Towards a User-Friendly DRM

W3C Workshop on Digital Rights Management
22 & 23 January 2001 - Sophia Antipolis

pierre.vannel@gemplus.com
Affirmations

- The Internet user: both a consumer and an author/publisher.
  - Example: a student writing a paper might quote copyrighted works and publishing them on his personal Web pages.

- Digital rights: economic + moral rights
  - Economic rights: transferable rights
  - Moral rights: irrevocable authors’ rights
Requirements (1/2)

- DRM cannot offer less than current systems
  - anonymous access to content
  - free disposal of protected content (e.g. sale, gift, loan)
  - portability: the use of a digital content should not be attached to a single device (e.g. to listen a music on hi-fi system, car radio or walkman of a given individual)
  - off-line use of a protected content
Requirements (2/2)

More:

- interoperability between DRM systems:
  - so that the user does not have to juggle with DRM systems
  - to provide a lingua franca for the digital rights associated with a resource
  - to allow the aggregation of resources protected by different DRM systems

- superdistribution

- protection of personal contents (e.g. “I forbid the commercial use of the pictures on my personal pages”)
Features of an Ideal DRM System

- Interoperable: a common platform to run different protection systems (IPMP approach)
- Upgradeable: secure dynamic downloading of new protection systems into the platform
- Support for the exchange of rights: secure exchange of digital rights with another trusted platform, including superdistribution
- Privacy protection: anonymous access to information
- Fair use (aggregation) control: enforcement of author rights
- Non-Specific Network architecture: Web, peer-to-peer...
Security Issues (1/2)

- Truisms:
  - the Internet is not secure
  - neither end-users nor providers are trustworthy

- Deployment of a new IPMP: how should we allow installation?
  - From the end-user point of view: we need an IPMP certified by a Trusted Third Party (TTP)
  - From the IPMP provider: the core DRM system should not be tampered with

- Secure communication channels (authentication, integrity, confidentiality) required to exchange sensitive data (rights, IPMP…) with an end-user
  - secure repository for key storage
Security Issues (2/2)

- Use of copyrighted resources should be controlled: how can we prevent rights infringements by the end-user?
  - secure repository for the license data controlling the use of the corresponding content/service

- Fair use needs to be guaranteed while ensuring at least partial anonymity for end-users
  - Certain certified information about the end-user’s profile is needed (e.g. he is a student)
  - Need for a secure repository to store the fair use policy of the provider and for a secure engine to check this policy.
Framework Approach

- Open and portable framework, based on existing standards (in cryptography, communications …etc.)
  - To package a protected content
  - To run/render a protected content

Main Features

- Support of various pluggable protection solutions (IPMP modules)
  - pure software-based
  - hardware-based (e.g. smart card)
- Support of both free content and protected content
Smart Card-Based Solution

Splitting of an IPMP module in two parts: off-card and on-card
- on-card part handles securely the sensitive rights holder data
- delegated control: the smart card acts as a rights holder representative

Smart card used to control the IPMP installation

Smart card used to protect the cardholder’s personal information

Smart card features
- multi-application smart card (i.e. JavaCard, Windows for Smart Card [WfSC], MultOS)
- on-board cryptographic algorithms
Pros / Cons (1/2)

Pros

- Protection & control of the rights: secure storage and processing of provider data
- Portability of rights: the use of a protected content is not tied to a single device
- Privacy protection: strong authentication which is not linked to the user’s identity
- End-to-end security:
  - ✔ secure exchange of rights with another trusted device
  - ✔ secure downloading of an IPMP system
- Multi IPMP support
- Upgradeability: downloading of a new IPMP, updating an existing IPMP
Pros / Cons (2/2)

Cons

- Infrastructure: card reader must be incorporated in a trusted device
- Smart cards must be deployed
Areas for Standardization

- Specify an interoperable platform
  - Digital rights description language
  - Secure protocol to exchange rights
  - Digital rights reporting/tracking to Authors Associations
    - distribution follow-up
    - composition follow-up
  - DRM framework
  - Secure protocol to install new DRM modules

- Enforce the end-user’s privacy
  - to define a portable privacy wallet