

Profiling and Binary Encoding of the MPEG REL for Embedded DRM Systems

Xin Wang
Chief Scientist, ContentGuard, Inc.

CSD-741

**Design Issues in Digital Rights Management
Embedded Systems Conference, San Francisco 2005**

Outline

- Overview of MPEG REL
- Embedded DRM System Constraints and REL Requirements
- An MPEG REL Profile and its Binary Encoding
- Conclusions

MPEG REL

- Is an International Standard, ISO/IEC 21000-5
- Is a language for specifying rights and their terms and conditions.
 - E.g., “Alice says that Bob has the right to play a video file for a week if he pays \$3”.
- Defines syntax and semantics of a machine interpretable language that can be used to specify rights unambiguously
- Provides an authorization model to determine if a principal has the right to perform an action on a resource according to REL expressions
- Supports many business models in the end-to-end distribution value chain
- Has its baseline technology
 - XrML 2.0 from ContentGuard, Inc., selected for its expressiveness and unambiguity over ODRL

Why Develop REL

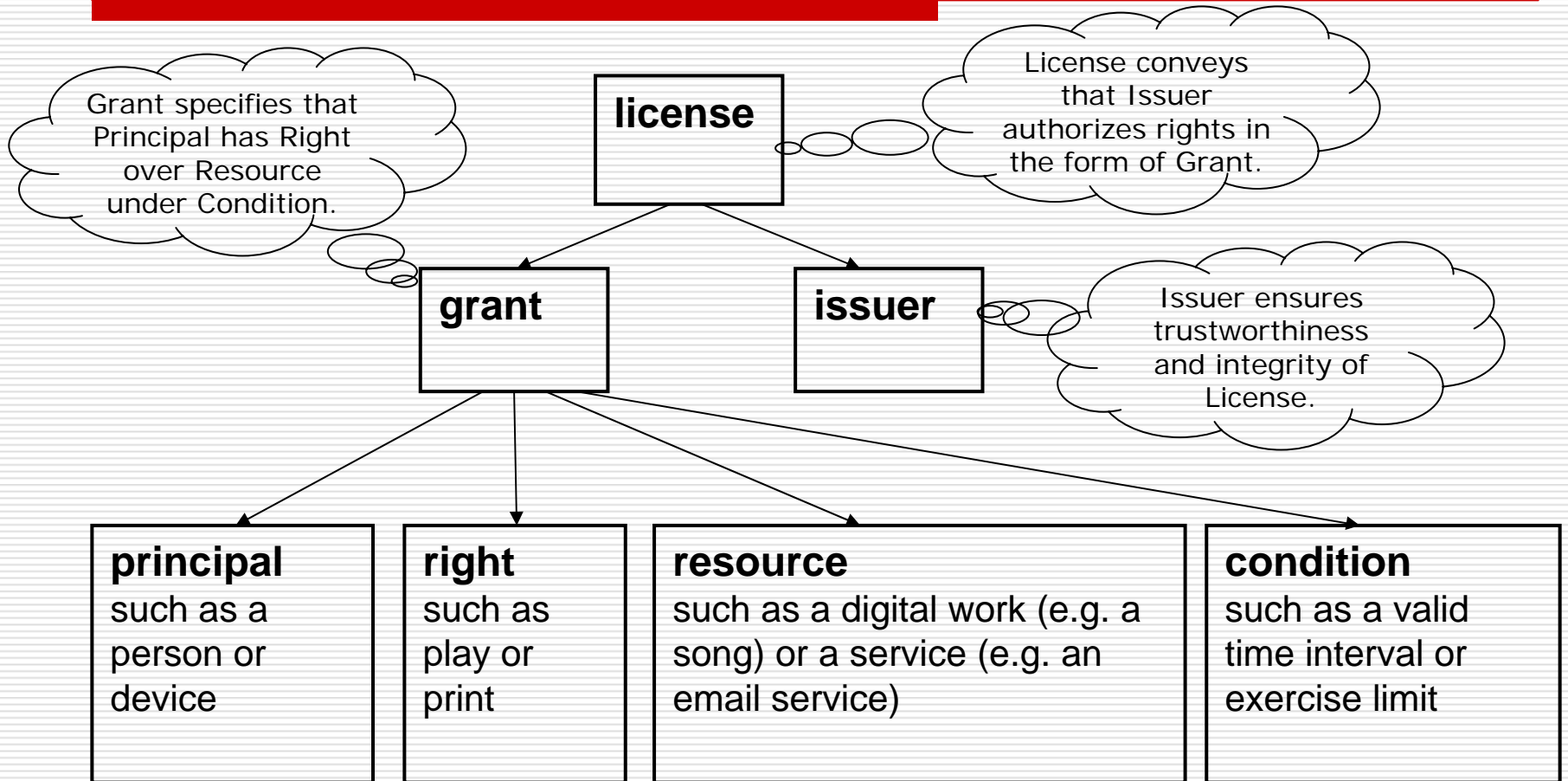
DRM Systems that ...

- ❑ Secure and protect digital contents and services across the end-to-end value chain
- ❑ Persistently honor usage rights, conditions and obligations specified for digital contents and services

A Common Language that ...

- ❑ Provides a uniform mechanism to describe specifications of rights and their conditions and obligations for distributing and using digital contents and services
- ❑ Enables trusted systems to exchange digital contents and interoperate for end-to-end DRM

REL Data Model



A Simple REL License

```
<license xmlns="urn:mpeg:mpeg21:2003:01-REL-R-NS"
  xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
  xmlns:mx="urn:mpeg:mpeg21:2003:01-REL-MX-NS"
  profileCompliance="urn:embedded:rel-profile">
  <grant>
    <keyHolder licensePartID="Alice">
      <info><dsig:KeyValue>
        <dsig:RSAKeyValue><dsig:Modulus>oRUTUiTQk ... </dsig:Modulus>
          <dsig:Exponent>AQABAA==</dsig:Exponent></dsig:RSAKeyValue>
        </dsig:KeyValue></info>
      </keyHolder>
      <mx:play/>
      <mx:diReference>
        <mx:identifier>urn:PDQRecords:song:WhenTheThistleBlooms.mp3</mx:identifier>
      </mx:diReference>
      <validityInterval>
        <notBefore>2003-02-13T15:30:00</notBefore>
        <notAfter>2003-03-13T15:30:00</notAfter>
      </validityInterval>
    </grant>
    <issuer licensePartID="PDQRecords">
      <dsig:Signature><dsig:SignatureValue>zIRYaxl5EX ... </dsig:SignatureValue>
        <dsig:KeyInfo><dsig:KeyValue><dsig:RSAKeyValue><dsig:Modulus>yQ== ...
          </dsig:Modulus><dsig:Exponent>AQAB==</dsig:Exponent></dsig:RSAKeyValue>
          </dsig:KeyValue></dsig:KeyInfo></dsig:Signature>
        </issuer>
    </license>
```



REL Primitive Elements

- Principal
 - keyHolder, allPrincipal
- Right
 - play, print, modify, adapt, install, uninstall, ...
 - issue, obtain, possessProperty, revoke
- Resource
 - diReference, digitalResource, ...
- Condition
 - validityInterval, exerciseLimit, flatFee, perUseFee, ...

Typical REL Licenses

- End-user license
 - rights to *play, print, modify, ...*
- Attribute license
 - right to *possessProperty*
- Distribution license
 - right to *issue* other rights
- Offer license
 - right to *obtain* other rights
- Revocation license
 - right to *revoke* other rights
- Hybrid licenses

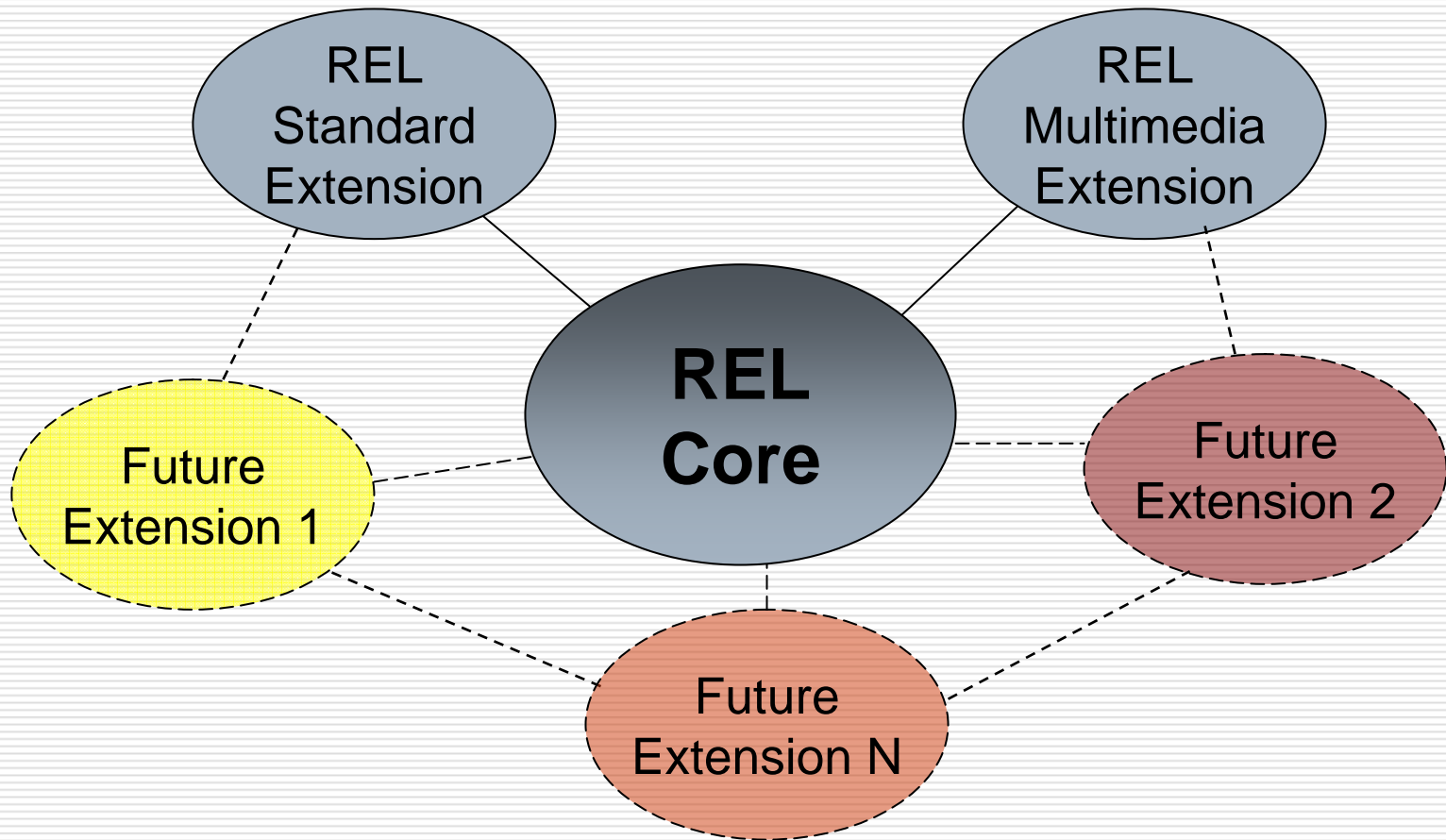
REL Advanced Features

- Variable
 - Flexibility to specify an element instance at the time of exercising right, but not at the time of issuing the license
 - Convenience for a collection of elements with common properties
- Pattern
 - Capability of specifying a set of element instances according to some rules
- Service Reference
 - Encapsulation of information necessary to interact with a service
 - Support interoperability for stateful conditions
- Delegation
 - Allowance and control on how rights can be delegated and transferred

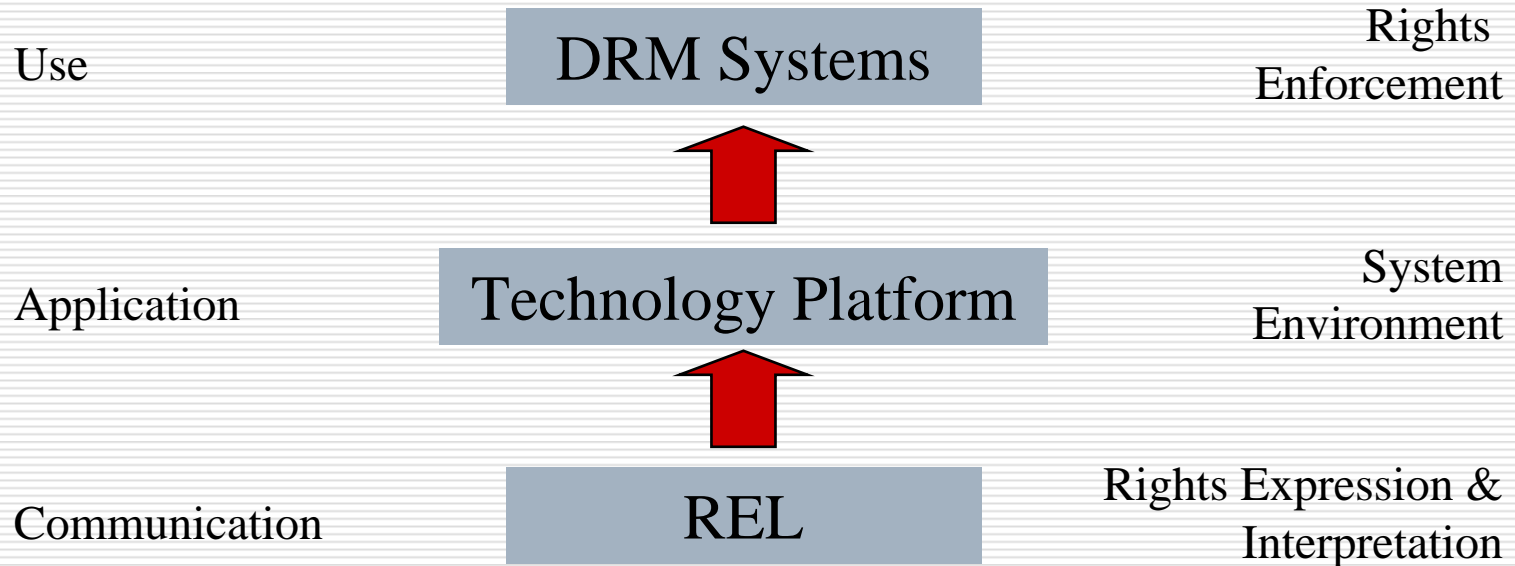
REL Supported Business Models

- Unlimited usage
- Flat fee sale
- Pay per view
- Preview
- Promotion
- Subscription/Membership
- Transfer
- Gifting
- Personal lending
- Library loan
- Site/volume license
- Rent
- Multi-tier models
- Territory restricted
- Component based model
- User types based model
- Payment to multiple rights Holders
- Super-distribution
- Composite content

REL Structure and Extensibility



Use of REL in DRM



Embedded DRM System Constraints

□ Limited Processing Capabilities

- Import, render, and maybe export content
- But no content editing, no license issuance

□ Limited Processing Resources

- Relatively slow CPU, limited memory and low bandwidth
- May not have XML Schema parser

Mobile Requirements on REL

- ❑ R-1: support specification of the issuer of rights, in order to ensure trustworthiness of the rights
- ❑ R-2: support the following rights
 - play, execute, and print
- ❑ R-3: support restrictions over the rights
 - the number of times a resource may be accessed
 - a time interval during which a resource may be accessed
- ❑ R-4: support uniquely identifiable digital resources
- ❑ R-5: support a specific user or device to exercise rights over an identified digital resource.

What's a Profile?

- Concept
 - a subset of baseline specifications
 - with restricted syntax, semantics, and processing rules
- Target
 - a community (e.g., mobile DRM),
 - an application (e.g., streaming DRM),
 - a function (e.g., certificating and attesting assertions)
 - an environment (e.g., North America, or Europe).
- Conformance
 - conforming to the profile is also to the baseline specifications, but not reversely

An MPEG REL Profile (1/3)

Element / Child Element	Occurrence in Profile	Occurrence in REL	Comments
r:license			
r:grant	1..∞	0.. ∞	mandatory in MOEG REL.
r:issuer	1..1	0.. ∞	(R-1) included as required.
sx:profileCompliance	0..1	0..1	Included to allow any “r:license” to claim the profile compliance.
r:grant			
r:keyHolder	0..1	0..1	(R-5) used as the actual and only allowed principal.
mx:play mx:print mx:execute	1..1	1..1	(R-2).
mx:diReference	1..1	0..1	(R-4) Used to identify a resource.
r:validityInterval sx:validityIntervalFloating sx:exerciseLimit r:allConditions	0..1	0..1	(R-3) Two types of interval conditions are included. “r:allConditions” is used for specifying more than one conditions conjunctively.

An MPEG REL Profile (2/3)

Element / Child Element	Occurrence in Profile	Occurrence in REL	Comments
r:keyHolder			
r:info	1..1	1..1	Information about a key.
mx:diReference			
mx:identifier	1..1	0..1	the identifier is now required for identifying a resource.
r:allConditions			
r:condition	0.. ∞	0.. ∞	
r:validityInterval			
r:notBefore	0..1	0..1	Start time of an interval.
r:notAfter	0..1	0..1	End time of an interval.
sx:validityIntervalFloating			
sx:duration	1..1	0..1	Duration of a floating interval.
sx:exerciseLimit			
sx:count	1..1	0..1	Required to specify the limit explicitly.
r:issuer			
r:keyHolder	1..1	0..1	The actual issuer is specified as an "r:keyHolder".

An MPEG REL Profile (3/3)

Element	Additional Restrictions
r:license	A license may have more than one grant. But all the grants in a particular license must apply to the same principal and the same resource.
r:keyHolder	Its child element "info" contains one and only one "dsig:KeyName" element.

XML Binary Encoding

- A process which consists in encoding a description in XML form into an equivalent and more compact binary form.
- Aiming at significant savings in
 - bandwidth
 - memory usage
 - CPU consumption
- No standard yet
 - ASN.1 based
 - BiM
 - gzip (compression)

Binary Encoding of the REL Profile

- ❑ Recursively encoding according to the order and cardinality of the permitted elements in the profile
- ❑ Each element or attribute e is encoded with its
 - Name code (could be optimized using Huffman code)
 - Value code
 - ❑ None, if e has no value
 - ❑ binary encoding of the value of e , if e is a leaf element or attribute
 - ❑ concatenation of binary encoding of its child elements and their attributes, if e has a child element or an attribute

Conclusions

- ❑ MPEG REL is comprehensive, scalable and extensible
- ❑ MPEG REL can be easily profiled, driven and guided by domain specific requirements
- ❑ A recipe (concept, methodology and an example) is given for creating these profiles
- ❑ profiled licenses can be both compact and expressive to support desired business models, such as in mobile DRM applications
- ❑ lightweight licenses can reduce the computational resources required by mobile devices

Thank You



xin.wang@contentguard.com