FINAL
DRAFT

AMENDMENT

ISO/IEC 16512-2:2008 FDAM 1

ISO/IEC JTC **1**

Secretariat: **ANSI**

Voting begins on:
2011-03-04

Voting terminates on:
2011-05-04

Information technology — Relayed multicast protocol: Specification for simplex group applications

AMENDMENT 1: Security extensions

Technologies de l'information — Protocole de multidiffusion relayé: Spécification relative aux applications de groupe simplex

AMENDEMENT 1: Extensions de sécurité

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 16512-2:2008/FDAmd 1
https://standards.iteh.ai/catalog/standards/sist/2f395fc9-dd14-4c98-a464-ee4f79918642/iso-iec-16512-2-2008-fdamd-1

Please see the administrative notes on page ii-1

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/IEC 16512-2:2008/FDAM 1:2011(E)

© ISO/IEC 2011

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 16512-2:2008/FDAmd 1
https://standards.iteh.ai/catalog/standards/sist/2f395fc9-dd14-4c98-a464-ee4f79918642/iso-iec-16512-2-2008-fdamd-1

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester.

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

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

© ISO/IEC 2011 – All rights reserved

In accordance with the provisions of Council Resolution 21/1986, this document is **circulated in the English language only**.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 16512-2:2008/FDAmd 1
https://standards.iteh.ai/catalog/standards/sist/2f395fc9-dd14-4c98-a464-ee4f79918642/iso-iec-16512-2-2008-fdamd-1

© ISO/IEC 2011 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 16512-2:2008/FDAmd 1
https://standards.iteh.ai/catalog/standards/sist/2f395fc9-dd14-4c98-a464-ee4f79918642/iso-iec-16512-2-2008-fdamd-1

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.

Amendment 1 to ISO/IEC 16512-2 was prepared 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.603.1 (2007)/Amd.1 (11/2009).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 16512-2:2008/FDAmd 1
https://standards.iteh.ai/catalog/standards/sist/2f395fc9-dd14-4c98-a464-ee4f79918642/iso-iec-16512-2-2008-fdamd-1

© ISO/IEC 2011 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 16512-2:2008/FDAmd 1
https://standards.iteh.ai/catalog/standards/sist/2f395fc9-dd14-4c98-a464-ee4f79918642/iso-iec-16512-2-2008-fdamd-1

INTERNATIONAL STANDARD
RECOMMENDATION ITU-T

Information technology – Relayed multicast protocol: Specification for simplex group applications

Amendment 1

Security extensions

1) Clause 1, Scope

Delete the existing text and replace it 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 16512-2:2008/FDAmd 1
https://standards.iteh.ai/catalog/standards/sist/2f395fc9-dd14-4c98-a464-ee4f79918642/iso-iec-16512-2-2008-fdamd-1

2) Clause 2, Normative references

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

2.1 Identical Recommendations | International Standards

– Recommendation ITU-T 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 2094 (1997), *Group Key Management Protocol (GKMP) Architecture*.

– 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*.

FINAL DRAFT / PROJET FINAL

3) Clause 3, Definitions

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, 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.

3.15 secure RMCP-2 protocol: The relayed multicast protocol supporting security features for simplex group applications defined in clauses 9-12.

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, resulting from agreement of the security mechanisms defined in 10.1.4.

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

3.19 TLS_PSK mode: A mode of the TLS defined in IETF RFC 4279 for the 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 16512-2:2008/FDAmd 1
https://standards.iteh.ai/catalog/standards/sist/2f395fc9-dd14-4c98-a464-ee4f79918642/iso-iec-16512-2-2008-fdamd-1

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, Abbreviations

Add the following abbreviations to clause 4:

ACL	Access Control List
AUTH	Authentication
CEK	Contents Encryption Key
CP	Content Provider
HRSREQ	Head Required Security Request
HRSANS	Head Required Security Answer
KEYDELIVER	Key Delivery
SECAGREQ	SECurity AGreement REQuest
SECAGANS	SECurity AGreement ANSwer
SECALGREQ	SECurity ALgorithms REQuest
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.

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 85, corresponds with that in the basic RMCP-2 protocol (see 5.1).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 16512-2:2008/FDAmd 1
https://standards.iteh.ai/catalog/standards/sist/2f395fc9-dd14-4c98-a464-ee4f79918642/iso-iec-16512-2-2008-fdamd-1

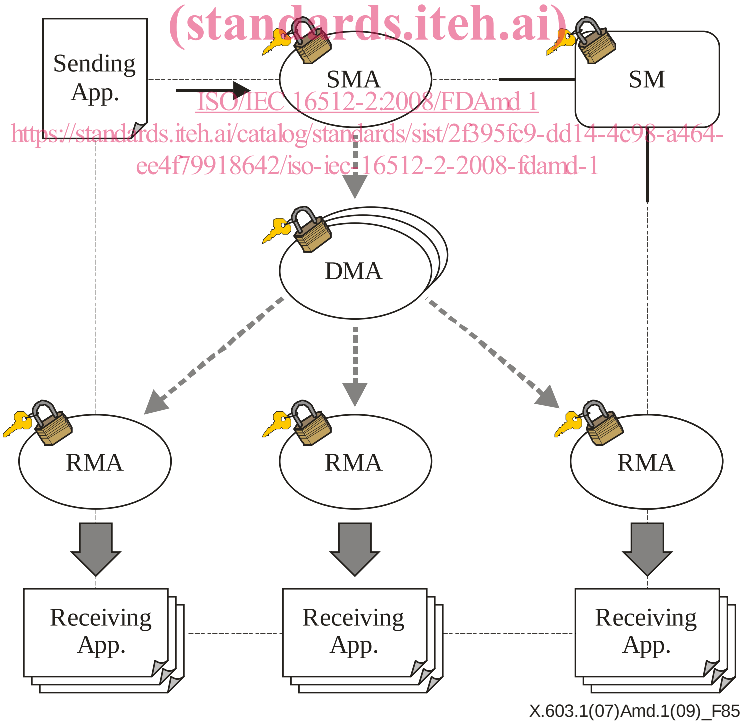


Figure 85 – RMCP-2 service topology with security

FINAL DRAFT / PROJET FINAL

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 86 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;

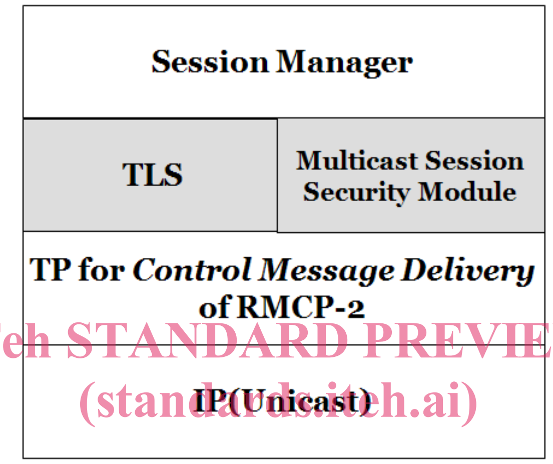
b) Session admission management;

c) Session key management;

d) Access Control list management;

e) Secure group and membership management;

f) Message encryption/decryption.


Session Manager
TLS
Multicast Session Security Module
TP for *Control Message Delivery* of RMCP-2
IP(Unicast)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 16512-2:2008/FDAmd 1
https://standards.iteh.ai/catalog/standards/sist/2f395fc9-dd14-4c98-a464-ec4f79918642/iso-iec-16512-2-2008-fdamd-1

Figure 86 – 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 87 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

a) Secure tree configuration;

b) Session key management;

c) Secure group and membership management.

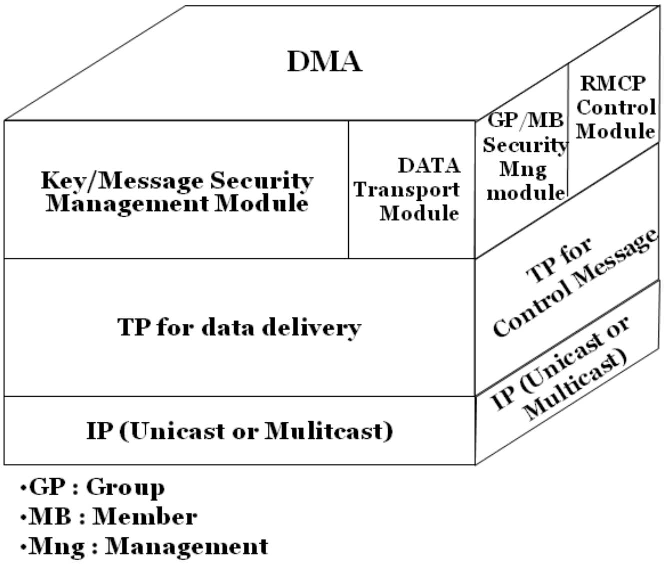


Figure 87 – Internal structure of DMAs

9.2.4 Sender and receiver multicast agents

The internal structure of the SMA and the RMAs is shown in Figure 88. The structure is the same as for DMAs except that the Group Security Management Module is not included.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 16512-2:2008/FDAmd 1
https://standards.iteh.ai/catalog/standards/sist/21595fc9-dd14-4c98-a464-ee4799f18642/iso-iec-16512-2-2008-fdamd-1

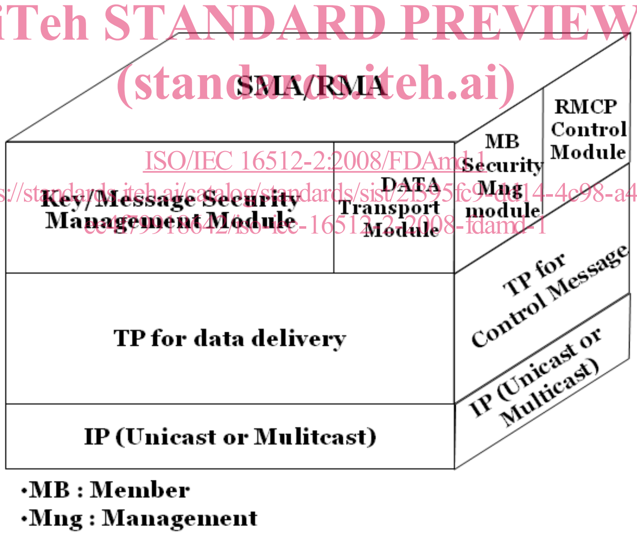


Figure 88 – Internal structure of the SMA and RMAs

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 89, 90 and 91. 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.

FINAL DRAFT / PROJET FINAL

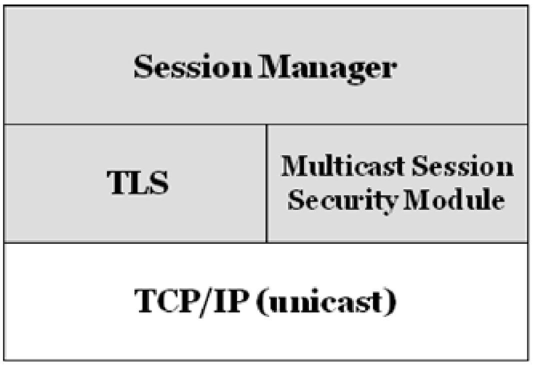


Figure 89 − Protocol block of the SM

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

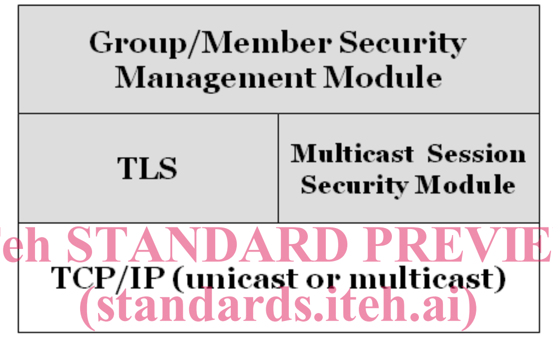

Group/Member Security Management Module
TLS
Multicast Session Security Module
TCP/IP (unicast or multicast)

Figure 90 − Protocol block for the group/member security management of MAs

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 16512-2:2008/FDAmd 1
https://standards.iteh.ai/catalog/standards/sist/2f395fc9-dd14-4c98-a464-ce4f79918642/iso-iec-16512-2-2008-fdamd-1

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.

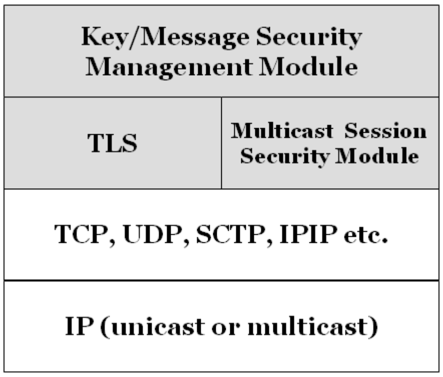

Key/Message Security Management Module
TLS
Multicast Session Security Module
TCP, UDP, SCTP, IPIP etc.
IP (unicast or multicast)

Figure 91 − 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 9 shows the messages that are specific to the secure RMCP-2 protocol. They complement the messages listed in Table 1 (see 5.4).

Table 9 – 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	

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO/IEC 16512-2:2008/FDAmd 1
https://standards.iteh.ai/catalog/standards/sist/2f395fc9-dd14-4c98-a464-ed4f70918642/iso-iec-16512-2-2008-fdamd-1

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.

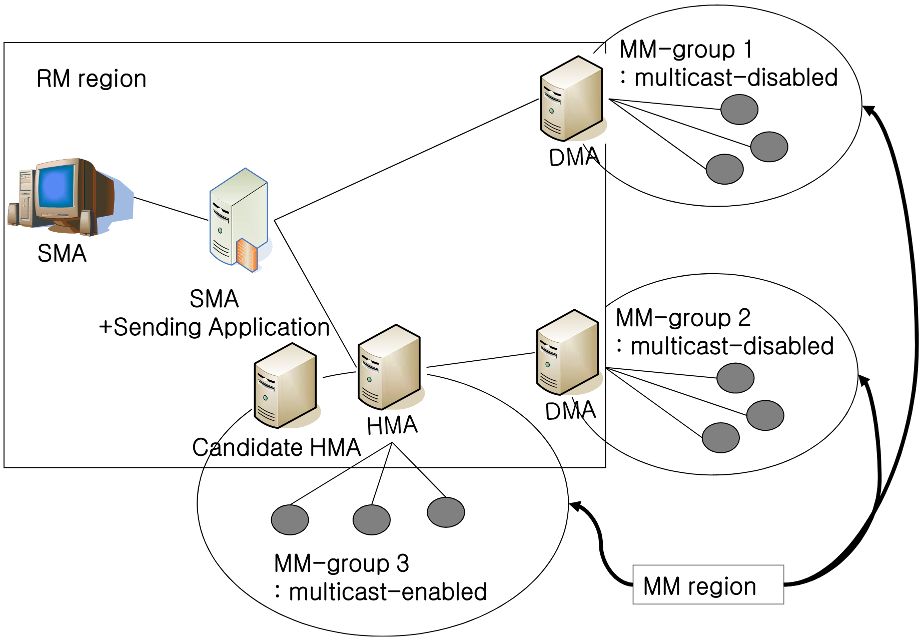


Figure 92 – Security management regions

FINAL DRAFT / PROJET FINAL