMMENTS ON THE REVIEW TEXT FOR ISO/IEC 16512-2/FPDAM 1

4.1 Specification of message formats**.**

It is important that this specification is done in a consistent manner with the same level of detail throughout clause 11. The successful exchange of messages relies on a common understanding between the originator and the recipient of the message.

We wish to emphasize the following points:

a) The phrases 'Message type' and 'control type' have been used for headings in the figures for messages and for headings for specific fields; elsewhere 'message' and 'control' are used on their own [this has been based on a decision on usage of these terms reached in Tokyo for Amendment 2];

b) The formal specifications for specific fields are expressed as complete sentences [this normally involves the addition of 'This field' to the existing text];

c) Where the content of a specific field has a fixed value, the actual value is included in the specification;

d) In all cases where a code value is specified in clause 12, this is referenced in the specification for the field in clause 11;

e) For length fields, the units are expressed as 'length in bytes';

f) Where the lengths of controls (or of specific parameters) are variable, the specification is expressed as 'This field shall be set to …' rather than 'This field denotes …' [this avoids duplication in trying to explain both the meaning and the value of the field];

g) Whenever there is a choice of values, they are expressed in the following form: 'Its value shall be set to one of the code values in Table aaa'. [this places the onus of setting the correct message format on the sender of the message;

h) The 'Control data' field has been rewritten to identify the valid controls for each message and to state any conditions that might apply to the use of these controls [there is little consistency of the treatment of this field in the existing text].

Example:

11.2.8.1 The format of the SECAGANS message is shown in Figure 125. The description of each field is as follows:

a) *Ver* – This field denotes the current version of RMCP. Its value shall be set to 0x04.

b) *NT* – This field denotes the message issuer's node type. Its value shall be set to one of SMA, DMA or RMA coded as in Table 14.

c) *Message Type* – This field denotes SECAGANS message. Its value shall be set to 0x23 (see Table 15)

d) *Length* – This field shall be set to the total length in bytes of the SECAGANS message including the control data.

e) *Session ID* – This field shall be set to the 64-bit value of the Session ID as defined in 7.1.1.

f) *MAID* – This field denotes the MAID of the SECAGANS originator. Its value shall be formatted as defined in 7.1.2.

g) *Control data* – The SEC_RETURN control specified in 11.2.8.2 is a mandatory part of the SECAGANS message.

4.2 Use of the terms 'code' and 'encoding/decoding'

In English the term 'code' is used to define the representation of the meaning, and the terms 'encoding/decoding' are used to describe the mechanism for converting plain text to code and vice-versa.

The correct usage for the code tables in clause 12 is to use the term 'code' rather than 'encode'. This usage is applied in character code standards and the three-letter codes for international airports.

The use of encryption/decryption in 10.2.7 and Figure 104 is correct.

4.3 Consistency of figures for message specification

It is important for the presentation of the Amendment that consistency is maintained in the style of the figures.

The style of figures 94 and 95 need to be consistent with Figures 96 and 97, etc, particularly with respect to the thickness of lines.

Similarly, the style of Figures 100 and 102 need to be consistent with Figures 101 and 103, particularly with respect to thickness of lines, fonts for the text and colouring.

Are the changes the responsibility of the Project Editor or the TSB editors?

The suffixes in Figure 104 are difficult to read and we suggest that this figure should be enlarged to cover the whole width of the text area.

4.4 Correct English

The English language text for the content of the specification has been rewritten to allow for correct usage of definite and indefinite articles (the, a, an), distinction between single and plural forms of nouns, use of appropriate words, etc.

4.5 Typographical errors

These mainly involve paragraph spacing and word spacing

4.6 Table and figure headings

These headings have been corrected to start with a capital letter and with the renaming words starting with lower case letters (except for words used with capital letters throughout the standard) in accordance with the requirements of the Guide for ITU-T and ISO/IEC JTC 1 cooperation