

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: Security extensions

Recommendation ITU-T X.603.1 (2007) –
Amendment 1

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS

Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199

OPEN SYSTEMS INTERCONNECTION

Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299

INTERWORKING BETWEEN NETWORKS

General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379

MESSAGE HANDLING SYSTEMS

DIRECTORY	X.400–X.499
-----------	-------------

OSI NETWORKING AND SYSTEM ASPECTS	X.500–X.599
-----------------------------------	-------------

Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699

OSI MANAGEMENT

Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799

SECURITY	X.800–X.849
----------	-------------

OSI APPLICATIONS

Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899

OPEN DISTRIBUTED PROCESSING	X.900–X.999
-----------------------------	-------------

INFORMATION AND NETWORK SECURITY	X.1000–X.1099
----------------------------------	---------------

SECURE APPLICATIONS AND SERVICES	X.1100–X.1199
----------------------------------	---------------

CYBERSPACE SECURITY	X.1200–X.1299
---------------------	---------------

SECURE APPLICATIONS AND SERVICES	X.1300–X.1399
----------------------------------	---------------

For further details, please refer to the list of ITU-T Recommendations.

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

Amendment 1

Security extensions

Summary

Amendment 1 to Recommendation ITU-T X.603.1 | ISO/IEC 16512-2 describes the security functionalities of an application-level relayed multicast protocol for one-to-many group applications. The protocol provides various security facilities to fulfil 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.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.603.1	2007-02-13	17
1.1	ITU-T X.603.1 (2007) Amend.1	2009-11-13	11
1.2	ITU-T X.603.1 (2007) Amend. 2	2010-03-01	11

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 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/>.

© ITU 2010

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

	<i>Page</i>
1) Clause 1, Scope	1
2) Clause 2, Normative references.....	1
3) Clause 3, Definitions	2
4) Clause 4, Abbreviations.....	2
5) New clauses 9-12.....	3
6) New Annex E	36
7) New Annex F	38

Document ID: 123456789

**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.

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.*

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.

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).

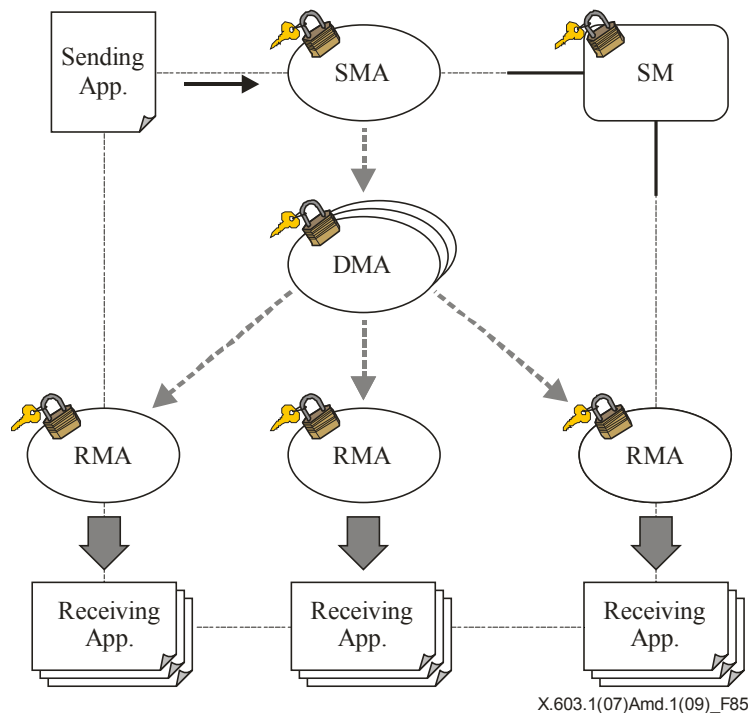


Figure 85 – RMCP-2 service topology with security

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 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.

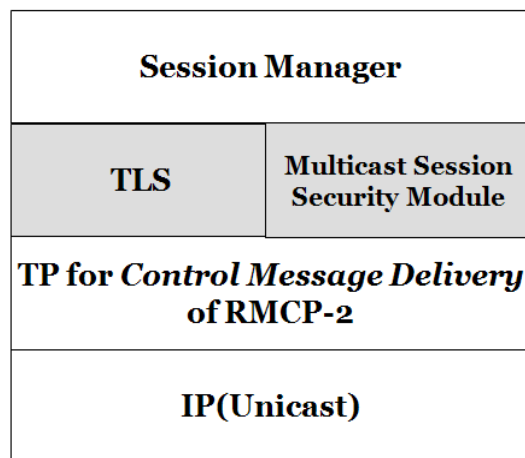


Figure 86 – Internal structure of the SM

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.

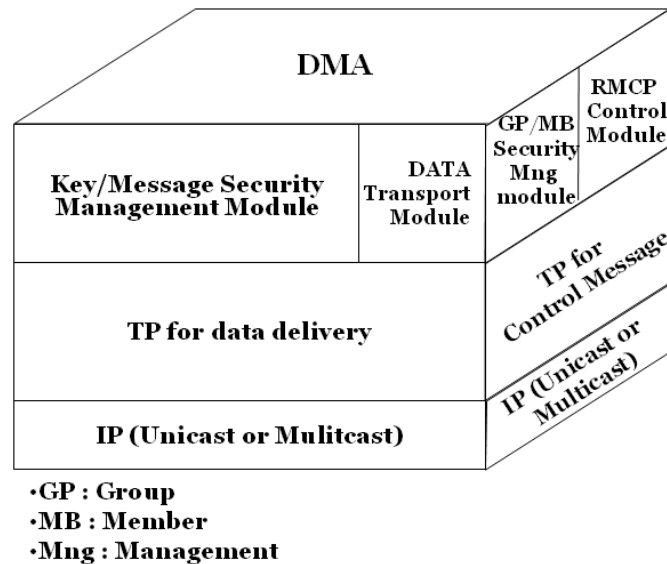


Figure 87 – Internal structure of DMAs

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.

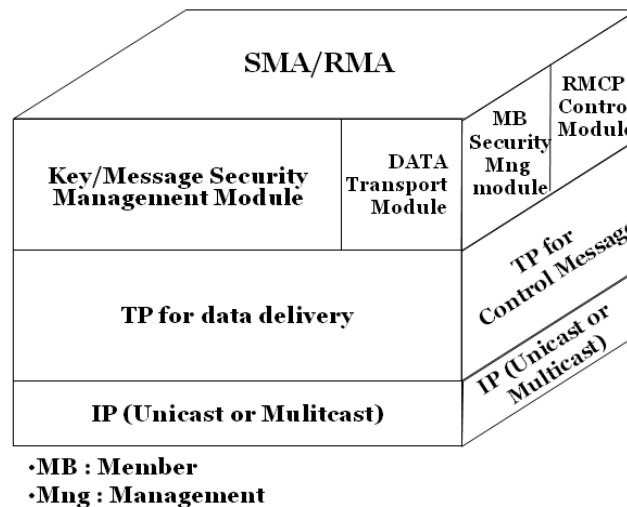


Figure 88 – Internal structure of the SMA and RMAs

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.

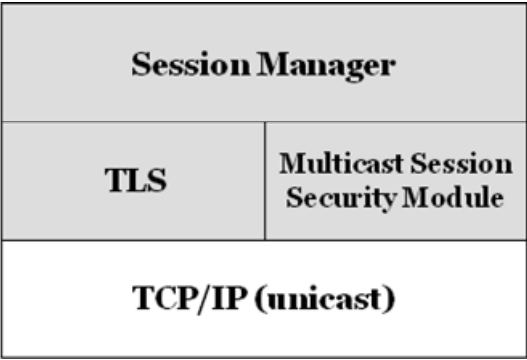


Figure 89 – Protocol block of the SM

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

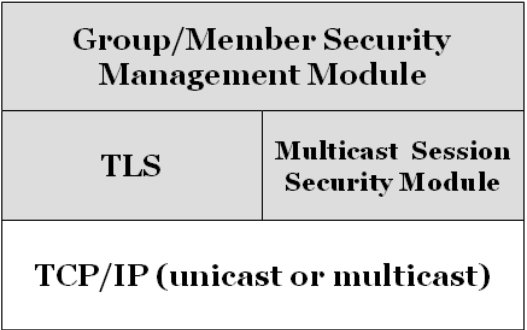


Figure 90 – Protocol block for the group/member security management of MAs

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.

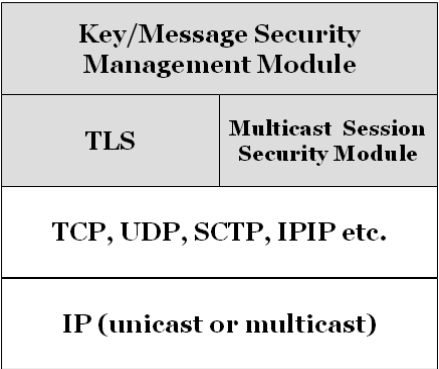


Figure 91 – Protocol block for the key/message security management of MAs

Copyright International Telecommunication Union/ITU Telecommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Full document details: ITU-T X.603.1 AMD 1 2009

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	

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.

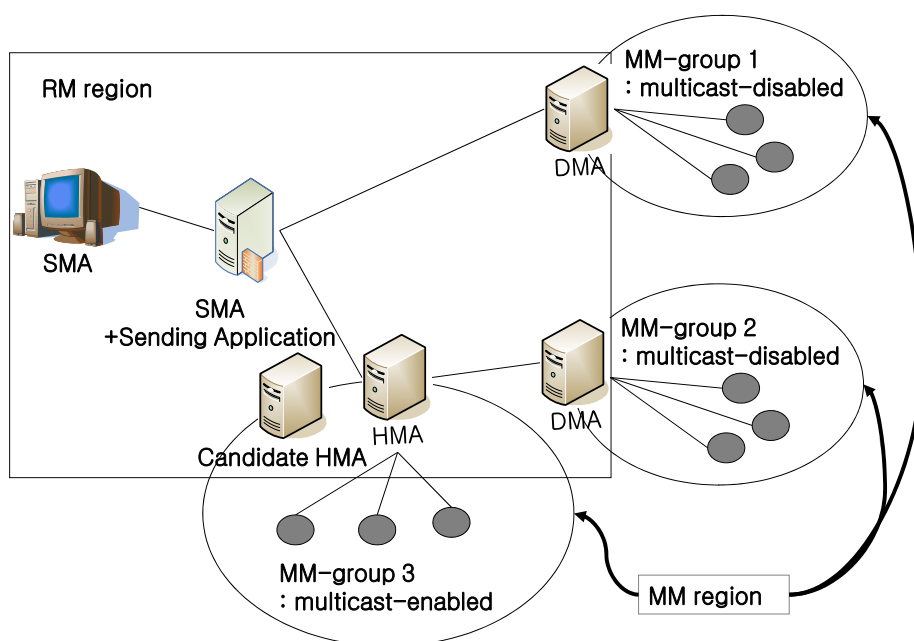


Figure 92 – Security management regions

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 K_s , 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 SUBSANS messages with the SM. As a result of this, the SMA receives the session key K_s 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 K_s 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 K_s . They join the RMCP-2 tree through the secure tree join procedure (see 10.2.4).