Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14014
Date:	2009-06-10
Replaces:	
Document Type:	Disposition of Comments
Document Title:	Disposition of Comments on ISO/IEC 16512-2:2008(ITU-T X.603.1) / Amendment 1, Simplex group applications – Security extensions
Document Source:	SC 6/WG 7 Tokyo meeting
Project Number:	
Document Status:	As per the SC 6 Tokyo resolution 6.7.8, the DoC is approved.
Action ID:	FYI
Due Date:	
No. of Pages:	44

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

6N14014

7TOK-25

Title: Disposition Report for ISO/IEC 16512-2:2008(ITU-T X.603.1) / Amendment 1

Source: ISO/IEC JTC 1/SC 6/WG 7 Meeting (Tokyo, June 2009)

Status: This document is a disposition report for UK comments, Draft Amendment 1 to ISO/IEC 16512-2:2008(ITU-T X.603.1) of June 2009 Tokyo ISO/IEC JTC 1/SC 6/WG 7 Meeting.

Template for comments and secretariat observations

Date: **March 2009**	Document: **ISO/IEC 16512-2/FPDAM 1**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

KR Responses for UK comments

GB 0	All		te	UK vote of disapproval The UK National Body submits a vote of disapproval on ISO/IEC 16512-2/FPDAM 1 based on the following comments: **GB 6 – 10** relating to the group attribute and open and closed groups; these are related comments that apply to different parts of the specification and they need to be considered together; **GB 11 – 17** relating to the SECAGREQ, SECLIST and SECAGANS messages. These comments ask a series of questions that need to be answered before the drafting of additional revised text; comments GB 13 -17 are related to the general comments in GB 11-12; Addition of the new paragraph in **GB 53** relating to the Membership Authentication procedure; the proposed text has been provided to link the specification of this procedure to ISO/IEC 9798-3:1993. Satisfactory resolution of these comments will convert the UK vote to one of approval.		**GB6-10** open and closed group parts are included -(Clause 3) additions of definitions 3.24 GP_ATTRIBUTE 3.25 Closed group 3. 26 Open group -(Clause 5) additions of admission of RMAs 10.1.1.4 Admission of RMAs to open groups 10.1.1.5 Admission of RMAs to closed groups - Table 21 is clarified in details for open and close group **GB11-17** solved. See belows in details **GB53** ‘‘The secure RMCP-2 membership authentication is based on the three pass authentication procedure in ISO/IEC 9798-3:1998.’ Is included in E.1

KR Responses for General UK comments

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
GB 1	-----		ge	<u>Synopsis</u> This Amendment is nearing publication stage. The FPDAM ballot is the last stage where technical change can be considered within ISO/IEC and this will be followed by ITU-T consent. The ITU-T draft will then be balloted as an FDIS (confirmation of approval of the text at which no technical changes can be considered) before publication.		
GB 2	All	All tables	ge, ed	<u>Table renumbering</u> The tables in the FPDAM are numbered from Table 1 onwards. The published Amendment will require that the table numbering follows on from the table numbering of the published standard. The last table in the published standard is Table 8. We propose that the tables in the Amendment are renumbered starting from Table 9 (see next column)	Table numbers in the FPDAM are in black and proposed temporary table numbers are in red. 1 9 2 10 3 11 4 12 5 13 6 14 7 15 8 16 9 17 10 18 11 19 12 20 13 21 14 22 15 23 16 24 17 25	**Accept** Table and Figure is renumbered aligned with Amd.2 - start from Table 11 - start from Figure 85
GB 3	All	All tables	ge, ed	<u>Conventions for table numbering</u> In order to avoid confusion, references to table numbers **in these comments** have the following form: Table ~~15~~ 23 where the figure in black with strikethrough is the figure number in the title of the table and the figure in red is the proposed table number in comment GB 2	This convention applies to the comments in this -ballot response and **not** to the text of the Amendment.	**Accept** Table and Figure is renumbered aligned with Amd.2 - start from Table 11 - start from Figure 85
GB 4	All		ge, ed	<u>Co-ordination of projects</u> The progression of this Amendment must be considered in conjunction with the recent/current ballots on ISO/IEC 16512-2/D.Cor 1 and	The UK National Body proposes that the Tokyo meeting should concentrate on aligning the references in the text to the proposed numbers (in red) in comment GB 2. No attempt should be made to altering the table numbers in FPDAM 1	**Accept** Table and Figure is renumbered aligned with Amd.2 - start from Table 11

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
				ISO/IEC 16512-2/PDAM 2. The Corrigendum adds two new code tables for node types and control data types which are essential for the operation of the standard. Amendment 2 adds or modifies several tables and figures to the base standard. The numbering of these tables and figures will affect the numbering of the tables and figures in Amendment 1. The SC 6 meeting in Montreux agreed to number the new tables in the Corrigendum with bis and ter suffixes in an attempt to overcome the numbering problem. We now consider that it highly unlikely the ITU-T and ITTF editors will accept this solution. The SC 6 meeting in Tokyo, June 2009, must take this into account and plan a course of action to allow a consistent overall numbering of tables and figures. UK proposals for dealing with Amendment 1 are given in the adjacent column.	until the situation has been sorted out for Corrigendum 1 and Amendment 2. If any tables are deleted from the FPDAM the current number should be deleted and no attempt should be made to change the numbering of subsequent tables. If further tables are added to the FPDAM they should be given temporary numbers of the form Table 17A, Table 17B (for new tables between the current Tables 17 and 18). This will give an unambiguous ordering. The same approach should be taken for figure numbers.	- start from Figure 85
GB 5	All	Tables and figures	ge, ed	Use of the ITU-T template. We make the following observations: a) there are inconsistencies in the style of clause and sub-clause headings at the same level; b) although there are cases where table and figure numbers have been tagged to maintain equivalence between their usage in the text and in the table and figure titles, there are many instances where this equivalence has not been maintained. Amendment 1 is nearing publication stage. At this stage it is important that no more errors are introduced in the referencing of clause, figure and table numbers.	When the changes to the Amendment have been made, the editor should ensure that the ITU-T template is used to produce correctly formatted clause and sub-clause headings and to keep the equivalence between table/figure numbers and references to them in the text. For the tables, this should be done so that there is consecutive numbering starting from Table 9 in the Amendment. If the ITU-T template is used properly there should be no difficulty in changing the numbering if further changes and made to Corrigendum 1 and Amendment 2. This action will save a lot of work at the TSB	**Accept** - The output document for PDAM is adjusted on Amendment of ISO/IEC and ITU-T common text format

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
					editing stage.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

KR Responses for UK comments on the group attribute and open and closed groups

GB 6	3		te	Definitions related to open and closed groups The UK National Body considers that that there is insufficient definition of open and closed groups in Amendment 1. The UK submits proposed changes to the Definitions clause.	Add the following definitions to clause 3: *Individual sub-clause numbers for the definitions to be provided after all proposals for new definitions have been decided.*	**accept** -(Clause 3) additions of definitions 3.24 GP_ATTRIBUTE 3.25 Closed group 3. 26 Open group

Reflected definitions on comment GB 6:

3.24 **Group attribute (GP_ATTRIBUTE):** an attribute that defines whether or not the Content Provider controls the admission of RMAs to the secure RMCP-2 session.

3.25 **Closed group**: an MM group in which all the RMAs have been allocated a service user identifier from the Content Provider before subscribing to the secure RMCP-2 session.

3.26 **Open group**: an MM group in which none of the RMAs require a service user identifier before subscribing to the secure RMCP-2 session.

GB 7	12.3	Table 19	ed, te	Changes to GP_ATTRIBUTE columns in Table ~~11~~ 19 We suggest that the 'Meaning' column should be into 'Attribute' and 'Meaning' columns (as has been done for Tables ~~8~~ 16 and ~~9~~ 17. Specific references to ISO/IEC standards require to be added to the References column.	Proposal for a revised table 19 is indicated below	**accept** - Table ~~19~~ 21 is reflected

Included Table 21 to comment GB 7:

Table 21 – GP_ATTRIBUTE Codes

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Code	Attribute	Meaning
0x01	OPEN	A service user identifier is not required by an RMA before subscribing to the secure RMCP-2 session
0x02	CLOSED	A service user identifier is required by an RMA before subscribing to the secure RMCP-2 session (see 10.1.1.5)

GB 8	10.11.4		te	Admission control for RMAs The admission control for RMAs needs to be described separately for open and for closed groups.	Split 10.1.1.4, ‘Admission of RMAs’ into two sub-clauses as indicated in the text below:	accept

Included texts on comment GB 8:

10.1.1.4 Admission of RMAs to open groups

A potential RMA will know from the announcement of the session whether or not the session supports open groups. The RMAs are authenticated by the SM through the TLS session and they join the session through the exchange of SUBSREQ and SUBSANS messages with the SM. They do not receive the session key Ks. They join the RMCP-2 tree through the secure tree join procedure (see 10.2.4).

10.1.1.5 Admission of RMAs to closed groups.

A potential RMA will know from the announcement of the session whether or not the session supports closed groups. Access to membership of closed groups is controlled by the content provider (CP). A potential RMA requests a service user identifier from the CP. The CP provides a service user identifier to the potential RMA and also sends the service user identifier, without revealing the identity of the potential RMA, to the SM. The CP is responsible for the format of this identifier and this is not defined in this Recommendation | International Standard.

When the session is opened to RMAs, the RMAs are authenticated by the SM through the TLS session and they join the session through the exchange of SUBSREQ and SUBSANS messages with the SM. The SUBSREQ message shall

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

contain the service user identifier. The SM shall send a rejection in the RESULT control data type of the SUBANS message if the SM does not hold an identical service user identifier.

The RMAs do not receive the session key Ks. They join the RMCP-2 tree through the secure tree join procedure.

GB 9	10.2.9 (new)		te	Service user identifier In order for an RMA to submit a service user identifier to the SM a new control will be required for the SUBSREQ message. Question. Is 16 bits sufficient for the service user identifier? It will allow for 65536 numeric entries. This will be reduced if alphabetic characters are included. The format of this identifier is outside of the scope of this standard.	Suggested text for a new SERV_USER_IDENTIFIER control for the SUBSREQ message for secure RMCP-2 is provided below. The format is based on the AUTH control for the RELREQ message for secure RMCP-2. *A provisional sub-clause number, 11.2.9, has been given for the SUBSREQ message for secure RMCP-2 following the specification of the message format. A more appropriate position would be for it to appear before 11.2.1, RELREQ message, but it recommended that it is not moved until the final editing of the revised FPDAM text.* *A new Figure 122A has been added. Again, it is recommended that it is not renumbered until the final editing of the revised FPDAM text.*	**Accept** - additions of 11.2.1 and 11.2.2 for service user identifier

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Including text on comment GB 9:

11.2.1. SUBSREQ message

11.2.1.1. The SUBSREQ message for RMCP-2 is defined in 7.3.1 and its common format fields are shown in Figure 40. For use in secure RMCP-2 the following common format fields in the SUBSREQ message shall be set as indicated below:

a) *Version*. - This field denotes the current version of RMCP-2. Its value shall be set to 0x04.

b) *Node Type*. - 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 12. When the SERV_USER_IDENT control is appended, the Node Type value shall be set to 0x03 (RMA).

The remaining common format fields for SUBSREQ messages shall be as specified in 7.3.1.

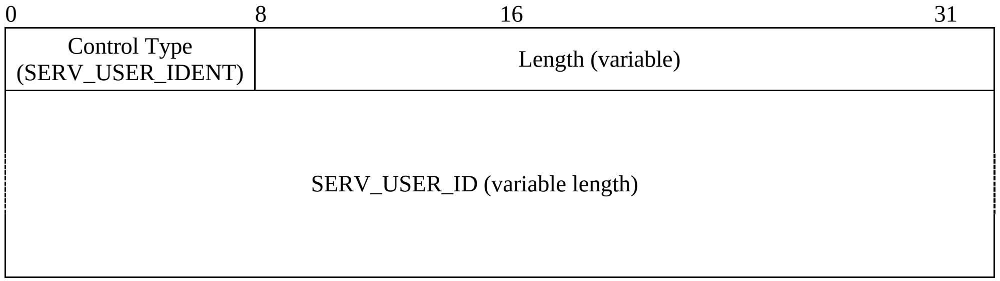

0
8
16
31
Control Type (SERV_USER_IDENT)
Length (variable)
SERV_USER_ID (variable length)

Figure 104A– SERV_USER_IDENT control data

11.2.1.2. This sub-clause defines an additional SERV_USER_IDENT control type for use in secure RMCP-2 in order to confirm that the RMA issuing the SUBSREQ message has been registered by the Content Provider for participation in closed groups (see 10.1.1.5). The SERV_USER_IDENT control type shall be used only when the RMA wishes to join a session in which the MM groups are defined as closed. Figure 104A shows the format of the SERV_USER_IDENT control type. The description of each field is as follows:

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com- ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

SERV_USER_IDENT

a) *Control type* – denotes ‘SERV_USER_IDENT’ control. Its value shall be set to 0x1E (see Table 16)

b) *Length* – denotes the length of the SERV_USER_IDENT control in bytes.

c) *Reserved* – is reserved for future use. Its value shall be set to 0x00.

d) *SERV_USER_ID* – denotes the service user identifier allocated to the RMA by the Content Provider (see 10.1.1.5). Its value shall be identical to that provided to the RMA by the Content Provider.

NOTE – The length of the SERV_USER_ID field and the SERV_USER_IDENT control will be dependent on the length of the identifier provided by the Content Provider.

11.2.2 SUBSANS message

Two additional result codes, specific to the secure RMCP-2 protocol, are defined in Table 23A in order to record reasons for rejecting the subscription of an RMA due to a missing or unrecognized SERV_USER_ID in the SUBSREQ message in cases where the session supports closed groups. These values extend the range of valid codes but do not affect the formatting of the of the RESULT control data type of the SUBANS message specified in 7.3.2.

GB 10	12.3	Table 14	te	Code value for SERV_USER_IDENT control type A code value for this control will be required in Table 14	Suggested table entry indicated below	**accept** Table 15 includes ‘SERV_USER_IDENT’

Reflected entry for Table 15:

New entry for Table 15 – Control Data Types for Secure RMCP-2

Control Data Type	Meaning	Value (hexadecimal)	Message types containing the Control Data Type
SERV_USER_IDENT	Service user identification	0x1E	SUBSREQ

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

KR Responses for UK comments relating to the specification of the SECAGREQ, SECLIST and SECAGANS messages.

GB 11	11.2.3 11.2.4 11.2.5		te	Analysis of attributes in SECAGREQ, SECLIST and SECAGANS messages	See below	**Accept**

Reflection for comment GB 11

0	8	16	24 31
Control Type (AUTH_ALG)	Length (= 4)	AUTH_ID	Reserved (0x00)

Figure 1 – AUTH_ALG control data for the SECLIST message

11.2.5.7 Figure 117 shows the format of the AUTH_ALG control type. The description of each field is as follows:

AUTH_ALG

a) *Control type* – denotes the AUTH_ALG control. Its value shall be set to 0x19 (see Table 16).

b) *Length* – denotes the length of the AUTH_ALG control in bytes. Its value shall be set to 0x04.

c) *AUTH_ID* – denotes the hash/MAC algorithm for the security policy. Its value shall be set to one of the code values in Table 20.

d) *Reserved* - is reserved for future use. Its value shall be set to 0x00

Table 1 – AUTH_ID Codes

Code	Acronym	Meaning	Reference
0x01	HMAC-SHA1	Hash Message Authentication Code – US Secure Hash Algorithm 1	ISO/IEC 9797-2
0x02	HMAC-MD5	Hash Message Authentication Code – Message-Digest Algorithm 5	ISO/IEC 9797-2
0x03	MD5	Message-Digest Algorithm 5	ISO/IEC 9797-2

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
GB 12	11.2.3 11.2.4 11.2.5		te	Questions relating to attributes in SECAGREQ, SECLIST and SECAGANS messages We consider that a number of improvements should be made to the message formats for the SECAGREQ, SECLIST and SECAGANS messages in order to improve the consistency of the specification. The following questions need to be answered before drafting the text for these improvements.		**Accept** - **Changes of part of message field names** - **New part is added**

New additions for comment GB 12

0	8	16	24	31
Control Type (SMA_PROPOSE)	Length (= 8)	GP_ATTRIBUTE	GK_MECHA	
CON_EN_DEC_ID	Reserved (0x00)			

Figure 2 - SMA_PROPOSE control data

11.2.5.8 Figure 108 shows the format of the SMA_PROPOSE control type. The description of each field is as follows:

- SMA_PROPOSE

a) *Control type* – denotes the SMA_PROPOSE control. Its value shall be set to 0x11 (see Table 16)

b) *Length* – denotes the length of the SMA_PROPOSE control in bytes. Its value shall be set to 0x08.

c) *GP_ATTRIBUTE* – denotes the group property proposed by the SMA. Its value shall be set to one of the code values in Table 21.

d) *GK_MECHA* – denotes the update property of the group key proposed by the SMA. Its value shall be set to one of the code values in Table 22.

e) *CON_EN_DEC_ID* – denotes the contents encryption algorithm proposed by the SMA. Its value shall be set to one of the code values less than 1x00 in Table 19.

Reserved – is reserved for future use. Its value shall be set to 0x00.

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

12.2.7. SECALGREQ message

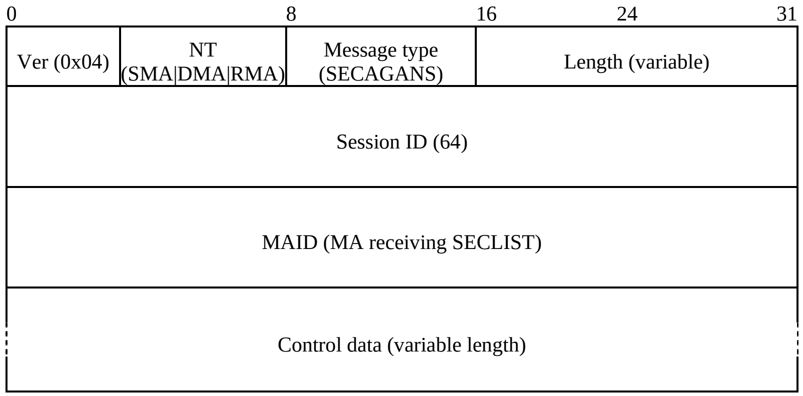


Figure 3 – SECALGREQ Message

12.2.7.1. Figure 118 shows the format of the SECALGREQ message. The description of each field is as follows:

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

b) *NT* –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* – denotes the SECALGREQ message. Its value shall be set to 0x27 (see Table 15)

d) *Length* – denotes the total length of the SECAGANS message including control data (in bytes)

e) *Session ID* – is set to the 64-bit value of the Session ID as defined in 7.1.1.

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

g) *Control data* – shall include all of the controls defined below

0 8 16 24 31

Control Type (GK_MECH_DELIVER)	Length (= 4)	GK_NAME	Reserved (0x00)

Figure 4 – GK_MECH_DELIVER control data

11.2.7.2 Figure 119 shows the format of the GK_MECH_DELIVER control type. It shall only be used by the MA sending the SECAGANS message when its configuration of the GK_NAME security algorithm has failed (see the agreement of security mechanisms procedure in 10.1.4). The description of each field is as follows:

- GK_MECH_DELIVER

a) *Control type* – denotes the GK_MECH_DELIVER control. Its value shall be set to 0x1A (see Table 16)

b) *Length* – denotes the length of GK_MECH_DELIVER control in bytes. Its value shall be set to 0x04.

c) *GK_NAME* –denotes the group key mechanism for the security policy. Its value shall be identical to that in the GK_MECH field of the SECLIST message (see 11.2.4.2.d).

d) *.Reserved* – this field is reserved and is not intended for future use. Its value shall be set to 0x00.

0 8 16 24 31

Control Type (AUTH_MECH_DELIVER)	Length (= 4)	AUTH_NAME	Reserved (0x00)

Figure 5 – AUTH_MECH_DELIVER control data

11.2.7.3 Figure 120 shows the format of the AUTH_MECH control type. It shall only be used by the MA sending the SECAGANS message when its configuration of the AUTH_NAME security algorithm has failed (see the agreement of security mechanisms procedure in 10.1.4). The description of each field is as follows:

- AUTH_MECH_DELIVER

a) *Control type* – denotes the AUTH_MECH_DELIVER control. Its value shall be set to 0x1B (see Table 16).

b) *Length* – denotes the length of the AUTH_MECH_DELIVER control in bytes. Its value shall be set to 0x04.

c) *AUTH_NAME* – denotes the authentication mechanism for the security policy. Its value shall be set to 0x01 denoting MEM_AUTH (see Table 25).

d) *Reserved* – this field is reserved and is not intended for future use. Its value shall be set to 0x00

0 8 16 24 31

Control Type (GK_EN_DEC_DELIVER)	Length (= 4)	CON_EN_DEC_ID	Reserved (0x00)

Figure 6 – CON_EN_DEC_DELIVER control data

11.2.7.4 Figure 121 shows the format of the CON_EN_DEC_DELIVER control type. It shall only be used by the MA sending the SECAGANS message when its configuration of the CON_EN_DEC_ALG security algorithm has failed (see the agreement of security mechanisms procedure in 10.1.4). The description of each field is as follows:

- CON_EN_DEC_DELIVER

a) *Control type* – denotes the CON_EN_DEC_DELIVER control. The value shall be set to 0x1C (see Table 16).

b) *Length* – denotes the length of the CON_EN_DEC_DELIVER control in bytes. Its value shall be set to 0x04.

c) *CON_EN_DEC_ID* – denotes the contents encryption algorithm for the security policy. Its value shall be identical to that in the CON_EN_DEC_ID field of the CON_EN_DEC_ALG control in the SECLIST message (see 11.2.4.4.c).

d) *Reserved* - is reserved for future use. Its value shall be set to 0x00

0 8 16 24 31

Control Type (GK_EN_DEC_DELIVER)	Length (= 4)	GK_EN_DEC_ID	Reserved (0x00)

Figure 7 – GK_EN_DEC_DELIVER control data

11.2.7.5 Figure 122 shows the format of the GK_EN_DEC_DELIVER control type. It shall only be used by the MA sending the SECAGANS message when its configuration of the GK_EN_DEC_ALG security algorithm has failed (see the agreement of security mechanisms procedure in 10.1.4). The description of each field is as follows:

- GK_EN_DEC_DELIVER

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

a) *Control type* – denotes the GK_EN_DEC_DELIVER control. The value shall be set to 0x1D (see Table 16).

b) *Length* – denotes the length of the GK_EN_DEC_DELIVER control in bytes. Its value shall be set to 0x04.

c) *GK_EN_DEC_ID* – denotes the ~~proposed~~ group key encryption algorithm for the security policy. Its value shall be identical to that in the GK_EN_DEC_ID field of the GK_EN_DEC_ALG control in the SECLIST message (see 11.2.4.5.c).

d) *Reserved* - is reserved for future use. Its value shall be set to 0x00

0	8	16	24 31
Control Type (AUTH_ALG_DELIVER)	Length (= 4)	AUTH_ID	Reserved (0x00)

Figure 8 – AUTH_ALG_DELIVER control data

11.2.7.6 Figure 123 shows the format of the AUTH_ALG control type for the SECAGANS message. It shall only be used by the MA sending the SECAGANS message only when its configuration of the AUTH_ALG security algorithm has failed (see the agreement of security mechanisms procedure in 10.1.4). The description of each field is as follows:

AUTH_ALG_DELIVER

a) *Control type* – denotes the AUTH_ALG_DELIVER control. The value shall be set to 0x1E (see Table 16).

b) *Length* – denotes the length of the AUTH_ALG_DELIVER control in bytes. Its value shall be set to 0x04.

c) *AUTH_ID* – denotes the hash/MAC algorithm for the security policy. Its value shall be identical to that in the AUTH_ID field of the AUTH_ALG control in the SECLIST message (see 11.2.4.5.c).

d) *Reserved* - is reserved for future use. Its value shall be set to 0x00.

GB 13	12.2	Table ~~15~~ 23	te, ed	Table ~~15~~ 23, AUTH_NAME code The entry for TESLA has deleted from the table leaving a single entry in the table.	Change title from AUTH_NAME codes to AUTH_NAME code. (Rationale: Only one code value is listed) Change 'See Annex E' to 'Procedure defined in Annex E'	**accept** - deleted

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

Modified table to comment GB 13

Table 2 – AUTH_NAME Codes

Code	Acronym	Meaning	Reference
0x01	MEM_AUTH	Membership authentication	See Annex E

GB 14	12.2	Table ~~14~~ 22	te	Table ~~14~~ 22. The AUTH_NAME and AUTH_ATTRIBUTES fields are twinned together in the AUTH_MECH controls of the SECLIST and SECAGANS messages. As MEM_AUTH is the only entry in the AUTH_NAME table, we consider it appropriate that MEMBERSHIP should be the only entry in the AUTH_ATTRIBUTE table.	Table ~~14~~ 22. Delete table entries for -- MESSAGE -- SOURCE -- USER -- NONE Retain table entry for MEMBERSHIP Change the code for MEMBERSHIP to 0x01	**Accept** - deleted

Modifications on comment GB 14

Table 3 - AUTH_ATTRIBUTE Codes

Code	Value	Meaning
0x01	MEMBERSHIP	'Membership' describes its authority is checked and defines its mechanism

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.

GB 15	10.1.3	Table ~~2~~ 10	ed, te	Changes to the multicast security policy (Table 10)	Table ~~2~~ 10	**Accept**

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
				resulting from comments GB 13 and 14. The changes to Tables ~~14~~ 22 and ~~15~~ 23 in GB 13 and 14 should be reflected in Table ~~2~~ 10	In the attribute column for SEC_NAME delete 'TESLA' In the attribute column for AUTH_ATTRIBUTE delete 'message, source, user and none' In the attribute column for AUTH_NAME delete 'PASSWD_MEM_AUTH', insert 'MEM_AUTH' (Rationale: PASSWD_MEM_AUTH is not used elsewhere in the Amendment). In the definition column for AUTH_NAME delete 'Notifies which authentication mechanism is used', insert 'Notifies the authentication mechanism used' (Rationale: There is no choice for the attribute in AUTH_NAME)	- deleted and changed with each deletion

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

This table is attached on comment GB 15

Table 4 – Multicast security policy

Item	**Attributes**	**Definition**	**Further details**
SEC_NAME	- KDC - GKMP - GDOI - MIKEY - GSAKMP - LKH - MEM_AUTH	Announces which security schemes are used	See Table 18
CON_EN_DEC_ID	- AES CBC Mode 128bit key - AES CTR Mode 128bit key - PKCS #1 - SEED	Notifies which encryption/decryption algorithm is used for content data	See Table 19
GK_EN_DEC_ID	- AES CBC Mode 128bit key - AES CTR Mode 128bit key - PKCS #1 - SEED	Notifies which encryption/decryption algorithm is used for content data for group keys	See Table 19
AUTH_ID	- HMAC-SHA - HMAC-MD5 - MD5	Notifies which hash/MAC algorithm is applied	See Table 20
GP_ATTRIBUTE	- closed - open (default)	Notifies the nature of the group	See Table 21
GK_MECHA	- static - periodic	Notifies updating properties of the group key	See Table 22

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

	- backward - forward - periodic+backward - periodic+forward - periodic+backward+forward		
GK_NAME	- KDC - GKMP - GDOI - MIKEY - GSAKMP - LKH	Notifies which group key mechanism is used.	See Table 23
AUTH_ATTRIBUTE	- membership	Notifies the type of authentication used	See Table 24
AUTH_NAME	MEM_AUTH	Notifies the authentication mechanism used	See Table 25

삭제됨:

삭제됨: -

삭제됨:

GB 16	11.2.1.2.c		te	Change to AUTH_NAME specification in the RELREQ message resulting from comment GB 13 The phrase 'as in the AUTH_NAME field in the AUTH_MECH control of the SECLIST' is not necessary as only one value (0x01) is specified in both instances	Proposed text indicated below	**accept**

Addition for comment GB 16

c) *AUTH_NAME* – denotes the authentication mechanism. Its value shall be set to 0x01 denoting MEM_AUTH (see Table 25)

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
GB 17	11.2.4.3		te	Change to AUTH_ATTRIBUTE and AUTH_NAME specifications in the SECLIST message resulting from comments GB 14 and 13.	Proposed text indicated below	**accept**

Attached text for comment GB 17

a) *AUTH_*ATTRIBUTE – denotes the authentication type for the security policy. Its value shall be set to 0x01 denoting MEMBERSHIP (see Table 24).

b) *AUTH_NAME* – denotes the authentication mechanism for the security policy. Its value shall be set to 0x01 denoting MEM_AUTH (see Table 25).

KR Responses for other UK comments relating to preliminary clauses (References, Definitions and Abbreviations)

GB 18	Title		te, ed	Title of Amendment We thought that the title of the Amendment had been changed from ‘Security extensions’ to ‘Secure RMCP-2 protocol’. We consider that the title should be ‘Secure RMCP-2 protocol’ Rationale: The amendment has been developed as a separate protocol with different entities, a different network configuration and a different version identifier (0x04). The scope of the Amendment goes beyond simple extensions of the basic RMCP-2 protocol.	Change title of Amendment to **Amendment 1 Secure RMCP-2 protocol**	**Accept**
GB 19	2.2		te	References	Add: ISO/IEC 9798-3:1998, *Information technology – Security techniques – Entity authentication mechanisms – Part 3. Entity authentication using a*	**accept**

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
					public key algorithm. Renumber Additional ISO/IEC References in numerical order.	
GB 20	3		te, ed	Definitions Definitions 3.20 – 3.23 have been written in improved English	Replace existing definitions as follows:	**accept**

Addtional definitions on comment GB 20

3.20 **Relayed Multicast region; RM region**: a management zone defined by the use of the session key Ks.

3.21 **Member Multicast region; MM region**: a management zone defined by the use of one or more group keys Kg.

3.22 **Member Multicast group; MM group**:

1. (in a multicast disabled area) a group consisting of one DMA and multiple RMAs sharing the same group key Kg.

2. (in a multicast enabled area) a group consisting of one HMA, multiple RMAs together with one or more candidate HMAs sharing the same group key Kg.

3.23 **Candidate HMA:** A DMA that is able to assume the role of an HMA should the original HMA leave or be terminated from a multicast-enabled MM group.

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

KR Responses for additional UK comments relating to clause 9, Overview

GB 21	9	Title	ed, te	Title of clause 9 The current title of clause 9, Overview of security parties in RMCP-2, only applies to 9.2. Other sub-clauses deal with protocol blocks, message types and regional security management.	Change title to read: **9. Overview of secure RMCP-2 protocol**	**accept**
GB 22	9.4 10.2.6 11.2 (all) 12.2	Table ~~1~~ 9 Table ~~3~~ 11 Table ~~5~~ 13	ed	Editorial order of RMCP-2 messages We note that the order of presentation of the secure RMCP-2 messages is not consistent across these tables and lists. We consider that when these are listed they should be in the following order: Message Code SUBSREQ 0x02 (SERV_USER_IDENT control) RELREQ 0x09 (AUTH control) RELANS 0x0C (AUTH_ANS control) SECAGREQ 0x21 SECLIST 0x22 SECAGANS 0x23 KEYDELIVER 0x24 HRSREQ 0x25 HRSANS 0x26 Apart from the addition of the SUBSREQ message for secure RMCP-2 (proposed in comment GB 9), this is the order in which the formats are listed in clause 11 and in		**accept**

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
				Table ~~5~~ 13. NOTE – Changes to the ordering in clause 11 will require significant changes to the cross referencing in the Amendment.		
GB 23	9.4	Table 9	ed, te	Table 9, Secure RMCP-2 messages The order of the messages in Table ~~1~~ 9 has been changed to that proposed in comment GB 22.	Proposed changes indicated below	**accept** As Table 11

Table attached to comment GB 23

Table 11 – Secure RMCP-2 messages

Messages	Meaning	Operations
SUBSREQ (control type = SERV_USER_IDENT)	Additional control type = SERV_USER_IDENT in SUBSREQ (Subscription Request)	Session initialization
RELREQ (control type = AUTH)	Additional control type = AUTH in RELREQ (Relay request)	Membership Authentication
RELREQ (control type = AUTH_ANS)	Additional control type = AUTH_ANS in RELANS (Relay answer)	
SECAGREQ	Security Agreement request	Establishment of Membership Security Policy
SECLIST	Security List	
SECAGANS	Security Agreement answer	
KEYDELIVER	Key Delivery	Key Distribution
HRSREQ	Head Required Security request	Group Member

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

HRSANS	Head Required Security answer	Authentication Group Key Distribution ACL Management

GB 24	10.2.6	Table ~~3~~ 11	ed, te	Table 11, Encryption of messages for the secure RMCP-2 protocol The current title could be misread as referring to encryption of messages in the basic RMCP-2 protocol. No encryption is defined for the basic RPCP-2 protocol.	Proposed changes indicated below The title of Table 11 has been changed. Missing SECAGREQ, SECLIST and SECAGANS messages have been added	**accept**

Modified table on comment GB 24

Table 5 – Encryption of basic & secure RMCP-2 Protocol Messages

Messages	**Meaning**	**Key**	
		DMA	**RMA**
SUBSREQ	Subscription request	*Ks*	K_{TLS}
SUBSANS	Subscription answer		K_{TLS}
PPROREQ	Parent probe request		N/A
PPROBANS	Parent probe answer		N/A
HSOLICIT	HMA solicit		N/A
HANNOUNCE	HMA announce		N/A
HLEAVE	HMA leave		N/A
RELREQ	Relay request		*KMAS*
RELANS	Relay answer		*KMAS*
STREQ	Status report request		*KTLS*
STANS	Status report answer		*KTLS*
STCOLREQ	Status collect request		*N/A*
STCOLANS	Status collect answer		*N/A*
LEAVREQ	Leave request		*KMAS*
LEAVANS	Leave answer		*KMAS*

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

HB	Heartbeat		*N/A*
TERMREQ	Termination request		*HASHED KTLS*
TERMANS	Termination answer		*HASHED KTLS*
SECAGREQ	Security agreement request		*KTLS*
SECLIST	Security list		*KTLS*
SECALGREQ	Security algorithm request		*KTLS*
SECAGANS	Security agreement answer		*KTLS*
KEYDELIVER	Key delivery		*KMAS, Kg*
HRSREQ	ACL request		*N/A*
HRSANS	ACL answer		*N/A*

GB 25	12.2	Table ~~5~~ 13	ed, te	Table ~~5~~ 13, Secure RMCP-2 Message Types and Code Values The title of Table 13 should state that these are secure RMCP-2 message types. The SUBSREQ, RELREQ and RELANS messages with secure RMCP-2 sub-controls are missing.	Proposed changes are indicated below	**accept** As Table 15

Modifications on comment GB 25

Table 6 – RMCP-2 Message Types and code Values

Message Type	Meaning	Value (Hexadecimal)	Cross reference to message format
SUBSREQ	Subscription request (Control type = SERV_USER_IDENT)	0x02	See 11.2.0
RELREQ	Relay request (Control type=AUTH)	0x09	See 11.2.1
RELANS	Relay answer (Control type =AUTH_ANS)	0x0C	See 11.2.2
SECAGREQ	Security Agreement Request	0x21	See 11.2.3

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Template for comments and secretariat observations

Date: **March 2009**	Document: **ISO/IEC 16512-2/FPDAM 1**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

SECLIST	Selected Security List	0x22	See 11.2.4
SECAGANS	Security Agreement Answer	0x23	See 11.2.5
KEYDELIVER	Key Delivery	0x24	See 11.2.6
HRSREQ	Head Required Security Request	0x25	See 11.2.7
HRSANS	Head Required Security Answer	0x26	See 11.2.8

NOTE – The code values for the SUBSREQ, RELREQ and RELANS messages are as specified in Table 2 for basic RMCP-2 message types

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

GB 26	9.5	Paragraphs 3 and 4	ed, te	Regional security management Paragraph 3 should be split into two paragraphs, one for the MM region and one for MM groups. The MM region may have several Kg keys, one for each MM group. The first sentence in the original text should define the region in terms of group keys, not the group key. A new sentence should be added to the proposed second paragraph to cover multicast-disabled MM groups. A further sentence should be added to state that the RMAs are logically connected direct to their parent DMA on the data delivery tree (Rationale: This is to cover the case where for local area networks, the physical connection 9.5from the RMA may not be direct to the DMA)		**accept**

Modified text on comment GB 26

Proposed replacement text in sub-clause 9.5:

The MM region is a management zone defined by the use of group keys (Kg). The MM region consists of DMAs and RMAs. They can be connected over a multicast-enabled or a multicast-disabled network. The MM region consists of one or more MM groups each using its own Kg group key.

Multicast-enabled MM groups consist of an HMA, one or more candidate HMAs and multiple RMAs that receive the same multicast messages. Candidate HMAs are DMAs that are not connected to the data delivery tree, but have the capability to assume the role of HMA if required. Multicast-disabled MM groups consist of one DMA and multiple RMAs. In both cases the RMAs are logically connected direct to their parent DMA on the data delivery tree.

Any change in an MM group is localized ~~in~~ within the scope of its own MM group

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

KR Responses for UK comments on clause 10, Protocol operation

GB 27	10.1.1.1	Last paragraph	te, ed	TLS authentication The individual key between the DMA and RMA is K_{MAS}, not K_{TLS}	The TLS session with ~~TMAs~~ RMAs is retained and not closed until membership authentication with their parent DMA in the secure tree join procedure (see 10.2.4) and the individual key ~~K_{TLS}~~ K_{MAS} has been established.	**accept** The TLS session with RMAs is retained and not closed until membership authentication with their parent DMA in the secure tree join procedure (see 10.2.4) and the individual key K_{MAS} has been established.
GB 28	10.1.4.1. 10.1.4.2		te	Download of failed security mechanisms 10.1.4.1. states that if any MAs do not have the algorithms of the security policy, the SM sends the corresponding modules to them. After configuration the MAs send an acknowledgement (SECAGANS) to the SM. This seems the wrong way round. The SECAGANS message contains a request for the failed configurations to be sent by the SM. This needs further consideration.	We are not in a position to provide text for resolving this problem at present.	**accept**

Addtional text on comment GB 27

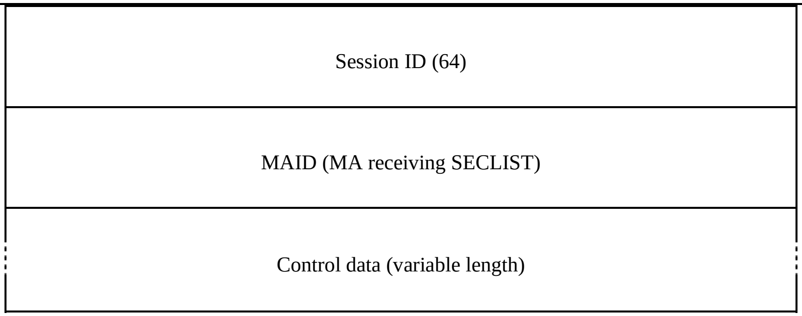
12.2.8. SECALGREQ message

<table>
<tr><td>0</td><td>8</td><td>16</td><td>24 31</td></tr>
<tr><td>Ver (0x04)</td><td>NT (SMA|DMA|RMA)</td><td>Message type (SECAGANS)</td><td>Length (variable)</td></tr>
</table>

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.



Session ID (64)

MAID (MA receiving SECLIST)

Control data (variable length)

Figure 9 – SECALGREQ Message

12.2.8.1. Figure 118 shows the format of the SECALGREQ message. The description of each field is as follows:

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

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

j) *Message Type* – denotes the SECALGREQ message. Its value shall be set to 0x27 (see Table 15)

k) *Length* – denotes the total length of the SECAGANS message including control data (in bytes)

l) *Session ID* – is set to the 64-bit value of the Session ID as defined in 7.1.1.

m) *MAID* –denotes the MAID of the SECALGREQ originator. Its value shall be formatted as defined in 7.1.2.

n) *Control data* – shall include all of the controls defined below

0 8 16 24 31

Control Type (GK_MECH_DELIVER)	Length (= 4)	GK_NAME	Reserved (0x00)

Figure 10 – GK_MECH_DELIVER control data

11.2.7.2 Figure 119 shows the format of the GK_MECH_DELIVER control type. It shall only be used by the MA sending the SECAGANS message when its configuration of the GK_NAME security algorithm has failed (see the agreement of security mechanisms procedure in 10.1.4). The description of each field is as follows:

- GK_MECH_DELIVER

e) *Control type* – denotes the GK_MECH_DELIVER control. Its value shall be set to 0x1A (see Table 16)

f) *Length* – denotes the length of GK_MECH_DELIVER control in bytes. Its value shall be set to 0x04.

g) *GK_NAME* –denotes the group key mechanism for the security policy. Its value shall be identical to that in the GK_MECH field of the SECLIST message (see 11.2.4.2.d).

h) *.Reserved* – this field is reserved and is not intended for future use. Its value shall be set to 0x00.

0 8 16 24 31

Control Type (AUTH_MECH_DELIVER)	Length (= 4)	AUTH_NAME	Reserved (0x00)

Figure 11 – AUTH_MECH_DELIVER control data

11.2.7.3 Figure 120 shows the format of the AUTH_MECH control type. It shall only be used by the MA sending the SECAGANS message when its configuration of the AUTH_NAME security algorithm has failed (see the agreement of security mechanisms procedure in 10.1.4). The description of each field is as follows:

- AUTH_MECH_DELIVER

e) *Control type* – denotes the AUTH_MECH_DELIVER control. Its value shall be set to 0x1B (see Table 16).

f) *Length* – denotes the length of the AUTH_MECH_DELIVER control in bytes. Its value shall be set to 0x04.

g) *AUTH_NAME* – denotes the authentication mechanism for the security policy. Its value shall be set to 0x01 denoting MEM_AUTH (see Table 25).

h) *Reserved* – this field is reserved and is not intended for future use. Its value shall be set to 0x00

0	8	16	24 31
Control Type (GK_EN_DEC_DELIVER)	Length (= 4)	CON_EN_DEC_ID	Reserved (0x00)

Figure 12 – CON_EN_DEC_DELIVER control data

11.2.7.4 Figure 121 shows the format of the CON_EN_DEC_DELIVER control type. It shall only be used by the MA sending the SECAGANS message when its configuration of the CON_EN_DEC_ALG security algorithm has failed (see the agreement of security mechanisms procedure in 10.1.4). The description of each field is as follows:

- CON_EN_DEC_DELIVER

  e) *Control type* – denotes the CON_EN_DEC_DELIVER control. The value shall be set to 0x1C (see Table 16).

  f) *Length* – denotes the length of the CON_EN_DEC_DELIVER control in bytes. Its value shall be set to 0x04.

  g) *CON_EN_DEC_ID* – denotes the contents encryption algorithm for the security policy. Its value shall be identical to that in the CON_EN_DEC_ID field of the CON_EN_DEC_ALG control in the SECLIST message (see 11.2.4.4.c).

  h) *Reserved* - is reserved for future use. Its value shall be set to 0x00

0	8	16	24 31
Control Type (GK_EN_DEC_DELIVER)	Length (= 4)	GK_EN_DEC_ID	Reserved (0x00)

Figure 13 – GK_EN_DEC_DELIVER control data

11.2.7.5 Figure 122 shows the format of the GK_EN_DEC_DELIVER control type. It shall only be used by the MA sending the SECAGANS message when its configuration of the GK_EN_DEC_ALG security algorithm has failed (see the agreement of security mechanisms procedure in 10.1.4). The description of each field is as follows:

- GK_EN_DEC_DELIVER

  e) *Control type* – denotes the GK_EN_DEC_DELIVER control. The value shall be set to 0x1D (see Table 16).

  f) *Length* – denotes the length of the GK_EN_DEC_DELIVER control in bytes. Its value shall be set to 0x04.

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

g) *GK_EN_DEC_ID* – denotes the ~~proposed~~ group key encryption algorithm for the security policy. Its value shall be identical to that in the GK_EN_DEC_ID field of the GK_EN_DEC_ALG control in the SECLIST message (see 11.2.4.5.c).

h) *Reserved* - is reserved for future use. Its value shall be set to 0x00

0 8 16 24 31

Control Type (AUTH_ALG_DELIVER)	Length (= 4)	AUTH_ID	Reserved (0x00)

Figure 14 – AUTH_ALG_DELIVER control data

11.2.7.6 Figure 123 shows the format of the AUTH_ALG control type for the SECAGANS message. It shall only be used by the MA sending the SECAGANS message only when its configuration of the AUTH_ALG security algorithm has failed (see the agreement of security mechanisms procedure in 10.1.4). The description of each field is as follows:

- AUTH_ALG_DELIVER

e) *Control type* – denotes the AUTH_ALG_DELIVER control. The value shall be set to 0x1E (see Table 16).

f) *Length* – denotes the length of the AUTH_ALG_DELIVER control in bytes. Its value shall be set to 0x04.

g) *AUTH_ID* – denotes the hash/MAC algorithm for the security policy. Its value shall be identical to that in the AUTH_ID field of the AUTH_ALG control in the SECLIST message (see 11.2.4.5.c).

Reserved - is reserved for future use. Its value shall be set to 0x00.

GB 29	10.1.5	Sentences 2 and 3	te	Access control for RMAs These sentences state that a DMA on joining the session requests an ACL and this is provided by the SM. 10.1.4 states that a security procedure between the SM the SMA and DMAs is completed before the session is opened for RMA subscription. This means that when these DMAs join the session there will be no RMAs in the ACL.	This needs to be corrected but we are not in a position to provide a solution.	**accept** "DMA can reject a RMA to join the group, if ACL list does not contain the information for RMA." Is added

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
		Sentence 4 Sentence 5		Questions Is the modified information polled by the DMA after the initial ACL distribution carried out through HRSREQ and HRSANS messages? We do not understand the intent of sentence 5. Does it specify the information that the SM must send to the DMA, does is specify the information that the DMA must hold, or is it a statement of fact indicating that the DMA might not have a complete list (because it has not carried out a poll for some time)? Does a DMA have to the power to reject an application from an RMA to join its MM group if that RMA is not listed in the ACL? If so, the DMA needs a complete up to date list. If not, what is the purpose of the DMA holding the list? What is the significance of the DMA having an ACL of ‘some of the RMAs in its own MM group’? The DMA must know the members of its own group as it shares a K_{MAS} with each of the members of its group.		
GB 30	10.2.1.1	Second paragraph	ed, te	Incorrect table reference	10.2.1.1. Second paragraph Change text as indicated: *Kg* is updated by the DMA or RMA according to the update conditions selected ~~during the agreement of group key mechanisms~~ for the security policy ~~(see Table 14)~~ (see Table ~~12~~ 20).	**accept** All of parts are modified
GB 31	10.2.3		ed, te	Incorrect correct cross reference to Annex E Membership authentication is defined in Annex E, not Annex F	10.2.3. Second paragraph delete ‘Annex F’, insert ‘Annex E’	**accept**
GB 32	10.2.3		te	Membership authentication for joining RMCP tree The changes to Tables ~~14~~ 22 and ~~15~~ 23 should be	10.2.3. Third paragraph. Second sentence delete ‘with the proposed authentication	**accept**

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
				reflected in 10.2.3, Membership authentication for joining RMCP tree. The word 'proposed' is inappropriate as there is no alternative authentication mechanism The referenced action is mandatory if the recipient is a DMA. The action in the last paragraph follows on directly from the last sentence of the previous paragraph and it should not be separated in a new paragraph.	mechanism', insert 'confirming the use of the membership authentication mechanism defined in Annex E. 10.2.3. Third paragraph. Last sentence. Delete 'includes', insert 'shall include' 10.2.3. Last paragraph. Move this sentence to the third paragraph to follow the current text of that paragraph.	
GB 33	10.2.4	Paragraph 2	ed, te	Secure tree join Missing Figure number and updated table references are required.	Proposed replacement text indicated below. Minor modifications to the text have been included.	**accept**

Modifications on comment GB 33

Replacement text for paragraph 2 of 10.2.4

The tree join procedure is illustrated in **오류! 참조 원본을 찾을 수 없습니다.**. Membership authentication (see **오류! 참조 원본을 찾을 수 없습니다.**) and group key distribution are processed. When the group key update is required (as indicated by the defined GK_MECHA code in the SECLIST, see **오류! 참조 원본을 찾을 수 없습니다.**), the parent DMA (see note) of the RMA joining the tree (the HMA in the case of multicast-enabled group) re-creates and distributes the group key to its RMAs using the GK_NAME mechanism selected for the security policy (see Table 23). When this procedure is completed, the TLS session between the SM and the RMA is closed.

NOTE – In the case of a multicast-enabled group the parent DMA will be the HMA.

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
GB 34	10.2.5.2		te	Question: Use of LEAVREQ and HLEAVE messages HLEAVE in basic RMCP-2 is sent by the HMA to its children MAs because any of its children can become an HMA. In Leave of HMA from a multicast-enabled area (10.2.5.2) the HMA sends a LEAVREQ followed by an HLEAVE to its children. Is the sending of the HLEAVE to the children of the HMA necessary? The reason for the HMA leaving has already been sent in the LEAVEREQ and the remaining control -acctypes are concerned with data required by the candidate HMAs. Should sending of the HLEAVE be restricted to candidate HMAs?	The proposed replacement text for 10.2.5.2. attached to comment GB 38 assumes that the HLEAVE is only sent to Candidate HMAs.	**accept** Figure 102 is modified
GB 35	10.2.5.2		ed	Leave of HMA from a multicast-enabled area The two paragraphs in 10.2.5.2 look like two separate attempts to describe the same procedure, one in general terms and one referencing specific RMAs. In both cases, several minor English language changes are required	Proposed replacement text based on the general description but with the HLEAVE being sent only to candidate HMAs (see comment GB 37) is indicated below. Minor changes have been made to improve the English	**accept**

Modified text comment on GB 35

Replacement text for 20.2.5.2.

Figure 102 illustrates the HMA leave procedure. The HMA issues a leave request to its members, and announces the leave to its candidate HMAs. The successful candidate HMA joins the RMCP-2 tree and announces its existence to the RMAs in its MM group. The RMAs request to re-join tree and perform membership authentication with the new HMA. The RMAs are the able to receive multicast data normally from the new HMA, and the old HMA leaves the RMCP-2 tree.

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
GB 36	10.2.5.2	Figure 102	te	Corrections to Figure 102 If the recipients of HLEAVE message are restricted to Candidate HMAs (see comment GB 38), the issue of HLEAVEs to RMAs should be removed from Figure 102. There are no LEAVANS messages in response to the LEAVREQ messages in Figure 102. Should these be added to the figure?		-accept Figure 102 is modified
GB 36	10.2.7	Figure 104	te	Question: Meaning of subscript suffixes in Figure 104 Do the subscript suffixes ‘a’ and ‘b’ in $E(Kc)_{Kg\_a}$, $D(Kc)_{Kg\_a}$, $E(Kc)_{Kg\_b}$ and $D(Kc)_{Kg\_b}$, in Figure 104 refer to separate Kg keys belonging to different DMAs?	If the answer to the question is yes: add the following sentence to the end of the text following the Title of Figure 104. ‘The suffixes $_{Kg\_a}$ and $_{Kg\_b}$ are used to distinguish different group keys used in separate MM groups.’	**accept**
GB 37	10.2.7	Figure 104	ed	Legibility of Figure 104 The subscript suffixes in Figure 104 are difficult to read in printed copies of the FPDAM text and in the electronic version (without zoom to X2).	Prepare new figure with more legible text. *This can probably be left to TSB when they prepare the final text before publication.*	**accept**

KR Responses for additional UK comments on clause 11, Format of secure RMCP-2 messages

GB 38	11.2.3.4.c		te	AUTH_ALG control type The AUTH_ID parameter denotes the hash/MAC algorithm.	Change the AUTH_ID field definition to read: ‘*AUTH_ID* – denotes the proposed hash/MAC algorithm. Its value shall be set to one of the code values in Table ~~10~~ 18.’	**accept** *AUTH_ID* – denotes a hash/MAC algorithm held by the SMA or DMA for possible use in the secure RMCP-2 session. Its value shall be set to one of the code values in Table 20.
GB 39	1.2.4.4.	Figure 114	ed	CON_EN_DEC_ALG control type	In Figure 114 change ‘EN_DEC_OID’ to ‘EN_DEC_ID’	**accept**

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Template for comments and secretariat observations

Date: **March 2009**	Document: **ISO/IEC 16512-2/FPDAM 1**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
					In the text of 11.2.4.4 change 'CONTENTS_EN_DEC_ALG' to 'CON_EN_DEC_ALG' (Four instances) In 11.2.4.4.b insert 'denotes' between '*Length –* ' and 'the proposed'	
GB 40	11.2.5.1.g		ed	SEGANS control data	Modify the first sentence in 11.2.5.1.g: 'The control data shall include the SEC_RETURN field ~~shall be added~~.'	**accept**

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Template for comments and secretariat observations

Date: **March 2009**	Document: **ISO/IEC 16512-2/FPDAM 1**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
GB 41	11.2.5.3		ed	SEGANS failed configuration of security mechanisms Our replacement text may have to be modified in response to answers to the questions in comment GB 12	Replace the first sentence with: 'If in response to the SECLIST message, the configuration of any of the security mechanisms has failed (see 10.1.4.1 and 10.1.4.2), the control data types corresponding to the failed mechanisms shall be included in the SECAGANS message. Their values shall be identical to the equivalent control data types in the SECLIST message (see 11.2.4).' Rationale: This is more explicit than the current text.	**accept**
GB 42	11.2.6.2.d		ed, te	KEY_INFO control type	Delete item d). This is no longer required as the control data and the sub-control data have been merged into a single figure.	**accept**

KR Responses for additional UK comments on clause 12, Parameters

GB 43	12.3	Table ~~6~~ 14	ed, te	Control data types For consistency ENDEC should be replaced by EN_DEC KEY_INFO should be used to maintain alignment with the message format specifications in Clause 11. This will also eliminate confusion with the KEY_MATERIAL sub-clause in Table 15 (and in Clause 11)	In the Control Data Type column Change 'ENDEC_ALG' to 'EN_DEC_ALG' Change 'CON_ENDEC_ALG' to 'CON_EN_DEC_ALG' Change 'GK_ENDEC_ALG' to 'GK_EN_DEC_ALG' Change 'KEY_MATERIAL' to 'KEY_INFO' In the Meaning column Change 'Key material' to 'Key information'	**Accept**

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
GB 44	12.3	Table ~~7~~ 15	ed, te	Sub-control data types	Delete the table entry for AUTH_INFO. (Rationale: This sub-control has been deleted from the RELREQ message). In the final column, change ‘REL_ANS’ to ‘RELANS’	**Accept**
GB 45	12.4	Tables ~~9~~ 17 and ~~10~~ 18	ed	EN_DEC ID codes (Title) Change table titles to align with changed parameter names EN_DEC_ID (in Figure 109 and 11.2.3.3.c) and AUTH_ID (in Figure 110 and 11.2.3.4.c). The tables are referenced from 11.2.3.3.c and 11.2.3.4.c	Table ~~9~~ 17. In the Title delete ‘EN_DEC_ALG codes’, insert ‘EN_DEC_ID codes’ Table ~~10~~ 18. In the Title delete ‘AUTH_ALG codes’, insert ‘AUTH_ID codes’	**accept** Table 19. In the Title delete ‘EN_DEC_ALG codes’, insert ‘EN_DEC_ID codes’ Table 20. In the Title delete ‘AUTH_ALG codes’, insert ‘AUTH_ID codes’
GB 46	12.4	Table ~~9~~ 17	ed, te	EN_DEC ID codes (1x01, 1x02,1x03) Question. Are the other modes defined by the SM for 1x01, 1x02 and 1x03 restricted to choices from ISO/IEC 18033-3?	Editorial comment: In the Meaning column, change entries for 1x01, 1x02 and 1x03 to ‘Values greater than 1x00 are reserved for other modes of AES and Triple DES defined by the SM’	**accept**
GB 47	12.4	Table ~~10~~ 18	ed	AUTH ALG codes We suggest that the ‘Meaning’ column should be split into ‘Acronym’ and ‘Meaning’ columns as in Tables ~~8~~ 16 and ~~9~~ 17 The correct ISO/IEC references also need to be added.	Proposed changes are shown below	**Accept**

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

attached table on comment GB 47

Table 20 – AUTH_ID Codes

Code	Acronym	Meaning	Reference
0x01	HMAC-SHA1	Hash Message Authentication Code – US Secure Hash Algorithm 1	ISO/IEC 9797-2
0x02	HMAC-MD5	Hash Message Authentication Code – Message-Digest Algorithm 5	ISO/IEC 9797-2
0x03	MD5	Message-Digest Algorithm 5	ISO/IEC 9797-2

GB 48	12.4	Table ~~12~~ 20	te	GK_MECHA codes An earlier version of the Amendment contained only the first four values in this table and indicated that additional code values could be expressed in terms of arithmetical combinations of these values. This concept could still be applied if a code value of 0x04 was allocated to FORWARD and 0x03 to PERIODIC+ BACKWARD. This would constitute a more logical allocation of codes.	Reallocation of codes 0x04 FORWARD 0x03 PERIODIC+BACKWARD Editorial comment in entry for FORWARD Change text to read 'whenever any member ~~join~~ joins the group'	**Accept**
GB 49	~~12.4~~ 12.5		ed	New sub-clause 12.5 Sub-clause 12.4 is titled 'Code values related to the RMCP-2 security policy'. Tables ~~16~~ 24 and ~~17~~ 25 do not define the security policy. They should be separated into a new sub-clause 12.5.	Create a new sub-clause for tables Tables ~~16~~ 24 and ~~17~~ 25: **12.5 Miscellaneous code values**	**Accept** Create a new sub-clause for tables Tables 27 and 28 with new Table 26

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
GB 50	~~12.4~~ 12.5	Table ~~16~~ 24	ed	SEC_RETURN codes These codes also apply to Auth_result codes.	Change Title to read ‘SEC_RETURN and Auth_result Codes’ In the entry for 0x04 change ‘FAIDED’ to ‘FAILED’; change ‘SEGANS’ to SECAGANS’.	**Accept**
GB 51	~~12.4~~ 12.5	Table ~~19~~ 25	ed, te	KEY_TYPE codes	In the Meaning column delete the word ‘material’ in all three lines (Rationale: the entry refers to the type of key; we think ‘material’ may be taken to imply material for generating the key and which will be transmitted in another field).	**Accept**

KR Responses for UK comments on Annex E, Membership authentication mechanism and comments on authentication in other clauses

1	2	(3)	4	5	(6)	(7)
GB 52	Annex E		te, ed,	Membership authentication The terms ‘member authentication’ and ‘membership authentication’ are both used for the same procedure. ‘Membership authentication’ occurs in clauses 1, 9.2.3, 10.1.1.1, 10.2.1.1, 10.2.1.3, 10.2.3, 10.2.4, 10.2.5.2, 10.2.5.3, 11.2.1.2, 11.2.2.2 and E.2, tables ~~1~~ 9, ~~2~~ 10,~~8~~ 16, ~~15~~ 23 and E.1, figures 100, 102 and 103 ‘Member authentication’ occurs only in Annex E. We propose replacement of ‘member authentication’ by ‘membership authentication’ on the grounds that ‘membership authentication’ is used more frequently.	Replace ‘member authentication’ by ‘membership authentication’ in -- the title of Annex E -- the text of E.1 (one occurrence) -- the title of figure E.1 -- the title of figure E.2	**Accept**

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
GB 53	Annex E E.2		te, ed	Membership authentication E.2 defines the procedure. The word ‘detailed’ in the title is unnecessary. ISO/IEC 9798-3 is not referenced from the text, nor are Figures E.1 and E.2 and Table E.1.	Change title of clause E.2 to: E.2 **Membership authentication procedure**. Add new paragraph immediately after the title of E.2: ‘The secure RMCP-2 membership authentication is based on the three pass authentication procedure in ISO/IEC 9798-3:1998. This procedure, as applied to secure RMCP-2, is described below and is illustrated in Figures E.1 and E.2. The variables used are listed in Table E.1.’ In the last sentence of E.2: delete ‘in the ‘auth_result’ in the RELAS message’, insert ‘in the AUTH_ANS control of the RELANS message.’ In figure E.2: delete ‘K_{HASED_KTLS}’ insert ‘K_{HASHED_KTLS}’ In Table E.1 Correct spelling mistakes For Variables ID_C and ID_S: Identifier For Variable g: Diffie~~d~~	**Accept**

[1] **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.