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

Xin Wang

ContentGuard, Inc., www.contentguard.com

1 Introduction

The Rights Expression Language (REL) [1] is an ISO/IEC standard developed by MPEG (Moving Picture Expert Group) for the purpose of expressing rights and their terms and conditions in order to govern use and distribution of multimedia content and other forms of digital objects and services during their lifecycles. The REL is a machine readable and XML-based declarative language with precise semantics. In the context of media distribution and consumption, content owners and distributors can use it to specify, according to their business models, how content can be used and distributed throughout the value chain from content packagers, via content distributors and retailers, to content consumers. Such an REL has become an essential component of any effective, interoperable and scalable end-to-end digital rights management (DRM) system.

The MPEG REL is designed to be domain-agnostic and comprehensive. However, most embedded systems have limitations on their capabilities and resources. For instance, they may have the capability to consume content but may not have the capability to edit content. Hence, granting the edit right to these systems and requiring them to process this right are extraneous and unnecessary. Additionally, many embedded systems may not have the resources (e.g., XML parser, sufficient memory and bandwidth) to process and transmit XML documents, and understanding licenses written in the MPEG REL imposes difficulty to adopt usage of the language. Hence, it is imperative to consider profiling the MPEG REL to fit the need of these embedded systems, and binary encoding MPEG REL licenses so that the embedded system can interpret the licenses efficiently.

The purpose of this paper is to provide a methodology for profiling and binary encoding MPEG REL for developing efficient and yet interoperable embedded DRM systems. This paper begins with a brief introduction of the MPEG REL, and a discussion of the concepts and general principles of profiles of any XML-based specification and their binary encoding. Then, this paper presents a case study of creating an example profile and binary encoding of the MPEG REL for the mobile domain. The case study covers collecting and analyzing requirements for current mobile DRM systems, presenting the profile to satisfy these requirements, and demonstrating how binary encoding of the profile can be carried out in a systematic way.

2 Brief Overview of MPEG REL

The MPEG REL [2,4] is an XML-based language for specifying rights and conditions to govern the use and distribution of digital content as well as access to services. Using the MPEG REL, anyone owning or distributing digital resources can identify principals (such as users, groups, devices, and systems) allowed to use those resources, the rights available to those principals, and the terms and conditions under which those rights may be exercised. The following diagram illustrates the basic MPEG REL elements used to encapsulate this information and their inter-relationships.

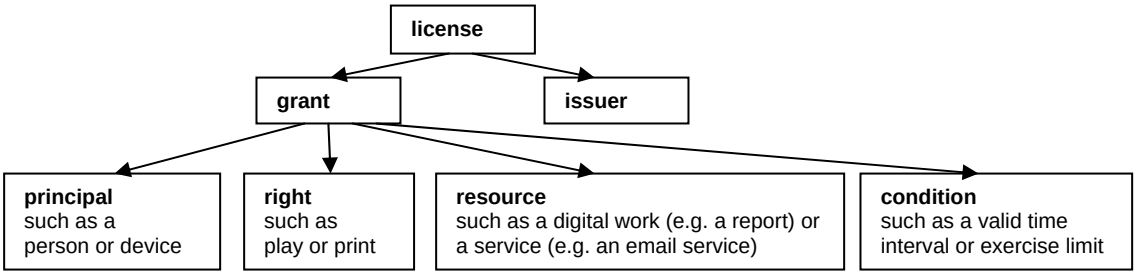

Figure 1: REL Data Model

A simple REL license is given in Figure 2 in its skeleton form. In this license, a principal (Alice) has been granted the right to play a resource (a song) under the condition that she can only play it for 3 weeks. This right is conveyed under the authority of the license issuer (PDQ Records).

```
license
    grant
        Alice                   -- principal
        Play                    -- right
        aSong.mp3               -- resource
        for 3 weeks             -- condition
    issuer
        PDQ Records
```

Figure 2: Example REL License

The license shown above provides only a simple illustration of the MPEG REL data model. It makes no attempt to fully illustrate the flexibility and expressiveness of the language. In fact, the MPEG REL defines two (2) principal, eighteen (18) right, eleven (11) resource and thirty-six (36) condition elements. It can be used to create licenses that address a wide variety of business models, including usage licenses, offers, distribution licenses (both single- and multi-tier), and certificates [1,4].

3 XML Profiles and Binary Encoding

This section describes the general concepts of profile and binary encoding, and provides a list of principles for profile specification and binary encoding for standards written using the W3C XML schema [4] like the MPEG REL.

3.1 Profiles

Concept. According to an ISO document on profiles [3], a profile identifies a set of one or more base standards (or specifications in general), together with appropriate options and parameters necessary to accomplish identified functions for a community (e.g., electronic books or mobile devices), an application (e.g., media streaming), a function (e.g., certificating and attesting assertions), or an environment (e.g., North America, Europe or Asia).

Specification. For standards written in the W3C XML Schema [4], a profile consists of syntactic, semantic, and processing rules for its intended use of the base standards:

- Syntactically, a profile must retain all required types, required elements, and their required attributes from the namespaces of the base standards. It must not introduce any new types, elements and attributes, which rules out any possible extension to the base standards.
- Semantically, a profile must preserve all essential semantics for the types, elements and attributes it contains. It may choose to preserve and eliminate some elective semantic constraints, and for those preserved constraints, it may specify semantic constraints that are more specific than those of the base standards. However, it must not introduce any semantic constraints that would cause non-conformance to the base standards.
- Processing-wise, a profile must keep all mandatory processing steps for all the types, elements, and attributes the profiles contains. It may choose to omit some optional processing steps, and impose additional processing steps that may refine, but must not contradict with, processing results as described in the base standards.

Conformance. With respect to conformance by any of its implementations, a profile should be considered an independent specification. Any implementation that creates REL expressions only using features in the profile should be considered as conformant to the base standards. On the other hand, any implementation that processes REL expressions with features in the base standards that are excluded from the profile may still be conformant to the profile, as long as the implementation conforms to the profile when it deals with the types, elements and attributes retained in the profile.

3.2 Binary Encoding

Binary encoding is a process which consists in encoding a description in XML form into an equivalent and more compact binary form. It allows that embedded, low-memory and/or low bandwidth systems make use of an interoperable, accessible, internationalised, standard representation for structured information, yet without the overhead of parsing an XML text document stream.

While there is currently no standard binary representation of XML documents, a number of efforts in this area (e.g., using an ASN.1 based, BiM, or even gzip) exist, aiming at significant savings in bandwidth, memory usage and CPU consumption.

4 An Example REL Profile and its Binary Encoding

This section illustrates the development process for an MPEG REL profile and its binary encoding, using a mobile domain as an example. The mobile domain is unique in several aspects: one is that mobile devices have less computational power than general purpose computing devices, and another is that mobile devices may only need to support simple usage and distribution rights and conditions due to their limited user interactions and the controlled environment of a service provider network. This section starts with some requirements from the mobile domain, converts them into ones for an REL profile, and finally defines the profile and its binary encoding.

4.1 Some Requirements from the Mobile Domain

DRM systems for mobile devices should enable an issuer to grant the rights to play, print, and/or execute a digital resource. In addition, these rights over the digital resources shall be constrained with time restrictions and count limitations. Moreover, a particular user or a particular device can be specified as the principal that can exercise the usage rights over the digital resources.

Furthermore, the computational power required to interpret rights shall be efficient, so that mobile devices can easily process and enforce the rights. Security concerns such as the ability to digitally sign a rights license may be required as well as the ability to specify trust information.

4.2 Analysis of the Mobile Requirements for the REL Profile

Based on the requirements in Subsection 4.1, the following set of requirements for the REL can be used to derive an REL profile:

R-1 The REL profile shall support an issuer to grant rights over digital resources. The profile must provide a mechanism to specify the issuer of these rights.

R-2 The REL profile shall support the following set of usage rights over a digital resource: play, execute, and print.

R-3 The REL profile shall support a limited set of restrictions over the usage rights:
- the number of times a resource may be accessed,
- a time interval during which a resource may be accessed

R-4 The REL profile shall support uniquely identifiable digital resources.

R-5 The REL profile shall support a principal (a specific user or a specific device) to exercise the stated usage rights over an identified digital resource.

4.3 Profile Elements

Based on the analysis of mobile domain requirements, the normative components of the REL mobile profile are presented in the following table, in terms of the syntax and cardinality of the permitted elements in the profile. These elements and their included child elements are listed along with the cardinality restrictions on the ones originally in the MPEG REL. Any optional child elements and attributes that are not listed are

excluded from the profile. The rationales for the selection and restriction (if any) of these elements are provided in the comments column.

Note that the namespace prefixes "r:", "sx:" and "mx:" for the elements stand for the namespaces of the core, standard extension, and multimedia extension of the MPEG REL, and that the R-1 to R-5 in the comments column refer to the five REL requirements in Section 4.2.

Element / Child Element	Occurrence in Profile	Occurrence in REL	Comments
r:license			
r:grant	1..∞	0.. ∞	"r:license" is a mandatory element in the MPEG REL, so it must be included in the profile. However, "r:grant" is mandatory in the profile so every profile license is used for granting at least some rights.
r:issuer	1..1	0.. ∞	"r:issuer" is included as a required element in the profile to meet R-1. However, one and only one issuer is allowed in each license in this profile.
sx:profileCompliance	0..1	0..1	"sx:profileCompliance" is an attribute, included in this profile as the mechanism to allow any "r:license" to claim that it is compliant with this profile.
r:grant			
r:keyHolder	0..1	0..1	The principal element of "r:grant" is an abstract type and must be substituted. In this profile, "r:keyHolder" is used as the actual principal and it's now the only allowed principal element. This satisfies R-5.
mx:play mx:print mx:execute	1..1	1..1	This profile only supports the "play", "print", and "execute" rights to comply with R-2.
mx:diReference	1..1	0..1	The "play", "print", and "execute" rights shall have an associated resource. Therefore, the profile requires this specific resource element to be present. It substitutes the abstract resource element of "r:grant". This satisfies R-4.
r:validityInterval sx:validityIntervalFloating sx:exerciseLimit r:allConditions	0..1	0..1	Zero or one condition may appear directly in a grant. The "r:condition" is an abstract element that will be substituted by the actual ones listed here. If more than one condition is to be specified conjunctively, then use the "r:allConditions" element.
r:keyHolder			
r:info	1..1	1..1	The child element "info" is retained in the profile (but its child elements are further restricted as shown in the next section).

mx:direference				
	mx:identifier	1..1	0..1	The rights supported in this profile must apply to a resource. Therefore, the identifier is now a required element in this profile.
r:allConditions				
	r:condition	0.. ∞	0.. ∞	The r:allCondition element is retained in the profile, so that other conditions can be grouped together by it and used conjunctively.
r:validityInterval				
	r:notBefore	0..1	0..1	"r:validityInterval" is a specific condition element that replaces the "r:condition" abstract type. This validity interval satisfies R-3.
	r:notAfter	0..1	0..1	See above.
sx:validityIntervalFloating				
	sx:duration	1..1	0..1	"sx:validityIntervalFloating" is a specific condition element that replaces the "r:condition" abstract type. This floating interval satisfies R-3.
sx:exerciseLimit				
	sx:count	1..1	0..1	"sx:exerciseLimit" is a specific condition element that replaces the "r:condition" abstract type. The "sx:count" element is now required when specifying an "sx:exerciseLimit". This satisfies the count restriction R-3.
r:issuer				
	r:keyHolder	1..1	0..1	The actual issuer must be specified using one "r:keyHolder".

An MPEG REL document that desires compliance with the REL mobile profile must use the elements in the profile as defined in the previous section. In addition, an MPEG REL license that seeks conformance with the profile must also adhere to restrictions listed in the table below:

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.

4.4 Binary Encoding

As the REL mobile profile are defined in terms of the order and cardinality of the permitted elements in the profile, it is fairly straightforward to come up a binary encoding in a recursive manner according to its structure.

For instance, at the top level, the binary encoding can have three blocks in the sequential order: one for "r:grant" elements, one for "r:issuer" element, and one for "sx:profileCompliance" attribute. Since there may be one or more the "r:grant" elements, its block can start with an integer *n* for its cardinality, followed by the binary encoding of

the *n* “r:grant” elements. As there is exactly one “r:issuer” element, its block can just contain the binary encoding of the “r:issuer” element. Because the “sx:attribute” attribute is optional, its block can start with a single bit, followed by the binary encoding of the attribute value if the bit has the value of 1 (for presence of the attribute).

The principle outlined above can be used recursively to define the binary encoding of the REL profile. For the sake of space limitation of this paper, the entire binary encoding is omitted.

5 Conclusion

Success of domain-specific DRM applications will benefit from appropriately developed profiles, as well as extensions, of the MPEG REL to meet specific needs. Developing profiles requires compliance with certain guidelines. A recipe (including concept, methodology and an example) is presented in this paper as a reference for creating these profiles. Not only does it illustrate a requirement-driven process and an effective mechanism for generating and presenting a resulting MPEG REL profile, but it also proves the scalability of the MPEG REL, as intended in design, to support DRM applications, systems and devices of different scales. The resulting profile, although hypothetical, has demonstrated that licenses written in the MPEG REL can be both compact and expressive to support many use cases in mobile DRM applications. The lightweight licenses can reduce the computational resources required by mobile devices to process these licenses and hence are suited for, while maintain the applicability beyond, the mobile applications.

References

1. MPEG REL Resources, http://www.contentguard.com/MPEGREL_reference.asp.
2. ISO/IEC 21000-5:2004, Information technology – Multimedia framework – Part 5: Rights Expression Language, 2004.
3. ISO TR 10000: Framework and Taxonomy of International Standardized Profiles.
4. XML Schema, Part 1: Structures and Part 2: Datatypes, W3C Recommendation, 2 May 2001. http://www.w3.org/TR/2001/REC-xmlschema-1-20010502, and http://www.w3.org/TR/2001/REC-xmlschema-2-20010502.
5. X. Wang, T. DeMartini, B. Wragg, and M. Paramasivam. The MPEG-21 Rights Expression Language. IEEE Transactions on Multimedia, (to appear).