INTERNATIONAL STANDARD

**ISO/IEC 16512-2**

Second edition
2011-12-01

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

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



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

**CONTENTS**

# 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 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 (03/2010).

This second edition cancels and replaces the first edition (ISO/IEC 16512-2:2008), which has been technically revised.

ISO/IEC 16512 consists of the following parts, under the general title *Information technology — Relayed multicast protocol*:

— *Part 1: Framework*

— *Part 2: Specification for simplex group applications*

**Introduction**

Introduction Relayed MultiCast Protocol Part 2 (RMCP-2) is an application-layer relayed multicast protocol for simplex group applications. RMCP-2 can construct an optimized and robust one-to-many relayed multicast delivery path over a unicast network with the help of RMCP entities defined by Rec. ITU-T X.603 | ISO/IEC 16512-1.

An RMCP-2 session consists of one SM and one or more MAs; SM initiates and terminates RMCP-2 session and manages RMCP-2 session and participated MAs; MA configures an RMCP-2 tree to deliver group data by exchanging a series of RMCP-2 control messages.

Along the relayed multicast delivery path, several types of data delivery channels can be constructed according to the requirement of application services.

**INTERNATIONAL STANDARD**
**RECOMMENDATION ITU-T**

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



## 1 Scope

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 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.

### 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 18033-3:2010, *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*.