XACML DRM Use Case Proposal

Thomas Hardjono *VeriSign*

Draft Version 0.1: July 27 2001

Executive Summary

This document proposes a Digital Rights Management (DRM) Scenario and Use Case for the XACML Oasis TC.

1 Entities

Digital Rights Management (DRM) distinguishes between a *Work* and the *Metadata* (or policy) governing the actions permissible on the Work. The two are elements within the larger ecosystem known as the *DRM Distribution Chain*. Although there are sub-chains or segments within the DRM Distribution Chain, for the purposes of XACML we distinguish for types of entities (Figure 1):

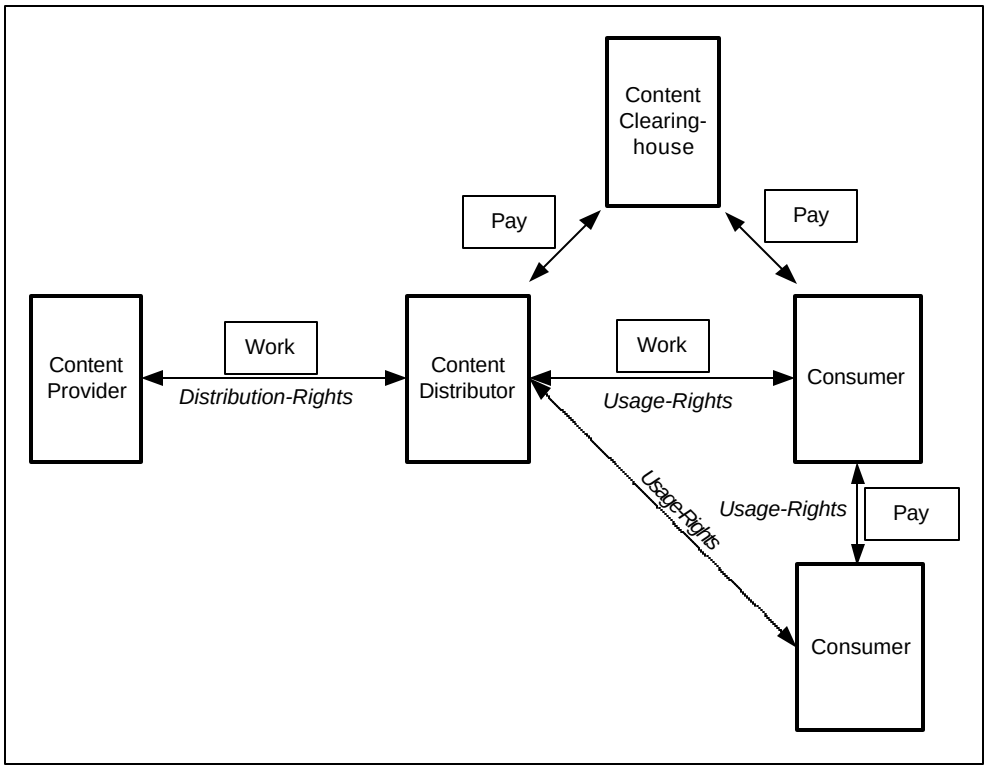

Figure 1: DRM Entities

- **Content Providers**: These are the entities that issue digital Works to the Distributors, and whom for our current need be defined also as entities owning the legal ownership *rights* to the Work. The Provider assigns distribution rights to the Distributor regarding a specific Work (or set of Works), and through the Distributor it assigns usage-rights to the Consumer. Some simplified examples of

Content Providers are record-labels (e.g. EMI) and book publishers (e.g. O'Reilly).

- **Content Distributors**: The Content Distributor is the entity that makes digital Works widely available to the Consumer. In this case, since the Work is in digital format, the Internet is perceived to be the transport medium. A Consumer buys usage-rights of a digital Work from the Distributor. The Distributor identifies and authenticates the Consumer, delivers the Work to the Consumer and ensures the Consumer pays for the Work. For our current example we assume the Consumer is not anonymous and that the Distributor correctly passes payments back to the Provider. Simplified examples of the Distributor entity are record shops (e.g. Tower Records) and on-line bookstores (e.g. Amazon). The Distributor is typically given the right to mass-reproduce instances of the Work (i.e. copies) to sell to individual Consumers.

- **Consumer**: The Consumer is the end-user of the digital Work. The Consumer typically purchases usage-rights for a given instance of the digital Work. The Consumer is expected to identify/authenticate the Distributor as a valid outlet for the Work, and the Distributor identifies/authenticates a Consumer as a legal entity possessing the ability to pay for the usage-rights. A Consumer may sell her usage-rights over a given instance of a Work to a second Consumer, though for simplicity we do not assume the Consumer to therefore take the role of the Distributor. When a usage-right of one Consumer is *conferred* to a second Consumer (through selling or trading), we assume that the second Consumer will notify the Distributor and obtain necessary parameters to enable (i.e. *exercise*) those rights. Although the Distributor (and Provider) may not gain addition revenues from rights-conferral, the Distributor is assumed to be involved in the conferral chain to identify/authenticate the second Consumer as the new holder of the usage-rights of that Work.

- **Content Clearinghouse**: The Clearinghouse is the general entity involved in the collection of payments from a Consumer to the Distributor for the purchase of usage-rights over a given instance of a digital Work. For simplicity the Clearinghouse is assumed to be a separate entity from the Distributor, though it is possible that a Distributor is in fact also a payments collector for a specific segment of the DRM market or for specific type of content. The Clearinghouse needs to identify/authenticate Consumers (for payment transactions) and identify the specific Works that the Consumer buys. In the case where one Consumer sells the usage-rights over a Work to a second Consumer, the Clearinghouse may be used by the two Consumers to conduct financial transactions.

2 Metadata

Within the DRM space the term *Metadata* is typically used to denote the information used to govern the control over the dissemination and usage of the digital Work. Depending on the implementation, Metadata for a specific Work can be disseminated together with the Work or separately, which requires the Consumer (or the Consumer's device) to also obtain the Metadata before using the Work.

When processing metadata for a given Work, the authenticity of the metadata must be established (e.g. digital signature).

A metadata for a given Work should be self-describing and sufficient for the Work in question. That is, in DRM implementations it is usually not expected that an additional layer of "meta" information is needed to govern the access or usage to the metadata. If a metadata file is located separately from the Work, then some minimal information is provide for the Consumer to download both the Work and its metadata. Some implementations indeed package together metadata and the Work, and encrypt both as a single ciphertext that is decipherable only by the Consumer. However, such systems also deploy additional cryptographic protection for the actual access to the content.

For the current document, we assume that only one layer of metadata is employed. However, it is possible that several metadata files (at the same layer) is used to describe various actions needed to be performed by the Consumer to finally obtain access to the Work (e.g. metadata for key download, metadata for e-payments, etc).

3 Specific Use Cases

In this section we focus on the specific interactions between the entities in the DRM Chain in the form of a number of simple Use Cases.

These are very simple examples and are high-level. Other more specific description of entities and functions in DRM have been put forward by other organizations [REF].

3.1 Use Case 1: Provider-to-Distributor Distribution-Rights Conferral

The assignment of distribution-rights in the content industry today is typically achieved using traditional legal contracts, which may cover a number of Work types and/or Works. Although in the traditional content distribution channels (e.g. Music stores) the Consumer never questions the rights of a Distributor to distribute a Work, in the digital world it is very likely that a Consumer may challenge an electronic Distributor to prove its rights to distribute a specific content.

For simplicity, we assume that the Distributor is given the task and rights to reproduce multiple instances of the Work to be sold to the Consumer. Examples include unique reproductions of music files and e-books. We thus assume that the Distributor will track information about the number of copies of a digital Work has been sold/used.

The Metadata expressing the conferring of distribution-rights should contain, among others:

- The identity of the Provider and Distributor.
- Identification information of the Works covered by the distribution-rights.
- The duration of the validity of the distribution-rights.
- The maximum number of unique reproductions of the Work allowed for the Distributor.
- The precise definition of the distribution-rights conferred from the identified Provider to the identified Distributor.
- The definition of other rights, if any, conferred from the identified Provider to the identified Distributor.
- Information about costs and payments to the Provider.
- The digital signature of the Provider.

3.2 Use Case 2: Distributor-to-Consumer Usage-Rights Conferral

When a Consumer pays for content, effectively the Distributor propagates or confers usage-rights for that content to the Consumer on behalf of the Provider.

Here, the Distributor is concerned about the illegal reproduction of the content, and thus has an interest in identifying the specific Consumer who has received the usage-rights. From a legal perspective, the Distributor would like to see the usage-rights conferral to be legally-binding to the Consumer, and thus would require digital signatures from the Consumer to acknowledge the Consumer's acceptance of the rights conferred.

There are a variety of information that needs to be conveyed within the usage-rights conferral process, some examples being:

- Identity of the Distributor and the Consumer
- Identification of the instance of the Work covered by the usage-rights. The identification should also identify the Work itself in addition to the copy-number.
- The duration of the validity of the usage-rights and usage-types (e.g. play-once, play-N-times, unlimited play, etc).
- Other rights permissible (e.g. Works can be sold once or N-times, or never be sold, etc)

- Information about metadata related to the Work (if it is separate from the Work)
- Digital signature of Consumer in the purchase
- Signed receipt from the Distributor or Clearinghouse
- Key management information

There is also the case where the Consumer purchases usage-rights for a collection of Works, based either on the Consumer's selection (e.g. any 10 songs) or pre-packaged by the Distributor (e.g. HBO channel). Additional metadata information about these packaged Works need to be conveyed in the usage-rights transfer from the Distributor to the Consumer.

3.3 Consumer-to-Consumer Usage-Rights Conferral

Access to the open Internet has borne the concept of trade in digital goods, an example of which is digital content such as music.

A proper and scalable DRM system should allow the selling of usage-rights from one Consumer to another, in the same way that paper-works are traded today. The transfer of usage-rights from one Consumer to another does not imply (illegal) reproduction of digital Works.

In other words, a DRM system should distinguish between the *conferring* of usage-rights from the *exercising* of that usage-rights. When a Consumer exercises a usage-rights (either purchased form a Distributor or another Consumer), that Consumer will still need to interact with entities within the DRM infrastructure (such as the Distributor, Clearinghouse or other commerce entities) to activate the access to the content.

When usage-rights are conferred from one Consumer to another, the information that is needed to support the transaction include, but not limited to:

- Identification of the instance of the Work (or collection of Works)
- Identity of both Consumers
- Identity of the original Distributor and signature
- Identity of the previous owner (if the Work has change hands several times) and signature
- Proof of purchase or rights-conferral, signed (and dated) by both seller and buyer
- Signed receipt from the seller

4 References

TBD.