INTERNATIONAL STANDARD

ISO/IEC 14496-13

First edition
2004-09-15

Information technology — Coding of audio-visual objects —

Part 13: Intellectual Property Management and Protection (IPMP) extensions

Technologies de l'information — Codage des objets audiovisuels — Partie 13: Extensions de gestion et protection de la propriété intellectuelle (IPMP)

Reference number
ISO/IEC 14496-13:2004(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

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 14496-13 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 29, *Coding of audio, picture, multimedia and hypermedia information*. ISO/IEC 14496-13:2004, together with ISO/IEC 14496-1:2004, cancels and replaces ISO/IEC 14496-1:2001/Amd.3:2004, which has been technically revised.

ISO/IEC 14496 consists of the following parts, under the general title *Information technology — Coding of audio-visual objects*:

— *Part 1: Systems*

— *Part 2: Visual*

— *Part 3: Audio*

— *Part 4: Conformance testing*

— *Part 5: Reference software*

— *Part 6: Delivery Multimedia Integration Framework (DMIF)*

— *Part 7: Optimized reference software for coding of audio-visual objects*

— *Part 8: Carriage of ISO/IEC 14496 contents over IP networks*

— *Part 9: Reference hardware description*

— *Part 10: Advanced Video Coding*

— *Part 11: Scene description and application engine*

— *Part 12: ISO base media file format*

— *Part 13: Intellectual Property Management and Protection (IPMP) extensions*

— *Part 14: MP4 file format*

— *Part 15: Advanced Video Coding (AVC)*

— *Part 16: Animation Framework eXtension (AFX)*

— *Part 17: Streaming text format*

— *Part 18: Font compression and streaming*

— *Part 19: Synthesized texture stream*

Introduction

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

The ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the ISO and IEC that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with the ISO and IEC. Information may be obtained from the companies listed in Annex G.

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

Information technology — Coding of audio-visual objects —

Part 13: Intellectual Property Management and Protection (IPMP) extensions

1 Scope

This International Standard specifies :

- The definition, as well as Extension tags, syntax and semantics for an `IPMP_Data_BaseClass` to support the following functionalities.
  - ✧ Mutual Authentication for IPMP tool to IPMP tool as well as IPMP tool to Terminal communication.
  - ✧ The requesting by IPMP tools of the connection/disconnection to requested IPMP tools.
  - ✧ The notification to IPMP tools of the connection/disconnection of IPMP tools.
  - ✧ Common IPMP processing.
  - ✧ IPMP tool to/from User interaction.
- Syntax and semantics for the carriage of IPMP tools in the bit stream.
- Syntax and semantics for IPMP information carriage to and from IPMP tools.
- Syntax and semantics for the requesting and transfer of content and IPMP Tools between Terminals as well as extension tags, syntax and semantics to the `IPMP_Data_BaseClass` ISO/IEC 14496-1 used therein.
- XML syntax and semantics for the description of the environment in which and MPEG-4 Terminal/application is operating.
- A list of registration authorities required for the support of the amended specifications found herein.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10646-1:1993, *Information technology – Universal Multiple-Octet Coded Character Set (UCS) – Part 1: Architecture and Basic Multilingual Plane*

ISO/IEC 14496-1:2004, *Information technology — Coding of audio-visual objects — Part 1: Systems*

XML Schema Part 0: Primer, Part 1: Structures, and Part 2: Datatypes, W3C Recommendation, 2 May 2001, available at <http://www.w3.org/TR/2001/REC-xmlschema-0-20010502>, <http://www.w3.org/TR/2001/REC-xmlschema-1-20010502>, and <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502>

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
Binary Representation
In the context of an IPMP Tool, this is the format of the implementation of that IPMP Tool, Examples: Platform Dependent Native Code, Java ™ bytecode.

3.2
Content
This implies part or whole of an MPEG presentation.

3.3
Content Consumption
Any experience of given Content implies consumption of that content. Access, Playback, Denial of Access and Creation of a Copy are all types of content consumption.

3.4

Content Stream
This is the incoming content, of MPEG-4 format.

3.5
IPMP Device
An implemented application that implements an MPEG-4 Terminal supporting the use of MPEG-4 IPMP.

3.6
IPMP Information
Information directed to a given IPMP Tool to enable, assist or facilitate its operation.

3.7
IPMP System
A monolithic IPMP protection scheme which requires implementation dependant access to protected streams at required Control Points and must provide any intra-communication within an IPMP System on an implementation basis.

3.8
IPMP Tool
IPMP tools are modules that perform (one or more) IPMP functions such as authentication, decryption, watermarking, etc. Conceptually the use of one or more IPMP Tools is combined to perform the functionality of an IPMP System. IPMP Tools, as opposed to IPMP Systems, are normatively identified as to which control points they function at as well as are provided normative methods for secure communications both within as well as outside of a given IPMP Tools comprised functional “IPMP System”. An additional difference between IPMP Tools and IPMP Systems is that IPMP Tools, or a combination thereof, may be used for the protection of Object streams.

In this specification the use of the term “IPMP System” is used in some cases to indicate either an actual IPMP System or a combination of IPMP Tools whose combination provides the functionality of an IPMP System. In cases where the distinction is important the proper respective terms are used.

3.9
IPMP Tool Manager

The IPMP Tool Manager is a conceptual entity within the Terminal that processes IPMP Tool List(s) and retrieves the Tools that are specified therein.

3.10
IPMP Tool Message

A message passed between any combination of IPMP Tool or Terminal.

3.11
IPMP Tool Stream

An elementary stream carrying an implementation of an IPMP Tool.

3.12
Message Router

A conceptual entity within the Terminal that implements the Terminal-side behavior of the Terminal-Tool interface.

3.13
Mutual Authentication

Protocols carried out to determine the proper and correct identity of a communicating entity and to secure the communication channels between communicating entities.

3.14
Parametric Configuration

Information that carries task-specific parameter specification, in an extensible form.

3.15
Representation Format

The binary format, platform and communication mechanisms applicable to a given implementation of an IPMP Tool or Terminal.

3.16
Scope of Protection

Scope of protection refers to the elementary stream and/or object governed by a given IPMP Tool instance.

3.17
Terminal

A Terminal is an environment that consumes possibly protected Content in compliance with the usage rules.

3.18
User

A hardware, software or human entity that is the initiator and/or target of content consumption.

4 Overview of IPMP Extensions (Informative)

4.1 IPMP Architecture

This subclause describes the general IPMP architecture. For detailed IPMP architecture linked to MPEG-4 system, please refer to 5.1.

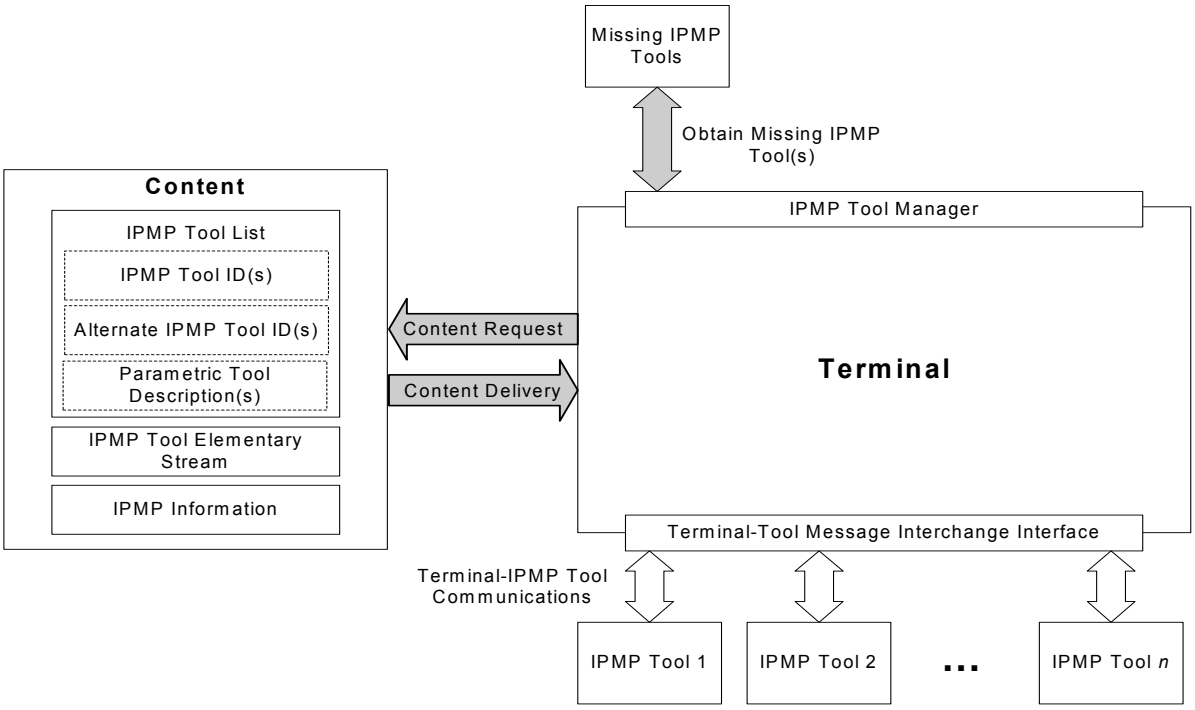

Figure 1 — Architecture Diagram for Walkthrough Concepts

4.1.1 Messaging

To facilitate the cooperation of multiple tools in the protection and governance of content, a message based architecture is provided. The message based architecture has three advantages over functional interface type architectures. The first is that security can more easily be maintained as messages are less difficult to protect in an open framework then parameters in a function parameters list. The second is that the only entities that need be concerned with a given message's definition are those that need to generate or act upon a given message and so additional functionality can be created and supported simply through the addition of required messages. The third is that full interoperability with IPMP tools can be easily achieved by using the `IPMP_ToolAPI_Config` [5.8.5] carried in IPMP Descriptor, or by defining a single messaging API by a third-party forum who adopts IPMP.

Physical routing of information and context resolution are handled by a conceptual entity called the Message Router. The Message Router abstracts all platform-dependent routing and delivery issues, from the IPMP Tools. The interface between the Message Router and the Tools, is non-normative and is not defined in this specification, however, the information on the messaging interface can be carried in `IPMP_ToolAPI_Config` to assist interoperability.

All IPMP Tool interactions take place via the Terminal. IPMP Tools do not communicate directly with each other within the scope of this standard.

The delivery of both bit stream sourced IPMP information as well as IPMP tool and Terminal generated information is supported through the use of three separate messages which are passed via the Message Router to IPMP tools. The three messages are, `IPMP_MessageFromBitstream` [5.8.2], which is used to deliver IPMP stream data, `IPMP_DescriptorFromBitstream` [5.8.3], which is used to deliver `IPMP_Descriptors` [ISO/IEC 14496-1] and `IPMP_MessageFromTool` [5.8.4], which is used to deliver messages from either other IPMP tools or the Terminal itself.

In these extensions, a core set of messages are provided which cover what are identified as core functional requirements.

4.1.2 Mutual Authentication

The most important aspect of a secure messaging architecture is the use of cryptographic algorithms and protocols that allow one to perform a number of important security functions.

At any point in IPMP Information or Content processing, IPMP Tools may be required to communicate with one another or the Terminal. The degree of security required for such communication is determined by a number of variables including information that may be included by the content provider in the Content and conditions of trust established between tool providers a priori and out of band. It is generally the case that a given ES is protected by multiple tools but that certain types of tools are complex (e.g. Rights Management tools) and others are utilities (e.g. Decryption engines). Complex tools may control the instantiation of other tools or make decisions about content use in response to usage queries from the terminal. Mutual authentication may occur between any pair of tools but the level of security required for this communication will in part be dictated by data contained in the bitstream in an opaque manner. The mechanism for making the determination of this security level is non-normative.

Mutual authentication is executed as follows:

1. The Tool that initiates mutual authentication with another tool determines the conditions of trust to be achieved by such authentication, i.e. the initiating tool determines whether it needs integrity protected communication or full secure, authenticated communication. This level may or may not be dictated by IPMP Information in the Content.

2. The communicating tools then engage in a message exchange to determine which authentication protocol will be used. In some cases, this protocol will have been determined by an a priori out of band negotiation between the tool providers in their security audits of one another.

These extensions provide a set of messages to support the identified functionalities. The first message `IPMP_InitMutualAuthentication` [5.3.1] may be used and delivered to a given IPMP tool such that the receiving IPMP tool is informed as to its required communication partner as well as security measures that must be in place. Following this message or the absence thereof, IPMP tools required to do so will use the `IPMP_MutualAuthentication` [5.3.2] message as required to determine or create secure channels of communication as needed based on the application.

As one purpose of Mutual Authentication is the verification of trust relationships existing between two entities these specifications provide for the carriage of trust and security metadata. This metadata may include zero or more certificates, credentials or integrity verification information. The creation or establishment of trust relationships are established by out of band relationships between the different entities involved in protecting and managing the content. However, the trust metadata that results from such relationships needs to be made available to permit static and dynamic verification of trust.

During the Mutual Authentication process the carriage of `IPMP_TrustSecurityMetadata` [5.3.2.7] is supported to provide additional security related data usable by IPMP tools to determine trust related information.

Once Mutual Authentication is performed, the `IPMP_SecureContainer` [5.3.3] may be used to pass information securely between IPMP tools and IPMP tools and Terminal.

4.1.3 IPMP tool acquisition

ISO/IEC 14496-1 defines `IPMP_ToolListDescriptor` which conveys the list of IPMP tools required to access the content associated with the `InitialObjectDescriptor` in which it is described, and may include a list of alternate IPMP tools or parametric descriptions of tools required to access the content. The conceptual entity Tool Manager parses the tool list, makes sure all tools are available, and retrieves missing tools if any.

If a given required tool is not present on a given Terminal, the `IPMPToolES_DecoderConfig` [5.4.3] descriptor can be used to indicate an IPMP tool bearing stream with `IPMP_ToolES_AU` [5.4.4] being used to actually carry the required tool.

A missing IPMP Tool can also be acquired from a neighbouring IPMP device via tool transfer messages defined in Annex D, or it can be acquired by connecting to a remote server and providing the terminal description as defined in Annex E.

4.1.4 IPMP Tool connection and disconnection

In the IPMP architecture, IPMP tool may be connected as the result of an `IPMP_DescriptorPointer` [ISO/IEC 14496-1] being processed and in addition may be connected due to requests from already connected IPMP tools. Note: Instantiation of the Tools to be connected is implementation dependent, however, the information on how to instantiate the Tools can be carried in `IPMP_ToolAPI_Config` [5.8.5] to assist interoperability.

Instantiation of the Tools to be connected is implementation dependent. A registration authority shall register instantiation mechanisms for particular platforms.

IPMP tools may use the `IPMP_GetTools` [5.4.1] and `IPMP_GetToolsResponse` [5.4.2] messages to request a list of tools available for connection that exist as well as a response to the request, respectively.

IPMP tools as well as the Terminal may also query a given IPMP tool as to its capabilities and functionality by using the `IPMP_ToolParamCapabilitiesQuery` [5.4.5] message with the tool being queried using the `IPMP_ToolParamCapabilitiesResponse` [5.4.6] message as a reply.

Knowing that a given tool is needed for processing, an IPMP tool may request the connection of another IPMP tool by using the `IPMP_ConnectTool` [5.4.7] message and may request the disconnection of another IPMP tool by using the `IPMP_DisconnectTool` [5.4.8] message. A connection may require the actual instantiation of a tool or may be accomplished through physical/electronic means.

The `IPMP_ConnectTool` message contains control point and sequence information to determine the exact location to connect the requested tool. Tools connected at the request of other tools inherit the same scope of protection as the requesting tool. Note that some control points are not associated with any known point on an Elementary Stream. Note also that there are issues with scoping and scenarios that are somewhat illogical, especially as related to BIFS nodes referencing ODs.

Each instantiation of an IPMP Tool shall establish a new logical instance of the tool, for a particular scope of protection. The Terminal assigns a context identifier for the logical instance of the tool, which maps to the specific tool instance, and therefore to the associated scope of protection. These context identifiers shall be unique to ensure unambiguous message addressing.

The process of instantiation involves the following steps

1. Establish a context for the Tool being instantiated
2. Establish a link between the MR and the Tool instance
3. Establish a link between the Tool instance and the MR.

Details of this process are implementation specific. The normative result is a context/address being made available for communication and use of the instantiated tool by other tools as well as the Terminal.

The tool requesting connection shall receive an `IPMP_NotifyToolEvent` [5.5.3] message indicating the instantiation of the IPMP Tool, and its associated context. The requesting tool and the instantiated tool may perform mutual authentication thereafter.

If an IPMP tool knows of another tool with which it must communicate has already been connected, it may use the `IPMP_GetToolContext` [5.4.9] message and will receive an `IPMP_GetToolContextResponse` [5.4.10] message in reply if the requested IPMP tool is already connected with the message containing the address through which the requesting tool may use to communicate with the requested tool.

4.1.5 Notification of IPMP Tool connection and disconnection

During the processing of IPMP protected content, a number of IPMP tools may be involved, for communication and various security purposes, notification messages are supplied to notify IPMP tools when other IPMP tools have either been connected, disconnected or processed watermark information. Additionally IPMP tools may request at any time a list of all the IPMP tools currently connected at various specifiable scopes of protection.

The `IPMP_AddToolNotificationListener` [5.5.1] message may be used to indicate the sending IPMP tools intent to receive notifications of events and scopes of protection as specified in the `IPMP_AddToolNotificationListener` message. To remove one's self from being notified in the future for specified events, an IPMP tool may use the `IPMP_RemoveToolNotificationListener` [5.5.2] to do so.

As events occur for which notifications have been requested, the `IPMP_NotifyToolEvent` [5.5.3] message is sent to requesting IPMP tools.

4.1.6 Common IPMP processing.

Direct support has been provided for the carrying out of common IPMP processing operations. Specific support and the related messages are as follows:

- `IPMP_CanProcess` [5.6.1] for the notification by an IPMP tool to the Terminal that stream processing may begin. All tools connected and processing data within a given stream must send permission before any tools in the stream receive stream data.
- `IPMP_Opaquedata` [5.6.2] for the carriage of user defined data.
- `IPMP_KeyData` [5.6.3] for the carriage of decryption key data as well as timing information to determine the validity period of time varying keys.
- `IPMP_RightsData` [5.6.4] for the carriage of rights expressions.
- `IPMP_SelectiveDecryptionInit` [Annex A] for the configuration of a decryption tool.
- `IPMP_AudioWatermarkingInit` [Annex B] for the configuration of an audio watermarking tool.
- `IPMP_SendAudioWatermark` [Annex B] for the sending of information to be embedded or that was extracted.
- `IPMP_VideoWatermarkingInit` [Annex C] for the configuration of a video watermarking tool.
- `IPMP_SendVideoWatermark` [Annex C] for the sending of information to be embedded or that was extracted.

4.1.7 IPMP tool to/from User interaction

During IPMP processing, direct interaction between IPMP tools and a User may be required. The `IPMP_UserQuery` [5.7.1] message is used to provide information to be relayed to a User and to request information as well. The `IPMP_UserQueryResponse` [5.7.2] is used to relay information provided by a User back to the originator of the User query.

5 Normative Elements

5.1 Extended MPEG-4 Architecture

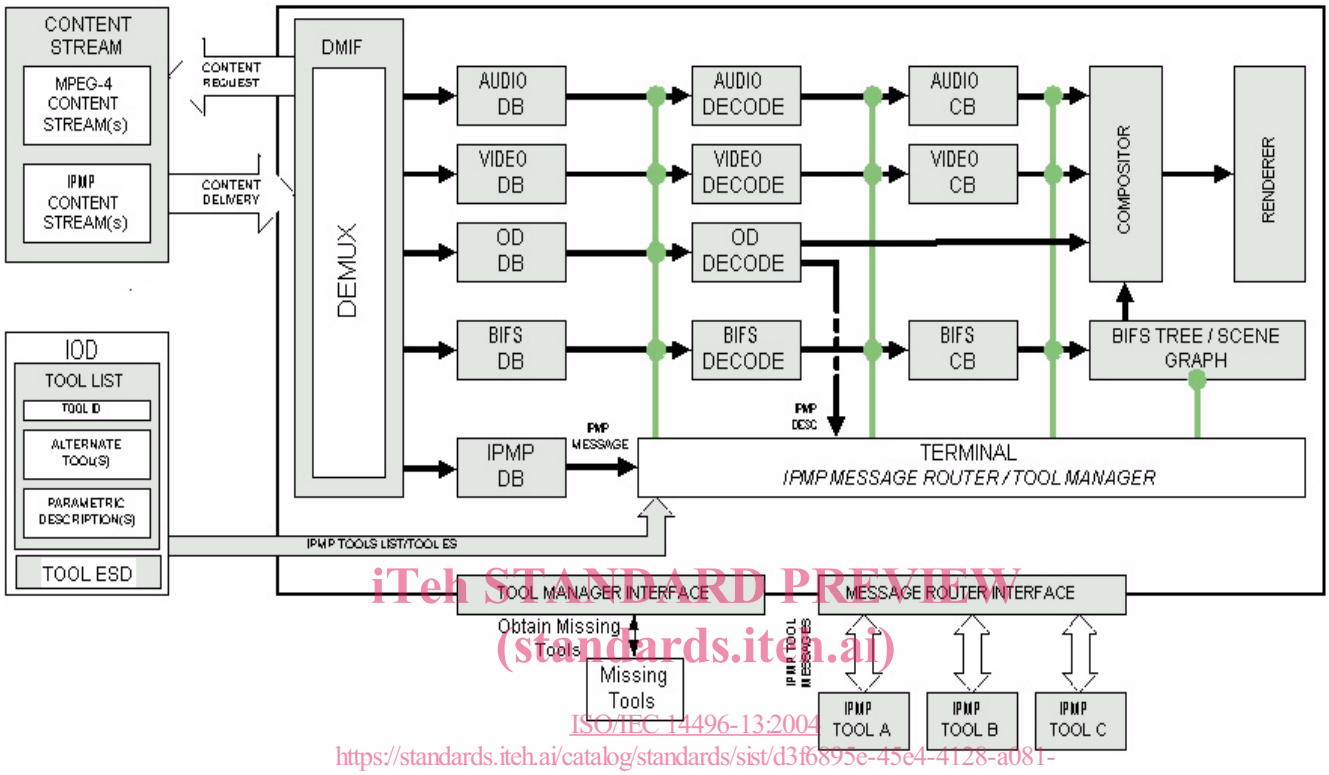

Figure 2 — Mapping of IPMP Extensions to MPEG-4 Systems Architecture

5.2 Extension tags for the IPMP_Data_BaseClass message

Table 1 — Tags for IPMP Data extending IPMP_Data_BaseClass

8-bit Tag Value	Symbolic Name
0x00	Forbidden
0x01	IPMP_OpaqueData_tag
0x02	IPMP_AudioWatermarkingInit_tag
0x03	IPMP_VideoWatermarkingInit _tag
0x04	IPMP_SelectiveDecryptionInit_tag
0x05	IPMP_KeyData _tag
0x06	IPMP_SendAudioWatermark_tag
0x07	IPMP_SendVideoWatermark _tag

0x08	IPMP_RightsData _tag
0x09	IPMP_Secure_Container_tag
0x0A	IPMP_AddToolNotificationListener_tag
0x0B	IPMP_RemoveToolNotificationListener_tag
0x0C	IPMP_InitAuthentication_tag
0x0D	IPMP_MutualAuthentication_tag
0x0E	IPMP_UserQuery_tag
0x0F	IPMP_UserQueryResponse_tag
0x10	IPMP_ParamtericDescription_tag
0x11	IPMP_ToolParamCapabilitiesQuery_tag
0x12	IPMP_ToolParamCapabilitiesResponse_tag
0x13	IPMP_GetTools_tag
0x14	IPMP_GetToolsResponse_tag
0x15	IPMP_GetToolContext_tag
0x16	IPMP_GetToolContextResponse_tag
0x17	IPMP_ConnectTool_tag
0x18	IPMP_DisconnectTool_tag
0x19	IPMP_NotifyToolEvent_tag
0x1A	IPMP_CanProcess_tag
0x1B	IPMP_TrustSecurityMetadata_tag
0x1C	IPMP_ToolAPI_Config_tag
0x1D– 0x3F	Reserved for Inter-device messages
0x40 – 0xCF	ISO Reserved
0xD0 – 0xFE	User Defined

5.3 Mutual Authentication

This subclause defines the syntax and semantics of messages used for mutual authentication and secure communications.