Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14090
Date:	2009-09-28
Replaces:	
Document Type:	National Body Contribution
Document Title:	NB of UK's comments on 6N14073, Request for Approval of revised text of Draft Amendment 1 to ISO/IEC 16512-2:2008 (ITU-T X.603.1 (2007)) for ITU-T Last Call
Document Source:	National Body of UK
Project Number:	
Document Status:	For your information.
Action ID:	FYI
Due Date:	
No. of Pages:	5
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	

![BSI logo]

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 7254

www.bsigroup.com
eddie.levio@bsigroup.com

Our Ref:

Date: 28 September 2009

UK NATIONAL BODY CONTRIBUTION ON SC 6 N 14073, REVISED TEXT OF AMENDMENT 1 TO ITU-T X.603.1 (2007) | ISO/IEC 16512-2:2008 FOR IUT-T LAST CALL

The UK National Body for ISO/IEC JTC 1/SC 6 approves the revised text of Amendment 1 to ITU-T X.603.1 (2007) | ISO/IEC 16512-2:2008 for ITU-T Last Call but requests minor changes to Figures 94, 95, 100, 101, 102 and 103 before publication. These changes clarify the figures and do not change the technical content of the Amendment.

The arrow heads shown in red in the following figures indicate the proposed re-positioning of the arrow heads and do not indicate the style of the arrow heads: the style should remain the same as in the original figures.
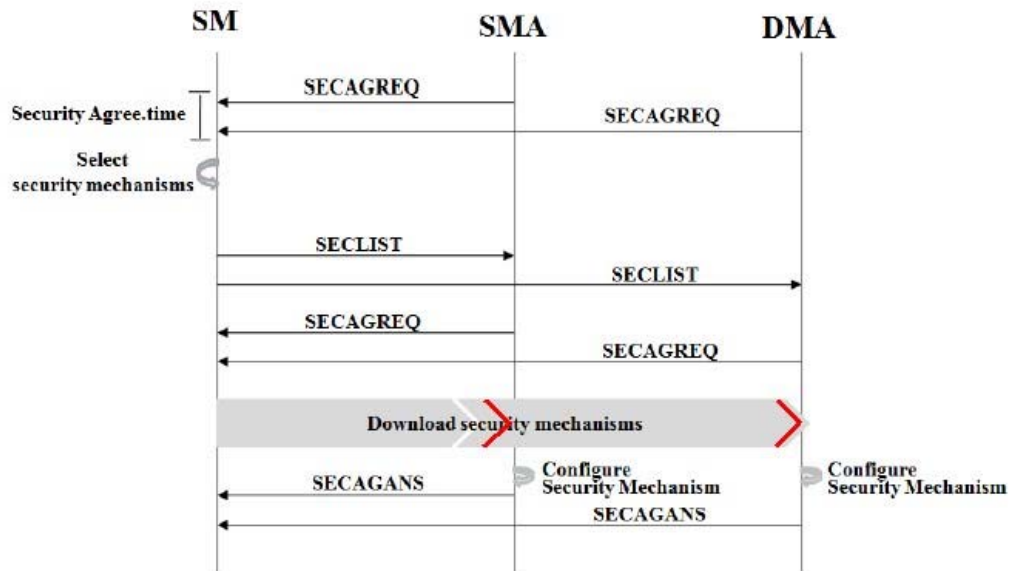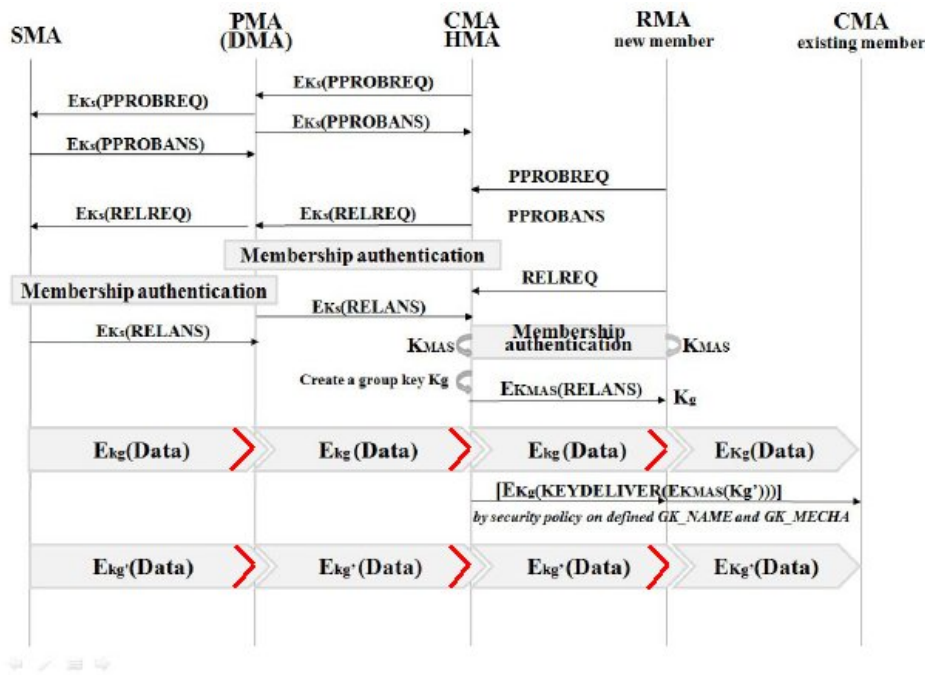
Figure 94 – Security agreement of DMA and SMA

Figure 94. Move arrow heads to coincide with the vertical lines representing SMA and DMA (as shown in red above).
Rationale: This emphasizes the delivery of security mechanisms to the SMA and individual DMAs.
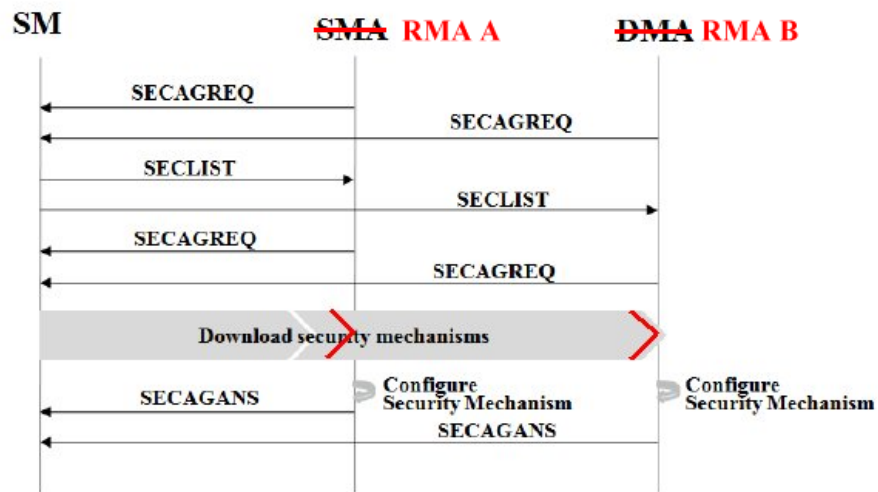

Figure 95 – Security agreement of RMAs

Figure 95. Change entity headings to RMA A and RMA B.
Move arrow heads to coincide with vertical lines representing RMAs (as shown in red above).
Rationale: This emphasizes the delivery of security mechanisms to individual RMAs.

Figure 100 – Secure tree join. The PPROBREQ, PPROBANS and RELREQ messages between RMA A and the HMA are not encrypted as RMA A has not yet received the K_{MAS} or K_g keys

Figure 100. Move arrow heads to coincide with vertical lines representing MAs (as shown in red above).
Rationale: This emphasizes the relaying of data between MAs at successive nodes of the RMCP-2 tree.
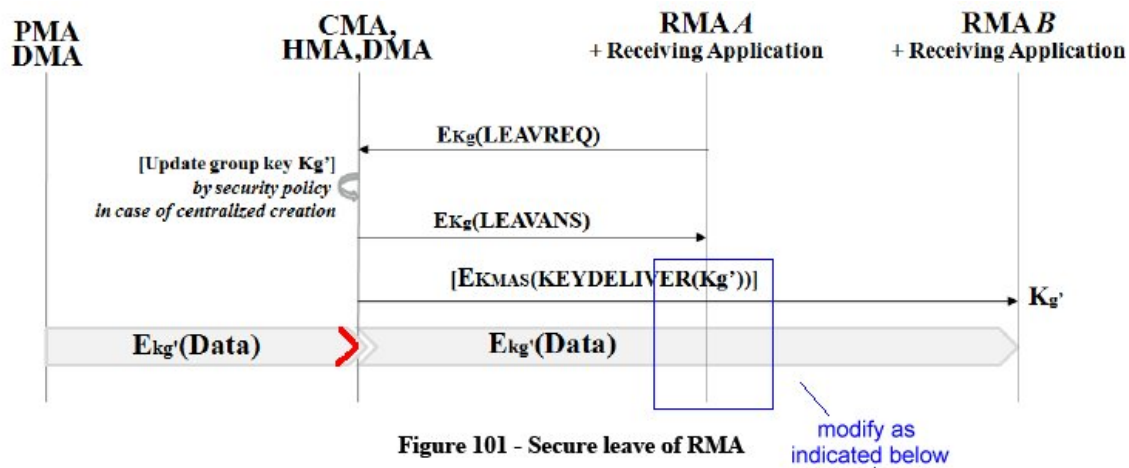
Figure 101 – Secure leave of RMA

Figure 101. Move arrow head to coincide with the vertical line representing the CMA (as shown in red above).
Rationale: This emphasizes delivery of data to the CMA.
Modify the data path at the vertical line representing RMA A.
Rationale. This emphasizes the non-delivery of data to RMA A which is leaving the RMCP-2 tree.

Figure 102 – HMA leave in multicast-enabled area

Figure 102. Move arrow head to coincide with the vertical line representing RMA A (as shown in red above).
Rationale: This emphasizes delivery of data to RMA A.
Delete the vertical line representing the Existing HMA immediately above and below the datapath (as shown in blue above).
Rationale: This emphasizes the non-delivery of data to the Existing HMA after leaving the RMCP-2 tree.

Figure 103 - DMA leave in multicast-disabled area

Figure 103. Move arrow heads to coincide with the vertical lines representing PMA A of B,C and CMA B (as shown in red above).
Rationale: This emphasizes delivery of data to these DMAs.