Trust in event reporting mechanisms for DRM

Eva Rodríguez, **Jaime Delgado**

Distributed Multimedia Applications Group (DMAG)

Universitat Politècnica de Catalunya
Dept. Arquitectura de Computadors
Barcelona (Spain)

jaime.delgado@ac.upc.edu
http://dmag.upf.edu

Contents

§ Notification of Events

§ MPEG-21 Standard

§ MPEG-21 Event Reporting

§ MPEG-21 IPMP

§ Issues to improve

§ Trusted and non-trusted systems

§ Contribution to MPEG-21 standard

§ Securing Event Reporting
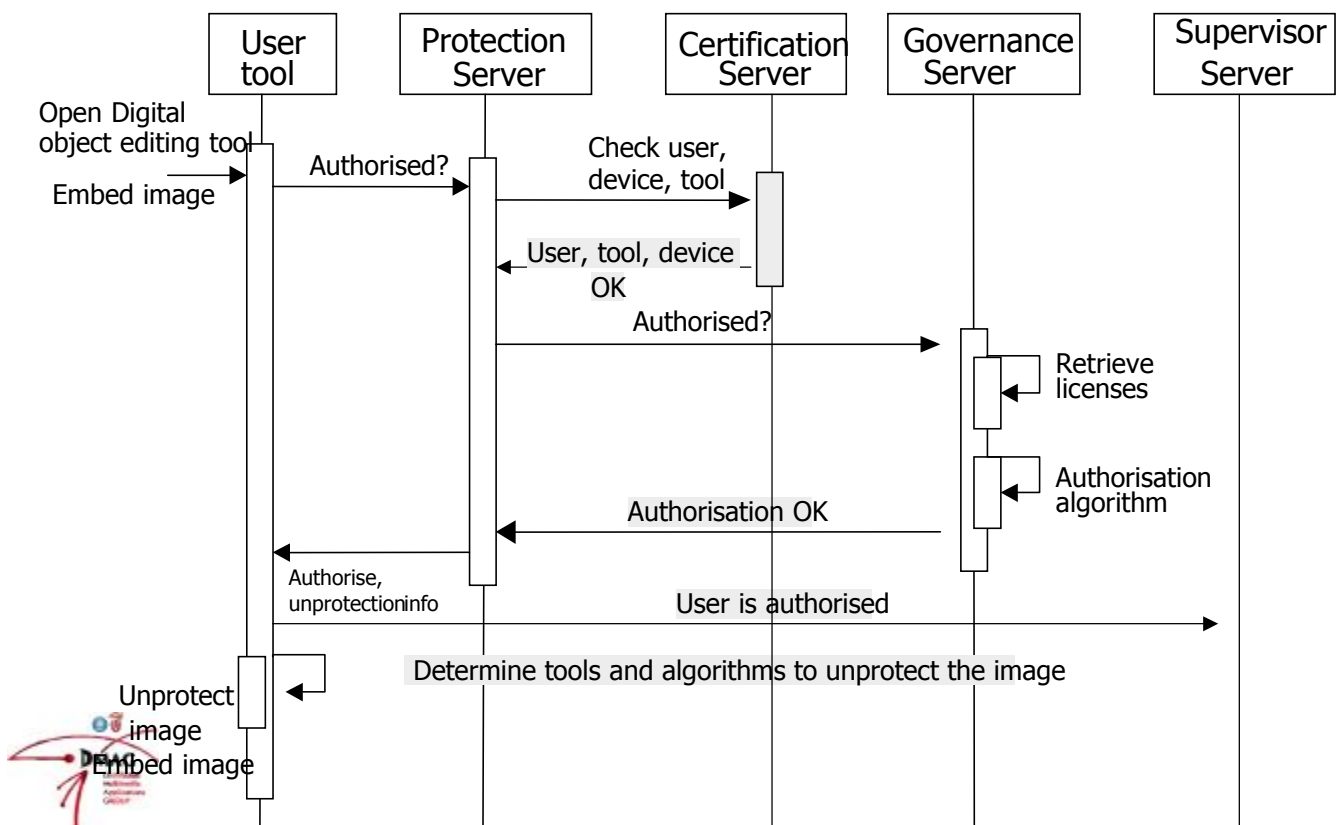
§ Conclusions and Future Work

Notification of events

DIGITAL VALUE CHAIN

§ Content creators, distributors, etc. can be informed of the usage of the multimedia objects they have provided

§ Users illegally distributing or consuming content could be prosecuted based on these activity records

§ Kind of notifications:

§ Object Action Notification

§ System Action Notification.

Notification of events – Use Case

User tool	Protection Server	Certification Server	Governance Server	Supervisor Server

Open Digital object editing tool

Embed image

Authorised?

Check user, device, tool

User, tool, device OK

Authorised?

Retrieve licenses

Authorisation algorithm

Authorisation OK

Authorise, unprotectioninfo

User is authorised

Determine tools and algorithms to unprotect the image

Unprotect image

Embed image

MPEG-21 structure

- § Part 1: Vision, Technologies and Strategy
- § Part 2: Digital Item Declaration
- § Part 3: Digital Item Identification
- § Part 4: Intellectual Property Management and Protection
- § Part 5: Rights Expression Language
- § Part 6: Rights Data Dictionary
- § Part 7: Digital Item Adaptation
- § Part 8: Reference Software
- § Part 9: File Format
- § Part 10: Digital Item Processing
- § Part 11: Evaluation Methods for Persistent Association Technologies
- § Part 12: Test Bed for MPEG-21 Resource Delivery
- § Part 13: Scalable Video Coding
- § Part 14: Conformance
- § Part 15: Event Reporting
- § Part 16: DID binarisation
- § Part 17: Fragment Identification for MPEG Media Types
- § Part 18: Digital Item Streaming
- § MPEG-21 Schema Files

MPEG-21 Standard

- § Open framework for multimedia delivery and consumption for use by all the players in the delivery chain
- § Divided into several parts dealing with different aspects of multimedia information management
  - § Part 2: Digital Item Declaration
  - § Part 4: Intellectual Property Management and Protection Components
  - § Part 15: Event Reporting

MPEG-21 Event Reporting

§ Provides standardised means for sharing information about Events amongst Peers and Users
- § Such Events are related to Digital Items and/or Peers that interact with them

§ Key concepts:
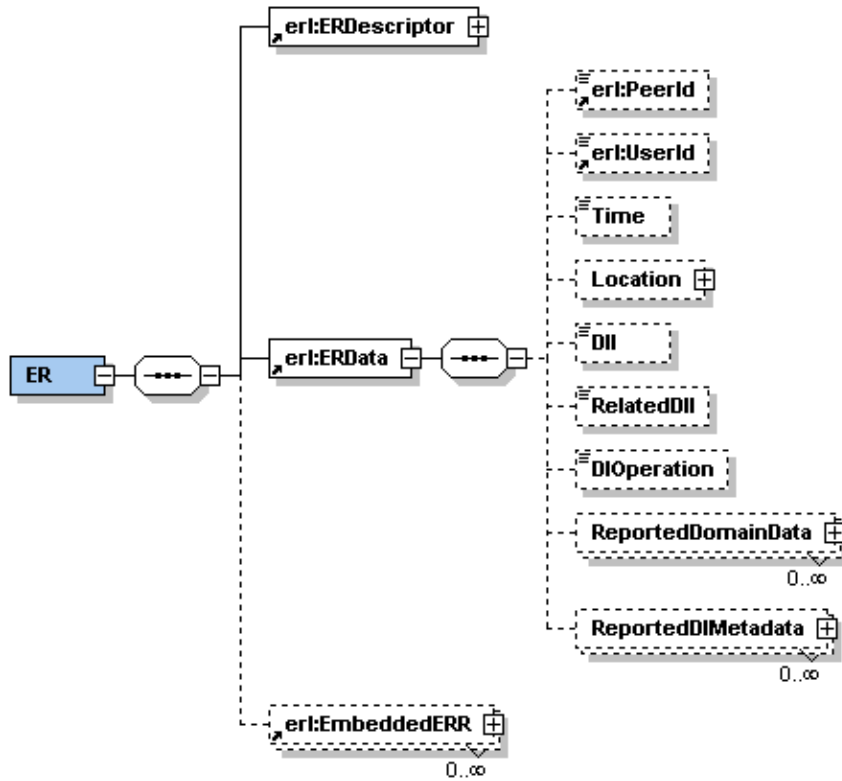- § ER: Event Report
- § ER-R: Event Report Request

MPEG-21 Event Reporting: Events

§ An Event occurs when a set of specified conditions are met

§ MPEG-21 specifies elements to define Conditions under which an Event is deemed to have occurred.
- § Time-based: specifies a time period in which the Event must occur
- § DI-related operations
- § Peer-related operations
- § Combinations thereof

MPEG-21 Event Report

MPEG-21 Event Report Request
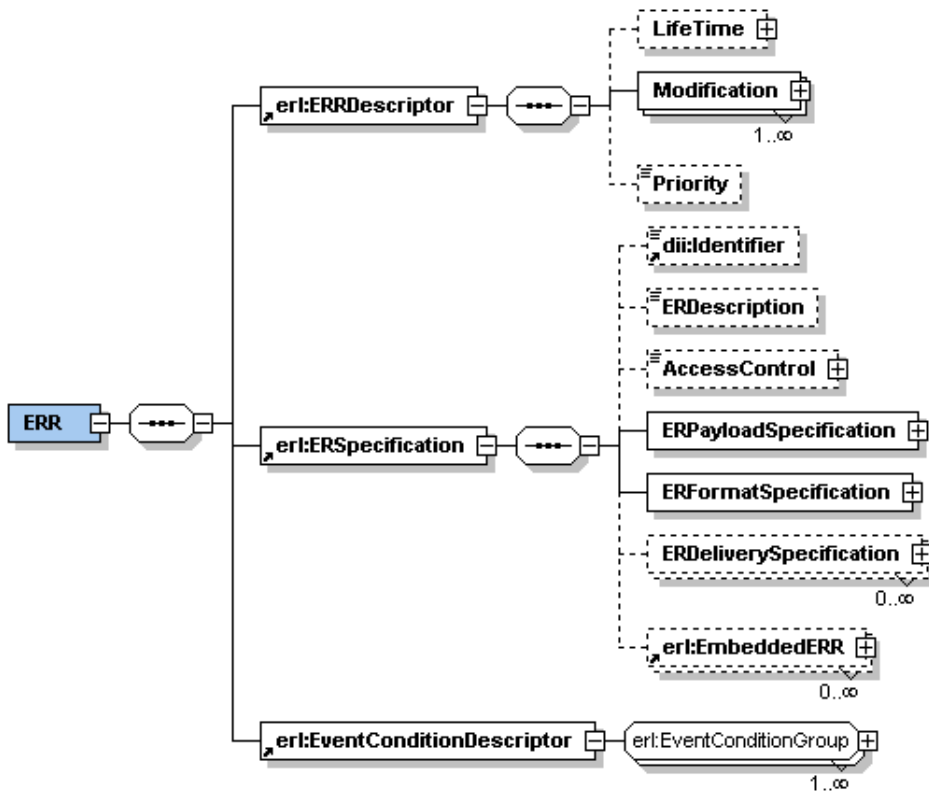
MPEG-21 IPMP Components

§ General solution for the management and protection of Intellectual Property

§ DIs protected to ensure that access to content is done according to license terms

§ Use of digital signatures and encryption techniques

§ These kinds of objects à IPMP DIDL documents

§ Protected object (or part of the DIDL document)

§ IPMP information expressions (protection + governance)

IPMP Info

§ DI protection info categories:

§ Information that pertains to the whole DI

§ Collections of general Licenses

§ List of tools

§ Information about the specific protection applied to a certain part of Digital Item hierarchy protected with IPMP DIDL:

§ specific tool applied, keys, licenses specific to that content …

Issues to improve

§ *Trust in Event Reporting*

§ Notification of Events in Trusted Systems
§ Securing Event Reports

Use Cases with respect to trust

System	ER-R	Application controls reportable events
Trusted	With	Yes
Trusted	*With*	*No*
Trusted	*Without*	*Yes*
Trusted	Without	No
Non-Trusted	With	Yes
Non-Trusted	*With*	*No*
Non-Trusted	*Without*	*Yes*
Non-Trusted	Without	No

Event Report Format

ER generated because of ER-R (Initial MPEG-21)		Extra fields needed if no ER-R used (Current MPEG-21)	
ER Identifier	Owner name	Time (Delivery)	Related DII
DII	License identifier	Access Control	Format of the report
DIOperation	Operation details	Recipient (Delivery)	DITransportation Service (Delivery)
UserId / PeerId	Object version		
Location	Status		
Time	Creation		
Tool Certifier Id	Work identifier		
Object distributor	Related DII		
Object creator	DIMetadata		
Original ER-R	*Embedded ER-R*		

Implementation – Non trusted system
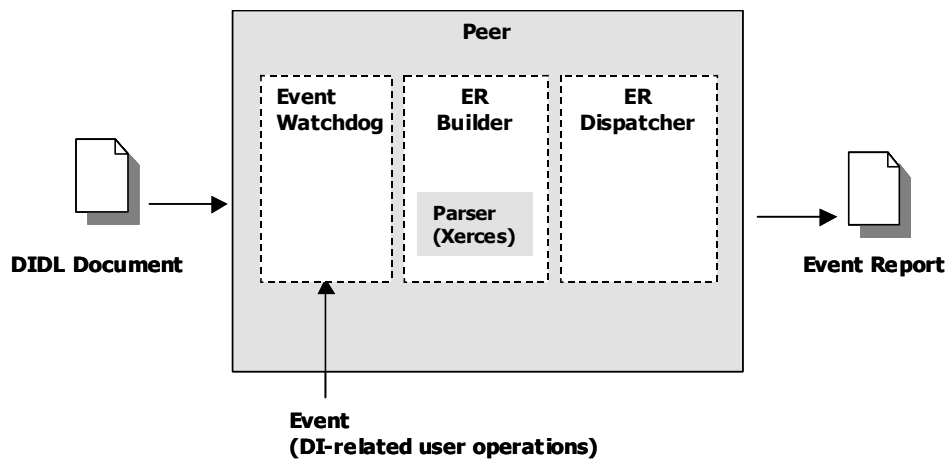
§ Tools not necessarily registered and certified

§ Users not necessary registered

  § Decision to issue an ER based on Event and ER-R
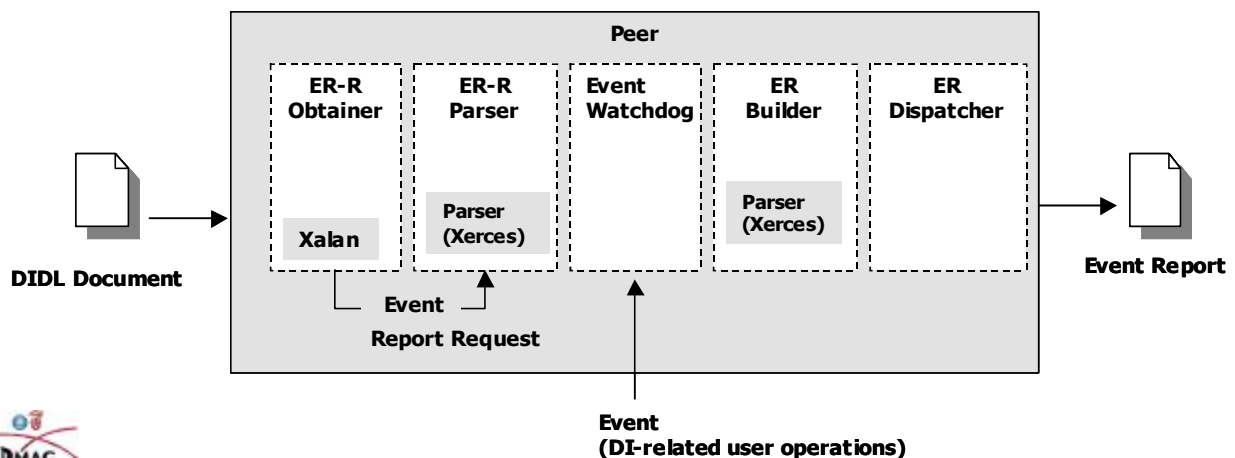
Implementation – trusted system

§ Application tools registered and certified
§ Users registered in the system
  § Application tools analyse conditions to decide when to issue ERs

Contribution to MPEG-21 Standard

§ Core Experiment:
  § Core Experiment proposal for MPEG-21 Event Reporting
  § Core Experiment on use of Event Report Requests:
    § Specification of Use Cases
    § Software Implementation
§ Use cases presented were analysed:
  § To evaluate the need of including ER-Rs in digital objects when reporting consumption and distribution of governed digital assets
§ The results of the CE were evaluated
§ **Recommendations** resultant from the CE were **accepted**

Contribution to MPEG-21 Event Reporting

§ Changes to the MPEG-21 Event Reporting standard:

    § Field Original ER-R (Source) *not mandatory*

    § New field added in the ER to contain information regarding to the events

        § Structured to place the information we noticed that should be necessary in an ER:

            § Access Control, Report Format, Recipient, Delivery Time and DI Transport Service.

    § Conditions expressed in the fields Time-based events, DI-related events and Peer-related events *not mandatory*

        § In trusted systems they are controlled by the application which creates the ER

Securing event reporting

MPEG-21 Event Reporting does not provide:

1. The way to ensure integrity and authenticity to *reported or requested data*

2. It is not possible to protect, i.e. encrypt, partially or totally ERs and ER-Rs

Data integrity and authenticity

- § To ensure authenticity and integrity to requested and reported data:
  - § use of digital signatures to sign ERs and ER-Rs or some elements within them

- § For each one of the elements (ER, ER-Rs …) add the *dsig:Signature* element as child element
  - § Signature elements will contain the digital signature for its parent element

Data integrity and authenticity

- § Sign the reported data (metadata that describe the DI related operation performed by the user)
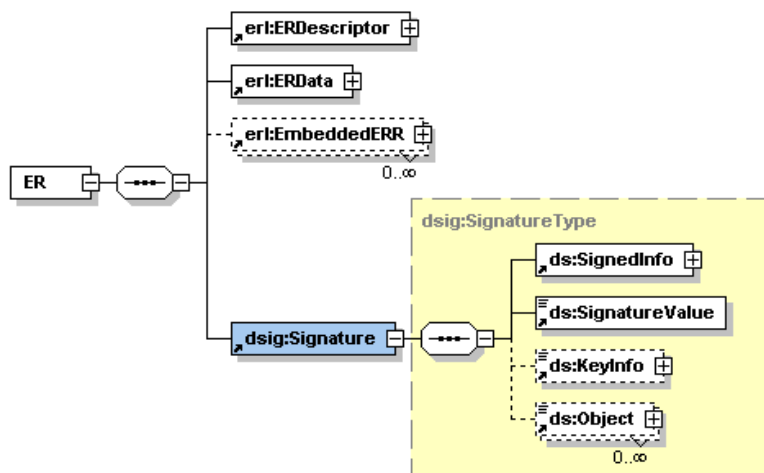
Data encryption

§ Encryption of ERs and ER-Rs or elements within them can be done at least in two different ways:

§ Define the equivalent encrypted elements for ER and ER-R according to W3C XML Encryption recommendation

§ Define the equivalent IPMP ER elements as done for IPMP DIDL elements

Data encryption

§ Definition of the equivalent encrypted elements for ER and ER-R elements and elements within them
§ Using W3C XML Encryption recommendation
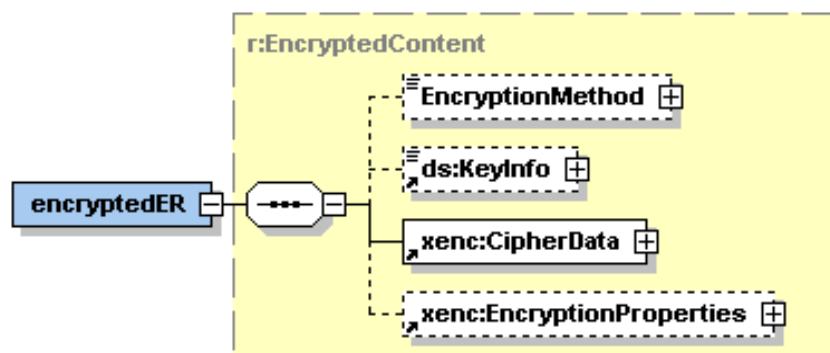
ER Protection in MPEG-21(I)

§ Definition of the IPMP ER schema:

§ to provide protection to the whole ER and ER-Rs or to elements within them.

§ Using this solution we can protect ER elements in different ways and

§ It also allows to govern ER and ER-Rs or elements within them

§ Combining two different parts of the MPEG-21 standard: ER and IPMP
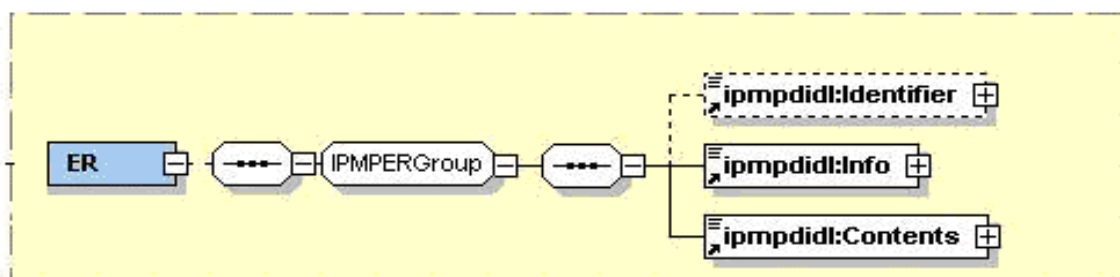
ER Protection in MPEG-21 (II)

§ Define the equivalent IPMP ER elements

§ IPMPERGroup:

§ Identifier

§ Info: about the mechanisms and licenses involved in the protection of the reported data

§ Contents: contains the protected ER data

Contents

§ Notification of Events

§ MPEG-21 Standard

   § MPEG-21 Event Reporting

   § MPEG-21 IPMP

§ Issues to improve

§ Trusted and non-trusted systems

   § Contribution to MPEG-21 standard

§ Securing Event Reporting

§ **Conclusions and Future Work**

Conclusions and Future Work

§ Different ways to manage and protect notifications of events in DRM systems.

§ Definition of mechanisms to report events in trusted systems.

   § Reported to MPEG-21 standard

   § Now part of the **MPEG-21 Event Reporting standard** specification

§ Event Reporting protection in MPEG-21 to be considered

§ Implementation in the AXMEDIS European Project.