ETSI TS 102 822-5-2 V1.2.1 (2006-01)

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 2: RMPI binding

Reference
RTS/JTC-TVA-PH1-19-05-02

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

Contents

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 2, 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: "System description";

Part 3: "Metadata";

Part 4: "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

"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 sub-parts 1 [3], 2 [4], 3 [5] and 4 [6]), Content Referencing (TS 102 822-4 [7]), Rights Management (TS 102 822-5 sub-parts 1 [8] and 2 (the present document)), Bi-directional Metadata Delivery (TS 102 822-6 sub-parts 1 [9], 2 [10] and 3 [11]) and Protection (TS 102 822-7 [12]), Interchange Data Format (TS 102 822-8 [13]) and Remote Programming (TS 102 822-9 [14]). The present document is to be used by manufacturers, service providers and content providers for the implementation of the features of the *TV-Anytime* specifications.

The present document specifies the methods for binding RMP Information to content in different environments.

1 Scope

Binding of Rights Management and Protection Information is a component of the TV-Anytime Rights Management and Protection system suite of specifications. When used in conjunction with the RMPI specification as components of an end-to-end RMP system, binding ensures that RMPI is appropriately applied.

TVAF RMP defines Binding as the process of creating a strong association between a given set of RMPI and the content to which it applies.

TVAF RMP defines Secure Binding as a Binding adequate to ensure that bound RMPI cannot be reassigned to unintended content without detection. Non-secure binding is binding which is not secure, and includes insufficient mechanisms to protect against tampering and/or modifications to RMPI.

The present document specifies methods for both Secure Binding and Non-Secure Binding.

Different binding methods are given for both content broadcast in the clear (e.g. free-to-air broadcast) and scrambled content (e.g. content protected by CA or DRM).

Different binding methods allow for the detection of RMPI tampering and/or unauthorized modifications to the binding. RMPI under such conditions is treated as invalid by the RMP system. Compliance bodies will specify RMP system detection obligations and required behaviours when either of the conditions (tampering/modification) occur.

It is mandatory that RMPI binding be verified before RMPI may be acted upon by the RMP system.

All the proposed binding methods in principle enable the binding of multiple RMPI, if so required.

The implementation of the present document requires the use of cryptographic technologies, however, the selection of such technologies are left to the compliance body. These include but are not limited to: ciphers, trust models, key management and watermark algorithms.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

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

[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: System description".

[3] ETSI TS 102 822-3-1: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 3: Metadata; Sub-part 1: Phase 1 - Metadata schemas".

[4] ETSI TS 102 822-3-2: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV Anytime"); Part 3: Metadata; Sub-part 2: System aspects in a uni-directional environment".

[5] ETSI TS 102 822-3-3: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 3: Metadata; Sub-part 3: Phase 2 - Extended Metadata Schema".

[6] ETSI TS 102 822-3-4: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 3: Metadata; Sub-part 4: Phase 2 - Interstitial metadata".

[7] 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".

[8] ETSI TS 102 822-5-1: "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".

[9] ETSI TS 102 822-6-1: "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; Sub-part 1: Service and transport".

[10] ETSI TS 102 822-6-2: "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; Sub-part 2: Phase 1 - Service discovery".

[11] ETSI TS 102 822-6-3: "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; Sub-part 3: Phase 2 - Exchange of Personal Profile".

[12] 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".

[13] 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".

[14] 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".

3 Definitions and abbreviations

3.1 Definitions

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

acquisition point: device through which content enters a TVA RMP domain

binding: process of creating a strong association between a given set of RMPI and the content to which it applies

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

Content Identifier: unique serial number associated with each piece of content

NOTE: The compliance body is responsible for the selection policy and the choice of the size of the content identifier. The content identifier for a given piece of content can be determined by an embedded watermark or some other means.

cryptogram: generic name for a MAC or a signature which requires a key to be generated

license: authenticated data structure which includes one RMPI, one Content Identifier and other information to identify and manage usage of a given piece of content

Message Authentication Code (**MAC):** cryptogram that is used to verify the integrity and the origin of a message

NOTE: It is computed and verified using a shared secret key.

non-Secure Binding: binding which is not secure, and includes insufficient mechanisms to protect against tampering and/or modifications to RMPI

RMP domain: A domain is a set of TVA RMP-compliant devices that are securely bound to each other for the purpose of exchanging protected content. It is an instance of a principal. The rules for creating and managing domains are outside the scope of TS 102 822-5-2.

secure binding: binding adequate to ensure that bound RMPI cannot be reassigned to unintended content without detection

signature: cryptogram that used to verify in a non-repudiable way the integrity and the origin of a message

NOTE: It is computed using a private key only known to the message sender. It can be verified using a public key that can be made widely available.

3.2 Abbreviations

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

CA	Conditional Access
CID	Content Identifier
DRM	Digital Rights Management
MAC	Message Authentication Code
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
TVAF	TV-Anytime Forum

4 Non-secure binding by transport

This binding method is only applicable to in-the-clear content. It protects against RMPI modifications, but does not protect against tampering with the binding itself.

In this method, the binding is provided by the content transport scheme: if RMPI is provided within the content transport scheme in a synchronous manner, that RMPI is considered bound to the content.

Using this method, the association of RMPI and CID is authenticated through the generation of a cryptogram that is appended to the RMPI. The cryptogram is verified to check the authenticity of the RMPI. If the verification fails, this means the RMPI has been tampered with. If no RMPI is present, see clause 7.

5 Secure binding by content scrambling

This method is applicable to scrambled content. The security of this binding method depends on the use of content scrambling keys that are sufficiently unique for each binding.

This method tests for the association of the content keys with the RMPI and then tests the content with the content keys.

The content license includes RMPI, content scrambling keys or a reference to their location, the Content Identifier and a cryptogram. Content scrambling keys, when present, are encrypted. The cryptogram is computed over RMPI, content identifier and clear scrambling keys.

Upon content usage, RMPI is retrieved. If no RMPI is present, content is unusable. Otherwise, scrambling keys are first deciphered or obtained from their location and the cryptogram is verified. A verification failure means RMPI has been tampered with. If verification is successful (and applicable rights are granted in the RMPI), scrambling keys are tested to descramble the content. If the keys do not descramble the content, the binding has been tampered with. Otherwise, binding verification is successful.

6 Secure binding by watermark and RMPI authentication

This method applies only to in-the-clear content.

In this method, the binding is provided using both cryptography and watermarking techniques. Successful use of this method depends upon the selection of watermarking technologies and cryptography which are sufficiently robust.

Prior to distribution, content is watermarked with a Content Identifier. Then, the RMPI is bound to the content using cryptography techniques. To that end, a cryptogram (a signature or a Message Authentication Code) is computed on the RMPI and the content identifier. The cryptogram ensures secure binding of the content identifier and the RMPI. The watermarking ensures the secure binding of the content and the Content Identifier.

The content license includes RMPI, the Content Identifier and the cryptogram.

Upon content reception, RMPI is retrieved. If no RMPI is present, the verifier tries to extract the watermark from the content. If a watermark is present, binding has been tampered with. Otherwise content is viewed as non-RMP content.

If RMPI is present, the cryptogram has to be first verified in order to check the authenticity of RMPI. If the verification fails, this means the RMPI has been tampered with.

After RMPI integrity has been verified, the RMP system extracts the watermark from the content and compares it with the Content Identifier. This comparison may be a one-to-one matching or any other mapping mechanism defined by the compliance body. This makes it possible to allow a single license to apply to multiple bodies of content (e.g. an entire catalogue, series, channel, producer, subscription…). If the verification fails (including if the content is not watermarked), this means the binding has been tampered with.

In addition to the case of content transmitted in the clear, this method may also be applied to content that is initially transmitted scrambled and is eventually carried within the domain in the clear or recorded in the clear (e.g. post domain acquisition). In order to obtain secure binding, content has to be watermarked before its initial transmission. "Secure binding by content scrambling" is applied (see clause 5) to the scrambled version of the content.

As the content is converted into the clear, the RMP system applies "secure binding by watermark and RMPI authentication" (see above). Since the content was initially watermarked, standard secure binding verification can be performed.

Legacy devices may not be able to deal with the watermark extraction. In this case, the compliance body may allow the non-secure binding by transport verification as described in 4. This would allow both legacy devices and devices capable of processing the watermark to share the same content.

7 Summary of Binding Approaches

The following illustrations provide a summary and overview of binding strategies for different types of content protection. According to the subsequent consumption model that applies to the content in question, different combinations of watermarking and scrambling may apply.

Table 1: Binding Overview

		Transmit Watermarked?	
		Y	N
Transmit Scrambled?	Y	Secure binding by Scrambling (see clause 5). Allows for binding to content when in the clear	Secure binding by Scrambling (see clause 5)
	N	Secure Binding by Watermark (see clause 6)	Non-Secure Binding (see clause 4) Or non-RMP content

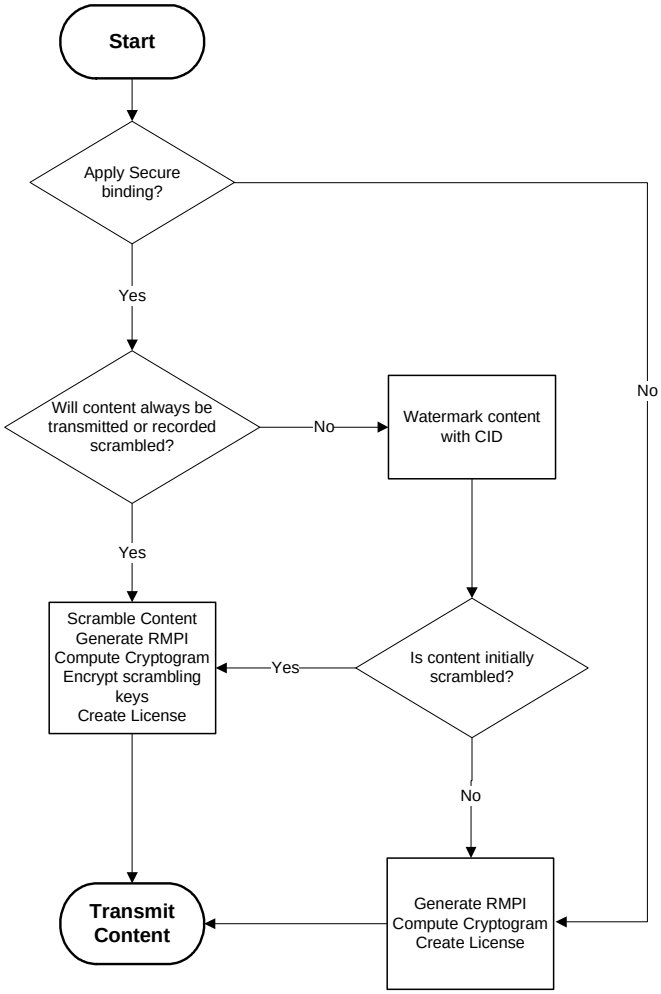

Figure 1: Binding RMPI to Content

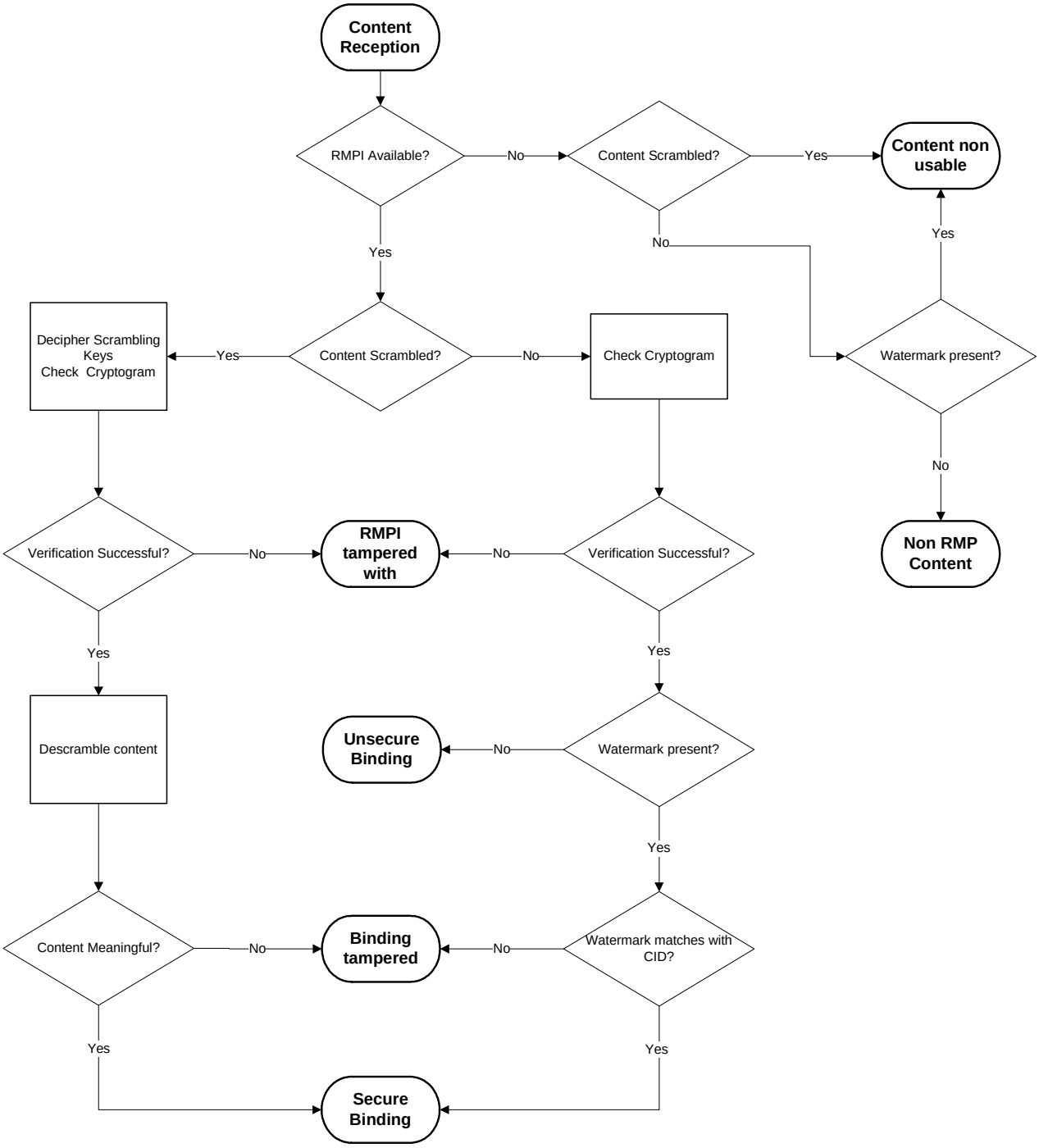

Figure 2: Binding Verification

8 Examples (informative)

8.1 Notations

a||b	The concatenation of string a and string b, string a being first.
E{K}(M)	The encipherment of message M using key K.
S{K}(M)	The signature of message M using key K.
MAC{K}(M)	The MAC of message M using key K.

RMPI-M(any)	RMPI post domain acquisition, rights granted to any domain extend rights and ancillary RMPI.
RMPI-MB(any)	RMPI prior to domain acquisition, rights granted to any domain extend rights and ancillary RMPI.
RMPI-M(receiving)	RMPI post domain acquisition, rights granted to receiving domain extend rights and ancillary RMPI.
RMPI-MB(receiving)	RMPI prior to domain acquisition, rights granted to receiving domain extend rights and ancillary RMPI.

8.2 Case of RMPI bound to clear content

8.2.1 Prior to Domain Acquisition

For clear content, secure binding prior to domain acquisition can be achieved as follows:

1) Watermark the content with its content identifier CID.

2) Compute a signature S_A over the content identifier and RMPI-MB(any):

$$S\_A = S\{K\_PrivLI\}(RMPI\text{-}MB(any)||CID)$$

The key K_PrivLI used in the signature computation is only known to the License Issuer.

3) Compute a signature S_R over the content identifier and RMPI-MB(receiving):

$$S\_R = S\{K\_PrivLI\}(RMPI\text{-}MB(receiving)||CID)$$

The key K_PrivLI used in the signature computation is the same as above.

4) Build the content license CL_B that includes RMPI-MB, content identifier and the computed signatures:

$$CL\_B = RMPI\text{-}MB||CID||S\_A||S\_R$$

Content license can be then carried with the content or separately.

8.2.2 In the Acquisition Point

Upon reception of the content, the Acquisition Point processes the content license as follows:

1) Check both signatures using clear content provider public key.

A false verification means CL_B has been tampered with.

2) Extract the watermark and compare it with the CID present in the license.

A false verification means the binding has been tampered with.

3) Compute a MAC_R over the content identifier and RMPI-M(receiving):

$$MAC\_R = MAC\{K\_AD\}(RMPI\text{-}M(receiving)||CID).$$

4) Build the content license CL_M that includes RMPI-M, the content identifier, MAC_R and S_A:

$$CL\_M = RMPI\text{-}M||CID||MAC\_R||S\_A$$

The key K_AD used in the MAC computation is established according to the context. It can be for instance a device key (for secure storage or in the case of a single point of control), a link key (for the secure transmission of the RMPI between different devices) or a domain key (if domain management is based on a domain key). Key K_AD provides authentication and protects the license within the receiving domain.

8.2.3 Post Domain Acquisition

To verify the binding, a device from the domain identified in the license processes the license as follows:

1) Check MAC_R using K_AD.

   A failed verification means the license has been tampered with.

2) Extract the watermark from the content.

3) Check whether the extracted watermark correctly corresponds to the content identifier.

   A successful verification means the binding is correct.

To verify the binding, a device from a domain not identified in the license processes the licence as follows:

1) Check S_A using license issuer public key (the license issuer could be identified in the RMPI or in the license itself, for example).

   A failed verification means the license has been tampered with.

2) Extract the watermark from the content.

3) Check whether the extracted watermark correctly corresponds to the content identifier.

   A successful verification means the binding is correct.

8.3 Case of RMPI bound to scrambled content

8.3.1 Prior to Domain Acquisition

For scrambled content, the proposed binding process is as follows:

1) Compute a Message Authentication MAC_B over RMPI-MB, the clear content scrambling keys (SK) and content identifier:

$$MAC\_MB = MAC\{K\_AP\}(RMPI\text{-}MB||CID||SK)$$

2) Encipher scrambling keys SK using a proprietary key K_CP.

3) Build the content license CL_B that includes RMPI-MB, content identifier, enciphered scrambling keys and the computed MAC:

$$CL = RMPI\text{-}MB||CID||E\{K\_CP\}(SK)||MAC\_MB.$$

Keys K_AP and K_CP are proprietary to the delivery mechanism. K_AP provides authentication while K_CP provides confidentiality. RMPI is thus bound to the portion of content that is protected by SK.

8.3.2 In the Acquisition Point

Once the CA/DRM hands over control of content to TVA RMP system, the Acquisition Point processes the license as follows:

1) Decipher the scrambling keys and check the MAC.

   If the verification fails, this means RMPI and or license has been tampered with.

2) Apply scrambling policy as specified in RMPI-MB.

3) Encipher the scrambling keys using a key K_CD.

4) Compute a MAC MAC_MR over the clear scrambling keys, the content identifier and RMPI-M(receiving):

$$MAC\_MR = MAC\{K\_AD\}(RMPI\text{-}M(receiving)||CID||SK)$$

5) Encipher the scrambling keys using a key K_CA.

6) Compute a MAC MAC_MA over the clear scrambling keys, the content identifier and RMPI-M(any):

$$MAC\_MA = MAC\{K\_AA\}(RMPI\text{-}M(any)||CID||SK)$$

7) Build the content license CL_M that includes RMPI-M, the two instances of encrypted scrambling keys (as derived in steps 3 and 5) and the two MAC:

$$CL\_M = RMPI\text{-}M||CID||E\{K\_CD\}(SK)||E\{K\_CA\}(SK)||MAC\_MR||MAC\_MA$$

Keys K_CD, K_AD, K_CA and K_AA are established according to the context. They can be for instance:

- device keys, for secure storage or in the case of a single point of control;
- link keys, for the secure transmission of the RMPI between different devices or domains;
- domain keys, when domain management is based on a domain key.

K_CD and K_CA are used to provide confidentiality while K_AD and K_AA are used to provide authentication. K_AD and K_CD protect this license within the receiving domain while K_AA and K_CA protect the license within any domain.

8.3.3 Post Domain Acquisition

To verify the binding, a device from the domain identified in the license processes the license as follows:

1) Decipher scrambling keys using K_CD.

2) Check MAC_MR using K_AD.

   A failed verification means the license has been tampered with.

3) Test the key to descramble the content.

   If descrambling is successful, binding is verified.

To verify the binding, a device from a domain not identified in the license processes the licence as follows:

1) Decipher scrambling keys using K_CA.

2) Check MAC_MA using K_AA.

   A failed verification means the license has been tampered with.

3) Test the key to descramble the content.

   If descrambling is successful, binding is verified.

8.4 Other cases

8.4.1 Case of content that is scrambled prior to domain acquisition and in the clear post domain acquisition

Content has to be first watermarked with its content identifier CID. Watermarking is required to maintain the secure binding since the content is to be eventually transmitted in the clear. For example, this happens when the RMPI-MB *scrambling_control* field indicates that the acquisition point shall remove the original scrambling and the *cipher* field indicates "No-cipher".

Once content is watermarked, the content provider applies binding as described in clause 8.3.1.

The Acquisition Point checks the binding as described in clause 8.3.2. It then descrambles the content and applies binding as described in clause 8.2.2.

Then, binding can be further verified as described in clause 8.2.3.

8.4.2 Case of content that is in the clear prior to domain acquisition and scrambled post domain acquisition

The content provider applies binding as described in clause 8.2.1.

The Acquisition Point checks the binding as described in clause 8.2.2. Then, it scrambles the content and applies binding as described in clause 8.3.2.

Then, binding can be further verified as described in clause 8.3.3.

List of tables

List of figures

History

Document history		
V1.1.1	March 2005	Publication as TS 102 822-5
V1.2.1	January 2006	Publication