

# Privacy rules over JPEG images

**Jaime Delgado**

**DMAG**

**UPC BarcelonaTECH**

*<http://dmag.ac.upc.edu>*

*[jaime.delgado@ac.upc.edu](mailto:jaime.delgado@ac.upc.edu)*

**October 2015**

# Introduction

- ***The objective***: To control access to images (partial, complete, metadata).
- ***The “tools”***: Privacy policies.
- ***The “mechanism”***: Evaluation & enforcement of policies.

# Introduction

- ***The objective***: To control access to images (partial, complete, metadata).
- ***The “tools”***: Privacy policies.
- ***The “mechanism”***: Evaluation & enforcement of policies.
- ***The issues (for standardization)***:  
How to express privacy rules.  
Authorization for access using privacy rules.



■ JPEG ■

# Main open issues to discuss

- **Privacy rules:**  
How to express them, level of detail,  
relationship to the images,  
*what to standardize, ...*
- **Authorization for access:**  
Mechanism, formalization,  
*what to standardize, ...*

# Scope

- Access control to specific images is defined with rules (privacy policies).
- Policies are defined either by the service provider or by the image owner.
- Policies/rules follow a standard for its representation and enforcement.

# Privacy rules/policies

- Rules / Policies could be based on conditions over information on:
  - **User**: individual, group, location, role, ...
  - **Context**: date and time, number of accesses, action (view, download, ...), ...
  - **Image**: quality, geo-location, author, date, semantic information, ...
  - **Action**: read, update, delete, ...

# Privacy rules/policies

- Rules / Policies could be based on conditions over information on:
  - **User:** WHO, group, location, role, ...
  - **Context:** HOW/WHEN/WHERE  
action (view, download, ...), ...
  - **Image:** ON WHAT  
quality, location, author, date, semantic information, ...
  - **Action:** WHAT  
update, delete, ...

# Privacy rules/policies example

- A specific example could be:  
“only my workmates can see the Christmas Dinner photo album and only during this month”
- In this case, the conditions are:
  - User: *my workmates*
  - Context: *this month*
  - Image: *Christmas Dinner photo album*
  - Action: *read* (“see”).



# Additional features

- Different parts of the image might have different privacy policies.
- Access to specific metadata elements might be limited.
- Provision of different levels of image quality based on roles or other conditions or context.
- Time restricted (image can become unusable after certain period of time).
- Images are physically kept in a specific repository or they are just referenced.

# Main open issues to discuss (*back*)

- **Privacy rules:**

How to express them, level of detail,  
relationship to the images,  
*what to standardize, ...*

# Main open issues to discuss (*back*)

- **Privacy rules:**

How to express them, level of detail, relationship to the images, *what to standardize, ...*

# Main open issues to discuss (*back*)

- **Privacy rules:**

How to express them, level of detail, relationship to the images, *what to standardize, ...*

**XACML**



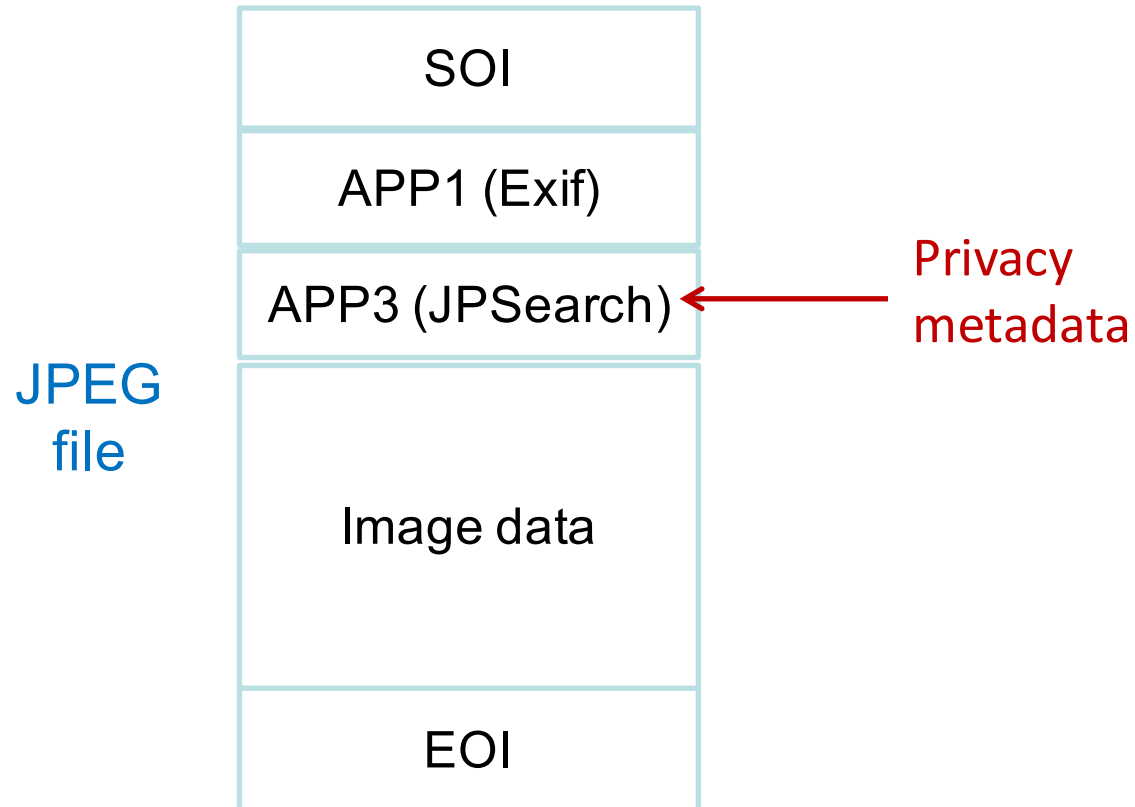
**XACML**  
(eXtensible Access Control  
Markup Language)

# What to standardize

- Where to keep (XML) privacy policies.
- RightsDescription element (JPSearch Part 2).

```
<RightsDescription>  
<RightsDescriptionInformation>  
  Location of the rights description standard.  
</RightsDescriptionInformation>  
<Description>  
  Textual description.  
</Description>  
<ActualRightsDescriptionReference>  
  Actual rights description.  
  It can be embedded or referenced.  
</ActualRightsDescriptionReference>  
</RightsDescription>
```

# What to standardize



# Main open issues to discuss (*back*)

- **Privacy rules:**  
How to express them, level of detail,  
relationship to the images,  
*what to standardize, ...*
- **Authorization for access:**  
Mechanism, formalization,  
*what to standardize, ...*

# Main open issues to discuss (*back*)

- **Privacy rules:**

How to express them, level of detail, relationship to the images, *what to standardize, ...*

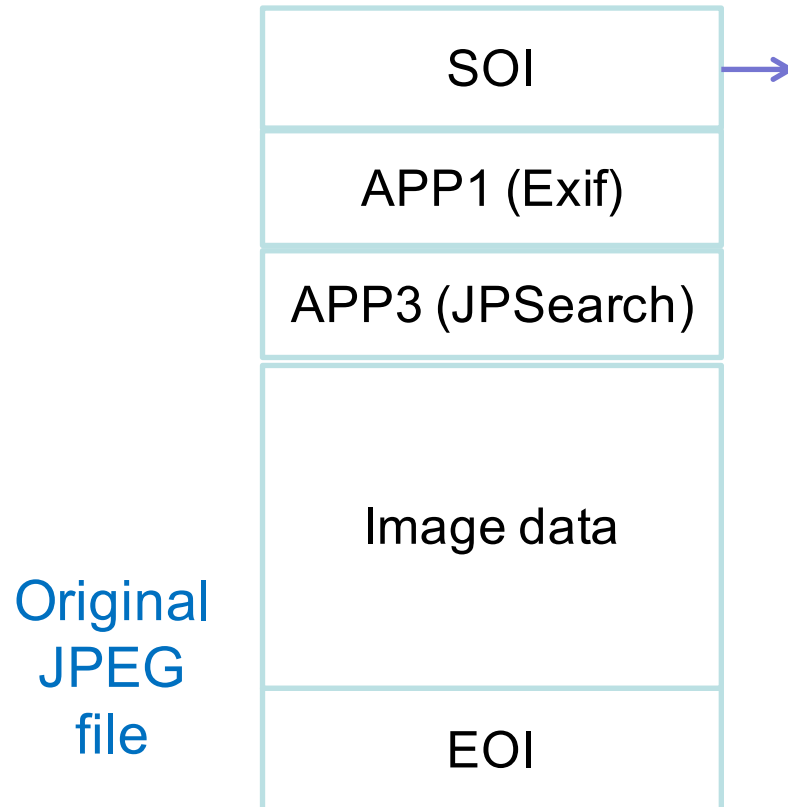
- **Authorization for access:**

Mechanism, formalization, *what to standardize, ...*

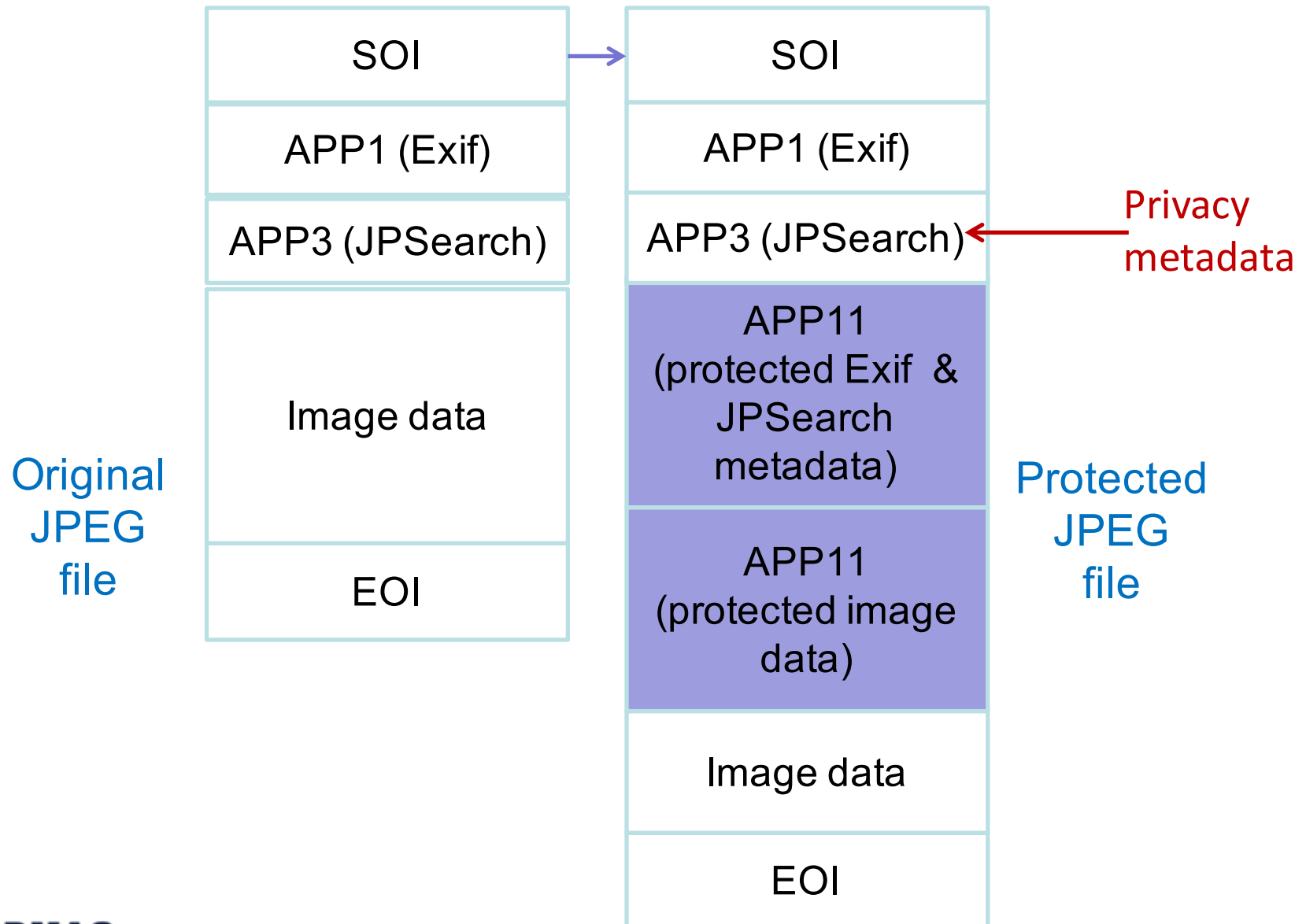
- Rules validity.
- Who does the enforcement?
- Keep information on the encryption / decryption tools used.



# What to standardize



# What to standardize



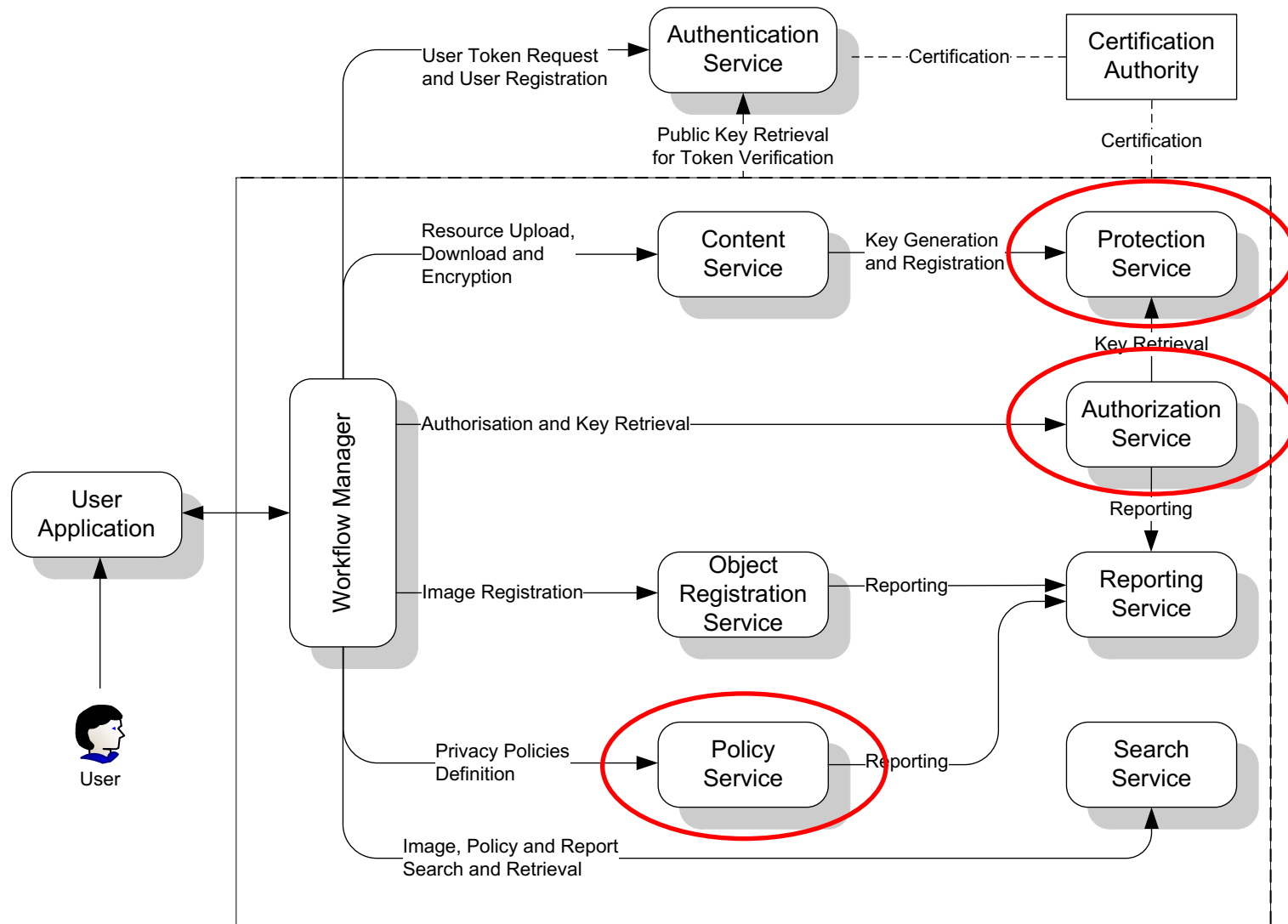
# Requirements for solutions

- Express privacy policies at enough level of detail.
- Include the policies (or a link to them) in the image file.
- Provide for the evaluation of privacy policies to authorize or not the access to partial or complete metadata and image data.

# Possible technologies

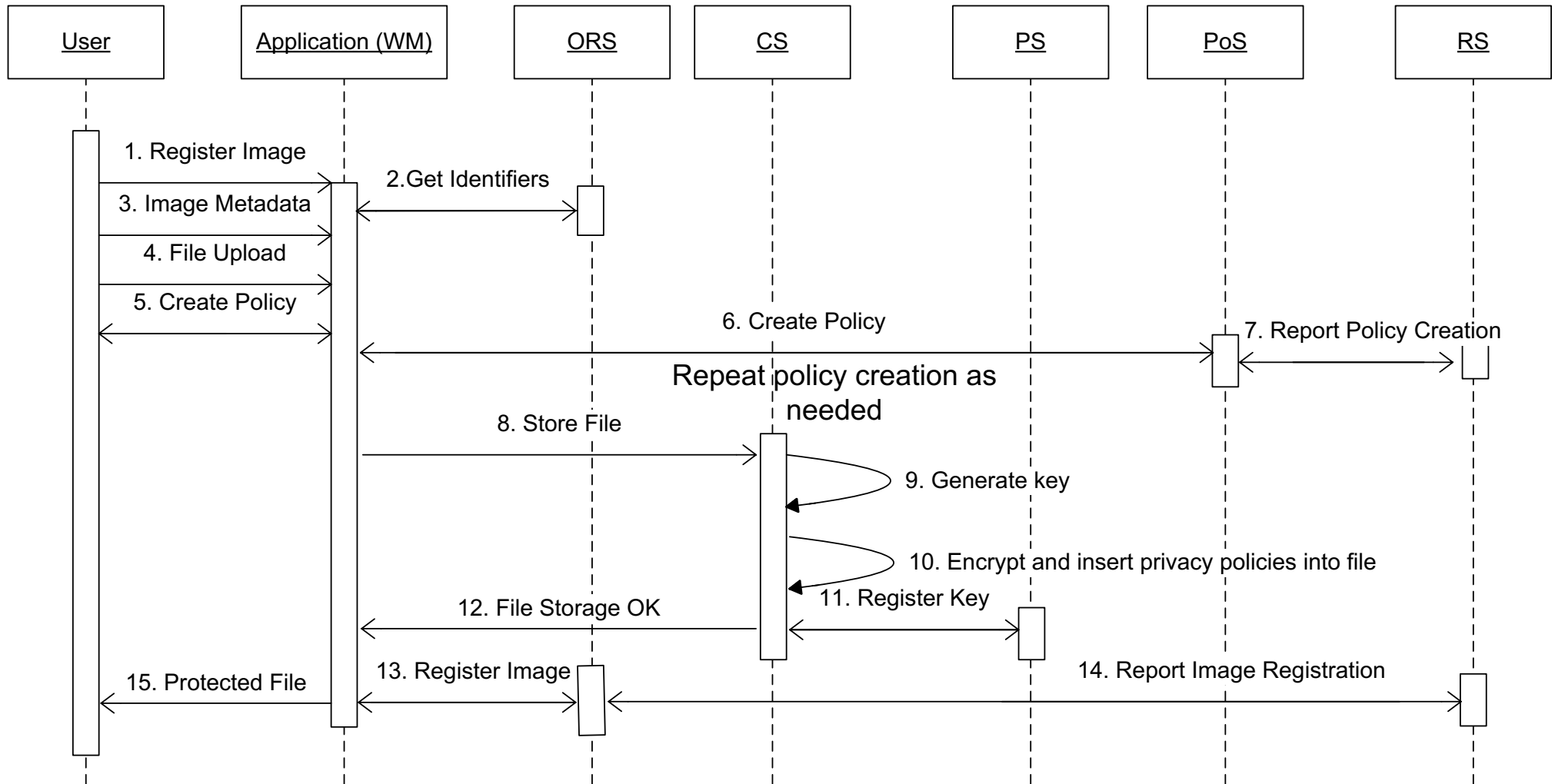
- **Privacy provision using external services:**
  - Privacy policies included in the image, but only a reference to an external system.
  - *External system handles everything:*
    - Creation of the privacy policies
    - Protection of the images (keys management)
    - Access to the privacy policies
    - Authorization of access to the images
    - etc.

# MIPAMS architecture for a solution

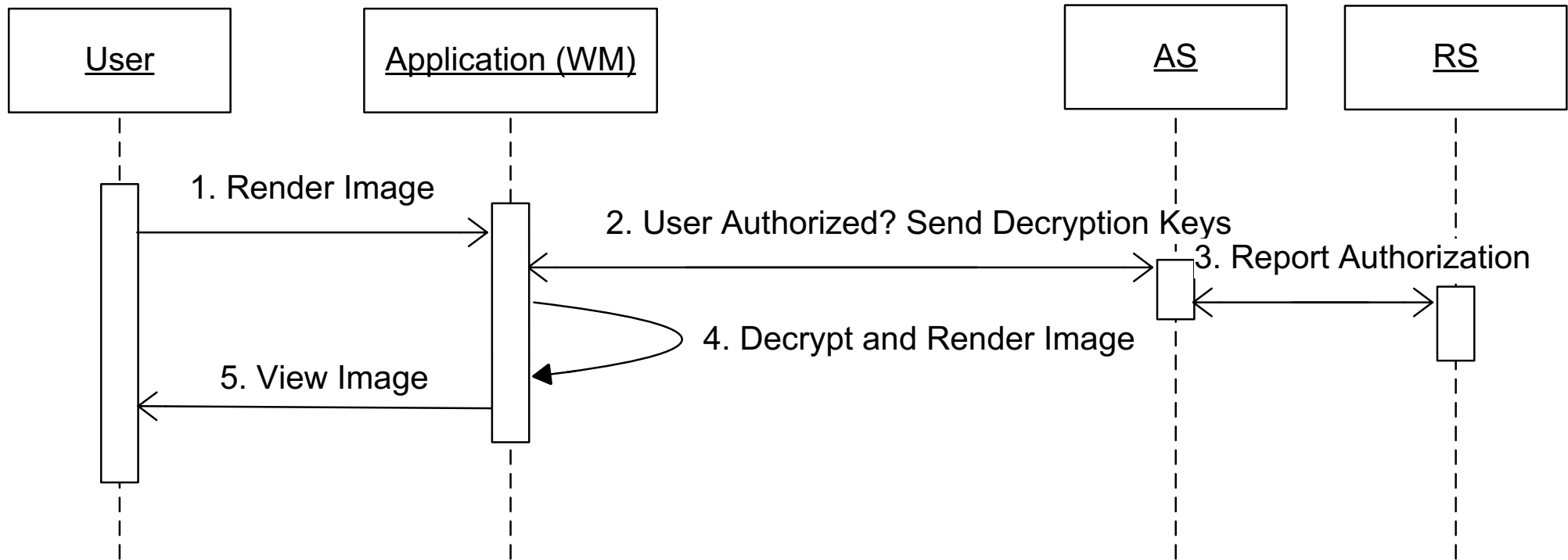


<http://dmag.ac.upc.edu/mipams/>

# Protection of an image with MIPAMS



# Authorization of access to a protected image



# Conclusions

- Definition of privacy rules to control access to JPEG images.
- XACML, a valid, already existing standard.
- JPSearch metadata as placeholder for policies.
- The highest possible level of granularity for rules.
- One example of technology: “External” services.
- **FUTURE: JPEG Privacy & Security standards.**



# Privacy rules over JPEG images

**Jaime Delgado**

**DMAG**

**UPC BarcelonaTECH**

*<http://dmag.ac.upc.edu>*

*[jaime.delgado@ac.upc.edu](mailto:jaime.delgado@ac.upc.edu)*

**October 2015**