INTERNATIONAL ORGANISATION FOR STANDARDISATION
ORGANISATION INTERNATIONALE DE NORMALISATION
ISO/IEC JTC1/SC29/WG11
CODING OF MOVING PICTURES AND AUDIO

ISO/IEC JTC1/SC29/WG11 MPEG2017/ m42600
April 2018, La Jolla, US

Source: **DMAG-UPC**
Status: **Proposal**
Title: **Ideas on privacy handling in MPEG-21 User Description**
Authors: **Jaime Delgado, Silvia Llorente (Distributed Multimedia Applications Group – Universitat Politècnica de Catalunya)**

Table of Contents

1 Introduction

A second WD for MPEG-21 User Description was produced in the 121st MPEG meeting [1]. Section 4.4.4 describes hoy to apply privacy protection to MPEG-21 UD.

This document describes a use case for supporting privacy protection using privacy rules in the context of MPEG-21 User Description. Several open issues are then introduced in section 3.

2 Applying privacy protection in MPEG-21 UD

2.1. Introduction

In order to provide privacy protection in MPEG-21 UD, we propose the use of privacy rules. The authorization to access to protected content could be specified by expressing access control rules (or, in fact, privacy rules). Different standards exist to express these rules. One example could be XACML [2].

Therefore, it is necessary first to specify how those rules are expressed with XACML (or any other chosen alternative), and, second, how to relate the rules to the content. Additionally, encryption may be needed to protect access when it is not authorized. Finally, two processes are to be defined: first, how to protect the content and create and integrate the rules; and, second, the steps to get authorization and access to the content.

The solution we are proposing is based on a similar one that we have contributed to JPEG as a response to the JPEG Privacy and Security Call for proposals [3] [4], which is currently under discussion.

This contribution to MPEG-21 UD, apart from suggesting an approach to privacy protection, also sketches the process of authorization and content access in an environment where MPEG-21 UD is used.

2.2. The original image-oriented approach

As a reference, Figure 1 shows how a user that wants to view a privacy protected image has to proceed (in a general environment, as it was considered in the JPEG proposal). Steps are explained next.

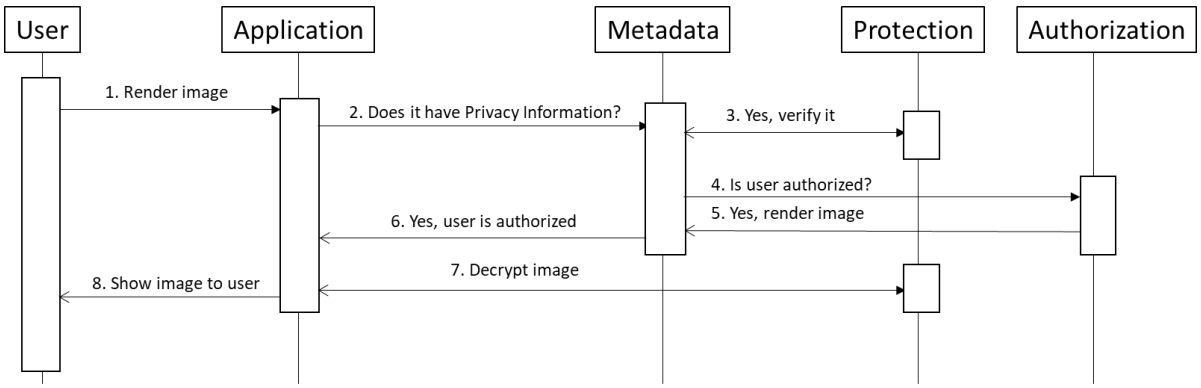

Figure 1. Authorization of access to a protected image

Steps in Figure 1:

1. A user wants to render the protected image.
2. The Application asks the Metadata module if it has associated privacy information.
3. The Metadata module detects privacy information, so it asks to the Protection module to verify it. A possible verification is a digital signature validation.
4. After positive verification, the Metadata module asks for authorization to the Authorization module. Authorization could be also applied to metadata elements, not only to the codestream.
5. After positive authorization, the User can view the image.
6. The Metadata module informs the Application that the User is authorized according to the privacy information contained in the image.
7. The Application requests image decryption to the Protection Module.
8. The User has been authorized to view (or the action indicated in the privacy policy) the image, so it is shown to her.

2.3. The proposal of steps in a MPEG-21 UD environment

Based on this previous proposal for images [4], and in order to provide privacy in MPEG-21 UD, we try to adapt the use case defined in subclause 4.4.4 of [1] following a similar approach.

In our previous use case, apart from the User and Application, we have modules for Metadata, Protection and Authorization.

In the 4.4.4 use case, there are also the User and Application modules, but the rest are the Recommendation Engine, the SD Manager and the UD Manager. We assume the SD Manager corresponds to the selected Service Provider.

The following figure sketches one possible sequence of steps adapting our general proposal to an MPEG-21 UD environment, and trying not to diverge too much from the current 4.4.4 use case of [1]. Steps are explained after the figure. However, there are many open issues in this approach, identified in section 3.

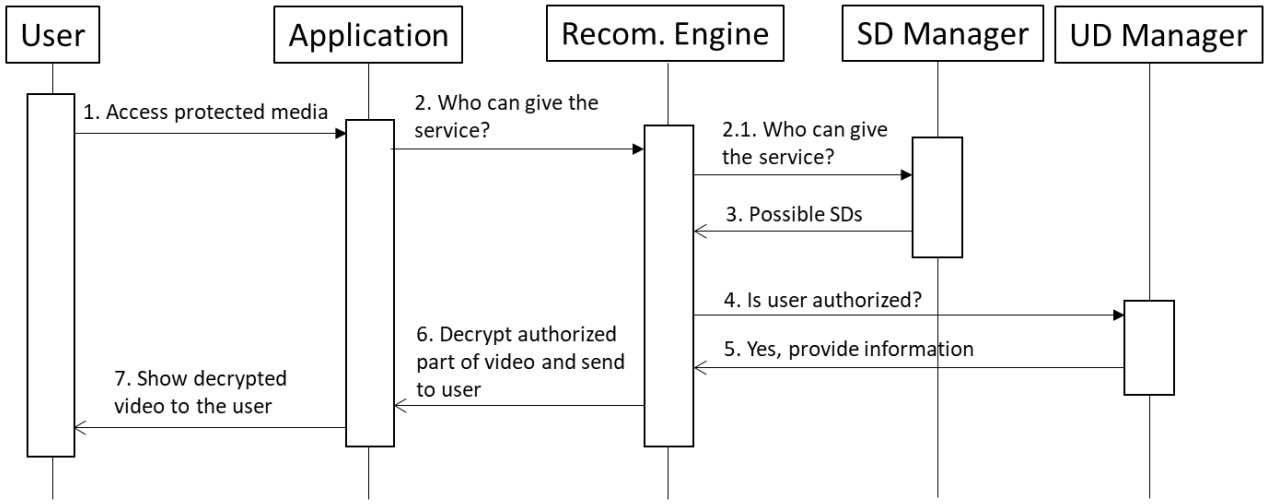

Figure 2. Applying privacy protection in MPEG-21 UD

Steps in Figure 2:

1. A User requests the protected media to the Application.
2. The Application requests a Service Provider to a Recommendation Engine
   2.1. It looks for proper Service Providers (SD Managers) and requests their Service Descriptions (SDs).
3. An SD Manager answers with information on service content.
4. The Recommendation Engine requests authorization for content access to the UD Manager.
5. UD manager answers with information on user authorization to the Recommendation Engine.
6. The Recommendation Engine decrypts the content and transfers the new adapted content to the application.
7. The Application shows the video to the user, where the authorized parts are visible.

3 Open issues

The explanation of steps in 2.3 have many open issues, since there is no clear mapping to the sequence of steps in 2.2 and the use case proposed in 4.4.4 of [1].

Some of these open issues to discuss include:

- Who is responsible to produce the rules? It should be the content owner. Is this related to the SD Manager? Is out of scope?
- Where are the rules stored? SD? UD?
- Should we need Context information (CD) to provide authorization based on the rules?
- Where is the authorization validated? UD Manager? SD Manager? External?
- Who has the content key needed for decryption? SD Manager?
- Who is doing the decryption? The Recommendation Engine? The SD Manager? The Application?

4 References

[1] ISO/IEC JTC1/SC29/WG11/ N17406, “WD of ISO/IEC 21000-22 2nd edition”, Gwangju, January 2018.

[2] eXtensible Access Control Markup Language (XACML) v3.0, http://www.oasis-open.org/specs/index.php#xacmlv3.0, 2013.

[3] Ishikawa, T. (Editor), ISO/IEC JTC1 SC29/WG1 N75007. ”JPEG Privacy and Security Call for Proposals”, March 2017.

[4] ISO/IEC JTC 1/SC 29 /WG 1 M77026, “DMAG-UPC’s answer to JPEG Privacy and Security Call for Proposals”, October 2017.