

# **From Patent License Facilitation to Marketplace Implementation: The MPEG LA DRM Reference Model**

**Marina Bosi  
Chief Technology Officer**



**CCNC05 DRM Workshop  
Las Vegas, NV  
January 6, 2004**

# Overview

- **What is Digital Rights Management?**
- **The structure of a DRM system**
- **MPEG LA's Reference Model Approach**
- **From Patent License Facilitation to Market Implementations**

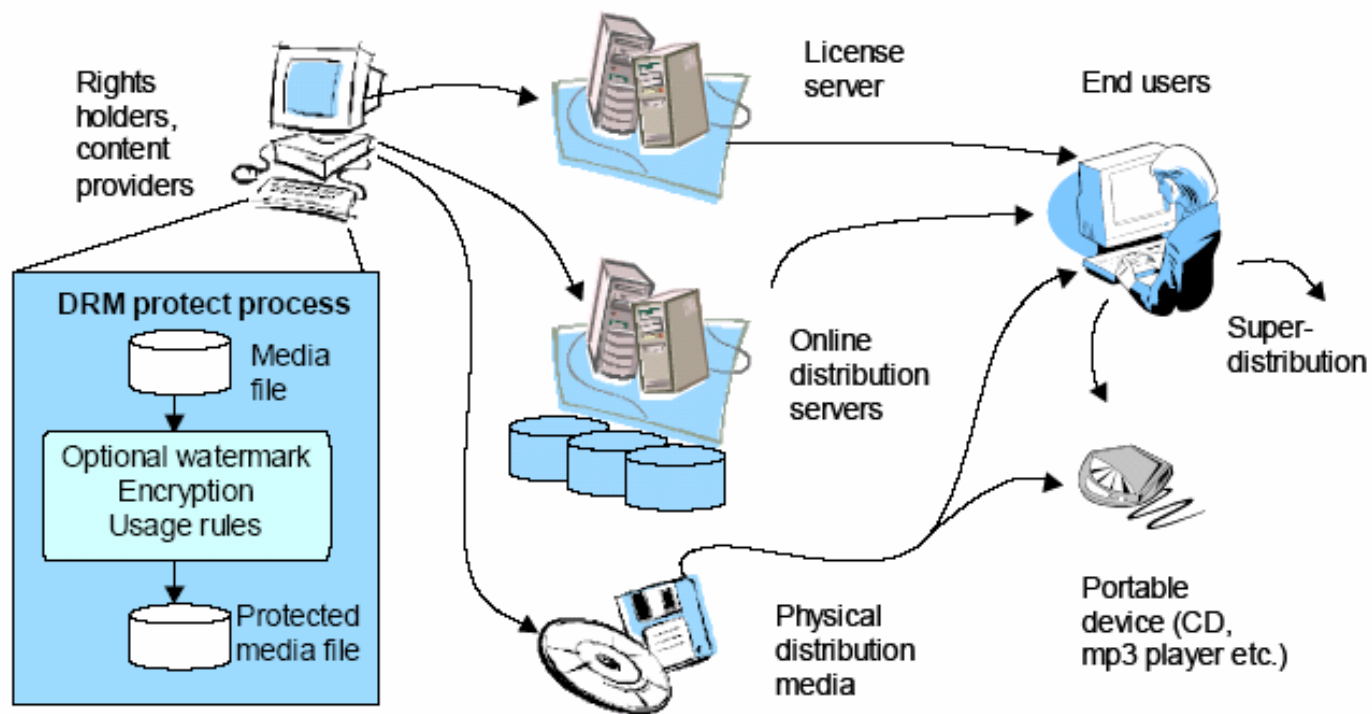
# What is Digital Rights Management (DRM)?

- **Numerous types of creative content have begun migrating into digital formats**
  - e.g., Software, Music, Movies, Books, Photographs
- **Owners of this content often look to sale or rental of that content as an important revenue source**
- **The transition to digital systems raises the spectre of unlimited perfect copies of proprietary content being distributed without compensation to the owner**
- **A DRM system is a set of technologies developed to support legal distribution of digital media while protecting appropriate property rights**

# Structure of DRM Systems

- **A DRM system needs to address three major areas:**
  - Ensuring that the content is packaged in a form that will prevent unauthorized copying/usage
  - Distribution of the content to the end user
  - Making sure the end user is able to make use of the content consistent with their rights
- **Increasingly, DRM systems treat packaged content and the rights to access that content as separate entities**
- **This adds a fourth area that a DRM system needs to address:**
  - Distribution of usage permissions to the device allowing the user to access the protected content

# Basic DRM Process Flow



From <http://www.medialab.sonera.fi/workspace/DRMWhitePaper.pdf>

## An Example: DVD-Video

- **DVD-Video content is protected using the Content Scrambling System (CSS) defined by the DVD Forum**
  - **Movies are put on the DVD disc in an encrypted format that requires a key to decode and view the content**
  - **The content distribution system is via stores that sell DVD discs to the end user**
  - **The manufacturers of DVD players need to register with the DVD forum to gain access to the decryption key to embed into their players (the license distribution system)**
  - **An end user then has the ability to watch the content of purchased DVDs an unlimited number of times on registered players**

# An Example: DVD-Video

- **Some Issues with the CSS structure**
  - **Its fixed encryption scheme can potentially be hacked**
    - **Not just of theoretical interest!**
  - **Possession of the decryption key allows full access to the content so limited access cannot be easily sold through the DVD-video format**
    - **Discs that self-destruct after limited contact with air are an attempt to deal with this limitation**
  - **Access to the decryption key allows access to all DVDs so it cannot be used as a basis for online distribution of movies (i.e., the license distribution is not linked to the particular content in any meaningful manner)**

# The MPEG LA Approach

- **MPEG LA decided to facilitate the development of a highly flexible reference model structure to facilitate creation of joint patent licenses that can be adapted to a wide variety of applications**
- **Our goal was to help promote the development of DRM systems without being constrained to one particular form of packaging or delivery platform or being delayed by standards development processes**
- **As license administrators, we were also looking to ensure that the market developed a common language and structure in implemented DRM systems so that common patent licensing structures can be utilized to access the underlying DRM technology**

# **MPEG LA's DRM Reference Model**

- **MPEG LA's DRM RM was conceived in order to provide a consistent basis for evaluating patents in order to offer patent licenses that enable diverse marketplace implementations**
- **A toolkit of generic DRM processes is specified**
- **Subsets or profiles of the generic DRM technology are also defined to enable support of specific standards and marketplace implementations**



# **MPEG LA's DRM RM: The DRM Toolkit**

- **Basic Tools:**

- **Package assets with application certification, credentialing, authentication and verification;**
- **Distribute assets**
- **Generate and issue license through rights expression language**
- **Enforce license and consume asset by controlling the execution of actions on assets received in packages based on licenses and rights expressions**
- **Asset and license confidentiality protection by encryption and integrity protection by signing**
- **Management of keys used for the asset and license confidentiality and integrity protection**
- **For further details please see**  
**<http://www.mpegla.com/pid/drm/>**

# **MPEG LA's DRM RM Version 3.0: Initial Applications**

- **Profiles of the generic DRM technology have already been defined to enable licensing and support of the following standards:**
  - **The Open Mobile Alliance (OMA) DRM version 1.0**
  - **OMA DRM version 2.0**
  - **Internet Music Transfer Service (IMTS)**

# Marketplace Implementations: OMA DRM 1.0

- **OMA DRM specifications are particularly tailored for mobile services**
- **OMA DRM version 1.0 provides basic access control to “light media content”**
  - **Forward Lock (prevents content from leaving the device)**
  - **Combined Delivery (adds rights definition to the content)**
  - **Separate Delivery (provides content encryption and supports “superdistribution” by separating the rights definitions from the content)**

## Marketplace Implementations: OMA DRM 2.0

- **OMA DRM version 2.0 provides a more sophisticated DRM system compared to version 1.0, allowing for protection of “premium content” and more usage flexibility**
  - Evolved from 1.0 Separate Delivery mode
  - A rights object governs how DRM content may be used through an XML-based Open Digital Rights Language (ODRL)
  - Public key encryption infrastructure (PKI) is utilized

## Marketplace Implementations: OMA DRM 2.0 (Cont)

- **OMA DRM version 2.0 new functionalities include:**
  - **Storage and backup: users can move content and/or rights to remote or removable storage and later restore the rights and/or content to device**
  - **Multiple devices: Users can move content and/or rights easily between several devices owned by the user (2nd phone, PC, music player, etc. )**
  - **Copy to secure removable media for a mobile music player**
  - **Ability to preview superdistributed content before purchase**
  - **Export to other copy protection schemes**

## Marketplace Implementations: OMA DRM 2.0 (Cont)

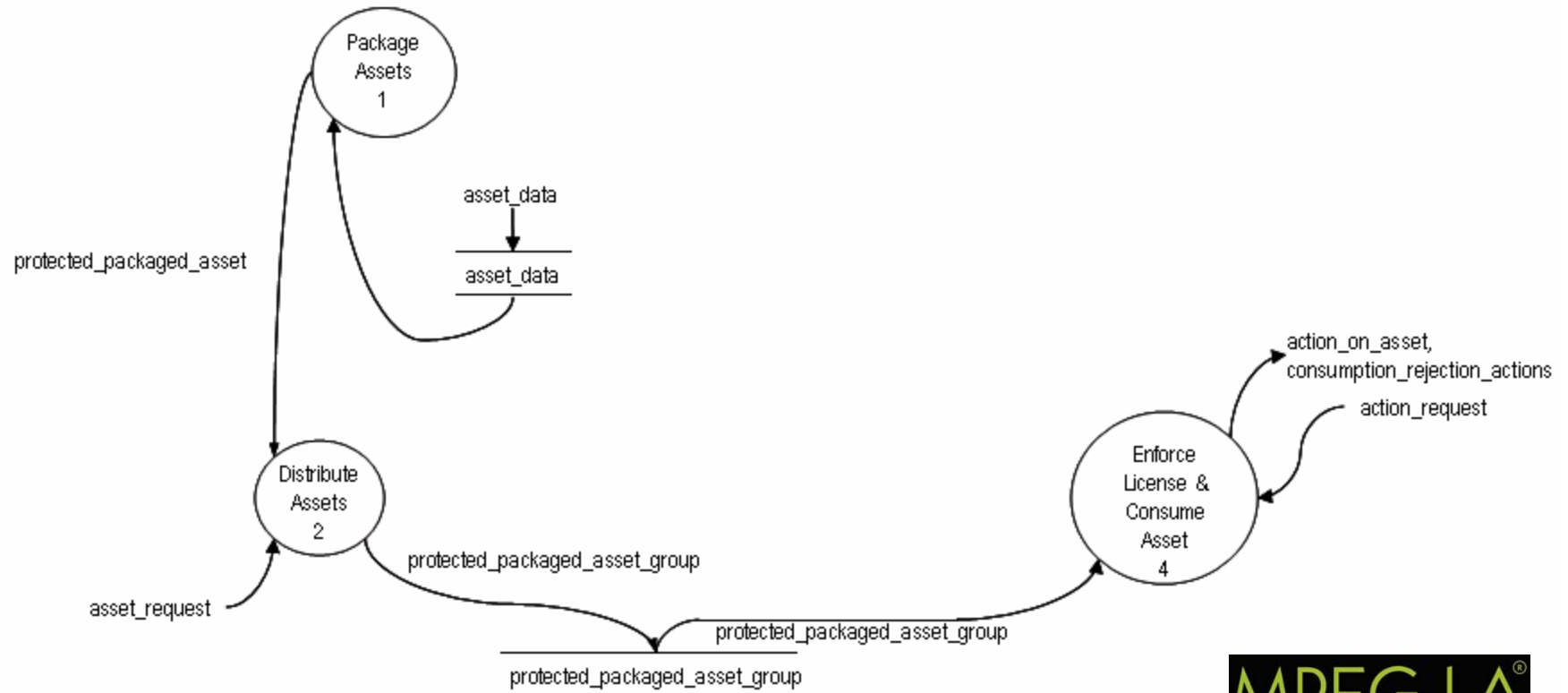
- **OMA DRM version 2.0 additional protections include:**
  - Individually encrypted rights using a device's public key to provide cryptographic binding
  - Integrity protection for content and rights
  - Mutual authentication between device and rights issuer
  - Device/rights issuer revocation
  - Secure multicast and unicast streaming
  - Metered time and usage constraints

# Marketplace Implementations: IMTS

- **The IMTS profile includes the following tools:**
  - Confidentiality protect asset using encryption
  - Consumer originating asset/license request specifying requested rights
  - Separately deliver license
  - Integrity protect license with public key encryption
  - Transfer asset action
  - Associate rights with asset
  - Distribute package by download/ streaming
  - Deliver asset key with license
  - Integrity protect package and rights
  - Transfer rights
  - Automated subscription license renewal
  - Authentication and verification application
  - Verify license for integrity and destination
  - Check consumer authorization

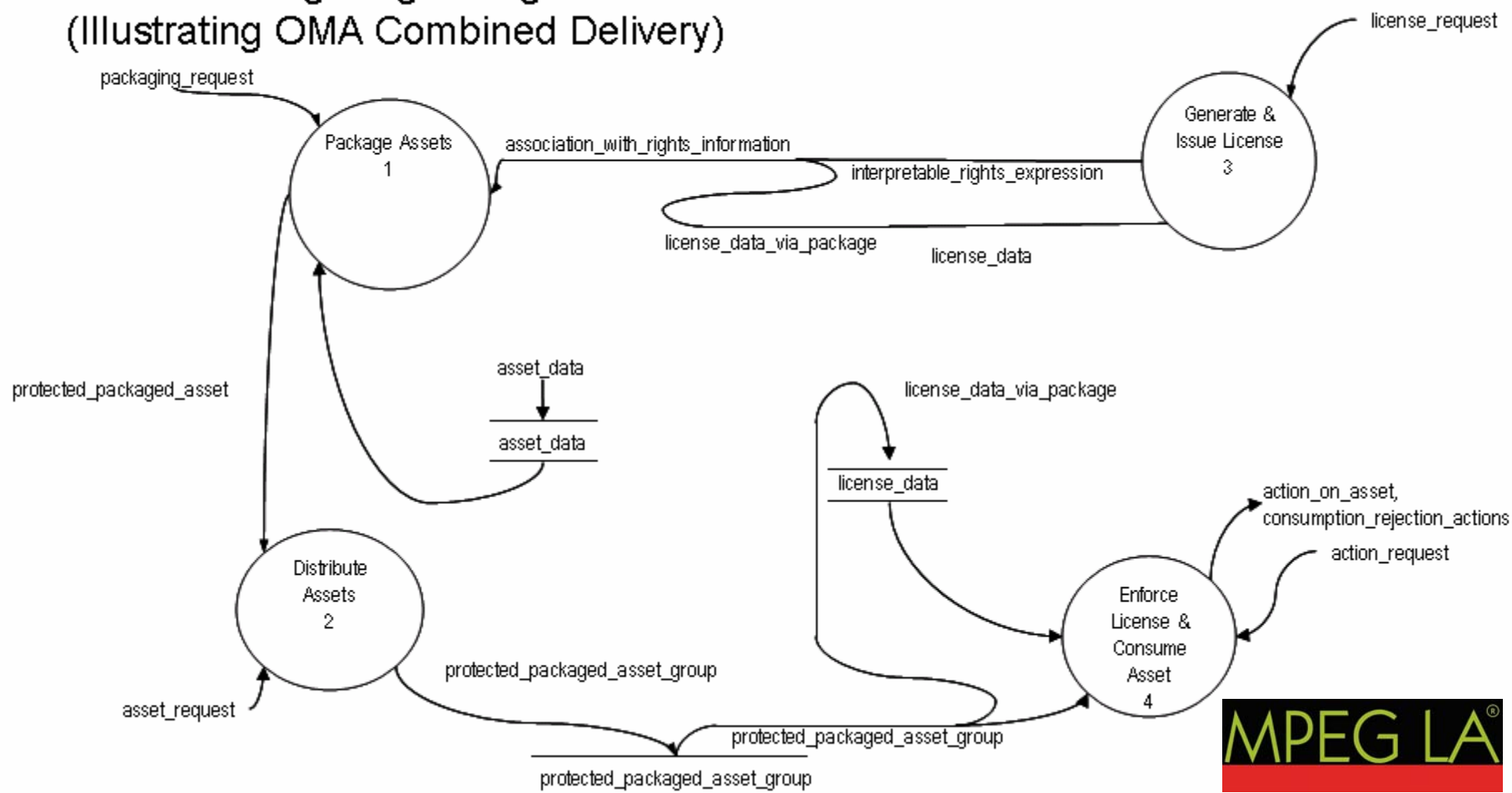
# Example: Applying MPEG LA's DRM RM to OMA Forward Lock

DFD 0: Manage Digital Rights  
(Illustrating Forward-lock delivery)



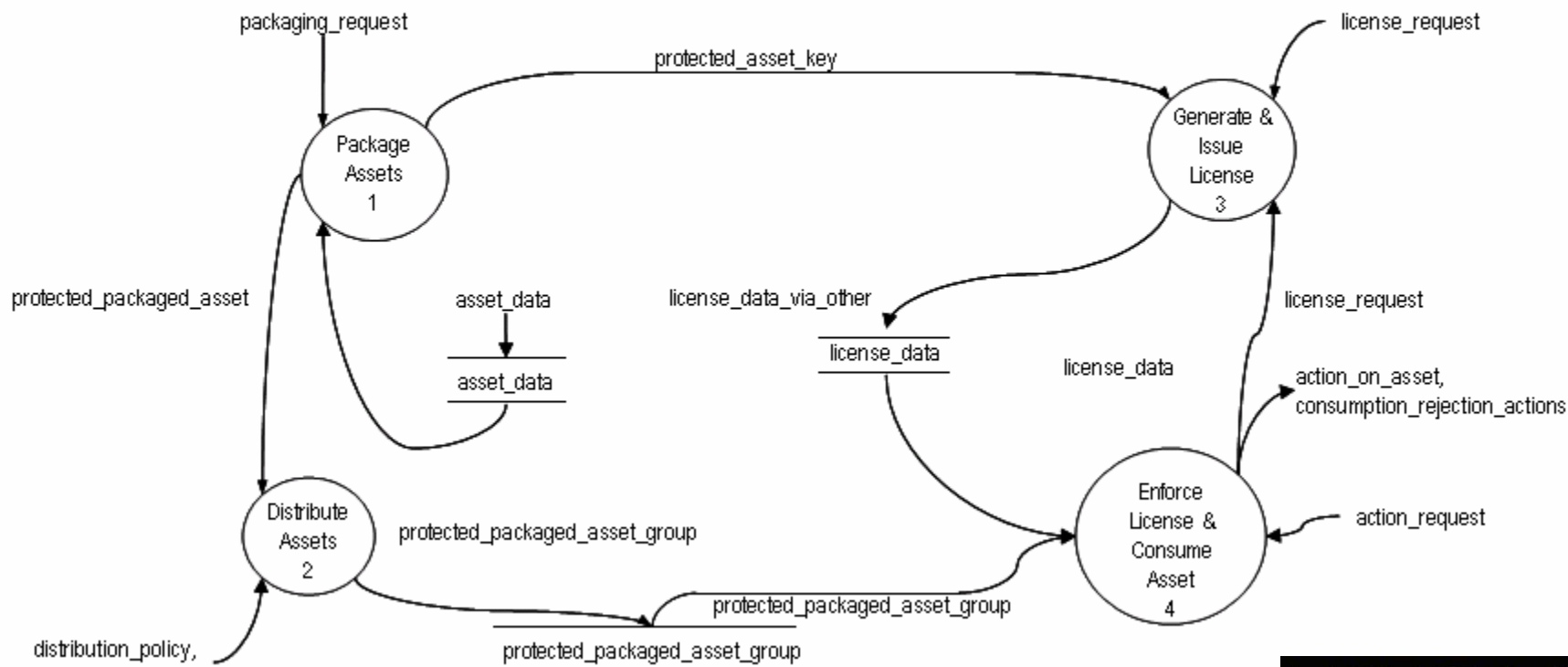
# Example: Applying MPEG LA's DRM RM to OMA Combined Delivery

DFD 0: Manage Digital Rights  
(Illustrating OMA Combined Delivery)



# Example: Applying MPEG LA's DRM RM to OMA Separate Delivery

DFD 0: Manage Digital Rights  
(Illustrating OMA Separate Delivery)



# Status Report

- **IP call for DRM RM version 1.0**
  - **2 October 2003** (<http://www.mpegla.com/pid/drm/>)
- **IP call for DRM RM version 2.0 including IMTS and OMA DRM 1.0**
  - **20 July 2004** (<http://www.mpegla.com/pid/drm/>)
- **Open IP call for OMA DRM 2.0**
  - **23 September 2004** (<http://www.mpegla.com/pid/drm/>)
- **Six companies involved in a patent pool for OMA DRM 1.0**

# Conclusions

- **MPEG LA's DRM RM:**
  - **Represents the connection between generic DRM technology and IP license**
  - **Allows users to access diverse DRM technology**
  - **Enables implementations of own technology choices**

**For Further Information,  
Please Contact**

**Marina Bosi**

**Chief Technology Officer**

**MPEG LA, LLC**

**250 Steele Street, # 300**

**Denver, CO 80206**

**Tel 303-331-1880**

**Fax 303-331-1879**

**Larry Horn**

**VP, Licensing & Business Dev.**

**MPEG LA, LLC**

**4601 Willard Avenue, # 200**

**Chevy Chase, MD**

**Tel 301-986-6660**

**Fax 301-986-8575**

**Website: [www.mpegla.com](http://www.mpegla.com)**