Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14212
Date:	2010-01-28
Replaces:	
Document Type:	Other document (Defined)
Document Title:	Revised text of FPDAM of ISO/IEC 16512-2 :2008(ITU-T X.603.1)/Amendment 1
Document Source:	SC 6/WG 7 Barcelona meeting
Project Number:	
Document Status:	As per the SC 6 Barcelona resolution 6.7.3, SC 6 approved the revised text of FPDAM.
Action ID:	FYI
Due Date:	
No. of Pages:	48

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

6N14212

7BCN-23

Title : Text for FDAM ballot of ISO/IEC 16512-2 :2008(ITU-T X.603.1)/Amendment 1

Source: ISO/IEC JTC1/SC6/WG7 Meeting (Barcelona, January, 2010)

Status : This an output document for FDAM ballot, Draft Amendment 2 to ISO/IEC 16512-2:2008(ITU-T 603.1) of January 2010 Barcelona ISO/IEC JTC1/SC6/WG 7 Meeting.

INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.603.1
Amendment 1
(11/2009)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

OSI networking and system aspects – Networking

Information technology – Relayed Multicast Protocol: Specification for simplex group applications

Amendment 1:

Secure RMCP-2 Protocol

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU [had/had not] received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

INTERNATIONAL STANDARD ISO/IEC 16512-2:2008/AMD.1
ITU-T RECOMMENDATION X.603.1(2007)/Amd.1

Information technology – Relayed Multicast Protocol: Specification for simplex group applications

Draft Amendment 1
Secure RMCP-2 Protocol

Summary

This amendment describes the security functionalities of an application-level relayed multicast protocol for one-to-many group applications. The protocol provides various security facilities to fulfill general as well as specific security requirements. Some detailed functions that can operate with a variety of standardized security mechanisms are provided. This amendment enforces the existing RMCP protocol security.

CONTENTS

INTERNATIONAL STANDARD ISO/IEC 16512-2:2008/AMD.1
ITU-T RECOMMENDATION X.603.1(2007)/Amd.1

Information technology – Relayed Multicast Protocol : Specification for simplex group applications

Draft Amendment 1
Secure RMCP-2 Protocol

1) Clause 1

Delete the existing text and replace with the following:

This Recommendation | International Standard specifies the Relayed MultiCast Protocol for simplex group applications (RMCP-2), an application-layer protocol, which constructs a multicast tree for data delivery from one sender to multiple receivers over the Internet where IP multicast is not fully deployed.

Clauses 5 – 8 define a basic RMCP-2 protocol without security features and clauses 9 – 12 define a secure RMCP-2 protocol that adds security features to the basic protocol. Both protocols specify a series of functions and procedures for multicast agents to construct a one-to-many relayed data path and to relay simplex data. They also specify the operations of the session manager to manage multicast sessions.

These protocols can be used for applications that require one-to-many data delivery services, such as multimedia streaming services or file dissemination services.

Annex E defines a membership authentication procedure for use with the secure RMCP-2 protocol. Annexes A – D provide informative material related to these protocols. Annex F contains an informative bibliography.

2) Clause 2.

Following the first paragraph, re-order the existing references and add new subheadings as follows:

2.1 Identical Recommendations | International Standards

– ITU-T Recommendation X.603 (2004) | ISO/IEC 16512-1:2005, *Information technology – Relayed multicast protocol: Framework*

2.2 Additional References

– ISO/IEC 9797-2:2002, *Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function*
– ISO/IEC 9798-3:1998*: Information technology -- Security techniques -- Entity authentication -- Part 3: Mechanisms using digital signature techniques*
– ISO/IEC 18033-2:2006, *Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers*
– ISO/IEC 18033-3:2005, *Information technology -- Security techniques -- Encryption algorithms --- Part 3: Block ciphers*
– ISO/IEC 18033-4:2005, *Information technology -- Security techniques -- Encryption algorithms -- Part 4: Stream ciphers*

– IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*
– IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing*
– IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*
– IETF RFC 4346 (2006), *The Transport Layer Security (TLS) Protocol Version 1.1*
– IETF RFC 4535 (2006), *GSAKMP: Group Secure Association Key Management Protocol*

3) Clause 3.

Add the following definitions to clause 3:

3.13 **RMCP-2 protocol**: A relayed multicast protocol for simplex group applications

NOTE – When used in clauses 5-8 of this Recommendation | International Standard this term has the same meaning as basic RMCP-2. It is expected that this term will be withdrawn and replaced by basic RMCP-2 protocol in future revisions of this Recommendation | International Standard.

3.14 **Basic RMCP-2 protocol**: The relayed multicast protocol for simplex group application defined in clauses 5-8 of this Recommendation | International Standard.

3.15 **Secure RMCP-2 protocol**: The relayed multicast protocol supporting security features for simplex group applications defined in clauses 9-12 of this Recommendation | International Standard.

3.16 **Dedicated Multicast Agent (DMA)**: An intermediate MA pre-deployed as a trust server by the Session Manager (SM) in an RMCP session

3.17 **Security policy**: The set of criteria for the provision of security services together with the set of values for these criteria as resulting from agreement of security mechanisms defined in 10.1.4.

3.18 **TLS_CERT mode** : a mode of the TLS defined in IETF RFC 4346 for authentication of MAs using a certificate.

3.19 **TLS_PSK mode** : a mode of the TLS defined in IETF RFC 4279 for authentication of MAs using a pre-shared key for the TLS key exchange

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.

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.

4) Clause 4.

Add the following abbreviations to clause 4:

ACL Access Control List

AUTH Authentication

CEK Contents Encryption Key

CP	Content provider
DMA	Dedicated Multicast Agent
HRSREQ	Head Required Security Request
HRSANS	Head Required Security Answer
KEYDELIVER	Key Delivery
SECAGREQ	SECurity Agreement REQuest
SECAGANS	SECurity Agreement ANSwer
SECLIST	Selected sECurity LIST
TLS	Transport Layer Security

5) New Clauses 9 - 12.

Add the following new clauses:

9. Overview of secure RMCP-2

9.1. Conventions

9.1.1 Use of basic RMCP-2 protocol

The term basic RMCP-2 protocol when used in clauses 9-12 refers to the protocol defined in clauses 5-8 of this Recommendation | International Standard.

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.

9.2. Secure RMCP-2 entities

9.2.1. Introduction

The secure RMCP-2 protocol supports security functions of the RMCP-2 used for relayed multicast data transport through unicast communication over the Internet.

The secure RMCP-2 protocol components correspond to those described in the basic RMCP-2 protocol except that a new type of MA, a Dedicated Multicast Agent(DMA), has been introduced. A Dedicated Multicast Agent is an intermediate MA pre-deployed as a trust server by the SM. For secure communication, each session consists of an SM, an SMA, DMAs, RMAs, together with a single sending application and multiple receiving applications. Their topology, as shown in Figure 88, corresponds with that in the basic RMCP-2 protocol (see 5.1).

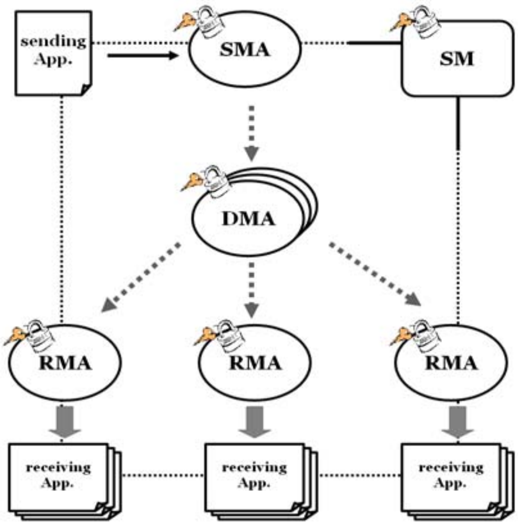


Figure 88 - RMCP-2 service topology with security

9.2.2. Session Manager

The SM is responsible for maintaining session security, which includes the management of service membership, the management of key and ACL for DMA and RMA, and message encryption/decryption together with the SM functions of basic RMCP-2. Figure 89 shows an abstract protocol stack for the operation of SM functions. The SM has TLS and multicast session security modules for the provision of security. TLS is used for the initial authentication of DMAs and RMAs when they join the session. The Multicast session security module performs the following security functions after the completion of TLS authentication:

(a) Security policy;

(b) Session admission management;

(c) Session key management;

(d) Access Control list management;

(e) Secure group and membership management;

(f) Message encryption/decryption.

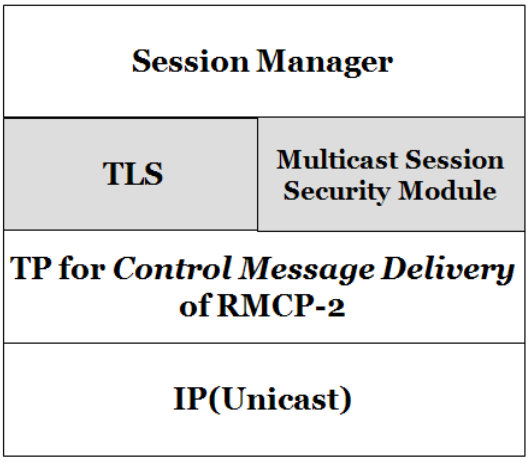


Figure 89 - Internal structure of the SM

9.2.3. Dedicated multicast agents

DMAs are in charge of the secure establishment and maintenance of the RMCP-2 tree, support of membership authentication and data confidentiality. Figure 90 shows the internal structure of the DMAs with modules for Key/Message Security Management and Group/Member Security Management. These modules support the following security functions:

Key/Message Security Management Module

(a) Group key management;

(b) Message encryption/decryption;

(c) Contents encryption key management;

Group/Member Security Management Module

(d) Secure tree configuration;

(e) Session key management;

(f) Secure group and membership management.

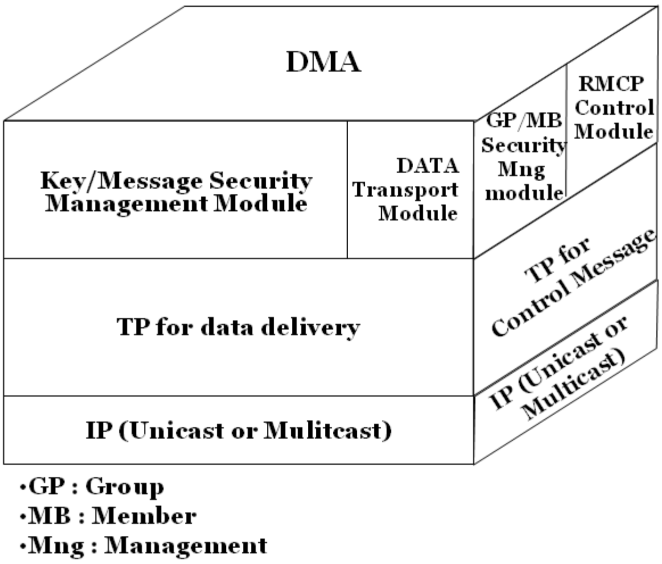


Figure 90 – Internal structure of DMAs

9.2.4. Sender and receiver multicast agents

The internal structure of the SMA and the RMAs is shown in Figure 91. The structure is the same as for DMAs except that the Group Security Management Module is not included.

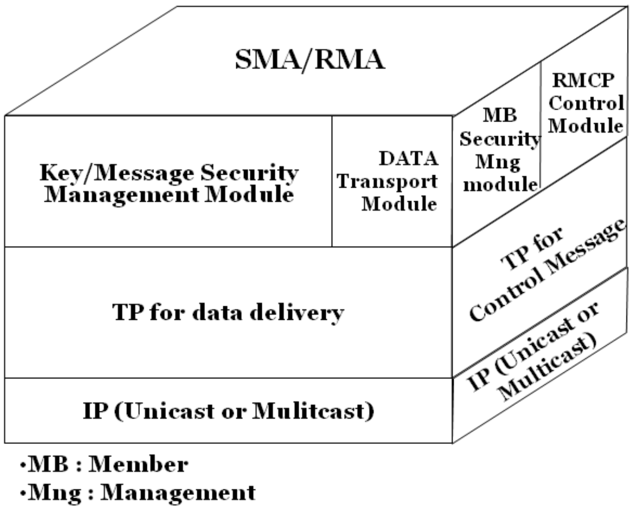


Figure 91 – Internal structure of the SMA and RMAs

9.3. Protocol blocks

The protocol blocks for the SM, Group/Member Security Management of MAs and Key/Message Security Management of MAs are shown in Figures 92, 93 and 94. They correspond to the protocol stacks in the basic RMCP-2 protocol in 5.2 (see figures 2, 3 and 4) but also include the TLS protocol and the Multicast Session Security Module.

The secure RMCP-2 protocol supports general encryption/decryption algorithms of TLS for a variety of common applications. The SM and MAs (SMA, DMAs and RMAs) share the security information described in the security policy. The Multicast Session Security Module contains common symmetric encryption/decryption algorithms, authentication mechanisms, and multicast security modules related to RMCP-2 security functions.

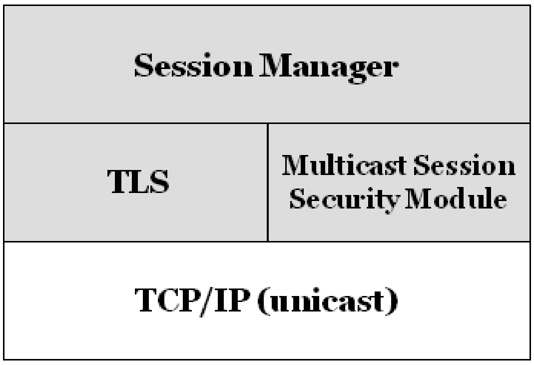


Figure 92 - Protocol block of the SM

The SM messages and the Group/Member Security Management messages of MAs are transmitted reliably through the TCP protocol.

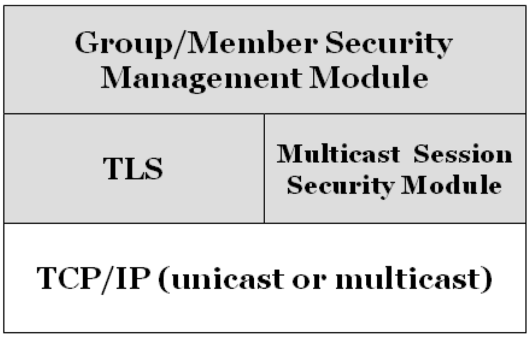


Figure 93 - Protocol block for the group/member security management of MAs

Key/Message Security Management messages may be transferred using any transport protocol. The transport protocol may be selected according to the nature of the transferred data types. TLS provides secure communication for TCP over unicast communication. The Multicast Security Encryption/Decryption and Authentication Modules protect the multicast packets. These modules contain common symmetric encryption algorithms, hash algorithms, and multicast security modules defined in this Recommendation | International Standard to protect the multicast packets.

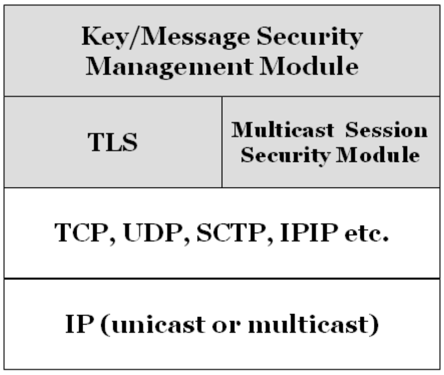


Figure 94 - Protocol block for the key/message security management of MAs

9.4. Types of Secure RMCP-2 protocol messages

Control messages are exchanged between secure RMCP-2 protocol nodes in a request-and-answer manner.

Table 31 shows the messages that are specific to the secure RMCP-2 protocol. They complement the messages listed in Table 23 (see 8.3.2).

Table 31 – 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
RELANS (control type= AUTH_ANS)	Additional control type=AUTH_ANS in RELANS (Relay answer)	
SECAGREQ	Security Agreement request	Establishment of Multicast Security Policy
SECLIST	Security List	
SECALGREQ	Security Algorithms request	
SECAGANS	Security Agreement answer	
KEYDELIVER	Key Delivery	Key Distribution
HRSREQ	Head Required Security request	Group Member Authentication Group Key Distribution ACL Management
HRSANS	Head Required Security answer	

9.5. Structure of regional security management

For scalable security management, the secure RMCP-2 protocol supports security functions in two independent regions: a RM (Relayed Multicast) region and a MM (Member Multicast) region.

The RM region is a management zone of the session key (Ks). It consists of the SM, the SMA and DMAs in a multicast disabled area.

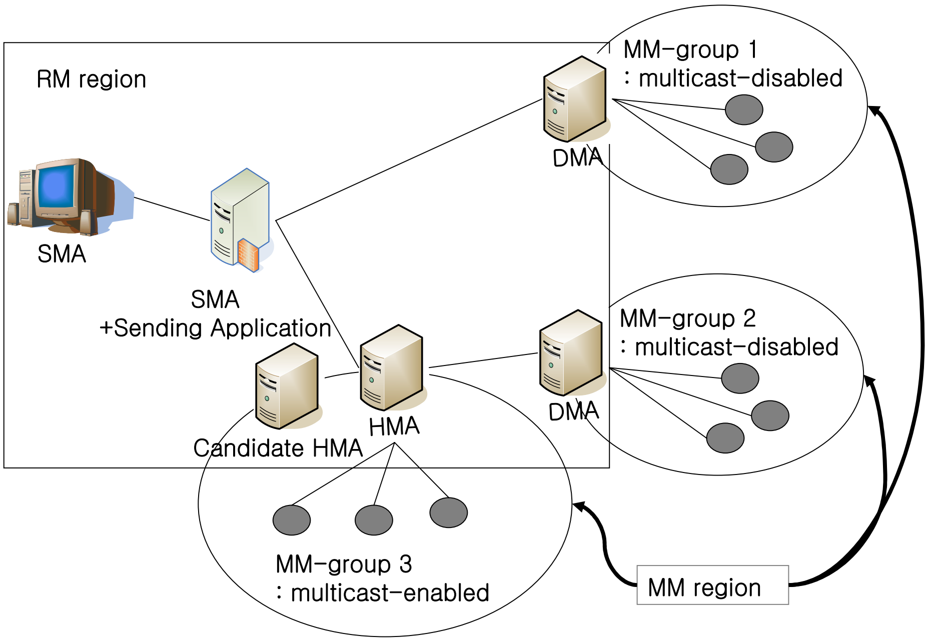


Figure 95 – Security management regions

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 within the scope of its own MM group

10. Protocol Operation

10.1. SM operation

The SM supports the establishment of security policies applied to each secure RMCP-2 session, and is responsible for user and MA security management such as user and MA authentication. It manages the session key for each RMCP-2 session through the creation, update, and distribution of key information. The SM also has message encryption and decryption abilities through the use of TLS and owned cryptography suites.

10.1.1. Admission control

10.1.1.1. TLS Authentication

TLS authentication is performed in advance of the subscription requests of MAs (SMA, DMAs or RMAs). An MA establishes a TLS session with the SM according to IETF RFC 3546. The SM, as part of the IETF 3546 procedure, decides which TLS mode, TLS_CERT or TLS_PSK, is applied for the verification of the parties concerned. The SM responds to the MA and, if the mutual authentication is successful, shares a secret key K_{TLS} with the MA.

The SM also delivers the session key Ks, encrypted using K_{TLS}, to the SMA and the DMAs, but not to the RMAs.

The TLS session with the SMA and DMAs is closed after the session key is delivered, since the SM, SMA and DMAs exchange control messages that have been encrypted with the session key. 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.

10.1.1.2. Admission of the SMA

A secure RMCP-2 session is initiated through the subscription of the SMA. The SMA first obtains authorization for providing the contents from the SM. The SMA is authenticated by the SM through the TLS session (see 10.1.1.1) and then joins the session by exchanging SUBSREQ and SUBANS messages with the SM. As a result of this, the SMA receives the session key Ks and is enabled to act as an administrative node of the secure RMCP-2 tree.

10.1.1.3. Admission of DMAs

The DMAs, as prospective trust parties, are invited by the SM to join the session and to establish the DMA network before the subscription of RMAs. The means of this invitation are outside the scope of this Recommendation International Standard.

The DMAs 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 receive the session key Ks from the SM and join the RMCP-2 tree through the secure tree join procedure (see 10.2.4).

The SM consults with the DMAs joining the session before the announcement of the opening of the secure RMCP-2 session, giving a date and time when the subscription of RMAs begins. The means of this announcement are outside the scope of this Recommendation | International Standard.

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 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 contain the service user identifier. The SM shall send a rejection in the RESULT control 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 (see 10.2.4).

10.1.2. Key management for which the SM is responsible

10.1.2.1. Session key

The session key (Ks) is shared between the SM, the SMA and DMAs and is used to encrypt/decrypt control messages in the RM region. It is initially created by the SM in the bootstrapping of the RMCP-2 session. Ks is encrypted by the individual key K_{TLS} (see 10.1.2.2) for delivery to the SMA and to each DMA through the data protection procedure of TLS following successful TLS authentication.

Ks is updated at regular intervals through the hash function. When a DMA is truncated or an abnormal situation occurs, the SM does not use the hash function, but instead creates a totally new session key Ks, without hashing. The new key is delivered to the SMA and all DMAs in the RMCP-2 session (See Figure 96).

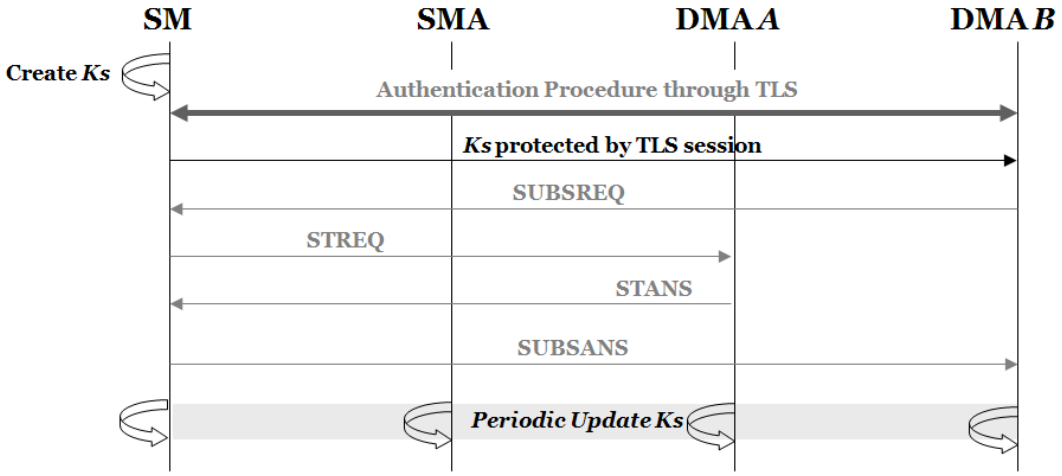


Figure 96 – Session key management

10.1.2.2. TLS key

The TLS key K_{TLS} is a private key generated through successful TLS authentication during admission control. Each MA (SMA, DMA and RMA) shares a different K_{TLS} with the SM , which is not shared with the other MAs. K_{TLS} is not updated during the lifetime of the RMCP-2 session.

10.1.3. Establishment of security policy

When a new RMCP-2 session is created, the SM, together with the SMA and the DMAs, establishes the security policy for the session. The policy is established through the exchange of SECAGREQ, SECLIST and SECAGANS messages that enable the selection of parameters in Table 32 to define the level of security that is to be provided, as well as the choice of algorithms to be used. The security policy is the set of selected attributes of policy items after the agreement on security mechanisms.

Table 32 – Multicast security policy

Item	Attributes	Definition	Further details
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 38**
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 38**
AUTH_ID	- HMAC-SHA - HMAC-MD5 - MD5	Notifies which hash/MAC algorithm is applied	See **Table 39**
GP_ATTRIBUTE	- closed - open (default)	Notifies the nature of the group	See **Table 40**
GK_MECHA	- static - periodic - backward - forward - periodic+backward	Notifies updating properties of the group key	See **Table 41**

	- periodic+forward - periodic+backward+forward		
GK_NAME	- KDC - GKMP - MIKEY -GSAKMP - LKH	Notifies which group key mechanism is used.	See **Table 42**
AUTH_ATTRIBUTE	- membership	Notifies the type of authentication used	See **Table 43**
AUTH_NAME	- MEM_AUTH	Notifies the authentication mechanism used	See **Table 44**

10.1.4. Agreement of security mechanisms

10.1.4.1. SMA and DMAs

The security procedure is initiated after the admission control. The messages are protected by the session key between the SM, SMAs and DMAs, and by the K_{TLS} between the SM and the RMAs. The SMA and the DMAs perform the procedure prior to RMA subscription because the server-oriented systems (SMA and DMAs) need to set up the security policy on order to provide a stable service. The SMA and DMAs (see Figure 97) each request a security agreement (SECAGREQ) containing their own security mechanisms and algorithms. After a Security Agree.time, the SM examines the SECAGREQ messages, determines the security policy for the session and sends the security policy (SECLIST) to the SMA and DMAs. If any of these MAs do not have the algorithms of the security policy, they request copies from the SM (SECALGREQ) and the SM sends the corresponding security modules to them. The method for the delivery of these modules is outside the scope of this Recommendation | International Standard. The SMA and each DMA configure the agreed security mechanisms. After configuration the MAs send an acknowledgement (SECAGANS) to the SM.

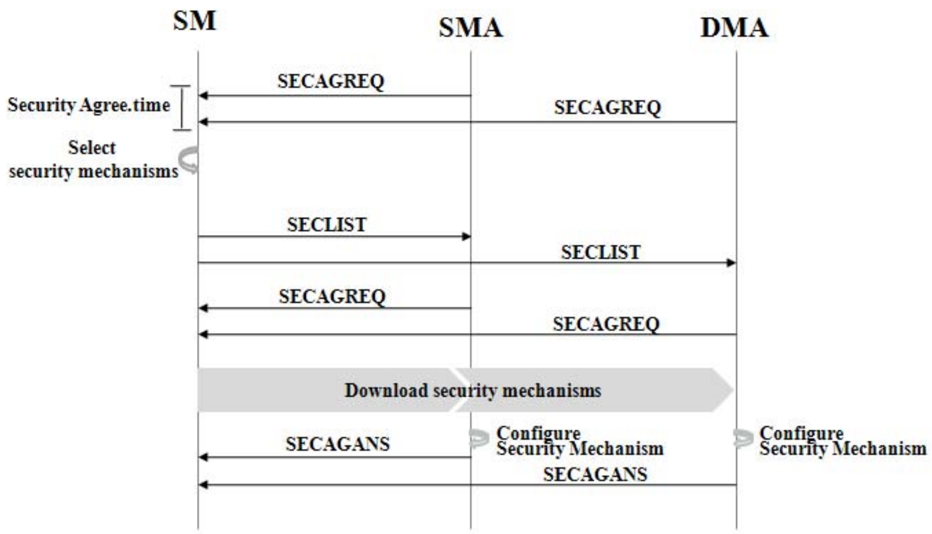


Figure 97 – Security agreement of DMA and SMA

10.1.4.2. RMAs

When the session is opened for RMA subscription, each RMA requests a security agreement (SECAGREQ) (see Figure 98). The SM sends the security policy (SECLIST) to the RMA, If the RMA does not have any of the algorithms of the security policy, it requests copies from the SM (SECALGREQ) and the SM sends the corresponding security modules to the RMA. The method for the delivery of these modules is outside the scope of this Recommendation | International Standard. The RMA configures the agreed security mechanisms and sends an acknowledgement (SECAGANS) to the SM.

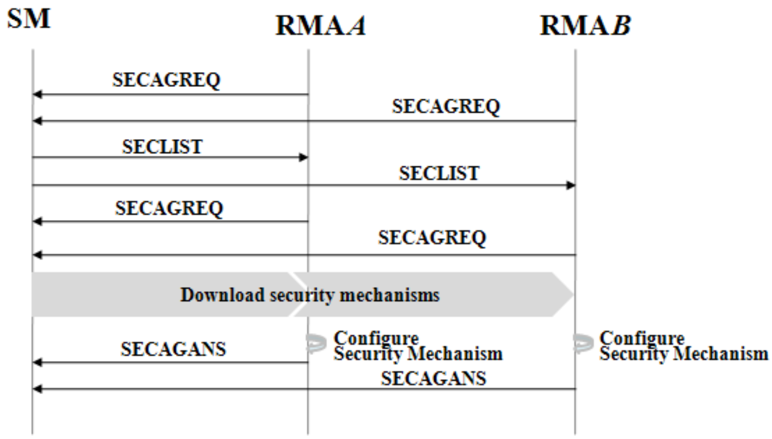


Figure 98 – Security agreement of RMAs

10.1.5. Access control for RMAs

The SM creates an access control list (ACL) containing hashed MAID and HASHED_AUTH for each authenticated RMA in the current session. Figure 99 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 encypted 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.

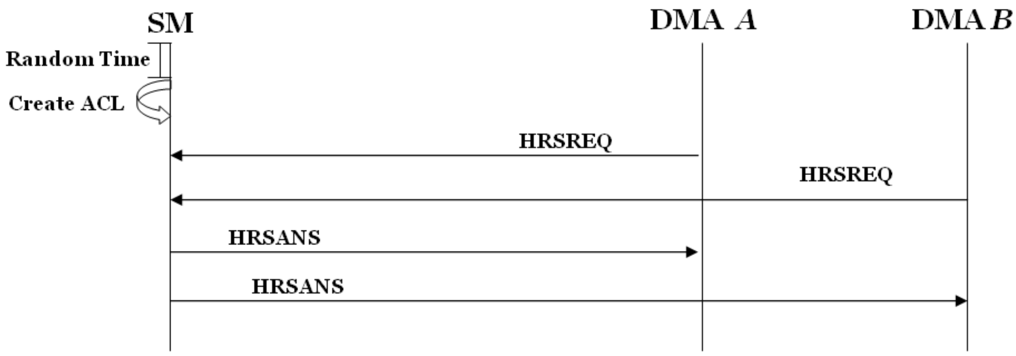


Figure 99 – ACL management

10.2. MA operation

As main components of the secure RMCP-2 protocol, the SMA and the DMAs are responsible for secure tree configuration and key management as well as for group and member management and message encryption/decryption.

10.2.1. Key management for which the SMA and DMAs are responsible

10.2.1.1. Group key management

A group key (Kg) is shared between a DMA and its child RMAs and it is used in an MM-group for data delivery. The Kg is initially created by the DMA and is encrypted by K_{MAS} (see10.2.1.3) for delivery to its RMAs in the RELANS message confirming successful membership authentication (see 11.2.4).

Kg is updated by the DMA or RMA according to the update conditions selected for the security policy (see the GK_MECHA control in Table 32).

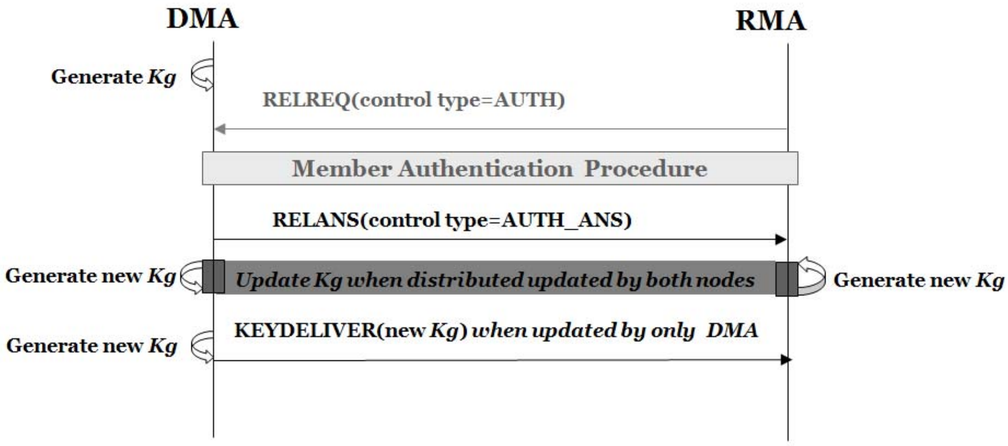


Figure 100 - Group key management

10.2.1.2. Contents encryption key management

The contents encryption key (Kc) is shared between the SMA and RMAs in the RMCP-2 session and is used to encrypt/decrypt contents data. Kc is generated by the SMA and is delivered to RMAs through the intermediate DMAs on the delivery path. Kc is encrypted by Ks for transmission between the SMA and DMAs and is encrypted by Kg for transmission between the DMAs and the RMAs. Kc key information need not be known by the SM or intermediate DMAs.

Kc is randomly updated by the SMA at periodic intervals. The delivery of Kc is synchronised with the delivery of the contents data (see 10.2.7).

10.2.1.3. Membership authentication Key

The membership authentication key K_{MAS} is a private key generated as a result of successful membership authentication between the RMAs and their parent DMA, as specified in Annex E. Each RMA shares a different K_{MAS} with the DMA and this is not shared with the other RMAs in the same group. K_{MAS} is not updated while the RMA remains a member of the relevant group.

10.2.2. Secure session subscription

The procedure for secure session subscription for the SMA, DMAs and RMAs is described in 10.1.1.2, 10.1.1.3, 10.1.1.4 and 10.1.1.5. This procedure is illustrated in Figure 101.

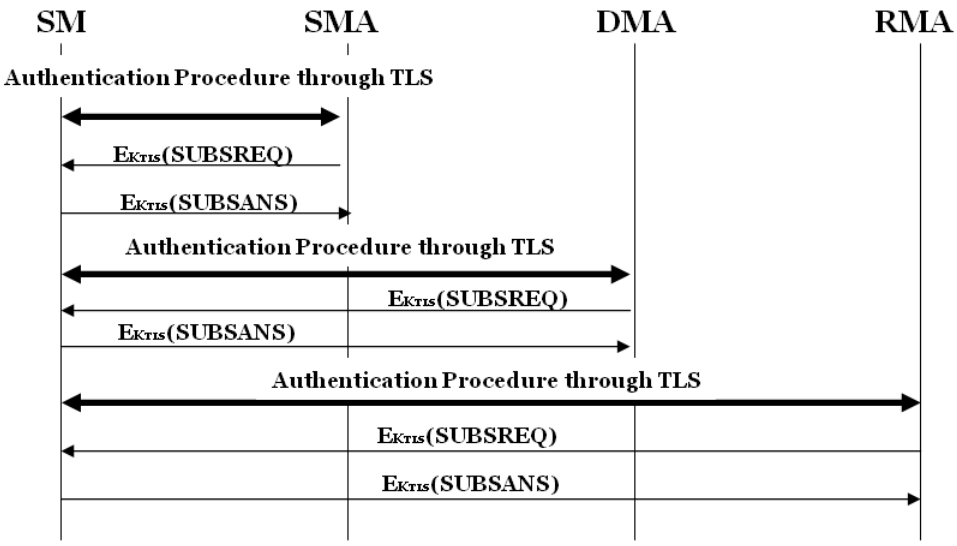


Figure 101– Secure MA subscription

10.2.3. Membership authentication for joining RMCP tree

Although DMAs are authenticated by the SM through TLS authentication, there is also a need for the DMAs and RMAs to verify their membership authority upon joining the RMCP tree and for construction of the pathway from the SMA to the RMAs. This procedure is important for the integrity of the RMCP-2 tree.

The membership authentication procedure defined in Annex E is used for mutual authentication.

The procedure is illustrated in Figure 102. The RMA|DMA sends a RELREQ message confirming the use of the membership authentication mechanism defined in Annex E. The SMA|DMA responds with a RELANS message containing the authentication result in the AUTH_ANS control. If the recipient is an RMA, the message to the RMA shall include the KEY_MATERIAL sub-control.

On receipt of confirmation by the RMA, the TLS session between the SM and the RMA need not be maintained.

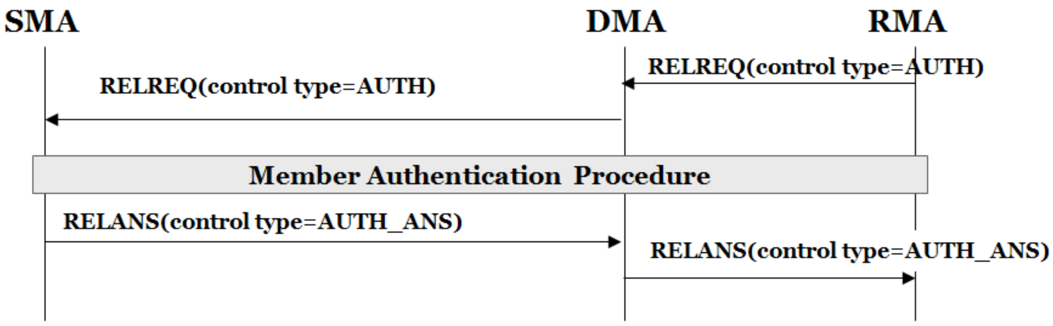


Figure 102 - Authentication between MAs

10.2.4. Secure tree join

Map discovery (see 6.2.2) occurs before the tree join procedure. Map discovery messages (PPROBREQ and PPROBANS) between DMAs are securely transmitted using Ks. Map discovery messages between RMAs and DMAs are delivered with hashed AUTH in plain text

The tree join procedure is illustrated in Figure 103. Membership authentication (see 10.2.3) 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 Table **41**), the parent DMA (see note) of the RMA joining the tree re-creates and distributes the group key to its RMAs using the GK_NAME mechanism selected for the security policy (see Table **42**). 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.

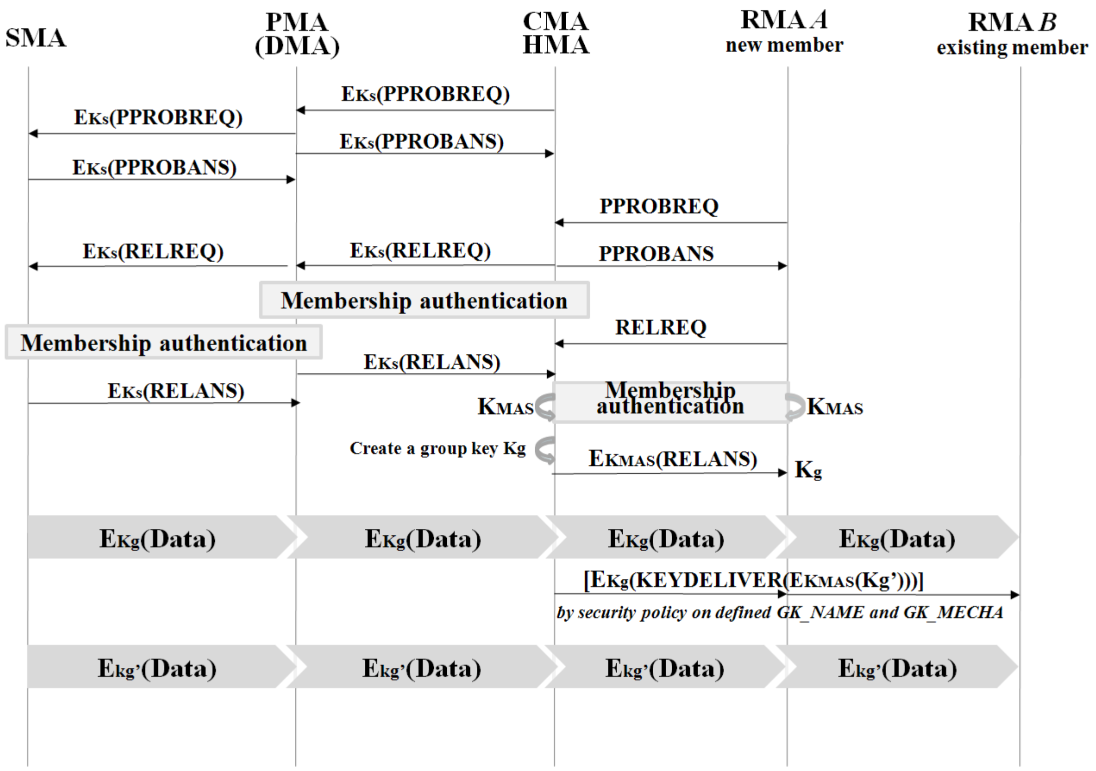


Figure 103 - Secure tree join. The PPROBREQ, PPROBANS and RELREQ messages between RMA A and the HMA are not encrypted as RMA A has not yet received the K_{MAS} or Kg keys

10.2.5. Secure tree leave

Whenever an HMA, DMA or RMA leaves the group, the group key or the session key may be updated on the defined GK_MECHA code of multicast security policy (see Table 42).

10.2.5.1. Leave of RMA from multicast-enabled and multicast-disabled areas

When an RMA leaves it notifies its parent DMA (its HMA in the case of multicast-enabled areas) and it is truncated from the tree. The DMA acknowledges the result, and updates and distributes the updated group key to remaining members (see Figure 104). No further notification is required.

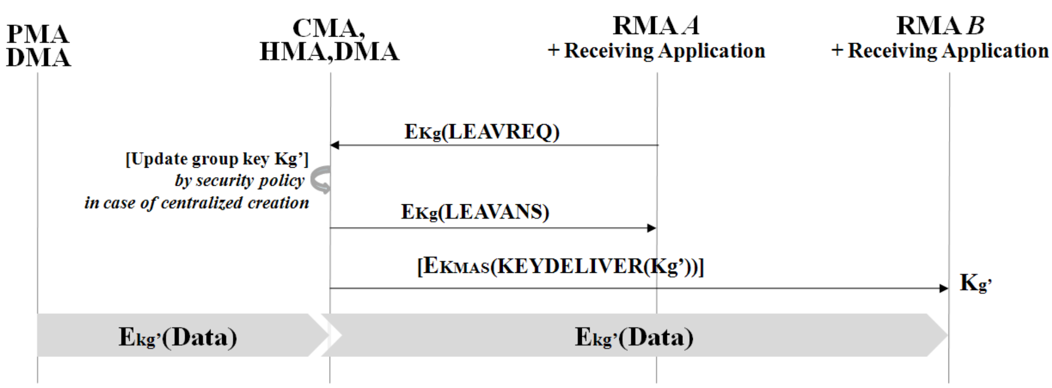


Figure 104 - Secure leave of RMA

10.2.5.2. Leave of HMA from a multicast-enabled area

Figure 105 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. (See Figure 105).

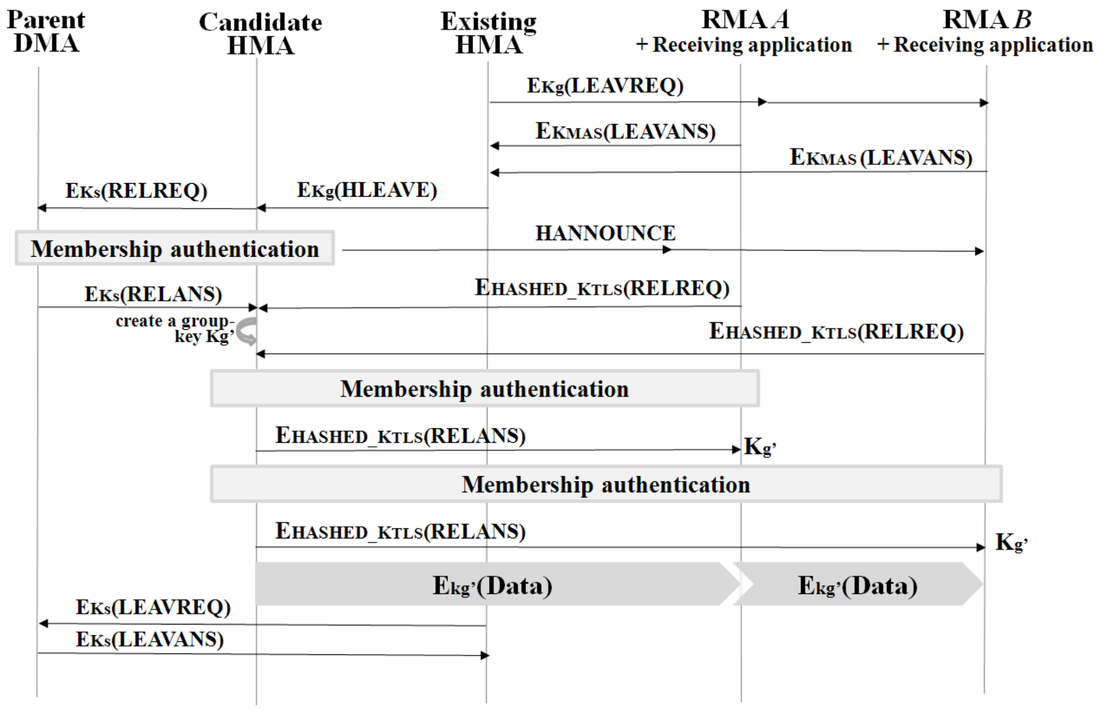


Figure 105 – HMA leave in multicast-enabled area

10.2.5.3. Leave of DMA from a multicast-disabled area.

Figure 106 illustrates the leave of a DMA from a multicast-disabled area. The DMA (PMA A of B, C) announces its departure from the RMCP tree to its children B, C. CMAs B and C search for their candidate PMA and perform the join procedure as shown in Figure 106. CMA B and C request to join at the RMCP tree at the node of the candidate PMA. The PMA verifies authenticity of CMA B and C, and if the authentication check is successful, it sends RELANS to confirm the graft to the RMCP tree. The PMA of B, C then initiates the leaving procedure with its PMA.

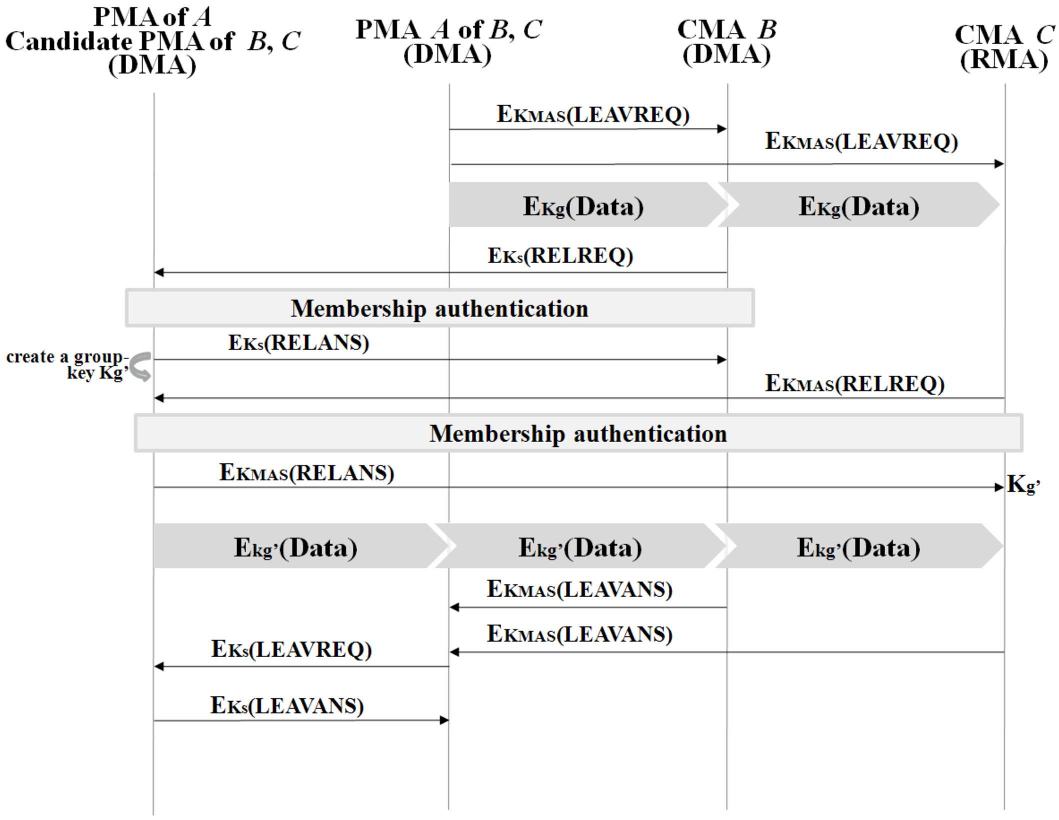


Figure 106 - DMA leave in multicast-disabled area

Membership authentication is performed between the RELREQ and RELANS messages in cases when a CMA is expelled by the PMA. If the SM expels an MA, the LEAVREQ and LEAVANS messages are en/decrypted.

10.2.6. Control message encryption/decryption

All secure RMCP-2 messages between the SM, SMA and DMAs are encrypted using agreed encryption algorithms in the SECLIST. Messages between RMAs and their parent DMA are encrypted by K_{MAS} as shown in Table 33.

Table 33 – Encryption of basic and 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		K_{MAS}
RELANS	Relay answer		K_{MAS}
STREQ	Status report request		K_{TLS}
STANS	Status report answer		K_{TLS}
STCOLREQ	Status collect request		*N/A*

STCOLANS	Status collect answer		*N/A*
LEAVREQ	Leave request		K_{MAS}
LEAVANS	Leave answer		K_{MAS}
HB	Heartbeat		*N/A*
TERMREQ	Termination request		*HASHED* K_{TLS}
TERMANS	Termination answer		*HASHED* K_{TLS}
SECAGREQ	Security agreement request		K_{TLS}
SECLIST	Security list		K_{TLS}
SECALGREQ	Security algorithm request		K_{TLS}
SECAGANS	Security agreement answer		K_{TLS}
KEYDELIVER	Key delivery		K_{MAS}, *Kg*
HRSREQ	ACL request		*N/A*
HRSANS	ACL answer		*N/A*

10.2.7. Encryption/Decryption and delivery of contents data

The contents are securely forwarded from the SMA to RMAs through the RMCP tree. Streaming or reliable data encrypted by *Kc* is delivered to individual RMAs without a decryption process at the intermediate nodes. In contrast the key information is encrypted at intermediate nodes. The SMA encrypts *Kc* using *Ks* and delivers it to DMAs. The DMAs then decrypt the key information and encrypt it using Kg for delivery to RMAs in their own MM groups. Figure 107 illustrates how the encryption and decryption may be implemented.

The data and key information may be delivered separately. If separately transmitted, they should be synchronized.

NOTE - The encrypted data is efficiently transmitted to the RMAs without change in order to reduce the time of encryption/decryption by the intermediate nodes. Faster transmission is enabled due to the considerably reduced computation time.

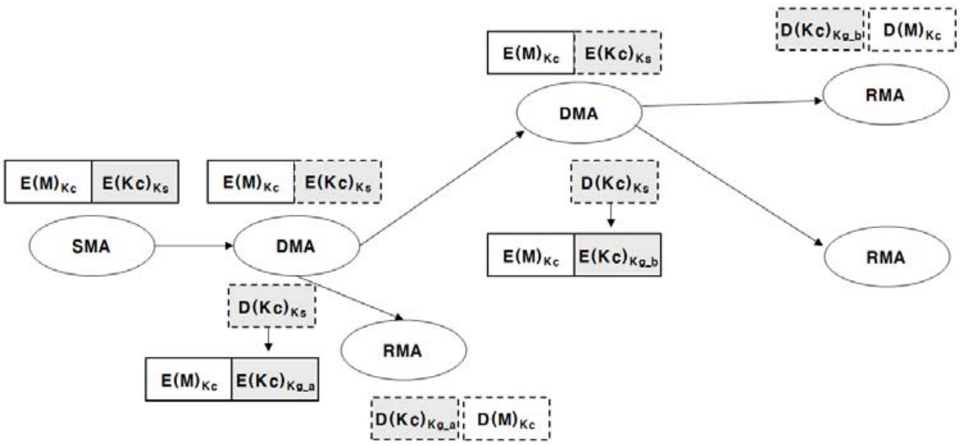


Figure 107 – Example of Data Encryption/Decryption. E(M) and D(M) refer to encrypted and decrypted data. E(Kc) and D(Kc) refer to encrypted and decrypted contents key information. Subscripts refer to keys used to encrypt (M) and (Kc). 'The suffixes $_{Kg\_a}$ and $_{Kg\_b}$ are used to distinguish different group keys used in separate MM groups.'

11. Format of Secure RMCP-2 messages

11.1. Common format for secure RMCP-2 messages

The common format for secure RMCP-2 messages is the same as for RMCP-2 messages (see 7.1 and Figure 31) except that:

a) all secure RMCP-2 messages, including those that are defined for RMCP-2 in 7.3 and used in the secure RMCP-

2 protocol, shall be defined as version 0x4; and

b) the range of valid Node Types for secure RMCP-2 messages is SM|SMA|DMA|RMA

11.2. Secure RMCP-2 messages

This sub-clause defines those messages that are specific to RMCP-2 security. They are used in addition to the messages already defined in 7.3. Specific reference is made to the values for individual parameters that are defined in tables associated with clause 12.

11.2.1. SUBSREQ message

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 0x4.

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 34.

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 108– SERV_USER_IDENT control data

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 joins a secure RMCP-2 session in which the MM groups are defined as closed.

The format of the SERV_USER_IDENT control type is shown in Figure 108. The description of each field is as follows:

· SERV_USER_IDENT

a) *Control type* – This field denotes SERV_USER_IDENT control. Its value shall be set to 0x22 (see Table 36)

b) *Length* – This field shall be set to the length in bytes of the SERV_USER_IDENT control in bytes.

c) *SERV_USER_ID* – This field 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 **45** 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 of the SUBANS message specified in 7.3.2.

11.2.3. RELREQ message

11.2.3.1. The RELREQ message for RMCP-2 is defined in 7.3.8 and its common format fields are shown in Figure 56. For use in secure RMCP-2 the following common format fields in the RELREQ message shall be set as indicated below:

a) *Version*. This field denotes the current version of RMCP. Its value shall be set to 0x4.

b) *Node Type*. This field denotes the message issuer’s node type. Its value shall be set to one of DMA or RMA coded as in Table 34.

The remaining common format fields for RELREQ messages shall be as specified in 7.3.8.

0	8	16	31
Control Type (AUTH)	Length (= 4)	AUTH_NAME	Reserved (0x00)

Figure 109 – AUTH control data

11.2.3.2. This sub-clause defines an additional AUTH control for use in secure RMCP-2 in order to initiate membership authentication. This control is a mandatory part of the secure RMCP_2 RELREQ message

The format of the AUTH control type is shown in Figure 109. The description of each field is as follows:

- AUTH
  a) *Control type* – This field denotes AUTH control. Its value shall be set to 0x23 (see Table 36)

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

  c) *AUTH_NAME* – This field denotes the authentication mechanism. Its value shall be set to 0x01 denoting MEM_AUTH (see Table **44**)

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

11.2.4. RELANS message

11.2.4.1. The RELANS message for RMCP-2 is defined in 7.3.9 and its common format fields are shown in Figure 58. For use in secure RMCP-2, the following common format fields in the RELANS message shall be set as indicated below:

a) *Version* – This field denotes the current version of RMCP. Its value shall be set to 0x4.

b) *Node Type* – This field denotes the message issuer’s node type. Its value shall be set to one of SMA or DMA coded as in Table 34.

The remaining common format fields for RELANS messages shall be as specified in 7.3.9.

0	8	16	24 31
Control Type (AUTH_ANS)	Length (= 4)	Auth_result	Key-Flag
Sub-control type (KEY_MATERIAL)	Length(= variable up to 0x804)		Key Type
Key_DATA			

Figure 110 - AUTH_ANS control, including KEY_MATERIAL sub-control

11.2.4.2. This sub-clause defines an additional AUTH_ANS control for use in secure RMCP-2 in order to notify the result of membership authentication. This control is a mandatory part of the secure RMCP_2 RELANS message

Figure 110 shows the format of the AUTH_ANS control type and its KEY_MATERIAL sub-control type. The description of each field of the AUTH_ANS control is as follows is as follows:

- AUTH_ANS
  a) *Control type* – This field denotes the AUTH_ANS control. Its value shall be set to 0x24 (see Table 37).
  b) *Length* – This field denotes the length in bytes of the AUTH_ANS control. Its value shall be set to 0x04.
  c) *Auth_result* – This field denotes the result of authentication. Its value shall be set to 0x01 for successful authentication; in the case of unsuccessful authentication the value shall be set to one of the other codes in Table 46.
  d) *Key_Flag* – This field denotes the presence or absence of key information in the KEY_MATERIAL sub-control of the AUTH_ANS control. Its value shall be set to 0x01 if key information is provided in the message; its value shall be set to 0x00 if this information is not provided.

11.2.4.3. The KEY_MATERIAL sub-control shall not be included in the RELANS message if the key flag is set to 0x00. The description of each field of the KEY_MATERIAL sub-control is as follows:

- KEY_MATERIAL
  a) *Sub-control type* – This field denotes the KEY_MATERIAL sub-control. Its value shall be set to 0x01 (see Table 37)
  b) *Length* – This field shall be set to the total length of the KEY_MATERIAL sub-control in bytes. Its value shall not exceed 0x804.
  c) *Key_Type* – This field denotes the type of the key information. Its value shall be set to one of the code values in Table 47.
  d) *Key_DATA* – This field shall contain key information resulting from 10.2.3 and it shall be included if the receiver is an RMA

11.2.5. SECAGREQ message

0	4	8	16 24 31
Ver (0x4)	NT (SMA|DMA|RMA)	Message type (SECAGREQ)	Length (variable)
Session ID (64)			
MAID (of the SECAGREQ sender)			
Control data (variable length)			

Figure 111 - SECAGREQ Message

11.2.5.1. The format of the SECAGREQ message is shown in Figure 111. The description of each field is as follows:

a) *Ver* – This field denotes the current version of RMCP. Its value shall be set to 0x4

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 34.

c) *Message Type* – This field denotes the type of SECAGREQ message. Its value shall be set to 0x21 (see Table 35)

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

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

f) *MAID* – This field denotes the proposed MAID of the SECAGREQ sender. Its value shall contain the local IP address and port number.

g) *Control data* – The controls associated with the SECAGREQ message are specified in 11.2.5.2 – 11.2.5.5. The following conditions apply to the use of these controls:

The SMA_PROPOSE control in 11.2.5.2 is used by the SMA to propose values to the SM for GR_ATTRIBUTE, GK_MECHA and CON_EN_DEC_ID and shall be included in a SECAGREQ message sent by the SMA. This control shall not be included in a SECAGREQ message sent by a DMA or an RMA.

The controls in 11.2.5.3 – 11.2.5.5 are used to indicate the capabilities of the SMA and DMAs during the establishment of the security policy (see 10.1.3 and 10.1.4). These controls shall not be included in a SECAGREQ message sent by an RMA or by a DMA that joins the session after the security policy has been established.

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

Figure 112 - SMA_PROPOSE control

11.2.5.2 The format of the SMA_PROPOSE control is shown in Figure 112. The description of each field is as follows:

- SMA_PROPOSE

a) *Control type* – This field denotes the SMA_PROPOSE control. Its value shall be set to 0x11 (see Table 36)

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

c) *GP_ATTRIBUTE* – This field denotes the group property proposed by the SMA. Its value shall be set to one of the code values in Table 40.

d) *GK_MECHA* – This field 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 41.

e) *CON_EN_DEC_ID* – This field 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 **38**.

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

0	8	16	24 31
Control Type (GK_MECH_CAPAB)	Length (= 4)	GK_NAME	PREFER
Control Type (GK_MECH_CAPAB)	Length (= 4)	GK_NAME	PREFER
Control Type (GK_MECH_CAPAB)	Length (= 4)	GK_NAME	PREFER

Figure 113 - GK_MECH_CAPAB control

11.2.5.3. The format of the GK_MECH_CAPAB control is shown in Figure 113. This control may be repeated in order to indicate several mechanisms, each with their own order of preference. The description of each field is as follows:

GK_MECH_CAPAB

a) *Control type* – This field denotes the GK_MECH_CAPAB control. Its value shall be set to 0x12 (see Table 36)

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

c) *GK_NAME* – This field denotes a security mechanism 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 42.

d) *PREFER* – This field denotes the priority of the proposed security mechanism in the preceding field. Its value shall be set to an integer in the range 1 to 6. The integer '1' shall indicate the highest priority.

0	8	16	24 31
Control Type (EN_DEC_CAPAB)	Length (= 4)	EN_DEC_ID	PREFER
Control Type (EN_DEC_CAPAB)	Length (= 4)	EN_DEC_ID	PREFER
Control Type (EN_DEC_CAPAB)	Length (= 4)	EN_DEC_ID	PREFER

Figure 114 - EN_DEC_CAPAB control

11.2.5.4. The format of the EN_DEC_CAPAB control is shown in Figure 114. This control may be repeated in order to indicate several mechanisms, each with their own order of preference. The description of each field is as follows:

· EN_DEC_CAPAB

a) *Control type* – This field denotes the EN_DEC_CAPAB control. Its value shall be set to 0x13 (See Table 36)

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

c) *EN_DEC_ID* – This field denotes proposed an encryption 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 **38**.

d) *PREFER* – This field denotes the priority of the proposed security mechanism in the preceding field. Its value shall be set to an integer in the range 1 to 5. The integer '1' shall indicate the highest priority.

0	8	16	24 31
Control Type (AUTH_ALG_CAPAB)	Length (= 4)	AUTH_ID	PREFER
Control Type (AUTH_ALG_CAPAB)	Length (= 4)	AUTH_ID	PREFER
Control Type (AUTH_ALG_CAPAB)	Length (= 4)	AUTH_ID	PREFER

Figure 115 - AUTH_ALG_CAPAB control

11.2.5.5. The format of the AUTH_ALG_CAPAB control is shown in Figure 115. This control type may be repeated in order to indicate several mechanisms, each with their own order of preference. The description of each field is as follows:

· AUTH_ALG_CAPAB

a) *Control type* – This field denotes the AUTH_ALG_CAPAB control. Its shall be set to 0x14 (see Table 36)

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

c) *AUTH_ID* – This filed 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 39.

d) *PREFER* – This field denotes the priority of the proposed security mechanism in the preceding field. Its value shall be set to an integer in the range 1 to 3. The integer '1' shall indicate the highest priority

11.2.6. SECLIST message

11.2.6.1. The format of the SECLIST message is shown in Figure 116. The description of each field is as follows:

0	8	16	24 31
Ver (0x4)	NT (SM)	Message type (SECLIST)	Length (variable)
Session ID			
MAID (of the SECLIST recipient)			
Control data (variable length)			

Figure 116 - SECLIST message

a) *Ver* – This field denotes the current version of RMCP. Its shall be set to 0x4

b) *NT* – This field denotes the message issuer's node type. Its value shall be set to the code value for SM in Table 34

c) *Message Type* – This field denotes the SECLIST message. Its value shall be set to 0x22 (see Table 35)

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

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

f) *MAID* – This field denotes the MAID of the SECLIST recipient. Its value shall be as defined in 7.1.2

g) *Control data* – The controls associated with the SECLIST message are specified in 11.3.5.2 – 11.3.5.6 . All of these controls are a mandatory part of the message.

0	8	16	24 31
Control Type (GK_MECH)	Length (= 8)	GP_ATTRIBUTE	GK_NAME
GK_MECHA	Reserved (0x00)		

Figure 117 - GK_MECH control

11.2.6.2. The format of the GK_MECH control is shown in Figure 117. The description of each field is as follows:

- GK_MECH

a) *Control type* – This field denotes the GK_MECH control. Its value shall be set to 0x15 (see Table 36)

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

c) *GP_ATTRIBUTE* – This field denotes the group property for the security policy. Its value shall be set to one of the code values in Table 40

d) *GK_NAME* – This field defines the group key mechanism for the security policy. Its value shall be set to one of the code values in Table 42

e) *GK_MECHA* – This field denotes the update property of group key for the security policy. Its value shall be set to one of the code values in Table 41.

0	8	16	24 31
Control Type (AUTH_MECH)	Length (= 4)	AUTH_ATTRIBUTE	AUTH_NAME

Figure 118 – AUTH_MECH control

11.2.6.3. The format of the AUTH_MECH control is shown in Figure 118. The description of each field is as follows:

· AUTH_MECH

a) *Control type* – This field denotes the AUTH_MECH control. Its value shall be set to 0x16 (see Table 36)

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

c) *AUTH_*ATTRIBUTE – This field denotes the authentication type for the security policy. Its value shall be set to 0x01 denoting MEMBERSHIP (see Table 43).

d) *AUTH_NAME* – This denotes the authentication mechanism for the security policy. Its value shall be set to 0x01 denoting MEM_AUTH (see Table 44).

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

Figure 119 – CON_EN_DEC_ALG control

11.2.6.4. The format of the CON_EN_DEC_ALG control is shown in Figure 119. The description of each field is as follows:

· CON_EN_DEC_ALG

a) *Control type* – This field denotes the CON_EN_DEC_ALG control. Its value shall be set to 0x17 (see **Table 36**).

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

c) *EN_DEC_ID* – This field denotes the contents encryption algorithm for the security policy. Its value shall be set to one of the code values in
Table **38**.

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

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

Figure 120 – GK_EN_DEC_ALG control

11.2.6.5. The format of the GK_EN_DEC_ALG control is shown in Figure 120. The description of each field is as follows:

· GK_EN_DEC_ALG

a) *Control type* – This field denotes the GK_EN_DEC_ALG control. Its value shall be set to 0x18 (see Table 36).

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

c) *GK_EN_DEC_ID* – This field denotes the group key encryption algorithm for the security policy. Its value shall be set to one of the code values in

Table **38**.

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

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

Figure 121 – AUTH_ALG control

11.2.6.6 The format of the AUTH_ALG control is shown in Figure 121. The description of each field is as follows:

· AUTH_ALG

a) *Control type* – This field denotes the AUTH_ALG control. Its value shall be set to 0x19 (see Table 36).

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

c) *AUTH_ID* – This field denotes the hash/MAC algorithm for the security policy. Its value shall be set to one of the code values in Table 39.

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

11.2.7. SECALGREQ message

0	4	8	16 24 31
Ver (0x4)	NT (SMA|DMA|RMA)	Message type (SECAGANS)	Length (variable)
Session ID (64)			
MAID (of the SECALGREQ sender)			
Control data (variable length)			

Figure 122 – SECALGREQ Message

11.2.7.1. The format of the SECALGREQ message is shown in Figure 122. The description of each field is as follows:

a) *Ver* – This field denotes the current version of RMCP. Its value shall be set to 0x4

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 34.

c) *Message Type* – This field denotes the SECALGREQ message. Its value shall be set to 0x27 (see Table 35)

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 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 SECALGREQ sender. Its value shall be formatted as defined in 7.1.2.

g) *Control data* – The controls associated with the SECALGREQ message, together with conditions applying to their use, are specified in 11.4.7.2 – 11.4.7.6.

0	8	16	24 31
Control Type (GK_MECH_DELIVER)	Length (= 4)	GK_NAME	Reserved (0x00)

Figure 123 – GK_MECH_DELIVER control

11.2.7.2 The format of the GK_MECH_DELIVER control is shown in Figure **123**. This control shall only be used by the MA sending the SECALGREQ message when it does not hold the GK_NAME security algorithm or when the configuration of this 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* – This field denotes the GK_MECH_DELIVER control. Its value shall be set to 0x1A (see Table 36)

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

c) *GK_NAME* – This field denotes the group key mechanism for the security policy. Its value shall be identical to that in the GK_NAME field in the GK_MECH control of the SECLIST message (see 11.2.6.2.d).

d) *Reserved* – This field is reserved 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 124 – AUTH_MECH_DELIVER control

11.2.7.3 The format of the AUTH_MECH control is shown in Figure 124. This control shall only be used by the MA sending the SECALGREQ message when it does not hold the AUTH_NAME security algorithm or when the configuration of this 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* – This field denotes the AUTH_MECH_DELIVER control. Its value shall be set to 0x1B (see Table 36).

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

c) *AUTH_NAME* – This field denotes the authentication mechanism for the security policy. Its value shall be set to 0x01 denoting MEM_AUTH (see Table 44).

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

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

Figure 125 – CON_EN_DEC_DELIVER control

11.2.7.4 The format of the CON_EN_DEC_DELIVER control is shown in Figure 125. This control shall only be used by the MA sending the SECALGREQ message when when it does not hold the CON_EN_DEC_ALG security algorithm or when the configuration of this 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* – This field denotes the CON_EN_DEC_DELIVER control. Its value shall be set to 0x1C (see Table 36).

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

c) *CON_EN_DEC_ID* – This field 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 11.2.6.4.c).

d) *Reserved* – This field 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 126 – GK_EN_DEC_DELIVER control

11.2.7.5 The format of the GK_EN_DEC_DELIVER control is shown in Figure **126**. This control shall only be used by the MA sending the SECALGREQ message when it does not hold the GK_EN_DEC_ALG security algorithm or when the configuration of this 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

a) *Control type* – This field denotes the GK_EN_DEC_DELIVER control. Its value shall be set to 0x1D (see Table 36).

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

c) *GK_EN_DEC_ID* – This field denotes the 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 11.2.6.5.c).

d) *Reserved* – This field 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 127 – AUTH_ALG_DELIVER control

11.2.7.6 The format of the AUTH_ALG control is shown in Figure 127. This control shall only be used by the MA sending the SECALGREQ message when it does not hold the AUTH_ALG security algorithm or when the configuration of this 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* – This field denotes the AUTH_ALG_DELIVER control. Its value shall be set to 0x1E (see Table 36).

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

c) *AUTH_ID* – This field 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 11.2.6.6.c).

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

11.2.8. SECAGANS message

<table>
<tr><td>0</td><td>8</td><td>16</td><td>24 … 31</td></tr>
<tr><td>Ver (0x4)</td><td>NT
(SMA|DMA|RMA)</td><td>Message type
(SECAGANS)</td><td>Length (variable)</td></tr>
<tr><td colspan="4">Session ID (64)</td></tr>
<tr><td colspan="4">MAID (of the SECAGANS sender)</td></tr>
<tr><td colspan="4">Control data (variable length)</td></tr>
</table>

Figure 128 – SECAGANS Message

11.2.8.1. The format of the SECAGANS message is shown in Figure 128. The description of each field is as follows:

a) *Ver* – This field denotes the current version of RMCP. Its value shall be set to 0x4

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 34

c) *Message Type* – This field denotes SECAGANS message. Its value shall be set to 0x23 (see Table 35)

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 sender. 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.

0	*8*	*16*	*24* … *31*
Control Type (SEC_RETURN)	Length (= 4)	SEC_RETURN	Reserved

Figure 129 – SEC_RETURN control

11.2.8.2. The format of the SEC_RETURN control is shown in Figure **129**. The description of each field is as follows:

· SEC_RETURN

a) *Control type* – This field denotes the SEC_RETURN control. Its value shall be set to 0x1F (see Table 36)

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

c) *SEC_RETURN* – This field denotes the result of SECAGREQ request. Its value shall be set to 0x01 for a successful return; the value for other results shall be indicated by one of the other remaining codes in Table 46.

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

11.2.9 KEYDELIVER message

<table>
<tr><th>0</th><th>8</th><th>16</th><th>24   31</th></tr>
<tr><td>Ver (0x4)</td><td>NT
(SM|SMA|DMA)</td><td>Message type
(KEYDELIVER)</td><td>Length (variable)</td></tr>
<tr><td colspan="4">Session ID (64)</td></tr>
<tr><td colspan="4">MAID (of the KEYDELIVER recipient)</td></tr>
<tr><td colspan="4">Control data (variable length)</td></tr>
</table>

Figure 130 - KEYDELIVER Message

11.2.9.1. Figure 130 shows the format of the KEYDELIVER message. The description of each field is as follows:

a) *Ver* –This field denotes the current version of RMCP. Its value shall be set to 0x4

b) *NT* – This field denotes the message issuer's node type. Its value shall be set to

- 0x01, the coded value for SM in Table 34, for the delivery of the Ks key information; or
- 0x05, the coded value for DMA in Table 34, for the delivery of the Kg key information; or
- 0x02 the coded value for SMA in Table 34, for the delivery of the Kc key information.

c) *Message Type* – This field denotes the KEYDELIVER message. The value shall be set to 0x24 (see Table 35)

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

e) *Session ID* – This field shall be set to the 64-bit value of Session ID as defined in7.1.1

f) *MAID* – This field denotes the MAID of the KEYDELIVER recipient. Its value shall be as defined in 7.1.2

g) *Control data* – The KEY_INFO control and its KEY_MATERIAL sub-control, specified in 11.2.9.2 and 11.2.9.3, are a mandatory part of the KEYDELIVER message.

11.2.9.2. The format of the KEY_INFO control and its KEY_MATERIAL sub-control is shown in Figure 130. The description of each field of the KEY_INFO control is as follows:

· KEY_INFO

a) *Control type* – This field denotes the KEY_INFO control. Its value shall be set to 0x20 (see Table 36)

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

c) *Key_type* – This field denotes the type of the proposed key information. Its value shall be set to one of the code values in Table 47

0	8	16	24	31
Control Type (KEY_INFO)	Length (= 4)	Key_type	Reserved (0x00)	
Sub-control type (KEY_MATERIAL)	Length(= variable up to 0x804)		Key_Type	
KEY_DATA				

Figure 131 - KEY_INFO control, including KEY_MATERIAL sub-control

11.2.9.3. The description of each field of the KEY_MATERIAL sub-control is as follows:

- KEY_MATERIAL
  a) *Sub-control type* – This field denotes the KEY_MATERIAL sub-control. Its value shall be set to 0x01 (see Table 37)
  b) *Length* – This field shall be set to the total length in bytes of the KEY_MATERIAL sub-control. Its value shall not exceed 0x804
  c) *Key_Type* – This field denotes the type of the key information. Its value shall be set to one of the code values in Table 47
  d) *KEY_DATA* – This field shall contain the time information and seed value needed to generate the key identified by Key_Type

11.2.10. HRSREQ message

0		8	16	24	31
Ver (0x4)	NT (DMA)	Message type (HRSREQ)	Length (variable)		
Session ID (64)					
MAID (of the HRSREQ sender)					

Figure 132 - HRSREQ Message

The format of the HRSREQ message is shown in Figure 132. The description of each field is as follows:

a) *Ver* –This field denotes the current version of RMCP. The value shall be set to 0x4

b) *NT* – This field denotes the message issuer's node type. Its value shall be set to the coded value for DMA in Table 34

c) *Message Type* – This field denotes the HRSREQ message. The value shall be set to 0x25 (see Table 35)

d) *Length* – This field denotes the length in bytes of the HRSREQ message. Its value shall be set to 0x14.

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

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

NOTE – There is no control data associated with the HRSREQ message

11.2.11. HRSANS message

0	8	16	24	31
Ver (0x4)	NT (SM)	Message type (HRSANS)	Length (variable)	
Session ID (64)				
MAID (of the HRSANS recipient)				
Control data (variable length)				

Figure 133 - HRSANS Message

11.2.11.1. The format of the HRSANS message is shown in Figure 133. The description of each field is as follows:

a) *Ver* – This field denotes the current version of RMCP. Its value shall be set to 0x4

b) *NT* – This field denotes the message issuer's node type. Its value shall be set to 0x01, the code value for the SM in Table 34.

c) *Message Type* – This field denotes the HRSANS message. Its value shall be set to 0x26 (see Table 35)

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

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

f) *MAID* – This field denotes the MAID of the HRSANS recipient. Its value shall be as defined in 7.1.2

g) *Control data* – The ACL_LIST control its ACL_DATA sub-control, specified in 11.2.11.2 and 11.2.11.3, are a mandatory part of the HRSANS message.

0	8	16	24	31
Control Type (ACL_LIST)	Length (= 2)	Sub-control type (ACL_DATA)	Reserved (0x00)	
Length (variable)		N_ACL		
DATA(HASHED MAID|| HASHED K_{TLS})				
DATA(HASHED MAID|| HASHED K_{TLS})				
:				

Figure 134 - ACL_LIST control, including ACL_DATA sub-control

11.2.11.2. The format of the ACL_LIST control and its ACL_DATA sub-control is shown in Figure 134. The description of each field of the ACL_LIST control type is as follows:

· ACL_LIST

a) *Control type* – This field denotes the ACL_LIST control. Its value shall be set to 0x21 (see Table 36)

b) *Length* – This field denotes the length in bytes of the ACL_LST control. Its value shall be set to 0x02.

11.2.11.3. The description of each field of the ACL_DATA sub-control is as follows:

· ACL_DATA

a) *Sub-control type* – This field denotes the ACL_DATA sub-control. Its value shall be set to 0x02 (see Table 37)

b) *Length* – This field shall be set to the length in bytes of the ACL_DATA sub-control.

c) *N_ACL* – This field shall be set to the number of the entries in the ACL-list.

d) *ACL_DATA* – This field shall contain the HASHED MAID, HASHED K_{TLS} for each authenticated RMA in the current session.

12. Parameters

12.1. Secure RMCP-2 node types and code values

Table 34 lists the node types and their corresponding code values.

Table 34 – Node Type Codes for secure RMCP-2

Code	Node type	Definition
0x01	SM	Session Manager
0x02	SMA	Sender Multicast Agent
0x03	RMA	Receiver Multicast Agent
0x05	DMA	Dedicated Multicast Agent

12.2. Secure RMCP-2 message types and code values

Table 35 lists the message types and their corresponding code values.

Table 35 – RMCP-2 Message Types and code Values

Message Type	Meaning	Code Value (hexadecimal)	Cross reference to message format
SUBSREQ	Subscription request (Control type = SERV_USER_IDENT)	0x02	See 11.2.1
RELREQ	Relay request (Control type=AUTH)	0x09	See 11.2.3
RELANS	Relay answer (Control type =AUTH_ANS)	0x0C	See 11.2.4
SECAGREQ	Security Agreement Request	0x21	See 11.2.5
SECLIST	Selected Security List	0x22	See 11.2.6
SECALGREQ	Security Algorithms Request	0x27	See 11.2.7
SECAGANS	Security Agreement Answer	0x23	See 11.2.8
KEYDELIVER	Key Delivery	0x24	See 11.2.9
HRSREQ	Head Required Security Request	0x25	See 11.2.10
HRSANS	Head Required Security Answer	0x26	See 11.2.11

NOTE – The code values for the SUBSREQ, RELREQ and RELANS messages are as specified in Table 23 for basic RMCP-2 message types

12.3. Secure RMCP-2 control types and code values

Table 36 lists the control types and their corresponding code values.

Table 36 - Control types for secure RMCP-2

Control Type	Meaning	Code Value (hexadecimal)	Message types containing the control type
SERV_USER_IDENT	Service User Identification	0x22	SUBSREQ
AUTH	Authentication	0x23	RELREQ

AUTH_ANS	Authentication Answer	0x24	RELANS
SMA_PROPOSE	Security profile values proposed by the SMA	0x11	SECAGREQ
GK_MECH_CAPAB	Group Key Mechanism Capabilites	0x12	SECAGREQ
EN_DEC_CAPAB	Encryption/Decryption algorithm Capabilities	0x13	SECAGREQ
AUTH_ALG_CAPAB	Hash/MAC Algorithm Capabilities	0x14	SECAGREQ
GK_MECH	Group Key Mechanism	0x15	SECLIST
AUTH_MECH	Authentication Mechanism	0x16	SECLIST
CON_EN_DEC_ALG	Contents Encryption/Decryption Algorithm	0x17	SECLIST
GK_EN_DEC_ALG	Group Key Encryption/Decryption Algorithm	0x18	SECLIST
AUTH_ALG	Hash/MAC Algorithm	0x19	SECLIST
GK_MECH_DELIVER	Group Key Mechanism Delivery Request	0x1A	SECALGREQ
AUTH_MECH_DELIVER	Authentication Mechanism Delivery Request	0x1B	SECALGREQ
CON_EN_DEC_DELIVER	Contents Encryption/Decryption Algorithm	0x1C	SECALGREQ
GK_EN_DEC_DELIVER	Group Key Encryption/Decryption Algorithm Delivery Request	0x1D	SECALGREQ
AUTH_ALG_DELIVER	Hash/MAC Algorithm Delivery Request	0x1E	SECALGREQ
SEC_RETURN	Security Return	0x1F	SECAGANS
KEY_INFO	Key Information	0x20	RELANS KEYDELIVER
ACL_LIST	Access Control List	0x21	HRSANS

Table 37 lists the sub-control types and their corresponding code values.

Table 37 – Sub-control types for secure RMCP-2

Sub-control Type	Meaning	Code Value (hexadecimal)	Message types containing the Control Type
KEY_MATERIAL	Key material to generate the key	0x01	RELANS KEYDELIVER
ACL_DATA	ACL-list	0x02	HRSANS

12.4. Code values related to the RMCP-2 security policy

Table 38 lists the EN_DEC_ID ,CON_EN_DEC_ID and GK_EN_DEC_ID codes for the security policy

Table 38 – EN_DEC_ID, CON_EN_DEC_ID and GK_EN_DEC_ID codes

Code	Meaning	Reference
0x01	AES CBC Mode 128bit key	ISO/IEC 18033-3:2005
0x02	AES CTR Mode 128bit key	ISO/IEC 18033-4:2005
0x03	PKCS #1	ISO/IEC 18033-2:2006
0x04	The SEED Encryption Algorithm	ISO/IEC 18033-3:2005
1x01	Values greater than 1x00 are reserved for other modes of AES and SEED defined by the SM	ISO/IEC 18033-3:2005
1x02		
1x03		

NOTE – EN_DEC_ID, CON_EN_DEC_ID and CON_EN_DEC_ID are located in separate fields of the secure RMCP-2 messages. Although the values for the EN_DEC_ID, CON_EN_DEC_ID and GK_EN_DEC_ID parameters may differ, the meaning of each code, as listed above, is identical wherever it is used.

Table 39 lists the AUTH_ID codes for the security policy

Table 39 – 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

Table 40 lists the GP_ATTRIBUTE codes for the security policy.

Table 40 – GP_ATTRIBUTE codes

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)

Table 41 lists the GK_MECHA codes for the RMCP-2 security policy.

Table 41 - GK_MECHA Codes

Code	Attribute	Meaning
0x00	STATIC	Only one Group Key is used per one session
0x01	PERIODIC	Group Key is updated periodically
0x02	BACKWARD	Group Key is updated whenever any member leaves the group
0x04	FORWARD	Group Key is updated whenever any member joins the group
0x03	PERIODIC+BACKWARD	
0x05	PERIODIC+FORWARD	
0x06	BACKWARD+FORWARD	
0x07	PERIOIDC+FORWARD+BACKWARD	

Table 42 lists the GK_NAME codes for the RMCP-2 security policy.

Table 42 – GK_NAME codes

Code	Acronym	Meaning	Reference
0x01	KDC	Group Key Management Protocol (GKMP) Architecture	IETF RFC 2094
0x02	GKMP	Group Key Management Protocol (GKMP) Specification	IETF RFC 2093
0x03	MIKEY	Multimedia Internet KEYing	IETF RFC 3830
0x04	GSAKMP	Group Secure Association Key Management Protocol	IETF RFC 4535
0x05	LKH	Key Management for Multicast: Issues and Architectures	IETF RFC 2627

Table 43 shows the AUTH_ATTRIBUTE code for the RMCP-2 security policy.

Table 43 - AUTH_ATTRIBUTE code

Code	Value	Meaning
0x01	MEMBERSHIP	Membership of the session is authenticated using the Membership Authentication procedure defined in Annex A

Table 44 shows the AUTH_NAME code for the RMCP-2 security policy.

Table 44 – AUTH_NAME code

Code	Acronym	Meaning	Reference
0x01	MEM_AUTH	Membership authentication	The procedure defined in Annex E

12.5. Miscellaneous code values

Table 45 lists two additional result codes that 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 result codes are specific to the secure RMCP-2 protocol and they supplement the code values in Table 23 that are also used in the secure RMCP-2 protocol.

Table 45 – Additional result codes for the RMCP-2 return value

Result code	Meaning
0x41	SERV_USER_ID missing
0x42	SERV_USER_ID not recognized

Table 46 lists the SEC_RETURN and Auth-result codes for the RMCP-2 security policy.

Table 46– SEC_RETURN and Auth_result codes

Code	Value	Meaning
0x01	OK	Authentication satisfactory
0x02	ERROR	Error found on authentication

0x03	RETRANSMISSION_REQ	Retransmission Requested
0x04	FAIDED CONFIGURATION	Applies only to SEC_RETURN in the SECAGANS message

Table 47 lists the KEY_TYPE codes for key delivery.

Table 47 – KEY_TYPE codes

Code	Value	Meaning
0x01	Ks	Session Key
0x02	Kg	Group Key
0x03	Kc	Contents Encryption Key

Annex E

Membership authentication Mechanism

(This annex forms an integral part of this Recommendation | International Standard)

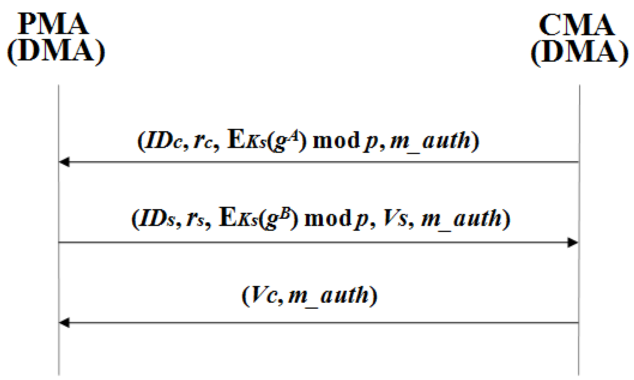
E.1 Overview

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.

Membership authentication checks whether a node is a session member; it plays the role of a member of the RMCP tree or local group of the MM region and assumes that any node trying to authenticate membership for the RMCP tree or the group is verified by SM in the RMCP-2 session in advance, since the procedure is executed based on the password information of the node. To configure the RMCP tree, PMA and CMA perform this procedure when CMA wants to be a child node of PMA. Likewise, DMA and RMA authenticate their counterparts to transmit multicast data to the regular members joining the MM group.

E.2 Authentication Procedure

The membership authentication is initiated on a RELREQ message containing an AUTH control in the RELREQ message (see 11.2.3). PMA and DMA can be servers, and CMA and RMA, client parties. The client requests the server to authenticate a membership using some authentication materials: identifier (IDc), random number (r_c), and encrypted value by hashed 'auth' ($E_k(g^A)$ mod p). The server then sends its authentication materials: IDs, r_s, $Ek(g^B)$ mod p, and Vs(Vector value). Finally, authentication is finished successfully when the client sends vector value Vc. The authentication procedure is based on the Diffie Hellman algorithm. Here, A and B are arbitrary values, and K_{MAS} as a shared key between the client and the server encrypts Kg in the local group of the MM region. Here, the random number *r* should be securely generated on cryptographically secure pseudo bit random generator (CGSPRBG) such as PKCS#1, Micali−Schnorr and Blum−Blum−Shub pseudo bit random generators. 'm_auth' is value created by a message digest algorithm for message integrity.The value is made by symmetrical or asymmetrical secure MAC functions. 'auth' is AUTH-information of the SUBSREQ message.



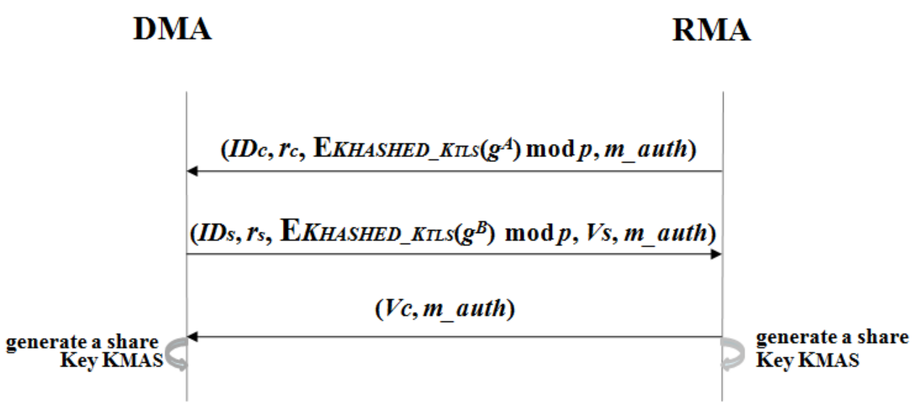
$$Vs = (\mathrm{H}(g^{AB} \oplus r_c \oplus r_s \oplus Ks)) \bmod p$$
$$Vc = (\mathrm{H}(Vs \oplus r_c \oplus r_s \oplus Ks)) \bmod p$$

Authentication

$\rightarrow$ PMA : $\mathrm{H}(g^{AB} \oplus g^A \oplus g^B \oplus IDc \oplus IDs \oplus Ks)$

?= CMA : $\mathrm{H}(g^{AB} \oplus g^A \oplus g^B \oplus IDc \oplus IDs \oplus Ks)$

Figure E.1 – Membership authentication between PMA and CMA



$$Vs = (H(g^{AB} \oplus r_c \oplus r_s \oplus Ks)) \bmod p$$
$$Vc = (H(Vs \oplus r_c \oplus r_s \oplus Ks)) \bmod p$$
$$K_{MAS} = H(g^{AB} \oplus g^A \oplus g^B \oplus IDc \oplus IDs \oplus K_{HASHED\_KTLS})$$

Authentication

$\rightarrow$ DMA : $H(g^{AB} \oplus g^A \oplus g^B \oplus IDc \oplus IDs \oplus K_{HASHED\_KTLS})$

?= RMA : $H(g^{AB} \oplus g^A \oplus g^B \oplus IDc \oplus IDs \oplus K_{HASHED\_KTLS})$

Figure E.2 – Membership authentication between DMA and RMA

Table E.1 – Definition of variables for membership authentication

Variables/Functions	Definitions
E(*x*)	Encryption function on defined multicast security policy
H(*x*)	Hash function on defined AUTH_ALG of multicast security policy
Mod	Modulation operator
IDc	Identifier of client-side; CMA and RMA
Ids	Identifier of server-side; PMA and DMA
r_c	Random number from client-side; CMA and RMA
r_s	Random number from server-side; PMA and DMA
G	generator on Diffie-Hellman algorithm
A	Arbitrary value by client-side; CMA and RMA
B	Arbitrary value by server-side; PMA and DMA
P	Defined value on Diffie-Hellman algorithm
Vs	Vector value on Diffie-Hellman algorithm from server-side; PMA and DMA
Vc	Vector value on Diffie-Hellman algorithm from client-side; CMA and RMA

Successful authentication is indicated by Auth_result with a value of 0x01 in the AUTH_ANS control of the RELANS message..

Annex F

Bibliography

(This annex does not form an integral part of this Recommendation | International Standard.)

F.1 Informative references

– IETF RFC 2093 (1997), *Group Key Management Protocol (GKMP) Specification*.

– IETF RFC 2627 (1999), *Key Management for Multicast: Issues and Architectures*.