INTERNATIONAL STANDARD

ISO/IEC 16513

First edition
2005-02-15

Information technology — Group management protocol

Technologies de l'information — Protocole de gestion de groupe

Reference number
ISO/IEC 16513:2005(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

CONTENTS

Page

1 Scope ... 1
2 Normative references ... 1
3 Definitions ... 1
3.1 Terms defined in ITU-T Rec. X.601 ... 1
3.2 Terms defined in ITU-T Rec. X.605 ... 2
3.3 Terms defined in this Recommendation | International Standard ... 2
4 Abbreviations ... 2
4.1 Message types ... 2
4.1.1 SM Message types ... 2
4.1.2 MM Message types ... 2
4.2 Miscellaneous ... 3
5 Conventions ... 3
6 Overview ... 3
6.1 Session Management ... 4
6.2 Membership Management ... 4
7 Protocol operations ... 6
7.1 Session Management ... 6
7.1.1 Session Creation ... 6
7.1.2 Session Announcement ... 7
7.1.3 Session Registration ... 7
7.1.4 Session Enrolment ... 8
7.1.5 Session Activation ... 8
7.2 Membership Management ... 9
7.2.1 Membership Update ... 11
7.2.2 User Information Request and Response ... 13
7.2.3 Session Leave ... 13
7.2.4 Session Termination ... 14
7.3 Security ... 15
8 GMP messages ... 17
8.1 Session Management message types ... 17
8.2 Session Management message formats ... 18
8.3 Membership Management message types ... 20
8.4 Membership Management message formats ... 20
9 GMP variables ... 22
9.1 Session-wide variables ... 22
9.2 Timers ... 22
Bibliography ... 23

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 16513:2005 was prepared jointly by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems* in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.602.

Introduction

Conventional multicast transport protocols do not include a dynamic mechanism for group management according to the join/leave of receivers and for the modification of membership information.

GMP provides a framework for multicast session management (SM) mechanism and membership management (MM), which supports the required management of multicast sessions and their members. This protocol can be key to reliable multicast communications.

GMP will operate over conventional transport protocols and/or ECTP as shown in Figure 1.

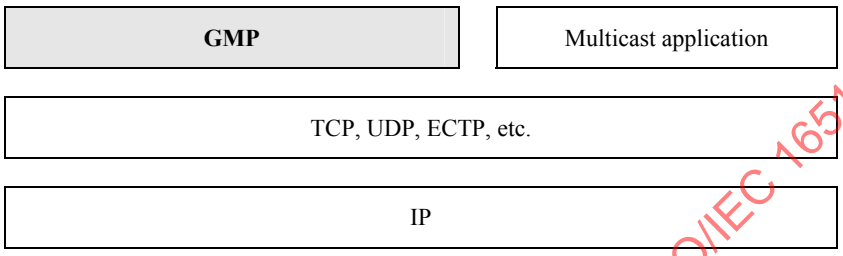

Figure 1 – GMP model (GMP protocol stack)

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Group management protocol

1 Scope

This Recommendation | International Standard provides a specification of a Group Management Protocol (GMP), which is an application-layer control protocol for creating a group session and for managing the group's participating members.

The GMP consists of session management (SM), membership management (MM), and the function of exchanging information between SM and MM. SM is responsible for session creation and deletion. MM manages the member lists based on session information retrieved from SM.

According to ITU-T Rec. X.601, "Multi-peer communications framework", the multi-peer communication service is achieved in seven distinct phases: registration, enrolment, activation, data transfer, deactivation, de-enrolment, and de-registration. Since one of these operations – data transfer – may be performed using ECTP or TCP, SM may perform the rest of operations: creation, announcement, registration, enrolment, activation, including session announcement. In addition, MM manages group members who are in enrolled or active groups.

SM may provide a convenient interface to users because it may be implemented on the Web. Operation of MM is transparent to users as in a transport protocol.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

- ITU-T Recommendation X.601 (2000), *Multi-peer communications framework.*
- ITU-T Recommendation X.605 (1998) | ISO/IEC 13252:1999, *Information technology – Enhanced Communications Transport Service definition.*
- ITU-T Recommendation X.606 (2001) | ISO/IEC 14476-1:2002, *Information technology – Enhanced Communications Transport Protocol: Specification of simplex multicast transport.*
- ITU-T Recommendation X.606.1 (2003) | ISO/IEC 14476-2:2003, *Information technology – Enhanced Communications Transport Protocol: Specification of QoS management for simplex multicast transport.*

3 Definitions

3.1 Terms defined in ITU-T Rec. X.601

This Recommendation | International Standard is based on the concepts developed in the Multi-Peer Communications Framework (ITU-T Rec. X.601) and makes use of the following terms defined in that Recommendation:

a) Multi-peer;

b) Multi-peer communication; and

c) Multicast transmission.

3.2 Terms defined in ITU-T Rec. X.605 | ISO/IEC 13252

This Recommendation | International Standard is based on the concepts developed in Enhanced Communications Transport Service Definition (ITU-T Rec. X.605 | ISO/IEC 13252) and makes use of the following terms defined in that Recommendation:

a) Enrolled Group;

b) Registered Group;

c) Active Group; and

d) TC-owner.

3.3 Terms defined in this Recommendation | International Standard

3.3.1 GMP client: An application program that sends and receives GMP. Clients store and acquire information through a server. All clients must log in to the server to acquire information from the server. Clients are largely divided between session creator and session participants.

3.3.2 GMP server: A server is an application program that is responsible for session management and membership management.

3.3.3 session creator: A client who creates and who may terminate a session. Logging on to the server through its own ID, the creator inputs information about creating a session and sends the information to the server. The server that received the request from the creator adds the information into the created session list. The Session creator may be a TC-owner defined in ECTS.

3.3.4 session client: A client who intends to be a Session Participant.

3.3.5 session participant: A Client who registers for a session intending to participate in that session. After registration, the session participant will join the session to be an active member (i.e., start session list and registered member list). A Session Participant may be a TC-participant defined in ECTS.

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply.

4.1 Message types

4.1.1 SM message types

SAREQ	Session Activation Request message
SCACC	Session Creation Accept message
SCCON	Session Creation Confirm message
SCINF	Session Creation Information message
SCREJ	Session Creation Reject message
SCREQ	Session Creation Request message
SDREQ	Session Deletion Request message
SDRES	Session Deletion Response message
SJREQ	Session Join Request message
SJRES	Session Join Response message
SRACC	Session Registration Accept message
SRREJ	Session Registration Reject message
SRREQ	Session Registration Request message
SRRES	Session Registration Response message

4.1.2 MM message types

KAREQ	Keepalive Request message
KARES	Keepalive Response message
UIREQ	User Information Request message

UIRES	User Information Response message
LVREQ	Leave Request message
TRREQ	Termination Request message
TRIND	Termination Indication message
KDUPT	Key Distribution Update message

4.2 Miscellaneous

ECTP	Enhanced Communications Transport Protocol
ECTS	Enhanced Communications Transport Service
MM	Membership Management
RMT	Reliable Multicast Transport
SAP	Session Announcement Protocol
SDP	Session Description Protocol
SM	Session Management
IP	Internet Protocol
LQA	Lowest Quality Allowed
MSS	Maximum Segment Size
OT	Operating Target
QoS	Quality of Service
RSVP	Resource reSerVation Protocol

5 Conventions

In this Recommendation | International Standard, the keywords "MUST", "REQUIRED", "SHALL", "MUST NOT", "SHALL NOT", "SHOULD", "SHOULD NOT", "MAY", and "OPTIONAL" are to be interpreted as described in IETF RFC 2119, and indicate requirement levels for compliant ECTP implementations. Those keywords are case-sensitive.

6 Overview

GMP is an application-layer control protocol for creating a group session and for managing the group's participating members.

Generally it is assumed that there is one GMP server, one session creating client (or Session Creator), and one or more session participating clients (or Session Participants) as shown in Figure 2.

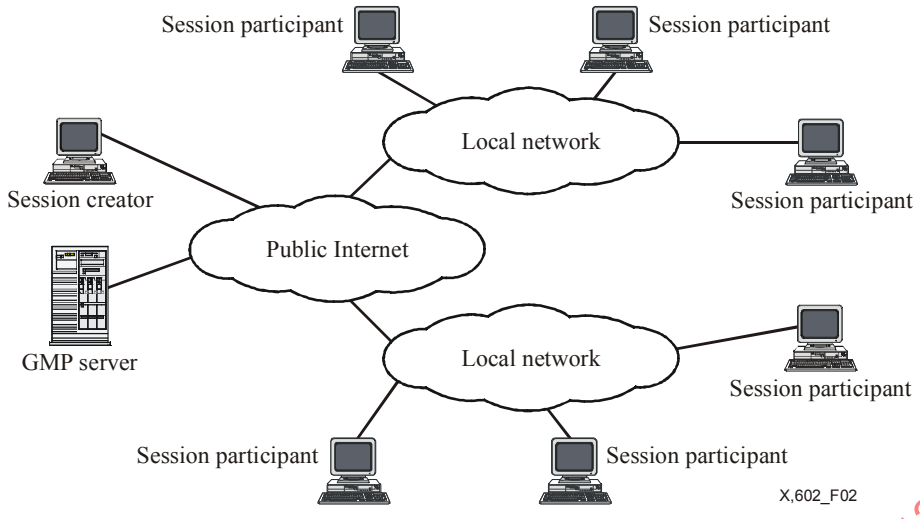

Figure 2 – Network configuration for GMP

GMP is composed of session management (SM), membership management (MM), and the function of exchanging information between SM and MM.

6.1 Session Management

SM may be achieved in eight distinct phases: creation, announcement, registration, enrolment, activation, de-registration, de-enrolment, and de-activation.

A particular client, called a session creator, creates a session. Then, SM updates the session list.

The session creator will send a Session Creation Request message to the server. If accepted, the session creator will receive the Session Creation Accept message from the server. Then the session creator will send the detailed session information to the server and receive the confirmation message. If the session cannot be created or the session creator does not have the necessary rights, then the Session Creation Reject message will be returned.

After successful session creation, the server will announce the new session to the clients. The announcement may be done by e-mail, web posting, and so on. From this point on, those clients may register in multicast groups.

A client may register for a session. Any client may register for the open-mode session, while some pre-authorized clients may register for the closed-mode session. After successful registration, the client belongs to the registered group.

When the session starts, the session's registered members will start a group application to send and receive session data. At this time, all preparations for the data transfer and group management are accomplished. The session's registered group member belongs to the enrolled group.

When the session creator sends real data or when the session's enrolled members receive real data, then those participants are said to be in active state. Membership management is then activated.

6.2 Membership Management

When a session is activated, the server immediately sends a status report request to each session's active member. The server will update the active members' list and other information based on information received from the participants. These updates will be accomplished periodically.

A session participant may leave the session by sending a leave message to the server.

To terminate an ongoing session, the session creator sends a session termination message to the server, which then will notify the session termination to every participant, and terminate the session.

Figure 3 shows an example of GMP operations and their relation between session status and multicast group phases defined in ITU-T Rec. X.601.

After a session is created and announced, three session clients, A, B, and C try to register for the session. However, one client C is rejected because this client is not authorized to do so, or has improper rights. When the session creator and clients send the session join request to the server, they enter the enrolled state. At this time, they are ready to communicate with each other. And they enter the active state by sending a specific active request message to the server. By that message, the MM will classify members, who are either in the active state, or in the enrolled state. The server

will update the active member list based on the periodic update request and reply. Session Participant A leaves the session, sending the leave message to the server. From that moment, the server will update the active list by sending the update request only to two active participants. When the session creator wants to terminate the session, the session termination request will be sent to the server, which will then send the session termination notice to the session participants.

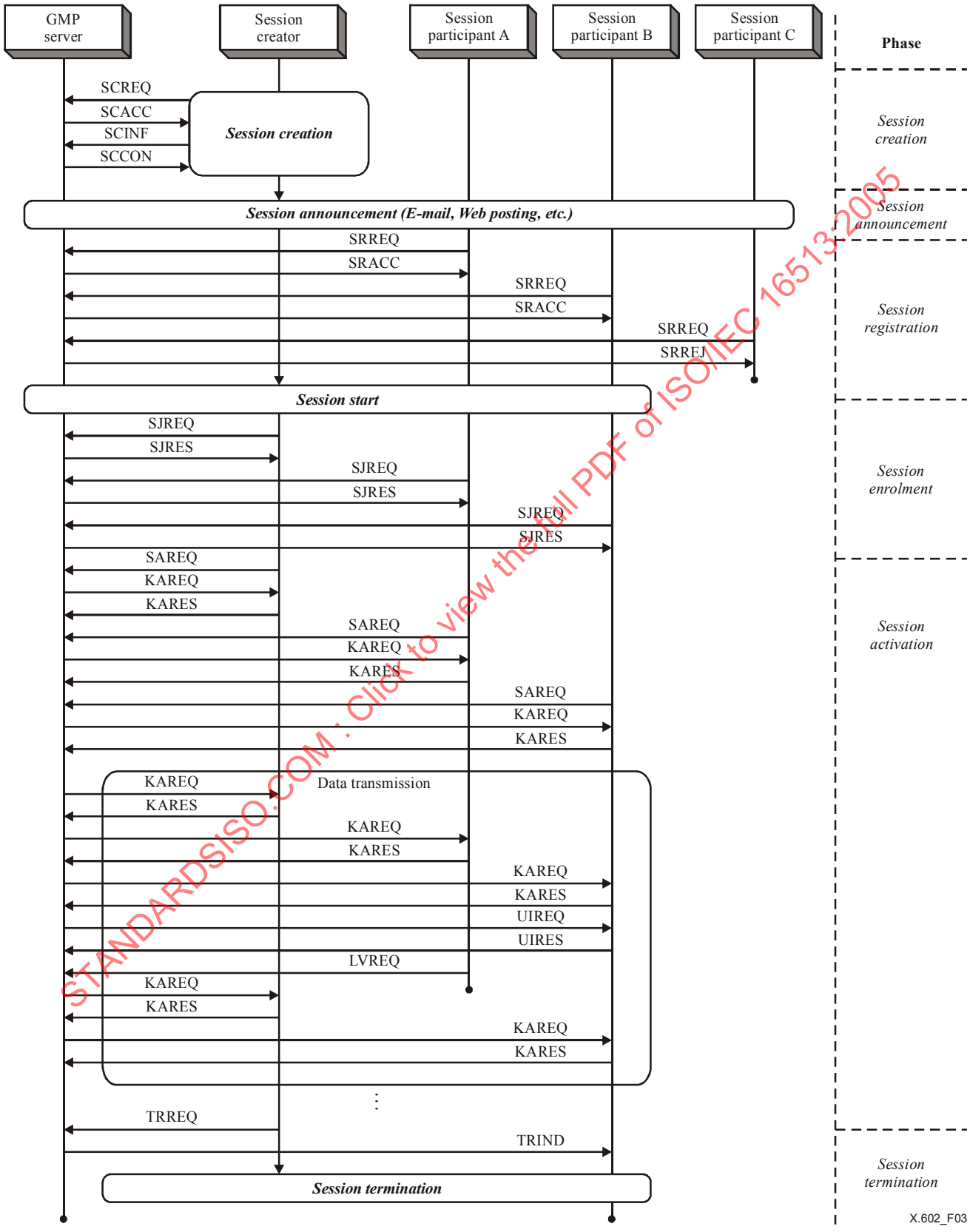

Figure 3 – An example of the GMP control

7 Protocol operations

7.1 Session Management

SM may be achieved in eight distinct phases: creation, announcement, registration, enrolment, activation, de-registration, de-enrolment, and de-activation.

SM is responsible for the following:

a) Session Creation: A session creator creates the session.

b) Session Announcement: An SM server typically announces information about the session to session clients.

c) Session Registration: Clients register for a session to the SM server.

d) Session Enrolment: After registration, an enrolment operation accomplishes the whole "set-up" that is necessary for multicast group communication.

e) Session Activation: After activation, a session participant in the session receives the data from the session creator. The session participants belong to the active group.

The mode of the session will be one of the following:

a) Closed mode;

b) Open mode.

In the closed mode, the session participation may be restricted by a session creator, who may distribute the access control message to the target participants. A participant will register for the session only after the authorization process. In the open mode, any client may register for the session.

7.1.1 Session Creation

Session creation is effected by a session creator, who will define and characterize the session with media type, application type, additional information, and so on.

A session creator may define core members, who should be registered or enrolled. If a requirement for a core member is not satisfied, the session may not start.

Figure 4 shows the successful session creation procedure. A Session Creator defines and characterizes a session and sends a Session Creation Request message, SCREQ, to the session server. SCREQ is a mere request asking whether a new creation is possible or not. Considering the multicast environment and its application, the server may allow a new session creation by replying with a Session Creation Accept message, SCACC. Then, the Session Creator will send detailed session information in Session Creation Information message, SCINF, which may include media type, application type, etc. The server will acknowledge successful session creation with a Session Creation Confirm message, SCCON, and then update its session list.

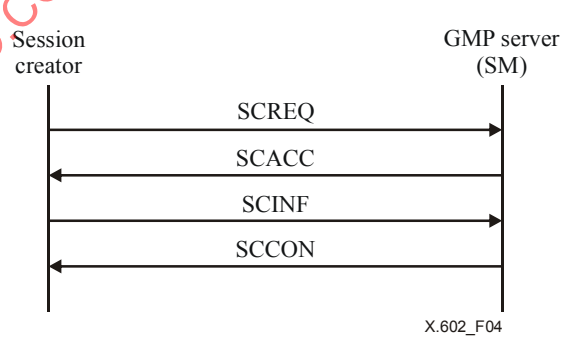

Figure 4 – Successful session creation procedure

Figure 5 shows an unsuccessful session creation procedure. When a Session Creator requests a new session creation from the server, if the server does not have enough sources, or if the requestor does not have the proper authorization, the request will be rejected by the server, and the server sends a Session Creation Reject message, SCREJ.

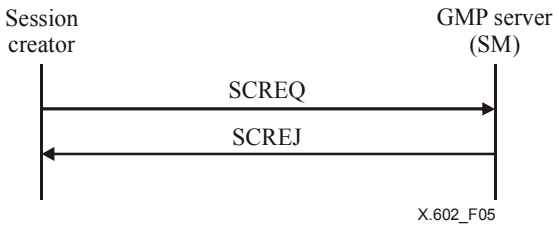

Figure 5 – Unsuccessful session creation procedure

7.1.2 Session Announcement

Session creation will be announced through e-mail, web posting or other off-line ways. Through this announcement, session clients will know the existence and the characteristics of all created sessions. Session participants may know whether the session is in the open mode or in the closed mode. In the closed mode, the access control message should be distributed to the selected clients by the session creator, with which the clients can access to the session information and register for the closed mode session later.

7.1.3 Session Registration

Session registration is to select a session and to let the server and creator know the intention of the participation.

In the open mode session, the session client will select a session and send the Session Registration Request message, SRREQ, to the server. The server will add the requesting client to the Registered Group Membership list, and reply to the requestor with Session Request Accept message, SRACC, as shown in Figure 6.

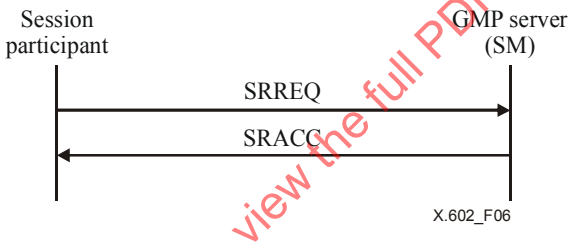

Figure 6 – Successful session registration procedure (Open mode)

In the closed mode session, the session client will select a session and send the Session Registration Request message, SRREQ to the server. Then the server will immediately reply with a Session Registration Response message, SRRES to indicate that the valid authorization process is initiated. If the registration is valid, then the server will send Session Registration Accept message, SRACC as shown in Figure 7.

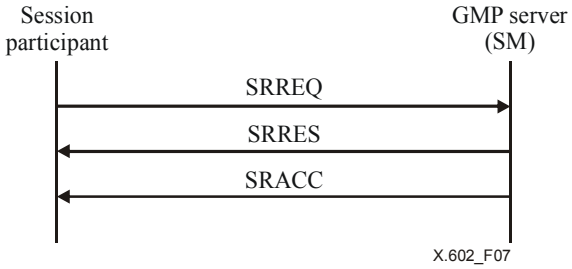

Figure 7 – Successful session registration procedure (Closed mode)

If the session registration request is not authorized in the closed mode session, the server will send the Session Registration Reject message, SRREJ, as shown in Figure 8.

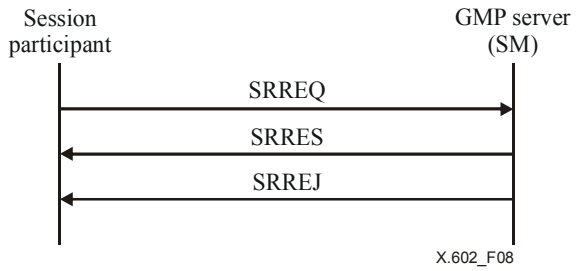

Figure 8 – Unsuccessful session registration procedure (Closed mode)

7.1.4 Session Enrolment

Session enrolment is the state where communication is possible among the session participants and the session creator. Session participants, including the session creator, should send the Session Join Request message, SJREQ. The server will add the participants to the Enrolled Group Membership list, and reply to the requestor with the Session Join Response message, SJRES, as shown in Figure 9.

Figure 9 – Successful session enrolment

MM manages a Registered Group Membership list separate from an Enrolled Group Membership list.

7.1.5 Session Activation

Session activation is the state where the session participants and the session creator are in the data transfer phase. Session participants, including the session creator, should send the Session Activation Request message, SAREQ. The server will reply with the Keepalive Request message, KAREQ. If the server receives the Keepalive Response message, KARES, from the session participants, then it updates the Active Group Membership list, as shown in Figure 10.

The server will maintain the Active Group Membership list based on the periodic KAREQ and KARES exchanges.

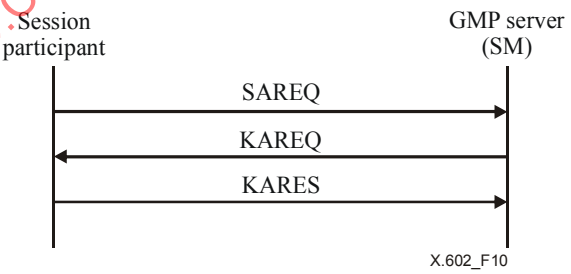

Figure 10 – Successful session activation

In the late join case, a session participant who is in the enrolled state will send the SAREQ to join the ongoing session.

If a session participant sends the KARES after receiving KAREQ, then the server will add that participant to the Active Group Membership list.

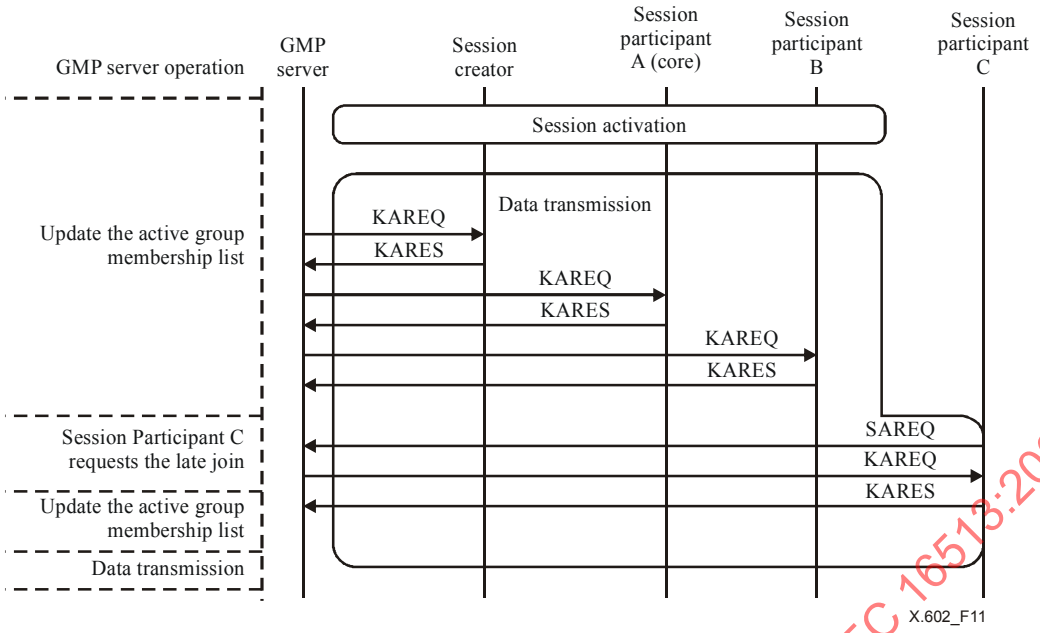

Figure 11 – Late join procedure

7.2 Membership Management

MM maintains and manages active group members.

Figure 12 shows the membership management updating the lists at the GMP server. Upon receiving KARES from the Session Participants, GMP membership management server will check whether the client belongs to the registered group list. If yes, GMP server will check whether the client belongs to the enrolled group. If the client does not belong to the enrolled group, the client will be added to the enrolled group. And if the client belongs to the enrolled group, then the GMP server will check whether the client belongs to the active group. If the client does not belong to the active group, the client will be added to the active group and reset the KeepAlive (KA) timer. If the client belongs to the active group, GMP server will reset the KA timer and waits for the next KARES.

If the GMP server does not receive KARES from a Session Participant and the KA timer to the Session Participant expires, the GMP membership management server will check which group the Session Participant belongs to. If the Session Participant belongs to the active group, that participant will be moved to the enrolled group. If the participant belongs to the enrolled group, that participant will be moved to the registered group. Then, the GMP server resets the KA timer.

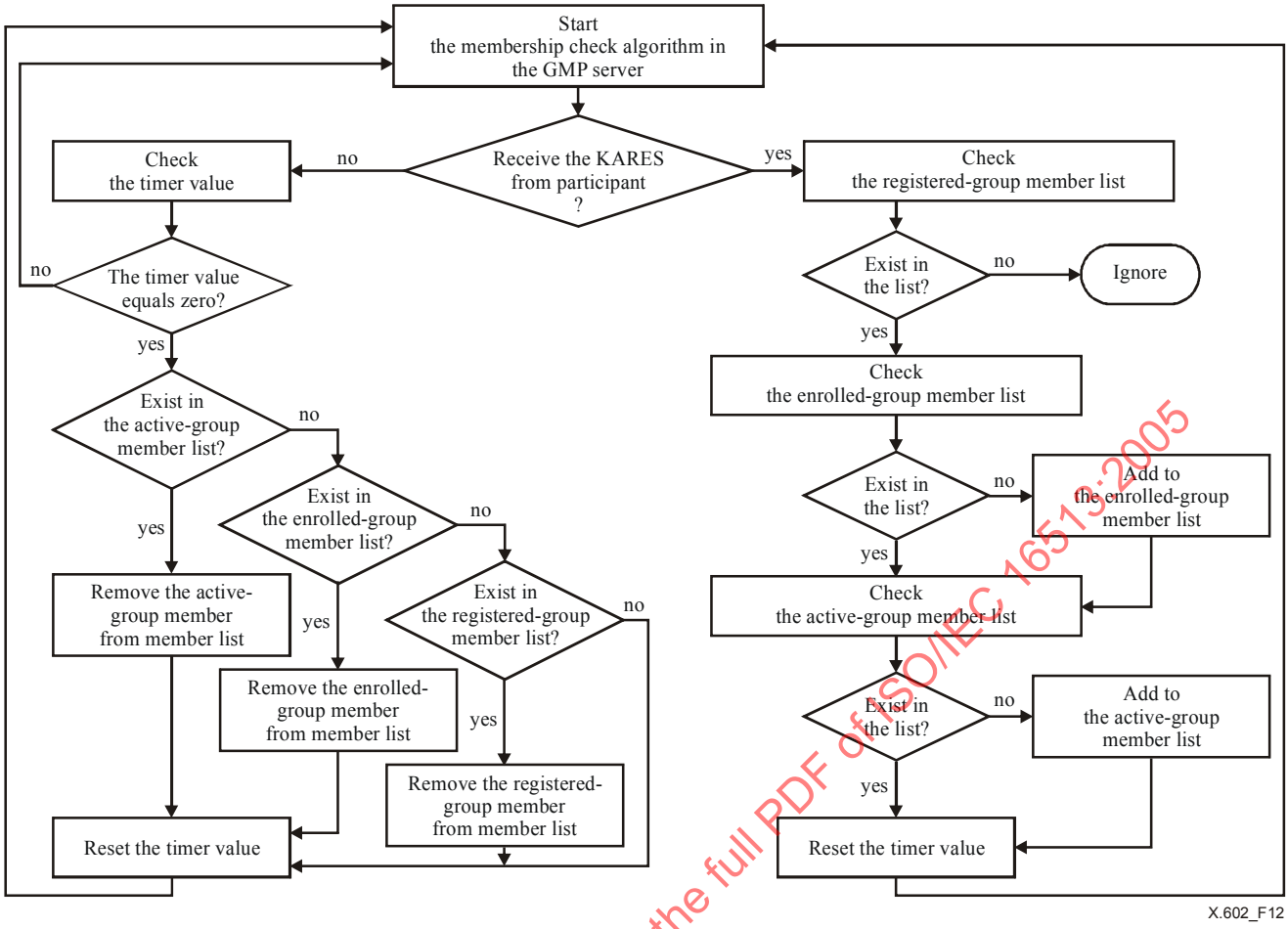

Figure 12 – Membership check algorithm in the server

Figure 13 shows the membership management message-receiving process at the GMP server.

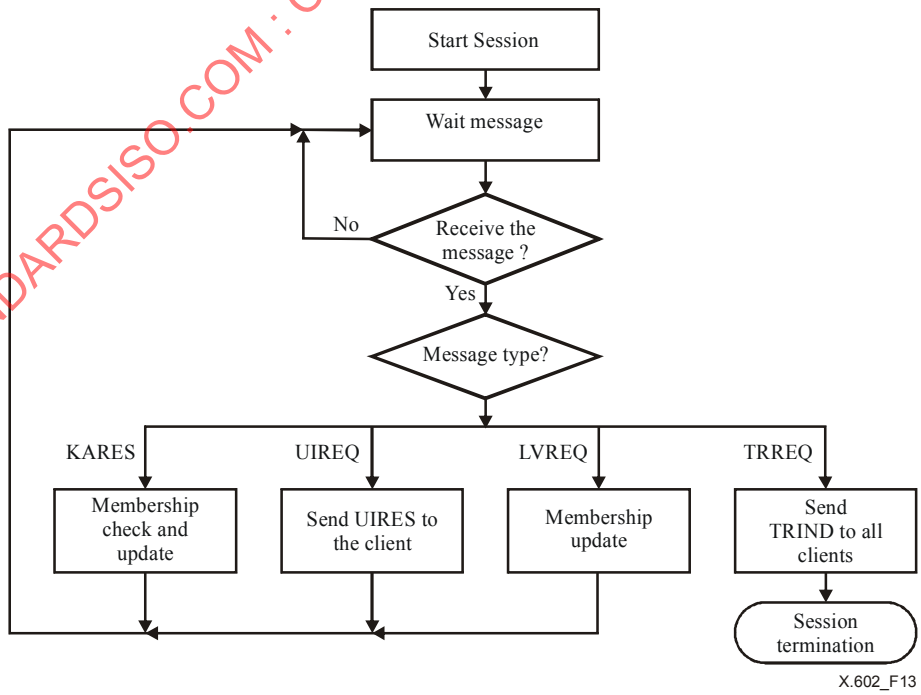

Figure 13 – GMP server (MM) operation algorithm

Figure 14 shows the membership management message sending process at the client.

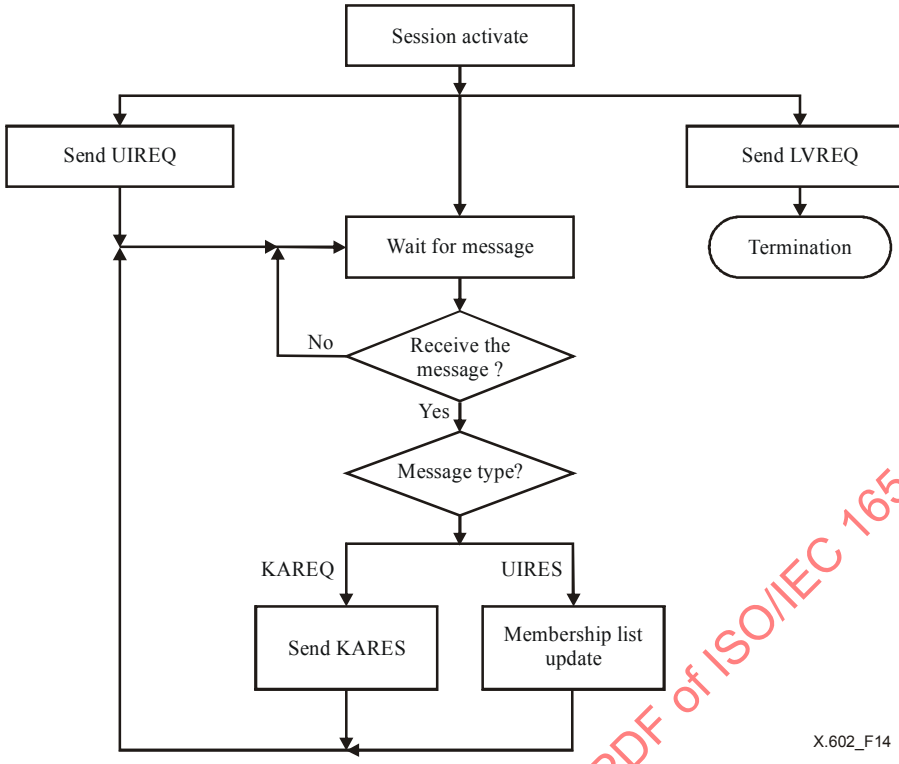

Figure 14 – MM client operation algorithm

7.2.1 Membership Update

7.2.1.1 Open mode

The server will send KAREQ periodically to all active session participants. However, the server will maintain the status information of core members and session creator from the received KARES, while the server may just count the number of other active participants from the received KARES or just ignore others, as shown in Figure 15.

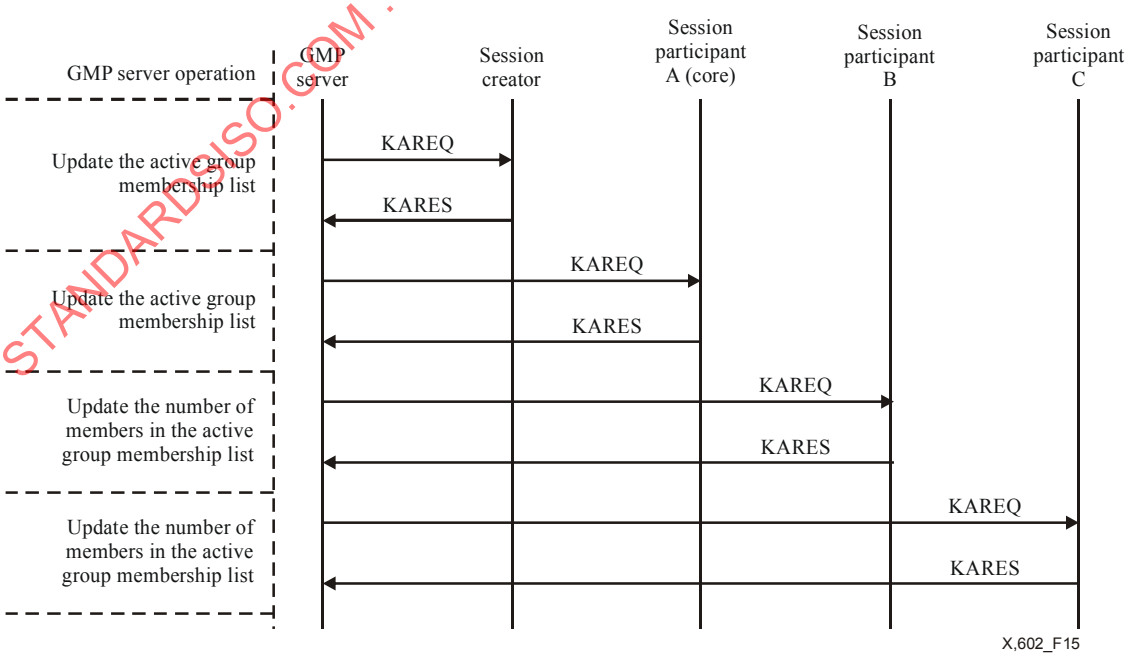

Figure 15 – Status reporting procedure (Open mode)

Any session participant can ask for the active group membership list from the server.

Figure 16 shows the session termination case: If the GMP server does not receive the valid KARES from the session creator and session core members before the predefined KA timer expires, the server will send notice that the session is terminating via a Termination Indication message, TRIND, and then terminate the session.

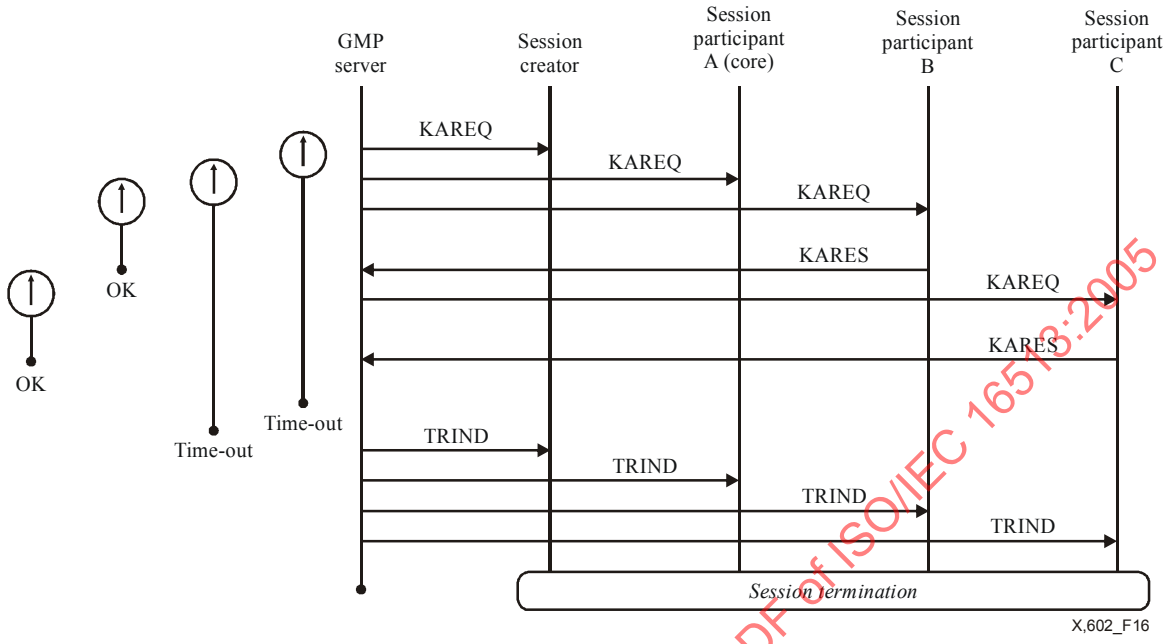

Figure 16 – Session termination (Open mode)

7.2.1.2 Closed mode

The server will send KAREQ periodically to all active session participants. The server will maintain the status information of all active members including core members and session creator from the received KARES as shown in Figure 17.

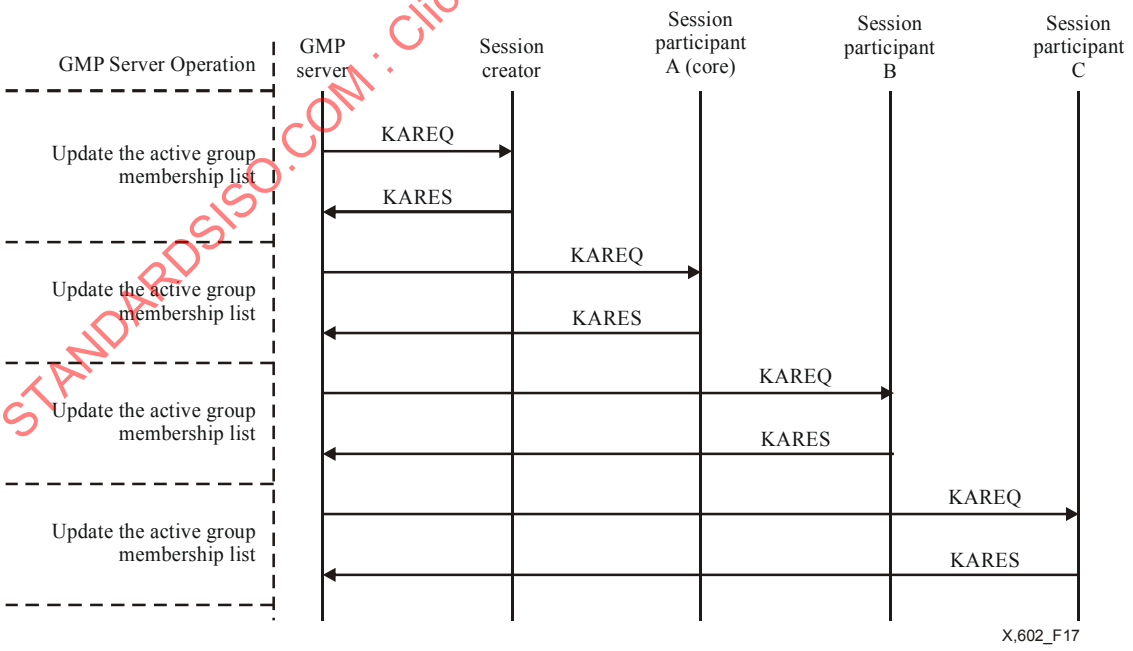

Figure 17 – Status reporting procedure (Closed mode)

Any session participant can ask for the active group membership list from the server.

7.2.2 User information request and response

An active group member can request for the Active Group Member list by sending a UIREQ to the GMP server. The GMP server will reply with a UIRES including the Active Group Member list, as shown in Figure 18.

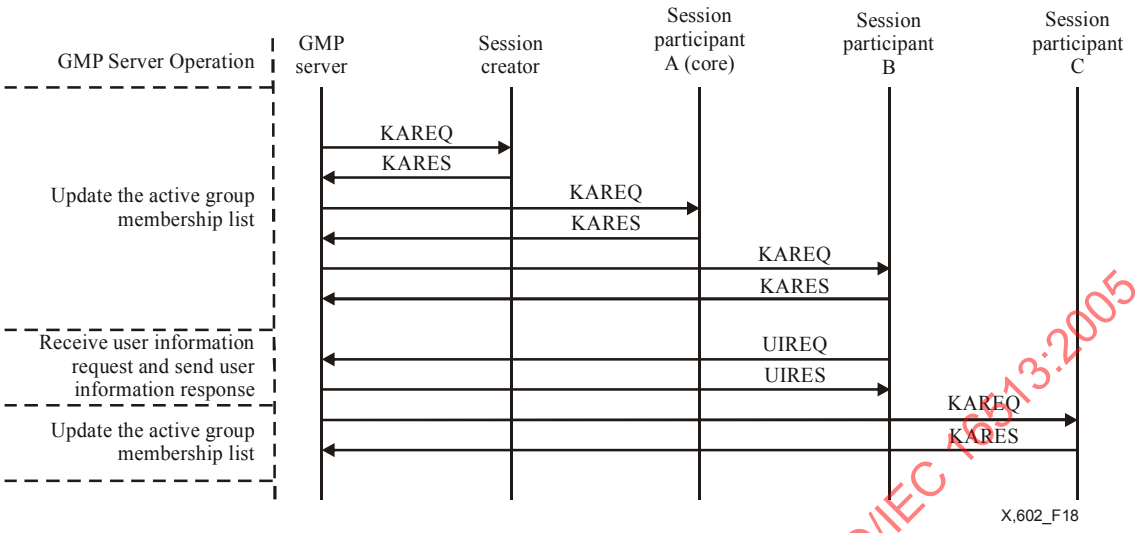

Figure 18 – UIREQ and UIRES

7.2.3 Session Leave

Usually an active Session Participant will leave the session by sending a LVREQ to the GMP server; the GMP server will then delete that client from the active group list and add that client to the enrolled group list, as shown in Figure 19.

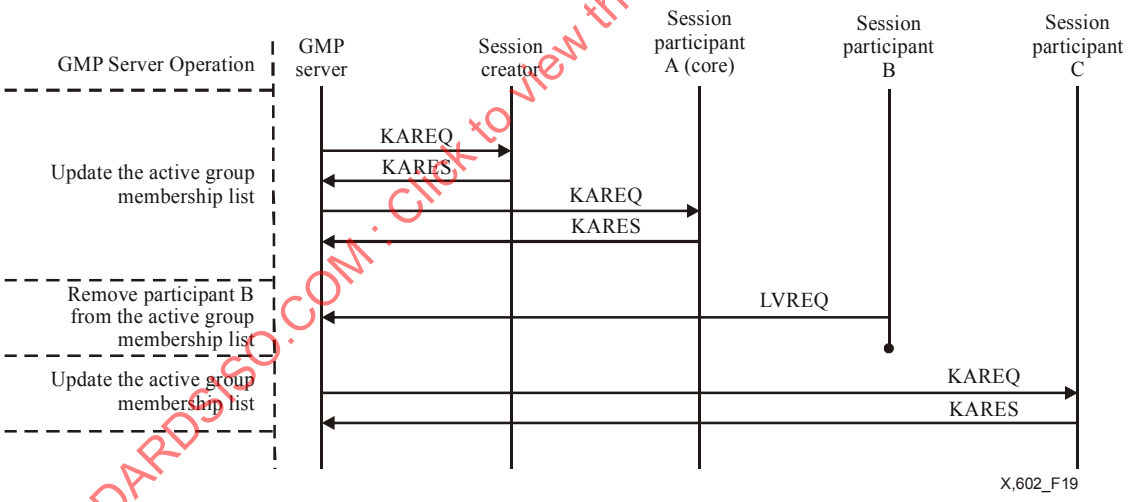

Figure 19 – LVREQ

However, if an active Session Participant, who is either the Session Creator or a Session Core member, leaves the session by sending a LVREQ, the GMP server who received the LVREQ will terminate the session, sending TRIND to every active Session Participant, as shown in Figure 20.

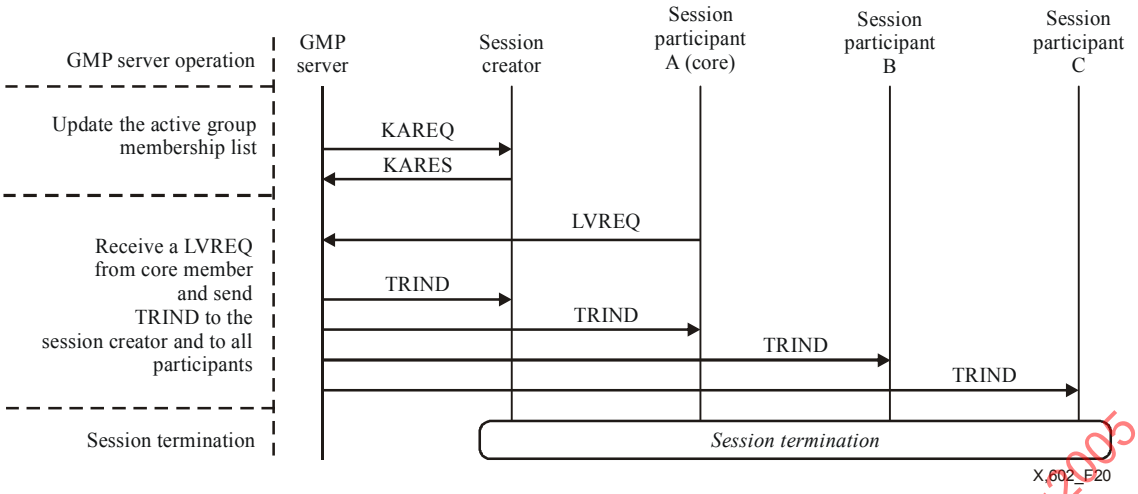

Figure 20 – LVREQ messages from core active member

7.2.4 Session Termination

To terminate a session, the Session Creator will send the TRREQ to the GMP server. The GMP server who received the TRREQ will terminate the session, sending TRIND to every active Session Participant, as shown in Figure 21.

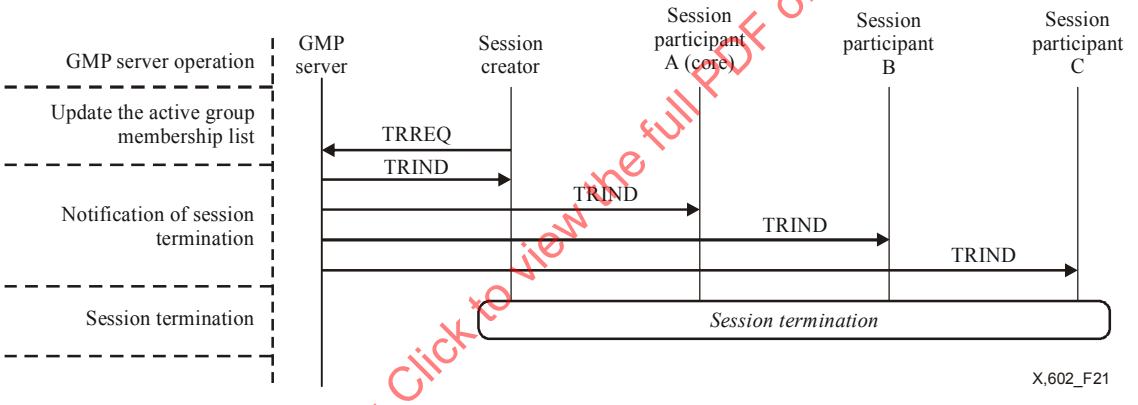

Figure 21 – Session termination

After the GMP server sends KAREQ, it activates the KeepAlive timer; if one or more responding KARESs from core active members have not arrived before the KeepAlive timer expires, the GMP server will terminate the session, sending TRIND to every active Session Participant, as shown in Figure 22.

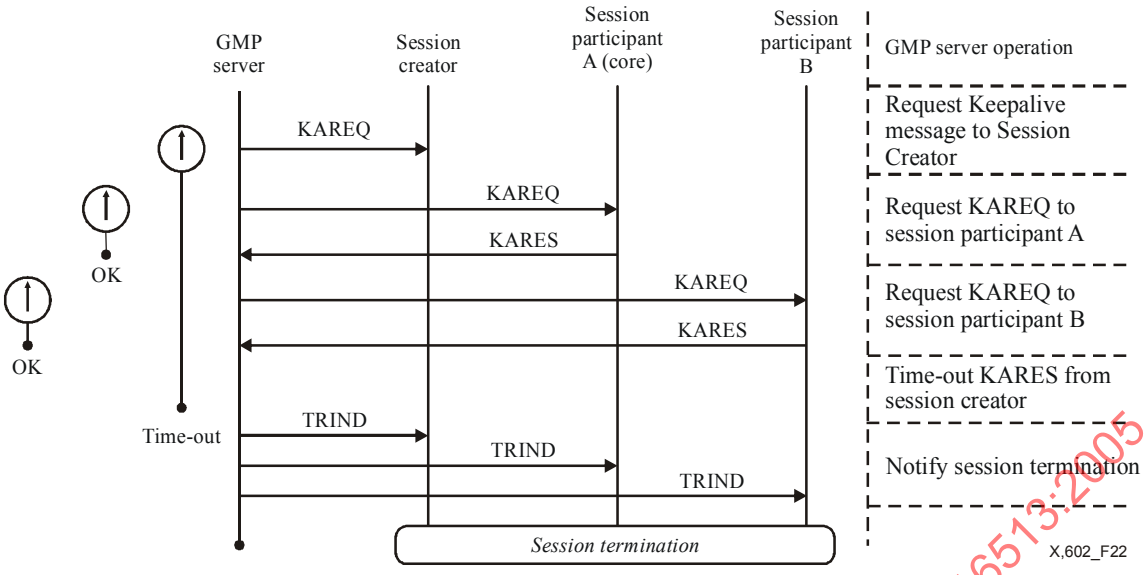

Figure 22 – Session termination

7.3 Security

GMP uses the key distribution to ensure the security of the group management protocol. Figure 23 shows the example of GMP control for the security of GMP.

If the Session Creator wants to create a session applied with security, the Session Creator sends to the GMP server a SCREQ with the 'S' bit set to ONE. However, although Session Creator requests to create a session applied with security, if the GMP server does not support the secure mode for a session, the GMP server sends to the Session Creator a SCREJ with 'S' bit set to ONE.

If the GMP server supports the secure mode for a session, the Session Participant receives SJRES with the 'S' bit set to ONE, including a Key in the enrolment phase.

If any Session Participant enrols or joins the ongoing session late, the GMP server will send SJRES with the 'S' bit set to ONE, including the Key which is currently used in the session.

Whenever any Session Participant de-enrols, the GMP server discards the Key, generates a new Key, and sends a KDUPT, including the new Key, to all enrolled group members.

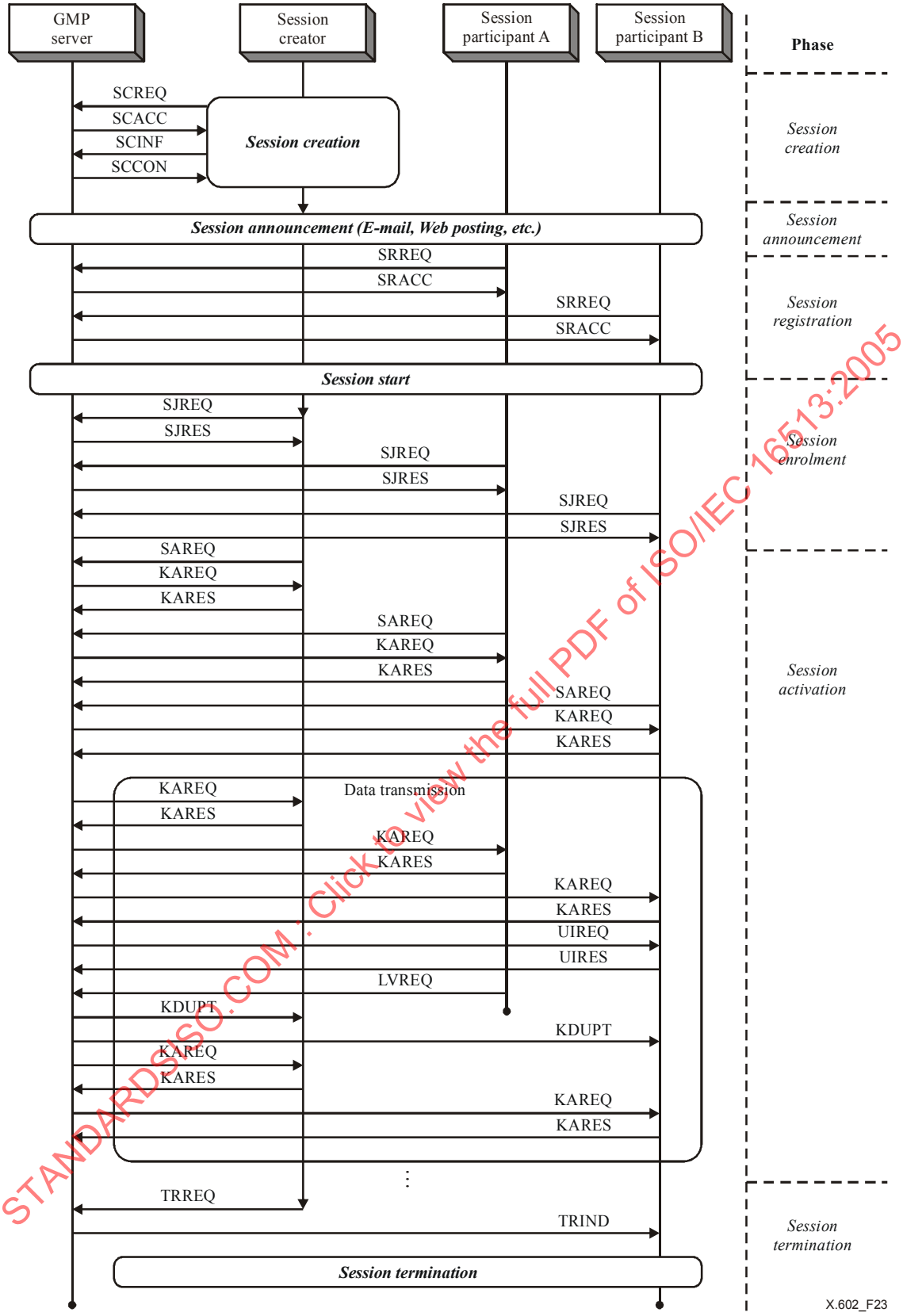

Figure 23 – An example of GMP control (secure mode)

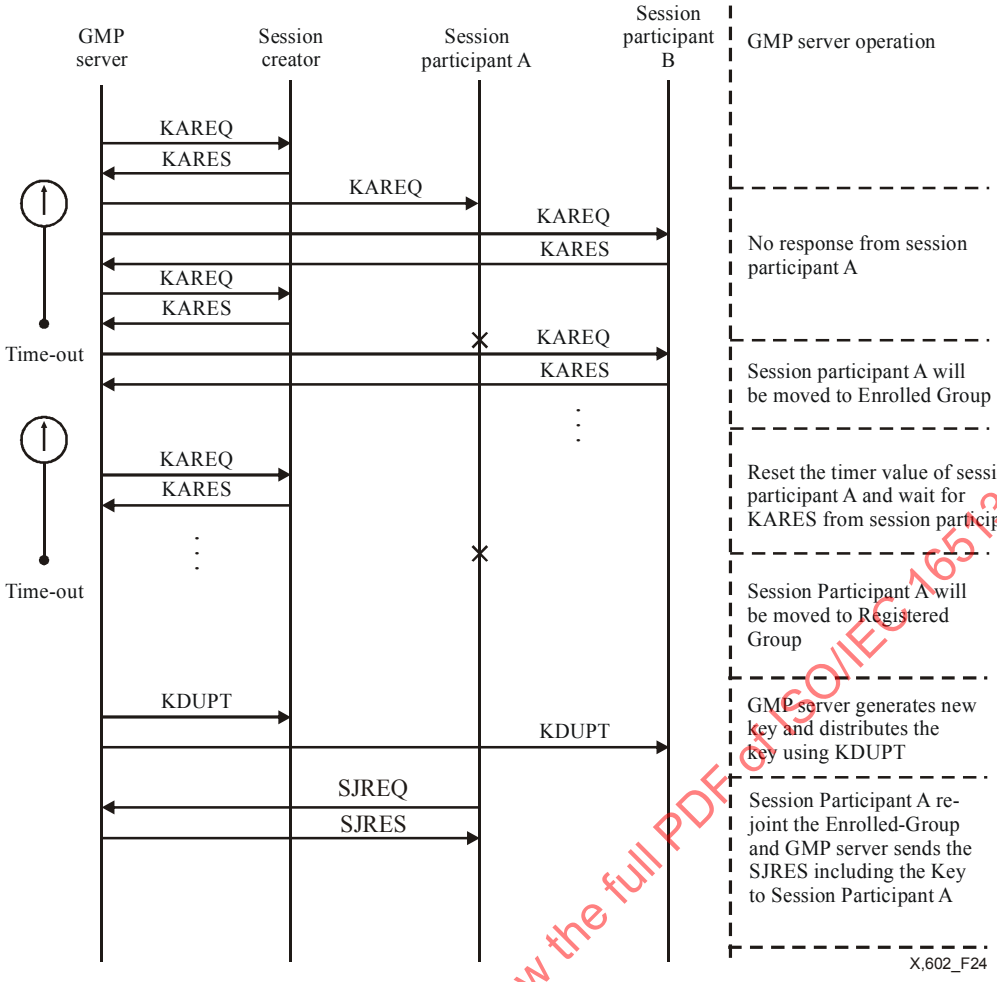

Figure 24 – Key distribution using the KDUPT

8 GMP messages

GMP messages are classified into Session Management and Membership Management messages.

8.1 Session Management message types

Table 1 summarizes the messages and their descriptions used in GMP session management.

Table 1 – Session Management message types

Message type	Generated by	Description
SCREQ	Session Creator	Session Creation Request message
SCACC	GMP Server (SM)	Session Creation Accept message
SCREJ	GMP Server (SM)	Session Creation Reject message
SDREQ	Session Creator	Session Deletion Request message
SDRES	GMP Server (SM)	Session Deletion Response message
SCINF	Session Creator	Session Creation Information message
SCCON	GMP Server (SM)	Session Creation Confirm message
SRREQ	Session Creator, Session Participant	Session Registration Request message
SRACC	GMP Server (SM)	Session Registration Accept message

Table 1 – Session Management message types

Message type	Generated by	Description
SRREJ	GMP Server (SM)	Session Registration Reject message
SRRES	GMP Server (SM)	Session Registration Response message
SJREQ	Session Creator, Session Participant	Session Join Request message
SJRES	GMP Server (SM)	Session Join Response message
SAREQ	Session Creator, Session Participant	Session Activation Request message

a) SCREQ: Session Creator generates this message and sends it to the GMP server to get the permission to create a new session.

b) SCACC: GMP server generates this message and sends it to the Session Creator to indicate the permission of session creation.

c) SCREJ: GMP server generates this message and sends it to the Session Creator to indicate that the requested session creation is not allowed for the following reasons:

- The GMP server does not have enough resource;
- Session Creator does not have proper authorization to create a session;
- Although Session Creator requests GMP server to create a session applied with security, the GMP server does not support the secure mode for a session.

d) SDREQ: Session Creator generates this message to request to delete an existing session from the session list in GMP server.

e) SDRES: GMP server generates this message and replies to the SDREQ.

f) SCINF: Session Creator generates this message to inform the detailed session characteristics and its criteria such as media type, application, core member list, session mode, etc., to the GMP server.

g) SCCON: GMP server generates this message to reply to SCINF that the session information is successfully loaded to the session list.

h) SRREQ: Session Clients generate this message to send it to GMP server to register for a session.

i) SRACC: GMP server generates this message and sends it to indicate the successful registration of a requested Session Client.

j) SRREJ: GMP server generates this message and sends it to the registration requested Session Client. The registration may be rejected if the Session Client does not have the proper qualification.

k) SRRES: In Closed mode, GMP server generates this message and sends it to the registration requested Session Client, indicating that the registration request is being processed based on the pre-defined authorization.

l) SJREQ: Session Creator and Session Clients who registered successfully will generate this message and send it to indicate that they are in enrolled state, ready to communicate.

m) SJRES: GMP server generates this message and replies to SJREQ to indicate that the session is going to be active. If the session supports the secure mode, GMP server generates SJRES including Key.

n) SAREQ: Session Creator and Session Clients who enrolled successfully will generate this message and send it to indicate that they are now in active state, being on line. SAREQ includes the port number of the client to start the membership management in the option field.

8.2 Session Management message formats

Figure 25 shows the structure of the Session Management messages.