

# Secure Content Management

Willem Jonker - Philips Research / Twente University

Frank Kamperman - Philips Research

# Content

- Content Protection
- Digital Rights Management
- Content Based Access

# Motivation Content Protection

- Network and encoding technology enables easy distribution of content
- Content owners want to maintain control over their content
- Consumers want unrestricted access

# Players in Content Protection

- The content generators (MPAA, RIAA, IFPI,..., Warner, Disney)
- The packagers (e.g. Broadcasters: Canal+, NDS, ..; web portals)
- The IT industry (Intel, Microsoft.....)
- The CE industry (Philips, Thomson, Sony, MEI, ..)
- The “solution providers” (Macrovision - Digimarc - Verance)
- The consumers (Home recording rights coalition, ..)
- The regulators (U.S. Federal Government, EU, ..)
- The standardization fora (DVD CPTWG, SDMI, MPEG, ....)
- Licensing agency, CCA (CSS), DTLA (5C), 4C ...
- The hackers, pirates, ... (anonymous)

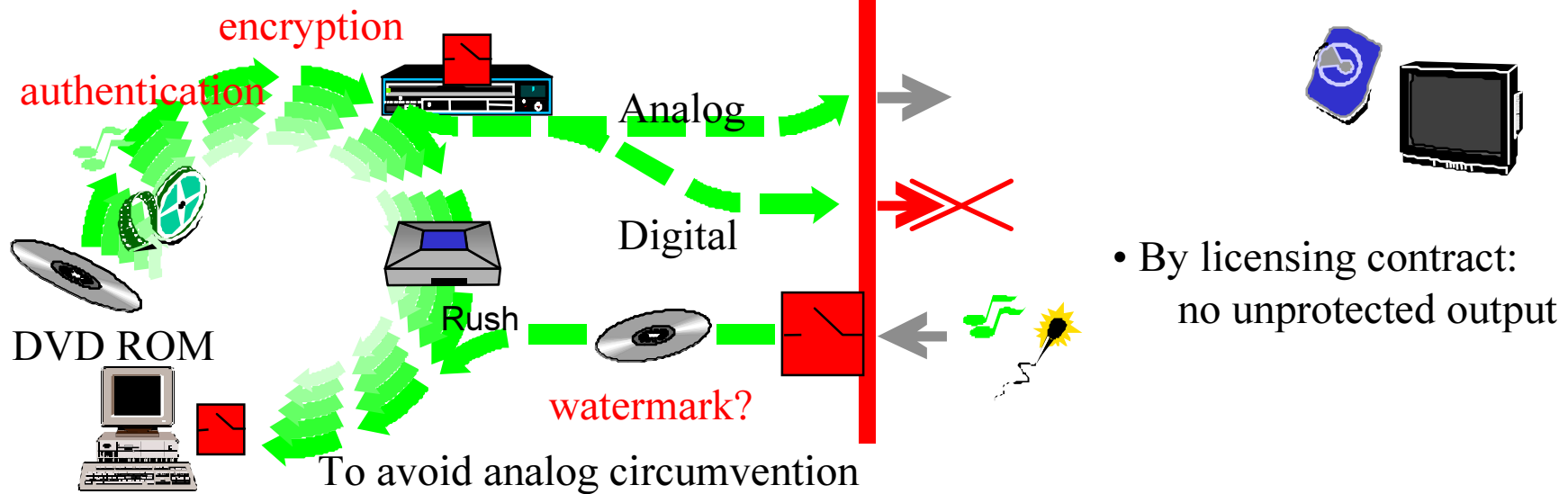
# Vision on Content Protection

## Compliant World

- All content is encrypted on all interfaces
- Controlled by CSS, 5C, 4C, Millennium, ...

## Non-Compliant World

- All analog devices, some digital



# Motivation Digital Rights Management

- DRM should go *beyond* copy protection
- DRM should enable *flexibility* in business models
- DRM should be an enabler for *E-commerce*
- DRM should deliver a flexible *rights enforcement system* for trading and management of digital content

# Current DRM solutions

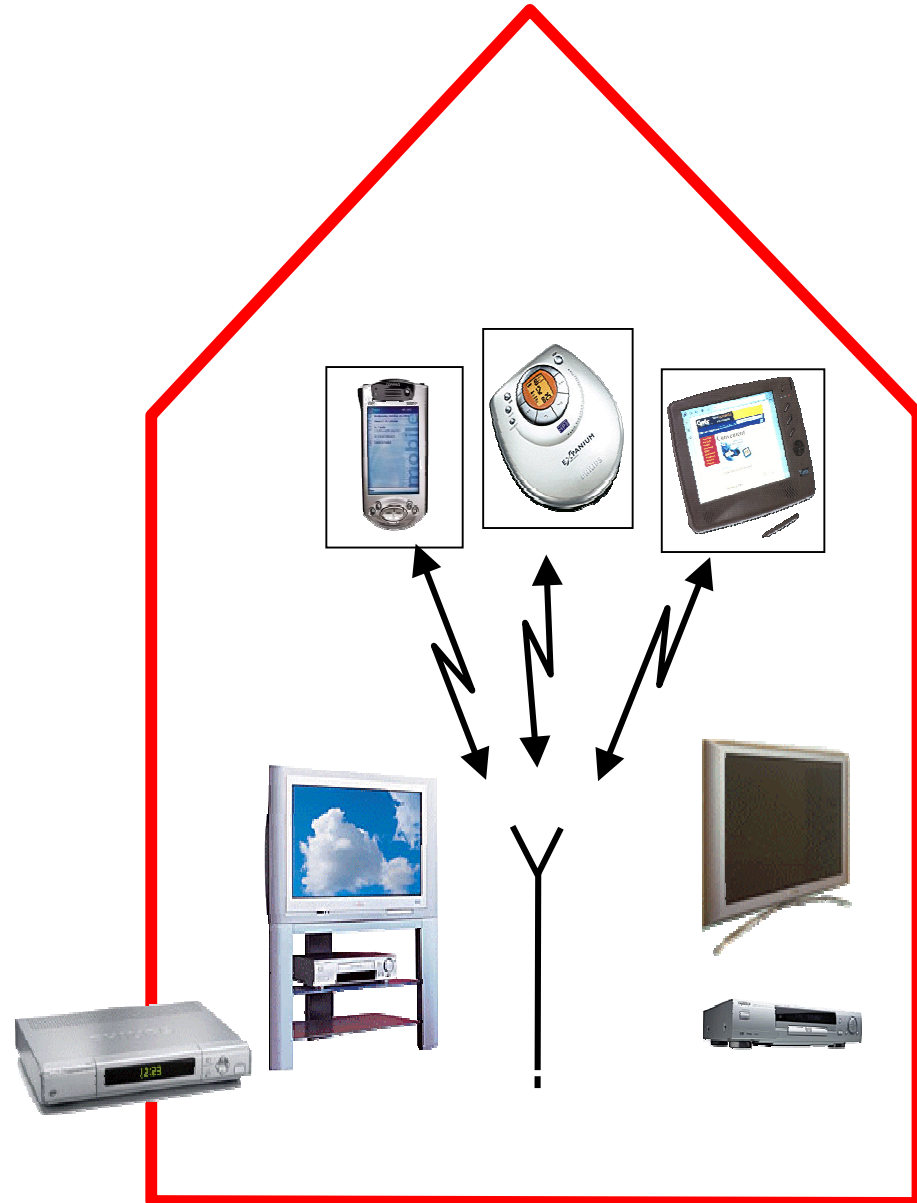
- Intertrust
- Microsoft media player / Windows XP
- Smartright (control the inhome network, smartcard)
- OCCAMM (just a secure ‘pipe’, end-to-end , ‘no’ storage, ‘no processing’)
- Open Magic Gate, SONY (started as secure flash card)
- IBM-EMMS

# DRM in home networks

*No restrictions on  
personal use of content  
at home*

*Controlled and legal  
import of content to the  
home*

*Controlled exchange  
between homes*



# Authorized Domain



# Authorized Domain

- Collection of devices
  - Belonging to a person or household
  - Size of the domain is limited
- Content within the domain
  - Multiple copies.
  - Free access.
  - Free processing.
- Import and export
  - Strict control of copyright rules.
  - From service provider / content owner.
  - Problem Inter-domain exchange.

# Technology: Domain management

- Secure inter-device communications
  - Secure Authenticated Channel (SAC).
  - Primarily for domain management information.
- Device registration
  - Device authentication and compliance check
  - Authentication based on certified cryptographic keys.
  - Device compliance check → revocation lists.
- Options for size limitation
  - Based on maximum number of devices.
  - Based on consumer identification.

# Technology: Content management

- Multiple copies allowed within domain
  - Copies are bound to the domain.
  - Access on EVERY domain device.
- Import of content.
  - Check for content rules at import
    - Watermarks
    - Digital licenses
  - Temporarily or permanent
    - Determined by the content provider
- Secure storage of licenses.
  - Distributed storage (together with the content)
  - Central database

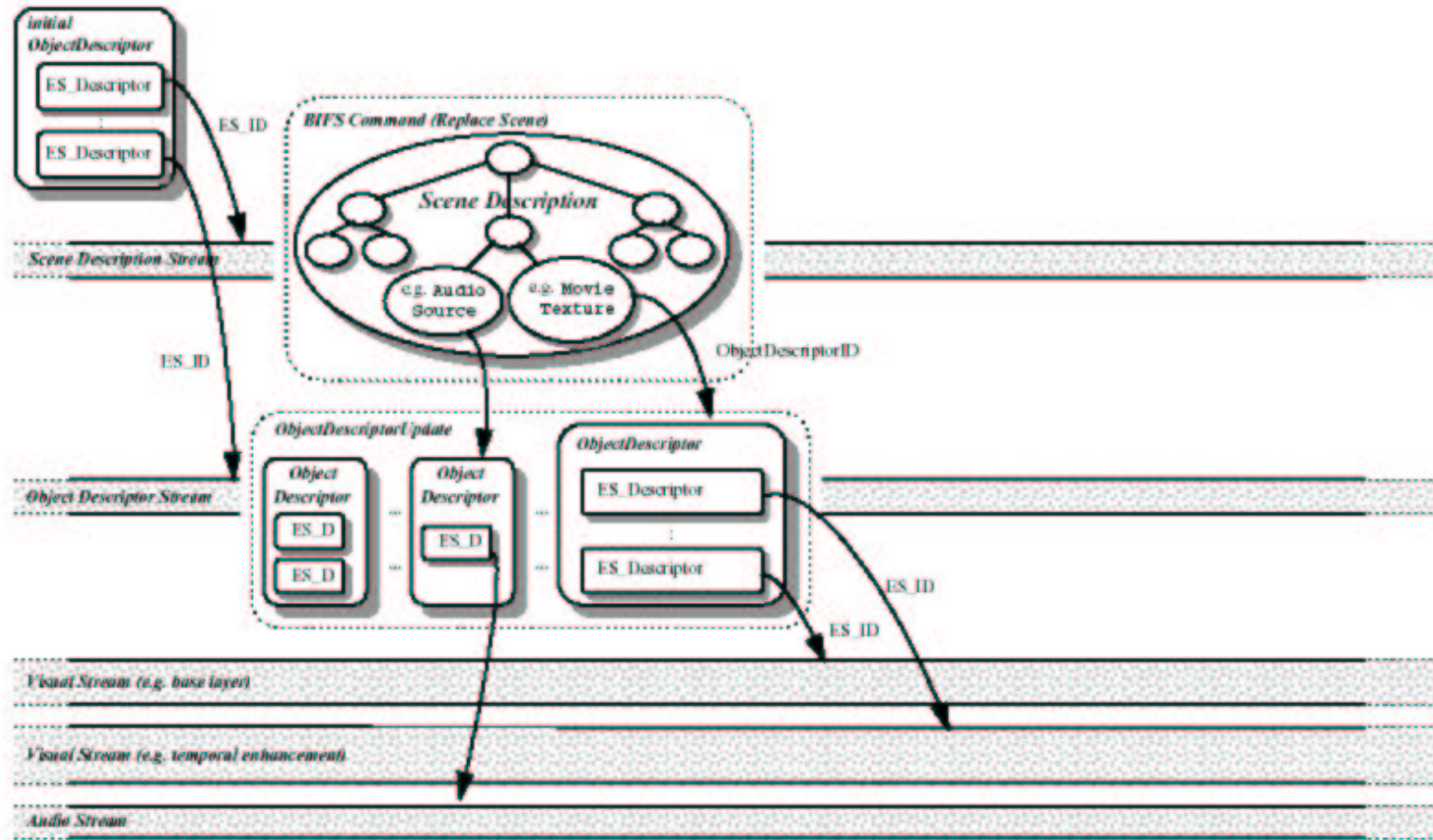
# Content Based Access (1)

- Motivation: Limit content access to authorized subjects
- Goal: Fine grained access to content
- Approach: exploit multi-media retrieval technology

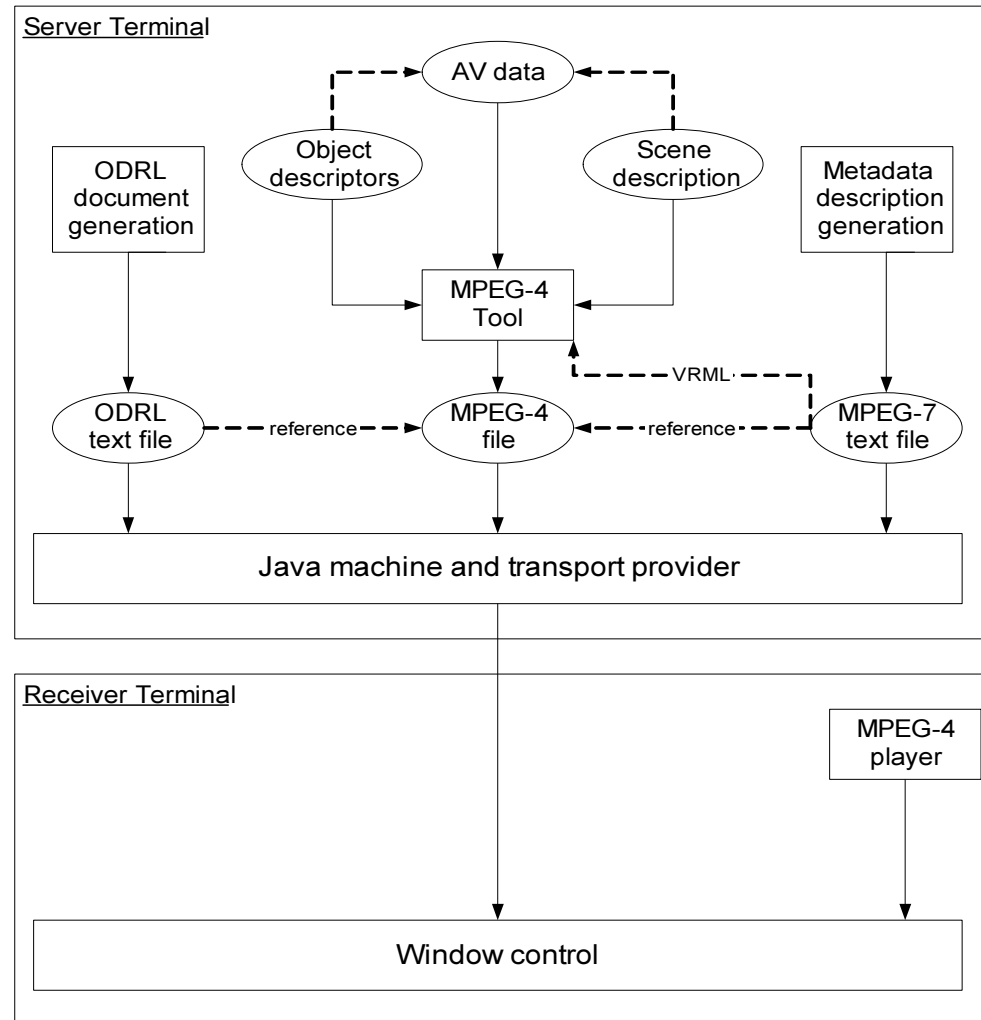
# Content Based Access (2)

- Selective Access to Video Material
- Ingredients
  - MPEG-4 (video coding)
  - MPEG-7 (meta data)
  - ODRL (access description)

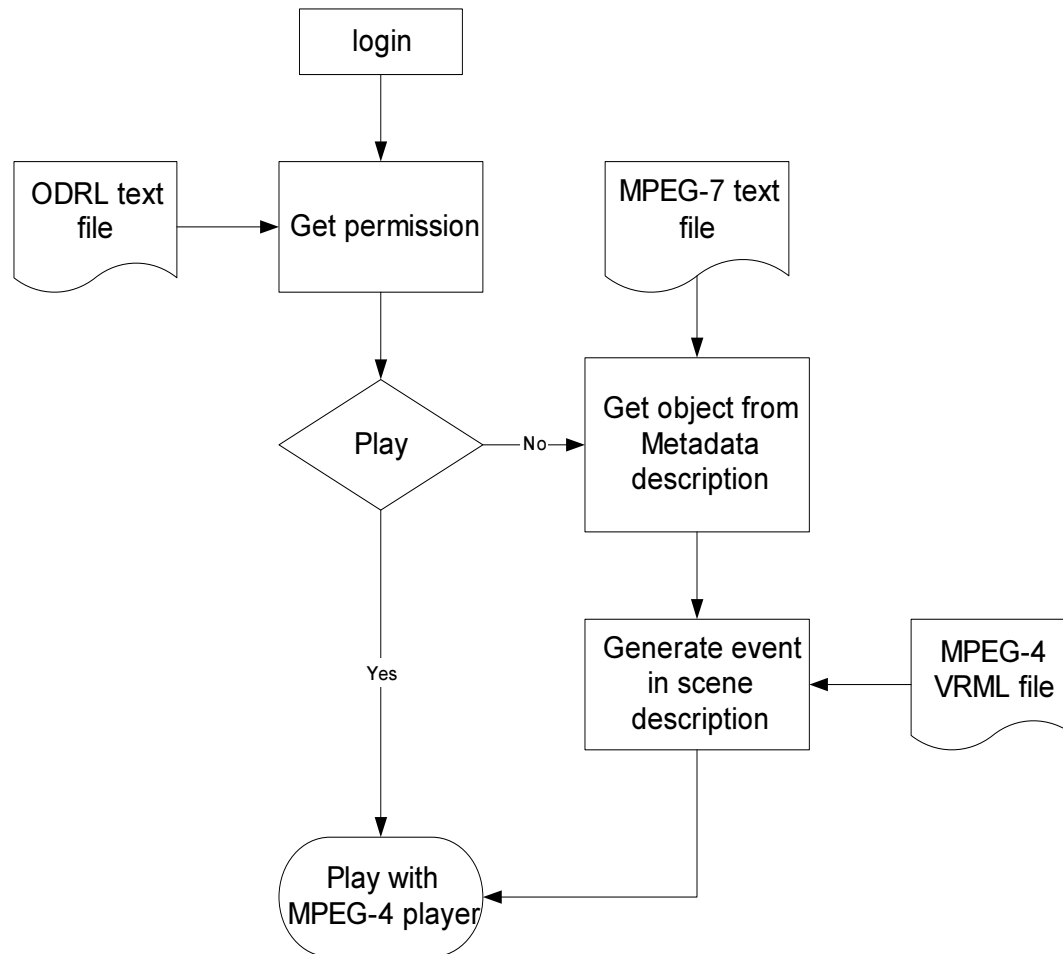
# Content Based Access (3)



# Content Based Access (4)



# Content Based Access (5)



# Content Based Access (6)



# Concluding remarks

- DRM is a crucial enabler for digital content distribution.
- Authorized Domains offer a balanced DRM solution between the interests of the various stakeholders.
- Content based access opens the way to new applications.