ISO /IEC JTC 1/SC 29 /WG 1 N83011
Date: 2019-03-07

ISO/IEC JTC1/SC29/WG1
(ITU-T SG16)

Coding of Still Pictures

JBIG
Joint Bi-level Image Experts Group

JPEG
Joint Photographic Experts Group

TITLE: Contribution to ISO/IEC DIS 19566-4:
Privacy Rules for JPEG Privacy and Security

SOURCE: Jaime Delgado, Silvia Llorente, Daniel Naro (DMAG-UPC)
Distributed Multimedia Applications Group (DMAG)
Universitat Politècnica de Catalunya – UPC BarcelonaTECH
Jordi Girona, 1-3. Mòdul D6 Campus Nord
08034 Barcelona, Spain
jaime.delgado@ac.upc.edu

PROJECT: ISO/IEC 19566-4 (JPEG Systems – Privacy, security and IPR features)

STATUS: Proposal

REQUESTED ACTION: Input contribution

DISTRIBUTION: WG1

Table of contents

1. Introduction

Document ISO/IEC JTC1 SC29/WG1 N81043 is ISO/IEC CD 19566-4 (JPEG Systems Part 4: Privacy, Security and IPR Features) that was under ballot before the 82nd JPEG meeting in Lisbon. Document ISO/IEC JTC1 SC29/WG1 N82084 is the Draft DCOR for the CD produced during that meeting.

This contribution is based on the ESNB comments to the mentioned ballot. In particular, it relates to comments ES027, ES028 and ES029. It proposes some small modifications for the DIS document to be produced during the 83rd JPEG meeting in Geneva.

The proposal includes extending the possible values of the METHOD parameter (in subclause A.2.3) in order to be able to identify an external box of XML type containing the access rules. In addition, an example of access rules in XACML is proposed for a new informative Annex B.

2. Proposed modifications to A.2.3

A.2.3 Protection Description box

The Protection Description box signals additional information about the protected content.

The type of a Protection Description box shall be 'pspd' (0x7073 7064). The contents of the Protection Description box is illustrated in Figure A.3.

Figure A.3 — Structure of the Protection Description box

The values of the METHOD parameter and corresponding meanings are given in Table A.1:

Table A.1 — METHOD Byte and field specifications

Binary value	Meaning	Details
0000 0000	External	Information about the used encryption method is provided in a referenced JUMBF box. The METHOD field shall be followed by exactly one LABEL field that contains the label of the JUMBF box as null terminated ISO/IEC 10646 characters in the UTF-8 encoding.
0000 0001	AES 256 CBC	The content of the Binary Filter Box is encrypted using AES 256 using the CBC cipher mode (ISO/IEC 18033-3). The Protection Description box shall not contain any other fields.
0000 0010	AES 256 CBC with IV	The content of the Binary Filter Box is encrypted using AES 256 using the CBC cipher mode (ISO/IEC 18033-3). The Initialization Vector (IV) is signalled after the METHOD field in the 256-bit length IV field.
0000 0011	External encryption and access rules	Information about the used encryption method and access rules is provided in two referenced JUMBF boxes. The METHOD field shall be followed by exactly two LABEL fields. The first one (for referencing the encryption method) shall contain the label of the JUMBF box as null terminated ISO/IEC 10646 characters in the UTF-8 encoding. The second one (for referencing the access rules) shall contain the label of a JUMBF box as null terminated ISO/IEC 10646 characters in the UTF-8 encoding.
0000 0100	AES 256 CBC encryption and external access rules	The content of the Binary Filter Box is encrypted using AES 256 using the CBC cipher mode (ISO/IEC 18033-3). Information about the access rules is provided in a referenced JUMBF box. The METHOD field shall be followed by exactly one LABEL field that contains the label of a JUMBF box as null terminated ISO/IEC 10646 characters in the UTF-8 encoding.
0000 0101	AES 256 CBC with IV encryption and	The content of the Binary Filter Box is encrypted using AES 256 using the CBC cipher mode (ISO/IEC 18033-3). The Initialization Vector (IV) is signalled after the METHOD field in the 256-bit length IV field. Information about the access rules is provided in

	external access rules	a referenced JUMBF box. The IV field shall be followed by exactly one LABEL field that contains the label of a JUMBF box as null terminated ISO/IEC 10646 characters in the UTF-8 encoding.
All other values are reserved for future use.		

3. New subclause in a new Annex B

B.1 Example of Inclusion of Access Rules in a JUMBF Box (informative)

As indicated in A.2.3, the access rules associated to an image, if any, are stored in a referenced JUMBF Box.

Access rules may be expressed using eXtensible Access Control Markup Language (XACML) [OASIS, eXtensible Access Control Markup Language (XACML) Version 3.0, 2013, Available: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cs-01-en.pdf], so the JUMBF Box must be of XML Content type.

Figure B.1 shows a JUMBF box with a complete XACML policy containing several access rules. The first rule inside the policy defines the conditions to indicate that any user can **view** the image **urn:mimage:Desert.jpg** before the end of the year (**31/12/2019**). The second one denies any other operation over the image.

Access Rules JUMBF box

JUMBF Description box
TYPE: xml

```
<Policy xmlns="urn:oasis:names:tc:XACML:3.0:core:schema:wd-17"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     PolicyId="urn:isdcm:policyid:1"
     RuleCombiningAlgId="urn:oasis:names:tc:XACML:1.0:rule-combining-algorithm:first-applicable"
     Version="1.0"
     xsi:schemaLocation="urn:oasis:names:tc:XACML:3.0:core:schema:wd-17
     http://docs.oasis-open.org/XACML/3.0/XACML-core-v3-schema-wd-17.xsd">

     <Description>Desert.jpg</Description>

     <Rule Effect="Permit" RuleId="urn:oasis:names:tc:XACML:2.0:ejemplo:Desert">
       <Description>
         Any user can view urn:mimage:Desert.jpg before the end of the year
       </Description>
       <Target>
          <AnyOf>
              <AllOf>
                  <!-- Which resource -->
                  <Match
                    MatchId="urn:oasis:names:tc:XACML:1.0:function:regexp-string-match">
                    <AttributeValue
                      DataType="http://www.w3.org/2001/XMLSchema#string">
                        urn:mimage:Desert.jpg
                    </AttributeValue>
                    <AttributeDesignator
                      AttributeId="urn:oasis:names:tc:XACML:1.0:resource:resource-id"
                      Category="urn:oasis:names:tc:XACML:3.0:attribute-category:resource"
                      DataType="http://www.w3.org/2001/XMLSchema#string"
                      MustBePresent="false"/>
                  </Match>

                  <!-- Which action -->
                  <Match MatchId="urn:oasis:names:tc:XACML:1.0:function:string-equal">
                    <AttributeValue
                      DataType="http://www.w3.org/2001/XMLSchema#string">
                         View
                    </AttributeValue>
                    <AttributeDesignator
                      AttributeId="urn:oasis:names:tc:XACML:1.0:action:action-id"
                      Category="urn:oasis:names:tc:XACML:3.0:attribute-category:action"
                      DataType="http://www.w3.org/2001/XMLSchema#string"
                      MustBePresent="false"/>
                  </Match>
              </AllOf>
          </AnyOf>
       </Target>
       <Condition>
          <Apply FunctionId="urn:oasis:names:tc:XACML:1.0:function:date-less-than-or-equal">
              <Apply FunctionId="urn:oasis:names:tc:XACML:1.0:function:date-one-and-only">
                  <AttributeDesignator AttributeId="accessDate"
                    Category="urn:oasis:names:tc:XACML:3.0:date"
                    DataType="http://www.w3.org/2001/XMLSchema#date" MustBePresent="false"/>
              </Apply>
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#date">
                  2020-01-01
              </AttributeValue>
          </Apply>
       </Condition>
     </Rule>
     <Rule RuleId="urn:oasis:names:tc:XACML:2.0:FinalRule" Effect="Deny"/>
</Policy>
```

Figure B.1 — Example of JUMBF Box containing an XACML policy with several access rules

4. Acknowledgements

The work presented in this contribution has been partially supported by the Spanish Government under the project GenCom (TEC2015-67774-C2-1-R) and by the Generalitat de Catalunya (2017 SGR 1749).