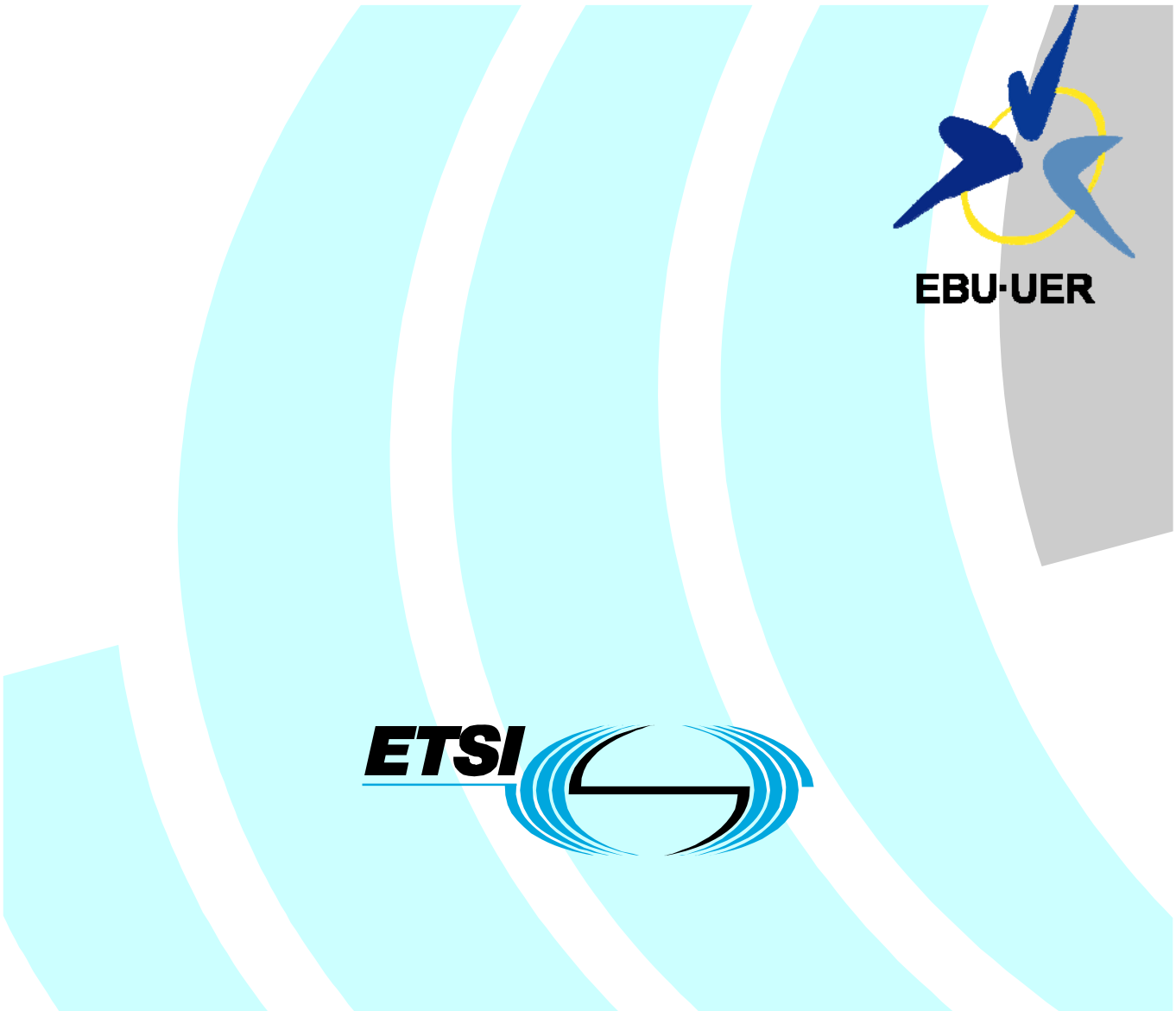
ETSI TS 102 822-5-1 V1.5.1 (2010-07)

Technical Specification

Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("*TV-Anytime*");
Part 5: Rights Management and Protection (RMP);
Sub-part 1: Information for Broadcast Applications



Reference
RTS/JTC-TVA-50-05-01

Keywords
broadcasting, content, system, TV, video

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2010.
© European Broadcasting Union 2010.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™, **TIPHON**™, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
LTE™ is a Trade Mark of ETSI currently being registered
for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights 4
Foreword 4
Introduction 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 7
4 Design principles and requirements 8
4.1 Positive assertion of rights 8
4.2 Operational approach 8
4.3 Compliance 8
5 RMPI - Micro Broadcast and RMPI - Micro semantics 8
5.1 Principals 8
5.2 Rights 9
5.3 Conditions 10
5.4 Ancillary RMPI-MB and ancillary RMPI-M 12
6 Syntax and encoding for RMPI-MB and RMPI-M 13
6.1 Introduction 13
6.2 RMPI-MB and RMPI-M payload 14
6.3 Ancillary RMPI 15
6.4 Rights 16
6.5 Conditions and identifiers 16
7 RMPI-MB and RMPI-M lifecycle 19
Annex A (informative): XML Expression of RMPI MB and M 21
A.1 Cipher Classification Scheme (CipherCS.xml) 21
A.2 RMPI Scheme (tva_rmpi_5-1_v141.xsd) 22
Annex B (informative): TV-Anytime RMPI Schemas 25
Annex C (informative): Bibliography 26
History 29

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by Joint Technical Committee (JTC) Broadcast of the European Broadcasting Union (EBU), Comité Européen de Normalisation ELECtrotechnique (CENELEC) and the European Telecommunications Standards Institute (ETSI).

NOTE: The EBU/ETSI JTC Broadcast was established in 1990 to co-ordinate the drafting of standards in the specific field of broadcasting and related fields. Since 1995 the JTC Broadcast became a tripartite body by including in the Memorandum of Understanding also CENELEC, which is responsible for the standardization of radio and television receivers. The EBU is a professional association of broadcasting organizations whose work includes the co-ordination of its members' activities in the technical, legal, programme-making and programme-exchange domains. The EBU has active members in about 60 countries in the European broadcasting area; its headquarters is in Geneva.

European Broadcasting Union
CH-1218 GRAND SACONNEX (Geneva)
Switzerland
Tel: +41 22 717 21 11
Fax: +41 22 717 24 81

The present document is part 5, sub-part 1, of a multi-part deliverable covering Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("*TV-Anytime*"), as identified below:

Part 1: "Benchmark Features";

Part 2: "Phase 1 - System description";

Part 3: "Metadata";

Part 4: "Phase 1 - Content referencing";

Part 5: "Rights Management and Protection (RMP)":

Sub-part 1: "Information for Broadcast Applications";

Sub-part 2: "RMPI binding";

Part 6: "Delivery of metadata over a bi-directional network";

Part 7: "Bi-directional metadata delivery protection";

Part 8: "Phase 2 - Interchange Data Format";

Part 9: "Phase 2 - Remote Programming".

Introduction

The present document is based on a submission by the *TV-Anytime* forum (http://www.tv-anytime.org).

The present document specifies the minimum set of usage rules and conditions required to enable protection of broadcast digital television content within a TVA Rights Management and Protection (RMP) compliant domain. When associated with a broadcast signal, RMP Information (RMPI) for Broadcast Applications is called RMPI-Micro Broadcast (RMPI-MB). When associated with content present in a TVA RMP compliant domain (post broadcast/acquisition) it is called RMPI-Micro (RMPI-M).

RMPI for Broadcast Applications can be used in conjunction with both free-to-air broadcasts and broadcasts protected by CA or DRM systems.

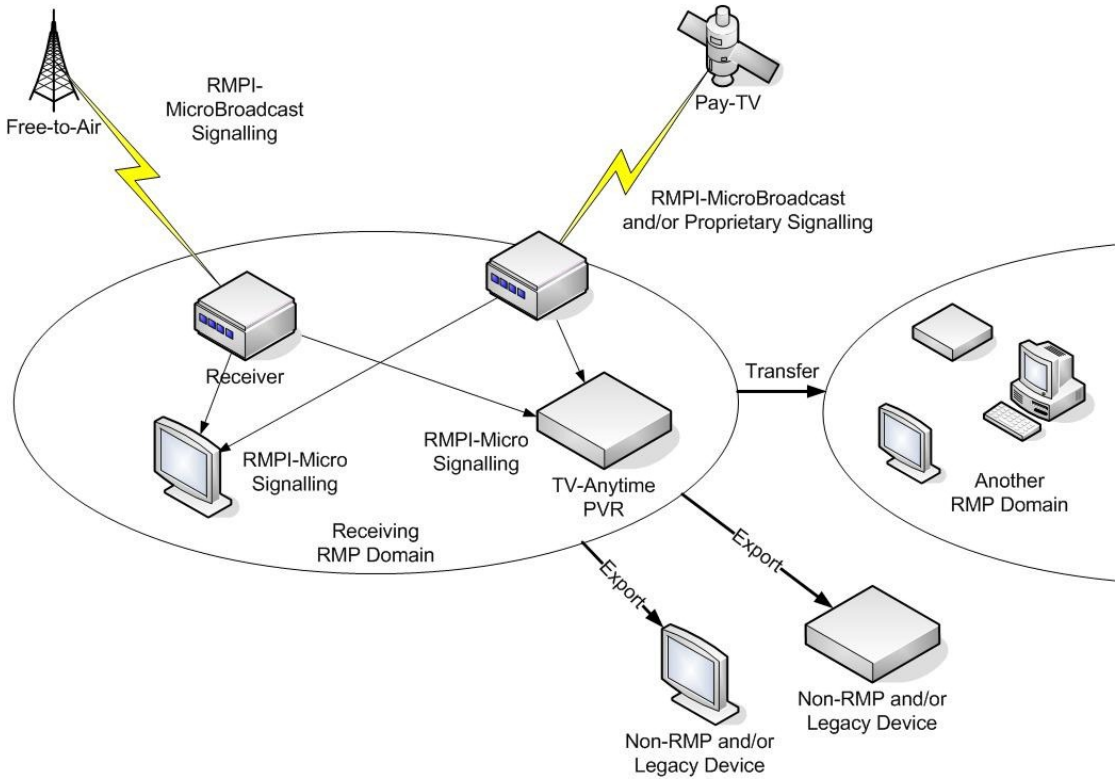


Figure 1: RMPI in the broadcast environment

In figure 1, transfer of content from one RMP domain to another is not regulated by the RMPI-M/MB but the use of this content is.

"TV-Anytime" (TVA) is a synchronized set of specifications established by the *TV-Anytime* Forum. TVA features enable the search, selection, acquisition and rightful use of content on local and/or remote personal storage systems from both broadcast and online services.

TS 102 822-1 [1] and TS 102 822-2 [2] set the context and system architecture in which the standards for Metadata, Content referencing, Bi-directional metadata and Metadata protection are to be implemented in the *TV-Anytime* environment. TS 102 822-1 [1] provides benchmark business models against which the *TV-Anytime* system architecture is evaluated to ensure that the specification enable key business applications. TS 102 822-2 [2] presents the *TV-Anytime* System Architecture. These two documents are placed ahead of the others for their obvious introductory value. Note that these first two documents are largely informative, while the remainder of the series is normative.

The features are supported and enabled by the specifications for Metadata (TS 102 822-3 [3]), Content Referencing (TS 102 822-4 [4]), Rights Management (the present document and TS 102 822-5-2 [5]), Bi-directional Metadata Delivery (TS 102 822-6 [6]) and Protection (TS 102 822-7 [7]), Interchange Data Format (TS 102 822-8 [8]) and Remote Programming (TS 102 822-9 [9]). The present document is to be used by manufacturers, service providers and content providers for the implementation of the Phase 1 features of the *TV-Anytime* specifications.

1 Scope

The present document addresses RMPI for Broadcast Applications, made up of RMPI-Micro Broadcast and RMPI-Micro. The present document is a component of the TV-Anytime Rights Management and Protection system suite of specifications.

The present document provides the semantics, syntax and encoding for the usage rights, controls and permissions to be conveyed in RMPI-MB and RMPI-M.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 102 822-1: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 1: Benchmark Features".

[2] ETSI TS 102 822-2: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 2: Phase 1 - System description".

[3] ETSI TS 102 822-3 (all sub-parts): "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 3: Metadata".

[4] ETSI TS 102 822-4: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 4: Content referencing".

[5] ETSI TS 102 822-5-2: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 5: Rights Management and Protection (RMP); Sub-part 2: RMPI binding".

[6] ETSI TS 102 822-6 (all sub-parts): "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 6: Delivery of metadata over a bi-directional network".

[7] ETSI TS 102 822-7: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime Phase 1"); Part 7: Bi-directional metadata delivery protection".

[8] ETSI TS 102 822-8: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 8: Phase 2 - Interchange Data Format".

[9] ETSI TS 102 822-9: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 9: Phase 2 - Remote Programming".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

Not applicable.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

compliance body: legal entity that adopts the specification and enforces a compliance regime

conditions: limitations on rights

grant: combination of one principal, one or more rights and zero or more conditions

principals: entities that perform actions

rights: actions that can be performed using a given piece of content

RMP-domain: set of TVA RMP-compliant devices that are **securely bound** to each other for the purpose of exchanging protected content

NOTE: It is an instance of a principal. The rules for creating and managing domains are outside the scope of the present document.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AES	Advanced Encryption Standard
bslbf	bit string left bit first
CA	Conditional Access
CCI	Copy Control Information
CSA	Common Scrambling Algorithm
DRM	Digital Rights Management
DVB	The Digital Video Broadcasting Project
HD	High Definition
HDCP	High bandwidth Digital Content Protection system
HDMI	High Definition Multimedia Interface
M2	Multi-2 encryption algorithm
RMP	Rights Management and Protection
RMPI	Rights Management and Protection Information
RMPI-M	Rights Management and Protection Information - Micro
RMPI-MB	Rights Management and Protection Information - Micro for Broadcast
SD	Standard Definition
TVA	TV-Anytime
uimsbf	unsigned integer most significant bit first
VCR	Video Cassette Recorder

4 Design principles and requirements

4.1 Positive assertion of rights

In TV-Anytime RMPI-MB rights are positively asserted and never implied. These rights are granted to the RMP System and not to a person. When a right is exercised, asserted conditions are validated. If those asserted conditions are not met then the right cannot be exercised, e.g. a user could hit pause without asking for permission, however hitting play after pause would cause the conditions to be validated and the rights to be acquired. If conditions are not asserted, then they do not constrain the rights.

4.2 Operational approach

The RMPI-MB and RMPI-M focus on the usage of content as opposed to the movement of content. As a consequence there is no notion of copy within the secure RMP-compliant domain as only those principals that have been granted rights to use the content are given access to the content under the conditions expressed in RMPI-MB and RMPI-M.

Usage of the content under the protection of the RMP system is explicitly defined and regulated. In the event that the broadcaster wishes to allow the content to leave the protection of the RMP system it is expressible with RMPI-MB and RMPI-M as an Export with appropriate conditions. One significant reason to permit this is to allow content to be consumed on legacy devices.

4.3 Compliance

TV-Anytime RMP does not mandate specific implementations or compliance and robustness rules. There are certain parameters in the specification that are left for assignment by the compliance bodies; for example geographic control, RMP domain identifier, single point of control identifier and security level. It is anticipated that compliance bodies that adopt the specification will define implementation requirements and associated compliance regimes to meet the needs of their respective environments. Compliance bodies may even choose an alternative encoding for RMPI-M or MB (e.g. XML expression given in annex A).

5 RMPI - Micro Broadcast and RMPI - Micro semantics

5.1 Principals

Table 1 gives the Principals that can be used by a broadcaster when granting rights with RMPI-MB and RMPI-M.

Table 1: Principals being used by broadcasters

Principal	Definition
Receiving Domain	The receiving domain is the first TVA RMP-compliant domain that receives the content and associated RMPI-MB via broadcast. Once the content is in the domain, the receiving domain is explicitly identified.
Any Domain	Any TVA RMP-compliant domain that can respond to the usage conditions stated within RMPI-MB and RMPI-M.

5.2 Rights

The set of rights listed in table 2, depending on their applied conditions, can be used to enable users to access content via a range of devices under a variety of different usage models. Note that terms PLAY and EXPORT below can both be used to enable content viewing, but under different consumption environments or constraints.

Table 2: Rights

Right	Description
Play	"Play" is the right to derive a transient and directly perceivable representation of content within the TVA RMP domain (see note 1).
Analogue Export	"Analogue export" is the right to create a user accessible analogue signal representing the content as an output, and thus outside of the TVA RMP system. An example of an analogue export would be sending the content over S-Video to a VCR or TV (see note 2).
Digital Export Standard Definition (SD)	"Digital Export Standard Definition" is the right to create a Standard Definition digital signal representing the content as an output outside of the TVA RMP system. An example of a Digital Export SD would be sending the content over a legacy digital output to a display or recorder with a standard definition digital input (see note 3).
Digital Export High Definition (HD)	"Digital Export High Definition" is the right to create a High Definition digital signal representing the content as an output outside of the TVA RMP system. An example of a Digital Export HD would be sending the content over a legacy digital output to a display or recorder with a high definition digital input (see notes 3 to 5).
Extend Rights	This right allows the RMP System to apply additional rights to the content. The absence of this right means that only the originally transmitted rights may be applied (see note 6).
NOTE 1: If the device that creates the human perceptible rendition of the content is not a TVA RMP device (e.g. an analogue television set), then this right is not applicable. In that case the appropriate right is required (see Analogue Export, Digital Export SD and Digital Export HD).	
NOTE 2: Until such time as there are more display devices that are directly under the control of RMP systems, the broadcaster is encouraged to allow analogue export with appropriate conditions or consumers will be unable to use their legacy analogue systems to create a viewable version of the programme.	
NOTE 3: If the consumer has digital devices outside the scope of the TVA RMP system, this right with appropriate conditions must be granted for those devices to be able to receive the content.	
NOTE 4: If both the Digital Export SD and Digital Export HD rights are granted, this is known as the Digital Export Any Definition Right. This means that any definition/resolution is permitted for digital export.	
NOTE 5: It is the compliance body that establishes which resolutions are HD and which ones are not.	
NOTE 6: Conditions to this right include at most one identified source for those additional rights. In the case that no condition is present with the right, then the RMP System implementation is permitted to extend rights based upon conditions specified by the compliance body.	

5.3 Conditions

Table 3 gives the Conditions that can be used by a broadcaster when granting rights with RMPI-MB and RMPI-M.

Table 3: Conditions

Condition	Description	Rights to which condition is applicable
Geographical Control	This condition limits the use of a right to within one or more specified territories. The granularity of territoriality is to be defined by the compliance body (see note 1).	Play, Analogue Export, Digital Export SD, Digital Export HD This condition is expressed once and applies to all of these rights.
Single Point of Control	The purpose of this condition is to allow for implementation of device-bound rights within the TVA RMP domain. If present in the broadcast this means that the broadcaster intends that once the content enters the TVA RMP domain, only one RMP entity can make usage decisions about the content based upon the expressed RMPI-MB. Upon reception a received instance of content is now married to a specific RMP entity and that entity can no longer be changed. The entity is then characterized by its identifier.	Play, Analogue Export, Digital Export SD, Digital export HD Only valid for the Receiving Domain principal. This condition is expressed once and applies to all of these rights.
Physical Proximity	This condition limits the use of a right to RMP compliant devices within close physical proximity of the receiver that first received the broadcast content. Close physical proximity is provisionally defined as immediate vicinity e.g. limited to the home network on the same local area network and is not permitted to be transmitted over a wide area network.	Play, Analogue Export, Digital Export SD, Digital Export HD Only valid for the Receiving Domain principal. This condition is expressed once and applies to all of these rights.
Buffer Duration	This condition limits the use of a right in such a way that each frame of broadcast content is used only within a specified duration after that frame was broadcast. For instance, if a buffer duration condition of 10 minutes were applied to the right to play content broadcast taking place from 8:00 to 9:00, the content broadcast at 8:00 would be playable until 8:10, the content broadcast at 8:25 would be playable until 8:35, and the content broadcast at 9:00 would be playable until 9:10. If a buffer duration condition of 0 were applied to the right to play content broadcast from 8:00 to 9:00, the content would be only immediately viewable, with no trick play allowed.	Play, Analogue Export, Digital Export SD, Digital Export HD This condition is expressed once and applies to all of these rights. Excludes Expiration Date NOTE: This condition is to be evaluated continually at a frequency to be defined by the compliance body or the implementer, and when the condition is no longer met, the right is no longer granted.
Time Window Start Date and Time Window End Date	These conditions define the window of time during which the rights are granted. It is defined as absolute start time and absolute expiry time.	Play, Analogue Export, Digital Export SD, Digital Export HD These conditions are expressed once and apply to all of these rights. They do not refer to the Extend Rights. Excludes Buffer Duration.

Condition	Description	Rights to which condition is applicable
Standard Definition Digital Export Control	This condition forwards content management rules to external content protection systems on standard definition outputs whilst exercising the Digital Export SD right: • for immediate viewing only; • bound to device or media for future viewing. If the content is marked "for immediate viewing only", then the external content protection system should treat it as "do not store". If the content is marked "bound to device or media for future viewing", then the external content protection system is instructed to permit the storage of the content as long as the playback of that content is in the presence of the single device or media to which it was exported. The content can be viewed as well as recorded or stored (see note 2).	Digital Export SD This condition applies both to the Digital Export Standard Definition Right and the Digital Export Any Definition Right. NOTE: If the Digital Export Any Definition Right is exercised, then the most restrictive of either SD or HD digital export control is used.
High Definition Digital Export Control	This condition forwards content management rules to external content protection systems on high definition outputs whilst exercising the Digital Export HD right: • for immediate viewing only; • bound to device or media for future viewing. If the content is marked "for immediate viewing only", then the external content protection system should treat it as "do not store". If the content is marked bound to device or media for future viewing, then the external content protection system is instructed to permit the storage of the content as long as the playback of that content is in the presence of that single device or media to which it was exported. The content can be viewed as well as recorded or stored (see note 2).	Digital Export HD NOTE: If Digital Export Any Definition Right is exercised, then the most restrictive of either SD or HD digital export control is used.
Analogue Export Signalling	This condition forwards content management rules to external content protection systems: • for immediate viewing only; • bound to device or media for future viewing (includes immediate viewing).	Analogue Export
Analogue Standard Definition (SD) control	This condition constrains the resolution of the exported analogue signal. If set then Standard Definition resolution only is permitted for an analogue output.	Analogue Export

Condition	Description	Rights to which condition is applicable
Security Level	This condition constrains the execution of rights based on the invoked components robustness level. Security levels are to be based upon the aggregate robustness of all invoked components needed to exercise a right.	Play, Analogue Export, Digital Export SD, Digital Export HD, Extend Rights Each grant may have a specific security level.
Simultaneous Rendering Count	This condition limits the number of simultaneous Plays, Analogue Exports and Digital Exports of content within a domain. For purposes of this condition a Play counts as a rendering, an Analogue Export counts as a rendering, a Digital Export SD counts as a rendering and a Digital Export HD counts as a rendering (see note 3).	Play, Analogue Export, Digital Export SD, Digital Export HD Only valid if principal is Receiving Domain This condition is being expressed once and applies to all of these rights.
Source of additional rights	This condition identifies the authority which may assign new rights to the content.	Extend Rights

NOTE 1: The present document assumes that devices belong to a territory regardless of where they are physically located.
NOTE 2: This expression may be used to enable HDCP on an HDMI output. CCI bits can be used to signal this information as follows: copy no more for immediate viewing only, copy one generation for bound to device or media for future viewing, and copy control not asserted if the condition is not present.
NOTE 3: It is expected that this condition will be used in conjunction with the Single Point of Control condition. However there may be implementations whereby Simultaneous Rendering Count is used on its own (e.g. there may be a secure simultaneous render counter service available within the domain).

5.4 Ancillary RMPI-MB and ancillary RMPI-M

Ancillary RMPI-MB and ancillary RMPI-M (table 4) do not convey usage rules or conditions, but carry further information that is required when handling the content.

Table 4: Ancillary RMPI-MB and ancillary RMPI-M

Ancillary RMPI-MB and ancillary RMPI-M	Information to be conveyed	Intent
Scrambling Control		This is to control the scrambling of content when it enters and is stored in the RMP controlled domain. Content is not to be scrambled when stored in the RMP controlled domain. However it may be scrambled when transmitted between devices or when bound to removable media.
	Maintain broadcast scrambling	Self explanatory, do not add RMP cipher.
	Apply RMP cipher	Remove broadcast scrambling if any and apply RMP cipher.
Cipher algorithm	AES Camellia DVB Common Scrambling Algorithm v1 DVB Common Scrambling Algorithm v2 3DES M2 Cipher outside of the control of TV-Anytime RMP	To specify the cipher algorithm used to (de)scramble the content within the TVA RMP Domain.
Version of RMPI	Version of RMPI specification	To identify version of RMPI specification.
Origin of RMPI	Identifier/pointer to authority having granted rights	For forensic purposes; this is not to authenticate the origin.

6 Syntax and encoding for RMPI-MB and RMPI-M

6.1 Introduction

The syntax and encoding for the RMPI-MB and RMPI-M payload is given below. The payload describes the minimum set of usage rights and rules that can be conveyed alongside a digital television broadcast. It is composed of at most four grants including:

- A grant for the "Receiving Domain" that signals the rights and conditions that apply to content once it has entered a given "Receiving Domain". This grant excludes the "Extend Rights" right.
- A grant for "Any Domain" that signals the rights and conditions that apply to content once it has entered "Any Domain". This grant excludes the "Extend Rights" right.
- A grant for the "Receiving Domain" that signals the "Extend Rights" right and associated conditions.
- A grant for "Any Domain" that signals the "Extend Rights" right and associated conditions.

The last two grants are always identical and therefore share the same encoding.

The encoding of the payload allows for the signalling of all relevant conditions for each of the rights expressed in each respective grant. The encoding also allows signalling that no rights have been granted by assigning null values to the respective rights flags. For example, a broadcaster to signal that rights were granted to a "Receiving Domain", and not to "Any Domain", then "Any Domain" rights flags would be set to null. The result of this would be that only those devices in the "Receiving Domain" would have access to the content based on the grants, unless the "Extend Rights" right provided for the acquisition of additional rights.

The present document does not address binding of RMPI-MB and RMPI-M to content, nor does it define rules for conveying a multiplicity of grants within a broadcast stream. However the payload data structure has been defined with processing efficiency in mind. Should an implementer or compliance body choose to signal a multiplicity of RMPI-MB (for example to support a variety of conditions within a large set of geographic territories), it is recommended that the binding to content allows for fast identification of relevant RMPI-MB by the receiver.

6.2 RMPI-MB and RMPI-M payload

Table 5 describes the fixed encoding of RMPI-MB and RMPI-M.

Table 5: RMPI-MB and RMPI-M codes

Syntax	No. of bits	Identifier
RMPI_MB_and_RMPI_M_payload (){		
Ancillary RMPI		
RMPI_type_flag	1	bslbf
Version_of_RMPI	15	bslbf
Origin_of_RMPI	128	bslbf
Scrambling_control	1	bslbf
Cipher	4	bslbf
Extend Rights (Grant is common to Receiving Domain and Any Domain)		
Extend_rights_flag	1	bslbf
Security_level	2	uimsbf
Source_of_additional_rights	128	bslbf
Grant to Receiving Domain		
Domain_ID	128	bslbf
Play_Right_flag	1	bslbf
Analogue_export_right_flag	1	bslbf
Digital_export_SD_right_flag	1	bslbf
Digital_export_HD_right_flag	1	bslbf
Buffer_duration	2	bslbf
Security_level	2	uimsbf
Time_window_start_date	16	uimsbf
Time_window_end_date	16	uimsbf
Geographic_control	128	bslbf
Analogue_export_signalling	2	bslbf
Analogue_SD_control	1	bslbf
Standard_Definition_digital_export_control	2	bslbf
High_Definition_digital_export_control	2	bslbf
Reserved_for_future_use	1	bslbf
Single_point_of_control_flag	1	bslbf
Physical_proximity_flag	1	bslbf
Simultaneous_rendering_count	4	uimsbf
Reserved_for_future_use	2	bslbf
Single_point_of_control_ID	128	bslbf
Grant to Any Domain		
Play_Right_flag	1	bslbf
Analogue_export_right_flag	1	bslbf
Digital_export_SD_right_flag	1	bslbf
Digital_export_HD_right_flag	1	bslbf
Buffer_duration	2	bslbf
Security_level	2	uimsbf
Time_window_start_date	16	uimsbf
Time_window_end_date	16	uimsbf
Geographic_control	128	bslbf
Analogue_export_signalling	2	bslbf
Analogue_SD_control	1	bslbf
Standard_Definition_digital_export_control	2	bslbf
High_Definition_digital_export_control	2	bslbf
Reserved_for_future_use	1	bslbf
}		

6.3 Ancillary RMPI

RMPI_type_flag: This 1-bit field indicates the type of RMPI carried (table 6).

Table 6: RMPI_type_flag

Value	Meaning
0	RMPI-Micro Broadcast (RMPI-MB)
1	RMPI-Micro (RMPI-M)

Version_of_RMPI: This 15-bit field is used to identify the version of RMPI for future-proofing purposes. 15 bits for version to be allocated by compliance body.

Origin_of_RMPI: This 128-bit field is used to identify the entity that originated the RMPI. 128 bits to be allocated by compliance body.

Scrambling_control: This 1-bit field indicates the scrambling policy to implement (table 7).

Table 7: scrambling_control

Value	Meaning for RMPI-MB	Meaning for RMPI-M
0	Maintain original scrambling status, including no scrambling. "cipher" field: cipher used in the broadcast.	Original scrambling status has been maintained, including no scrambling. "cipher" field: cipher currently used on the content.
1	Change scrambling including replacing scrambling "cipher" field: cipher to be used to scramble the content. It is assumed that the broadcast receiver knows which scrambling algorithm is used to protect the broadcast signal (e.g. DVB CSA for DVB receivers).	The original scrambling has been changed. "cipher" field: cipher currently used on the content.

Cipher: This 4-bit field specifies the cipher algorithm used to (de)scramble the content in the TVA RMP compliant domain (table 8).

Table 8: Cipher

Value	Meaning
0x0	No cipher.
0x1	AES.
0x2	Camellia.
0x3	DVB CSA 1.
0x4	DVB CSA 2.
0x5	3DES.
0x6	M2.
0x7	Scrambling/descrambling outside of the control of RMP.
0x8 to 0xF	Reserved.

NOTE 1: If the accompanying scrambling_control field is set to 1, then only "No Cipher" (value 0x0), AES (value 0x1), Camellia (value 0x2) and "Scrambling/descrambling outside of the control of RMP" (value 0x7) can be employed. Values 0x0, 0x1, 0x2 indicate that content is descrambled and rescrambled using the appropriate cipher. Value 0x7 indicates that a custom cipher or super-scrambling is to be used.

NOTE 2: Value 0x7 "Scrambling/descrambling outside of the control of RMP" includes super-scrambling whereby additional scrambling is applied to the already scrambled broadcast content at the time of entering the RMP Domain. It can be used in conjunction with "Single_Point_of_Control_ID" to determine the entity which is responsible for descrambling.

6.4 Rights

Extend_rights_flag: This 1-bit field indicates whether the Extend Rights right is granted (table 9).

Table 9: extend_rights_flag

Value	Meaning
0	Extend Rights right is not granted.
1	Extend Rights right is granted.

Play_right_flag: This 1-bit field indicates whether the Play right is granted (table 10).

Table 10: play_right_flag

Value	Meaning
0	Play right is not granted.
1	Play right is granted.

Analogue_export_right_flag: This 1-bit field indicates whether the Analogue Export right is granted (table 11).

Table 11: analogue_export_right_flag

Value	Meaning
0	Analogue Export right is not granted.
1	Analogue Export right is granted.

Digital_export_SD_right_flag: This 1-bit field indicates whether the Digital Export SD right is granted (table 12).

Table 12: digital_export_SD_right_flag

Value	Meaning
0	Digital Export SD right is not granted.
1	Digital Export SD right is granted.

Digital_export_HD_right_flag: This 1-bit field indicates whether the Digital Export HD right is granted (table 13).

Table 13: digital_export_HD_right_flag

Value	Meaning
0	Digital Export HD right is not granted.
1	Digital Export HD right is granted.

NOTE: If both the Digital Export SD and Digital Export HD rights are granted, then Digital Export is permitted for any definition/resolution. This is called the "Digital Export Any Resolution right".

6.5 Conditions and identifiers

Unless otherwise stated, conditions apply to Play, Analogue Export, Digital Export SD and Digital Export HD. If conditions are not asserted they do not apply.

Security_level: This 2-bit field indicates the minimum security level required to exercise the right. Security levels are to be defined by the compliance body.

NOTE 1: Security levels should be based upon the aggregate robustness of all invoked RMP components required to exercise the right.

NOTE 2: This condition applies to all rights, including extend rights.

Source_of_additional_rights: This 128-bit field identifies the entity from which new rights can be assigned to the content. 128-bit identifier to be allocated by compliance body.

NOTE 3: This condition only applies to Extend Rights.

Domain_ID: This 128-bit field identifies the RMP Domain to which the rights are granted. It is the first domain that has received the broadcast signal. 128-bit identifier to be allocated by compliance body.

NOTE 4: If the RMPI_type_flag is set to 0 then this field is not applicable.

Buffer_duration: This 2-bit field limits the use of a right in such a way that each frame of broadcast content is used only within a specified duration after that frame was broadcast (table 14). Buffer_duration is valid only if both Time_window_start_date and Time_window_end_date are not asserted.

Table 14: Buffer_duration

Value	Meaning
00	Condition not asserted.
01	Condition not asserted.
10	Condition set, no buffer (immediate viewing).
11	Condition set, buffer duration is a reasonable period of time to be determined by compliance body (e.g. 90 minutes).

Time_window_start_date: This 16-bit field defines the start date of the window of time during which the rights are granted. It is defined as absolute start time. It is expressed in number of days since January 1st, 2004. A value of 0x0000 means that the condition is not asserted (there is no start date).

Time_window_end_date: This 16-bit field defines the end date of the window of time during which the rights are granted. It is defined as absolute expiry time. It is expressed in number of days since January 1st, 2004. A value of 0xFFFF means that the condition is not asserted (unbounded end date).

Geographic_control: This 128-bit field is used to indicate geographical regions and territories for which the rights are valid. It is to be defined by the compliance body.

NOTE 5: It is suggested that the compliance body could use these bits for signalling up to four territories in the following format: 2 bytes ISO country code and 2 bytes region within the country. Alternatively the compliance body could decide to specify territories for which the rights are not granted. A value should be reserved for "condition not asserted".

Analogue_export_signalling: This 2-bit field is used to signal content management rules to an external analogue content protection systems (table 15).

Table 15: analogue_export_signalling

Value	Meaning
00	Condition not asserted.
01	Condition not asserted.
10	For immediate viewing only.
11	Bound to device or media for future viewing, does not preclude immediate viewing.

NOTE 6: This condition applies only to the Analogue Export right.

Analogue_SD_control: This 1-bit field constrains the resolution of the exported analogue signal (table 16).

Table 16: analogue_SD_control

Value	Meaning
0	Condition not asserted.
1	While doing analogue output Standard Definition resolution only is permitted.

NOTE 7: This condition applies only to the Analogue Export Right.

Standard_Definition_digital_export_control: This 2-bit field is to control the configuration of Standard Definition digital outputs as to whether the content can be recorded or only viewed immediately (table 17). This condition applies only to the Digital Export SD Right.

Table 17: standard_definition_digital_export_control

Value	Meaning
00	Export conditions not asserted. Hand-off to any non-RMP content protection system is permitted.
01	Export conditions asserted. Hand-off to compliance body certified non-RMP content protection system only is permitted. RMPI-MB/M is mapped to certified system as defined by compliance body.
10	Export conditions asserted, bound to device or media for immediate viewing, includes immediate viewing. Hand-off to compliance body certified non-RMP content protection system only is permitted.
11	Export conditions asserted, immediate viewing only. Hand-off to compliance body certified non-RMP content protection system only is permitted.

NOTE 8: This is not signalling digital copy control in the RMP domain, it is only relevant to the Digital Export Standard Definition right and external content protection systems such as HDCP.

High_Definition_digital_export_control: This 2-bit field is to control the configuration of High Definition digital outputs as to whether the content can be recorded or only viewed immediately (table 18). This condition applies only to the Digital Export HD right.

Table 18: high_definition_digital_export_control

Value	Meaning
00	Export conditions not asserted. Hand-off to any non-RMP content protection system is permitted.
01	Export conditions asserted. Hand-off to compliance body certified non-RMP content protection system only is permitted. RMPI-MB/M is mapped to certified system as defined by compliance body.
10	Export conditions asserted, bound to device or media for immediate viewing, includes immediate viewing. Hand-off to compliance body certified non-RMP content protection system only is permitted.
11	Export conditions asserted, immediate viewing only. Hand-off to compliance body certified non-RMP content protection system only is permitted.

NOTE 9: This is not signalling digital copy control in the RMP domain, it is only relevant to Digital Export High Definition right and external content protection systems such as HDCP.

NOTE 10: If the Digital Export Any Definition Right is exercised, then the most restrictive of either Standard Definition or High Definition digital export control is used.

Single_point_of_control_flag: This 1-bit field indicates that the broadcaster intends that once the content gets into the RMP Receiving Domain only one RMP entity can make usage decisions about the content based upon the expressed RMPI-MB (table 19). The content is irrevocably married to the device identified as single point of control, if that device is destroyed or lost, then this grant becomes no longer exercisable. Single point of control is only used in the context of Receiving Domain as principal.

Table 19: single_point_of_control_flag

Value	Meaning
0	Condition not asserted.
1	Single point of control applies.

Physical_proximity_flag: This 1-bit field limits the use of a right to RMP compliant devices within close physical proximity of the receiver that first received the broadcast content (table 20). When a device checks that condition, it needs to be in close physical proximity of the receiving device in order to exercise the right. Precise definition of close physical proximity is to be determined by compliance body. The compliance body may decide to limit the use of this condition to live broadcasts. For instance close physical proximity could be defined as immediate vicinity e.g. content use is limited to the home network on the same local area network and is not permitted to be transmitted over a wide area network. Physical proximity is only used in the context of Receiving Domain as principal.

Table 20: physical_proximity_flag

Value	Meaning
0	Condition not asserted.
1	Physical proximity applies.

Simultaneous_rendering_count: This 4-bit field limits the number of simultaneous independent Plays, Analogue Exports, Digital Export SDs and Digital Export HDs of content within a domain (table 21). For purposes of this condition a Play counts as a rendering, an Analogue Export counts as a rendering, a Digital Export SD counts as a rendering, and a Digital Export HD counts as one rendering. Simultaneous rendering count is only used in the context of Receiving Domain as principal.

Table 21: simultaneous_rendering_count

Value	Meaning
0	Condition not asserted.
1 to 15	Maximum permitted number of simultaneous renderings.

Single_point_of_control_ID: This 128-bit field identifies the entity that is the single point of control. This is triggered by the condition single point of control = 1 in the incoming RMPI-MB granted to the receiving domain. 128-bit identifier to be allocated by compliance body. This condition is only applicable if RMPI_type_flag and single_point_of_control flag are set to 1.

7 RMPI-MB and RMPI-M lifecycle

RMPI-MB is transmitted in conjunction with the broadcast signal. At the time of reception in the end user's TVA RMP Domain it is converted to RMPI-M. If RMPI-MB "scrambling_control" is set to 1, then transition from RMPI-MB to RMPI-M must be synchronized with the rescrambling of the content. Rights that are granted to the "Receiving Domain" and "Single Point of Control" (if present) in RMPI-MB are carried over in RMPI-M. Generic mentioning of the "Receiving Domain" and "Single Point of Control" (if present) in RMPI-MB is translated into explicit mentioning through the explicit statement of "Identifiers" in RMPI-M. In order to maintain the persistence of the rights assigned by the broadcaster or content provider, a TVA RMP compliant receiver shall not change any other value in RMPI. Rights granted to "Any Domain" are always carried over unchanged from RMPI-MB to RMPI-M. Figure 2 illustrates the transition from RMPI-MB to RMPI-M in a case where "Single Point of Control" is asserted.

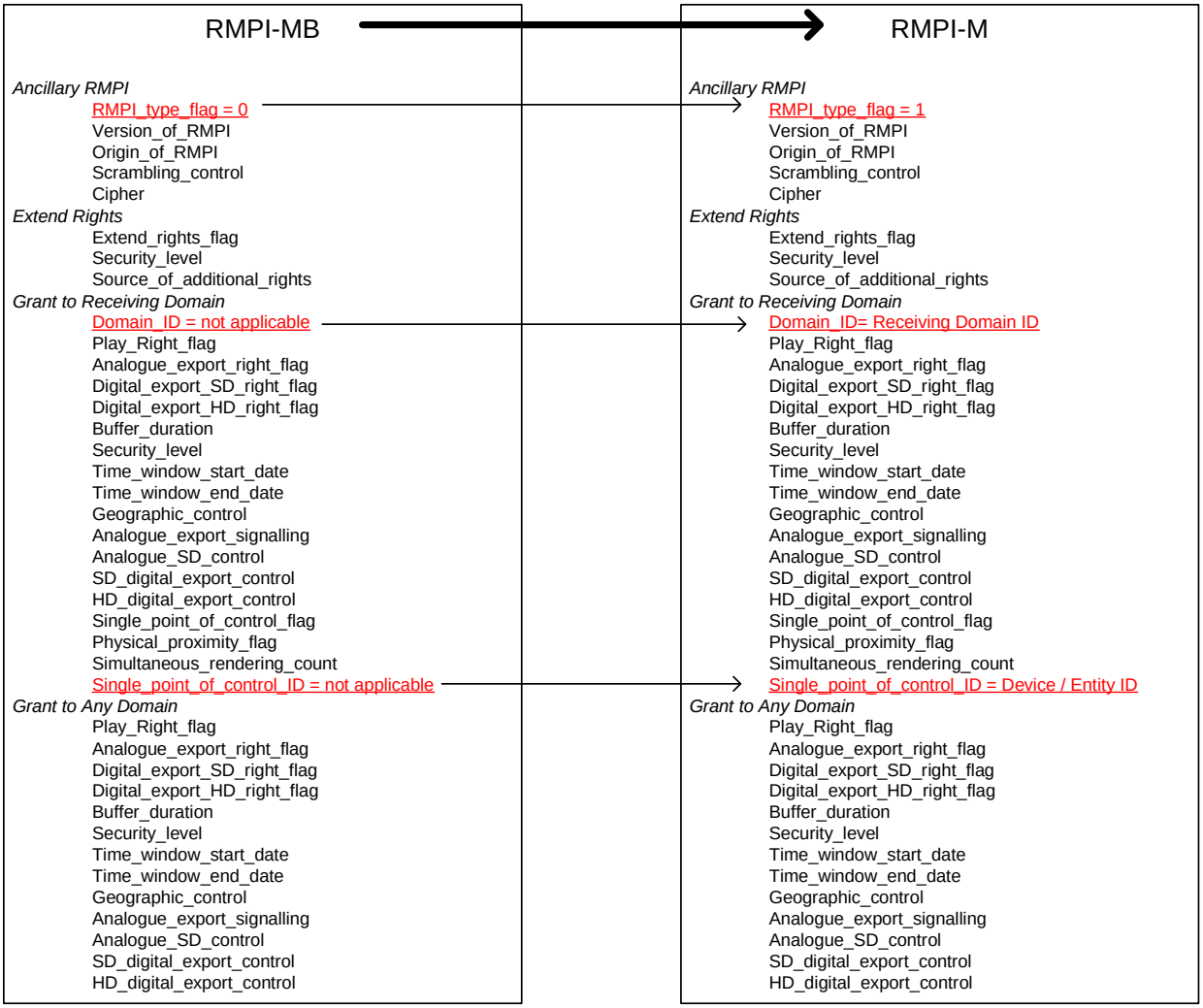


Figure 2: Transition from RMPI-MB to RMPI-M

Annex A (informative): XML Expression of RMPI MB and M

A.1 Cipher Classification Scheme (CipherCS.xml)

```
<?xml version="1.0" encoding="UTF-8"?>
<ClassificationScheme uri="urn:tva:rmpi:cs:CipherCS:2005">
    <!-- ########################################################################## -->
    <!-- Cipher -->
    <!--Definition: A series of definitions for possible values of the Cipher element in RMPI
metadata-->
    <!-- ########################################################################## -->
    <Term termID="0">
        <Name xml:lang="en">no cipher</Name>
    </Term>
    <Term termID="1">
        <Name xml:lang="en">AES</Name>
        <Definition xml:lang="en">FIPS PUB 197: "Specifications for the Advanced Encryption Standard
(AES)", 26 November 2001</Definition>
    </Term>
    <Term termID="2">
        <Name xml:lang="en">Camellia</Name>
        <Definition xml:lang="en">A 128-Bit Block Cipher Suitable for Multiple Platforms", IEITC
Transactions on Fundamentals of Electronics, Communications and Computer Science, Vol. E85-A, No.1,
The Institute of Electronics, Information and Communication Engineers, January, 2002. Kazumaro Aoki,
Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio
Tokita</Definition>
    </Term>
    <Term termID="3">
        <Name xml:lang="en">DVB CSA 1</Name>
        <Definition xml:lang="en">"Digital Video Broadcasting (DVB); Support for use of scrambling
and Conditional Access (CA) within digital broadcasting systems"; ETSI Technical Report ETR_289,
October 1996</Definition>
    </Term>
    <Term termID="4">
        <Name xml:lang="en">DVB CSA 2</Name>
        <Definition xml:lang="en">"Digital Video Broadcasting (DVB); Support for use of scrambling
and Conditional Access (CA) within digital broadcasting systems"; ETSI Technical Report ETR_289,
October 1996</Definition>
    </Term>
    <Term termID="5">
        <Name xml:lang="en">3DES</Name>
        <Definition xml:lang="en">FIPS PUB 46-3: "Data Encryption Standard", 25 October
1999</Definition>
    </Term>
    <Term termID="6">
        <Name xml:lang="en">M2</Name>
        <Definition xml:lang="en">Multi-2 encryption algorithm</Definition>
    </Term>
    <Term termID="7">
        <Name xml:lang="en">out of RMP control</Name>
    </Term>
</ClassificationScheme>
```

A.2 RMPI Scheme (tva_rmpi_5-1_v141.xsd)

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="urn:tva:rmpi:2010" xmlns:rmpi="urn:tva:rmpi:2010"
xmlns:tva="urn:tva:metadata:2010" xmlns:mpeg7="urn:tva:mpeg7:2008"
xmlns="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">

    <import namespace="urn:tva:metadata:2010" schemaLocation="tva_metadata_3-1_v161.xsd"/>
    <import namespace="urn:tva:mpeg7:2008" schemaLocation="tva_mpeg7_2008.xsd"/>

    <annotation>
        <documentation>TV-Anytime Forum (TVAF) Rights Management and Protection Information
(RMPI)</documentation>
    </annotation>
    <annotation>
        <documentation xml:lang="en">This schema consists of datatypes that are normatively defined
in ETSI TS 102 822-5-1 v1.5.1</documentation>
    </annotation>
    <complexType name="RMPI-MBAndMType">
        <sequence>
            <element name="AncillaryRMPI" type="rmpi:AncillaryRMPIType"/>
            <element name="ExtendRights" type="rmpi:ExtendRightsType"/>
            <element name="ReceivingDomainRights" type="rmpi:ReceivingDomainRightsType"/>
            <element name="AnyDomainRights" type="rmpi:AnyDomainRightsType"/>
        </sequence>
    </complexType>
    <complexType name="ExtendRightsType">
        <sequence>
            <choice>
                <sequence>
                    <element name="ExtendRightsFlagGranted" type="rmpi:GrantedType"/>
                    <element name="SecurityLevel" type="rmpi:SecurityLevelType"/>
                    <element name="SourceOfAdditionalRights" type="string"/>
                </sequence>
                <element name="ExtendRightsFlagNotGranted" type="rmpi:NotGrantedType"/>
            </choice>
        </sequence>
    </complexType>
    <simpleType name="SecurityLevelType">
        <restriction base="string">
            <enumeration value="level 0"/>
            <enumeration value="level 1"/>
            <enumeration value="level 2"/>
            <enumeration value="level 3"/>
        </restriction>
    </simpleType>
    <simpleType name="GrantedNotGrantedType">
        <restriction base="string">
            <enumeration value="granted"/>
            <enumeration value="not granted"/>
        </restriction>
    </simpleType>
    <simpleType name="GrantedType">
        <restriction base="string">
            <enumeration value="granted"/>
        </restriction>
    </simpleType>
    <simpleType name="NotGrantedType">
        <restriction base="string">
            <enumeration value="not granted"/>
        </restriction>
    </simpleType>
    <complexType name="BasicSetOfRightsType" abstract="true">
        <sequence>
            <element name="PlayRightFlag" type="rmpi:GrantedNotGrantedType"/>
            <element name="AnalogueExportRight" type="rmpi:AnalogueExportRightType"/>
            <element name="DigitalExportSDRight" type="rmpi:DigitalExportRightType"/>
            <element name="DigitalExportHDRight" type="rmpi:DigitalExportRightType"/>
            <element name="SecurityLevel" type="rmpi:SecurityLevelType"/>
            <choice minOccurs="0">
                <element name="BufferDuration" type="rmpi:BufferDurationType"/>
                <element name="TimeWindow" type="rmpi:TimeWindowType"/>
            </choice>
            <element name="GeographicalControl" type="string"/>
        </sequence>
```

```
    </complexType>
    <complexType name="AnalogueExportRightType">
        <sequence>
            <choice>
                <element name="AnalogueExportRightFlagNotGranted"
                type="rmpi:NotGrantedType"/>
                <sequence>
                    <element name="AnalogueExportRightFlagGranted" type="rmpi:GrantedType"/>
                    <element name="AnalogueExportSignalling"
                    type="rmpi:AnalogueExportSignallingType"
                    minOccurs="0"/>
                    <element name="AnalogueExportSDControl" type="rmpi:ControlType"
                    minOccurs="0"/>
                </sequence>
            </choice>
        </sequence>
    </complexType>
    <simpleType name="ControlType">
        <restriction base="string">
            <enumeration value="controlled"/>
        </restriction>
    </simpleType>
    <simpleType name="AnalogueExportSignallingType">
        <restriction base="string">
            <enumeration value="immediate viewing"/>
            <enumeration value="storage bound"/>
        </restriction>
    </simpleType>
    <complexType name="DigitalExportRightType">
        <sequence>
            <choice>
                <element name="DigitalExportRightFlagNotGranted"
                type="rmpi:NotGrantedType"/>
                <sequence>
                    <element name="DigitalExportRightFlagGranted" type="rmpi:GrantedType"/>
                    <element name="DigitalExportControl"
                    type="rmpi:DigitalExportControlType" minOccurs="0"/>
                </sequence>
            </choice>
        </sequence>
    </complexType>
    <simpleType name="DigitalExportControlType">
        <restriction base="string">
            <enumeration value="immediate viewing"/>
            <enumeration value="storage bound"/>
            <enumeration value="RMP trusted"/>
        </restriction>
    </simpleType>
    <simpleType name="BufferDurationType">
        <restriction base="string">
            <enumeration value="immediate viewing"/>
            <enumeration value="buffered viewing"/>
        </restriction>
    </simpleType>
    <complexType name="TimeWindowType">
        <sequence>
            <element name="StartDate" type="rmpi:TVATimeType" minOccurs="0"/>
            <element name="EndDate" type="rmpi:TVATimeType" minOccurs="0"/>
        </sequence>
    </complexType>
    <complexType name="TVATimeType">
        <sequence>
            <element name="TimePoint" type="mpeg7:timePointType"/>
            <element name="Duration" type="mpeg7:durationType" minOccurs="0"/>
        </sequence>
    </complexType>
    <complexType name="ReceivingDomainRightsType">
        <complexContent>
            <extension base="rmpi:BasicSetOfRightsType">
                <sequence>
                    <element name="SinglePointOfControl"
                    type="rmpi:SinglePointOfControlType" minOccurs="0"/>
                    <element name="PhysicalProximityFlag" type="rmpi:ControlType"
                    minOccurs="0"/>
                    <element name="SimultaneousRendering"
                    type="rmpi:SimultaneousRenderingType" minOccurs="0"/>
                    <element name="DomainId" type="string" minOccurs="0"/>
                </sequence>
```

```
            </extension>
        </complexContent>
    </complexType>
    <complexType name="AnyDomainRightsType">
        <complexContent>
            <extension base="rmpi:BasicSetOfRightsType"/>
        </complexContent>
    </complexType>
    <complexType name="SinglePointOfControlType">
        <sequence>
            <element name="SinglePointOfControlFlag" type="rmpi:ControlType"/>
            <element name="SinglePointOfControlId" type="string" minOccurs="0"/>
        </sequence>
    </complexType>
    <complexType name="SimultaneousRenderingType">
        <sequence>
            <element name="SimultaneousRenderingFlag" type="rmpi:ControlType"/>
            <element name="SimultaneousRenderingCount"
            type="rmpi:SimultaneousRenderingCountType"/>
        </sequence>
    </complexType>
    <simpleType name="SimultaneousRenderingCountType">
        <restriction base="integer">
            <minInclusive value="1"/>
            <maxInclusive value="15"/>
        </restriction>
    </simpleType>
    <complexType name="AncillaryRMPIType">
        <sequence>
            <element name="RMPITypeFlag" type="rmpi:RMITypeFlagType"/>
            <element name="VersionOfRMPI" type="string"/>
            <element name="OriginOfRMPI" type="string"/>
            <element name="Cipher" type="tva:ControlledTermType"/>
            <choice>
                <element name="MBScramblingControl" type="rmpi:MBScramblingControlType"/>
                <element name="MScramblingControl" type="rmpi:MScramblingControlType"/>
            </choice>
        </sequence>
    </complexType>
    <simpleType name="RMITypeFlagType">
        <restriction base="string">
            <enumeration value="RMPI-MB"/>
            <enumeration value="RMPI-M"/>
        </restriction>
    </simpleType>
    <simpleType name="MBScramblingControlType">
        <restriction base="string">
            <enumeration value="maintain"/>
            <enumeration value="change"/>
        </restriction>
    </simpleType>
    <simpleType name="MScramblingControlType">
        <restriction base="string">
            <enumeration value="maintained"/>
            <enumeration value="changed"/>
        </restriction>
    </simpleType>

</schema>
```

Annex B (informative): TV-Anytime RMPI Schemas

The *TV-Anytime* RMPI metadata schema listed in the present document has been aggregated into an archive ts_1028220501v010501p0.zip, attached to the present document, which contains the following files:

- "CipherCS.xml";
- "tva_rmpi_5-1_v141.xsd".

The RMPI metadata schema imports other files that need to be present in order to be valid:

- "tva_mpeg7_2008.xsd" that is available in archive ts_1028220301v010601p0.zip accompanying TS 102 822-3-1 [3];
- "tva_metadata_ 3-1_v151.xsd" that is available in archive ts_1028220301v010601p0.zip accompanying TS 102 822-3-1 [3];
- "xml.xsd" that is available in archive ts_1028220301v010601p0.zip accompanying TS 102 822-3-1 [3].

Annex C (informative): Bibliography

3DES: FIPS PUB 46-3: "Data Encryption Standard", 25 October 1999.

NOTE: Available at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.

AES: FIPS PUB 197: "Specifications for the Advanced Encryption Standard (AES)", 26 November 2001.

NOTE: Available at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

"Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms", IEITC Transactions on Fundamentals of Electronics, Communications and Computer Science, Vol. E85-A, No.1, The Institute of Electronics, Information and Communication Engineers, January, 2002. Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita.

NOTE: Available at http://info.isl.ntt.co.jp/crypt/eng/camellia/index.html.

ETSI ETR 289: "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems".

List of figures

Figure 1: RMPI in the broadcast environment 5

Figure 2: Transition from RMPI-MB to RMPI-M 20

List of tables

Table 1: Principals being used by broadcasters 8
Table 2: Rights 9
Table 3: Conditions 10
Table 4: Ancillary RMPI-MB and ancillary RMPI-M 12
Table 5: RMPI-MB and RMPI-M codes 14
Table 6: RMPI_type_flag 15
Table 7: scrambling_control 15
Table 8: Cipher 15
Table 9: extend_rights_flag 16
Table 10: play_right_flag 16
Table 11: analogue_export_right_flag 16
Table 12: digital_export_SD_right_flag 16
Table 13: digital_export_HD_right_flag 16
Table 14: Buffer_duration 17
Table 15: analogue_export_signalling 17
Table 16: analogue_SD_control 18
Table 17: standard_definition_digital_export_control 18
Table 18: high_definition_digital_export_control 18
Table 19: single_point_of_control_flag 19
Table 20: physical_proximity_flag 19
Table 21: simultaneous_rendering_count 19

History

Document history		
V1.1.1	March 2005	Publication as TS 102 822-5
V1.2.1	January 2006	Publication
V1.3.1	March 2008	Publication
V1.4.1	May 2009	Publication
V1.5.1	July 2010	Publication