



Protecting Digital Contents in Web2.0

2007.10

Talk@DC_Seminar_2007

Yongtae Shin, Ph.D.

School of Computing, Soongsil University

DigiCAPS Inc.

shin@ssu.ac.kr

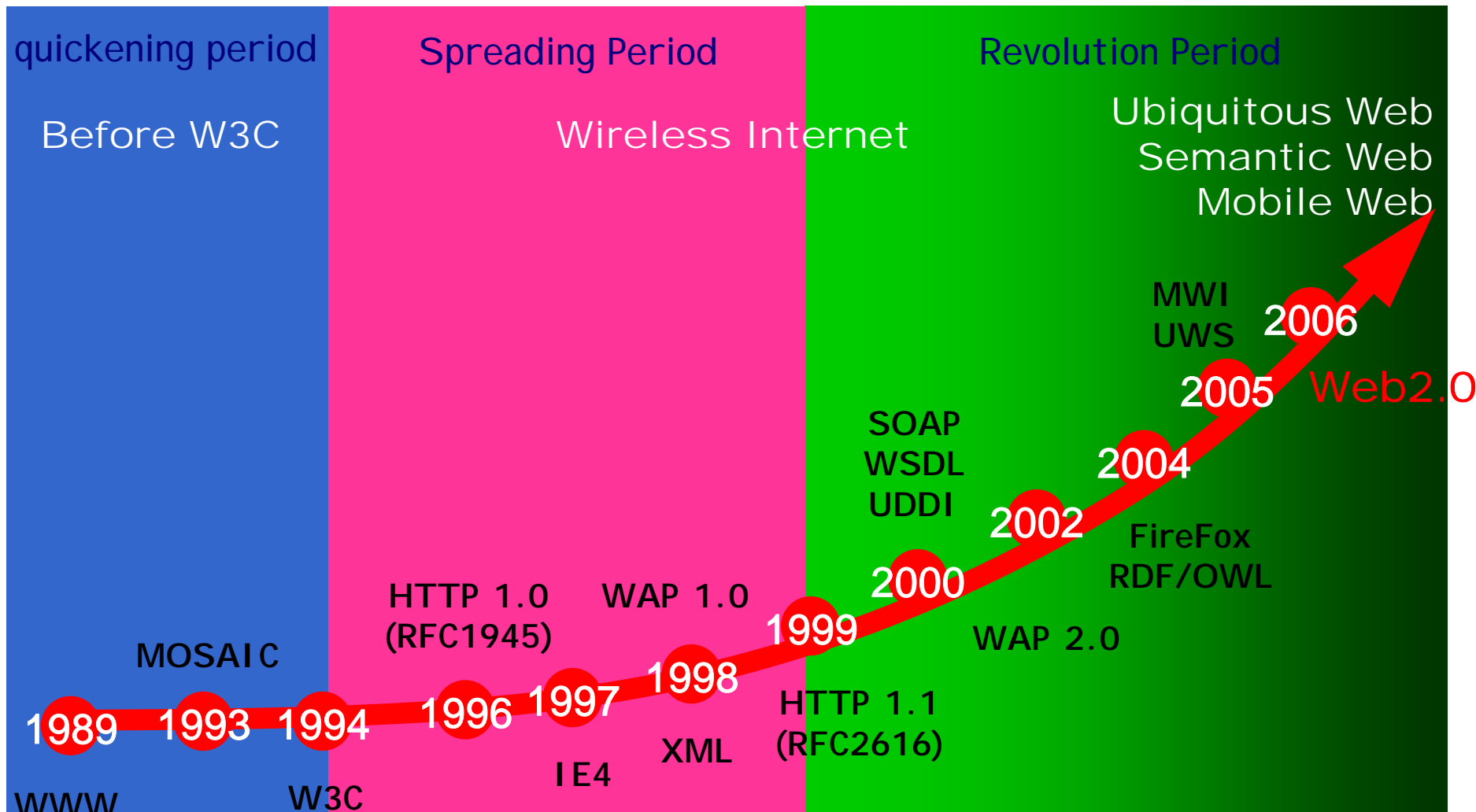
Table of Contents

- Toward Web2.0
- Emerging Platforms and Services
- Technology needed to Protect Contents
 - Digital Rights Management (DRM)
 - Conditional Access System (CAS)
- Conclusion



Toward Web2.0

Web Technology Trends



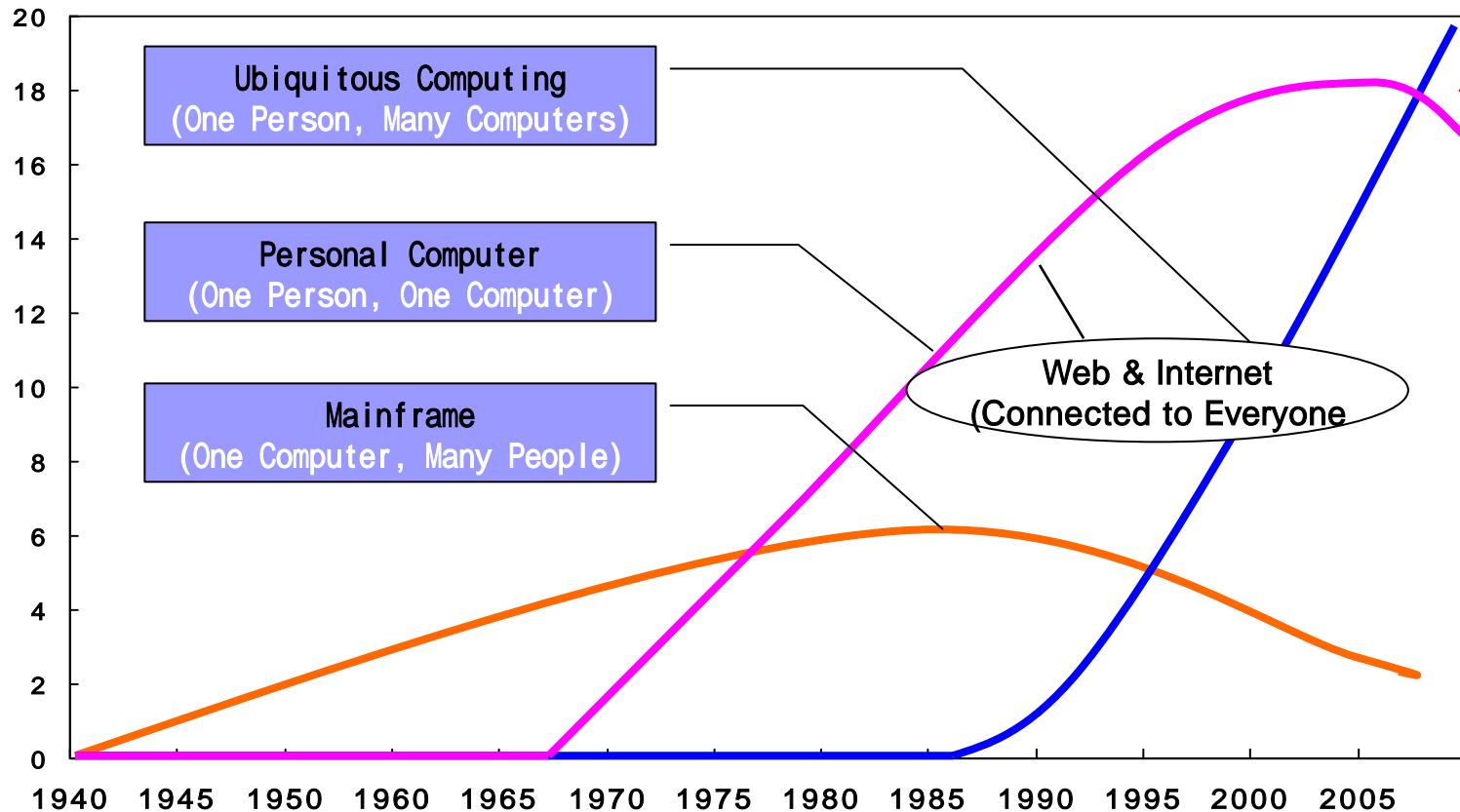
Web2.0 Overview

- Web as Platform
- You control your own contents
- Core Competencies
 - Services, not packaged software
 - Architecture of participation
 - Cost-effective scalability
 - Remixable data source and data transformations
 - Software above the level of a single device
 - Harnessing collective intelligence

IT Revolution Chart

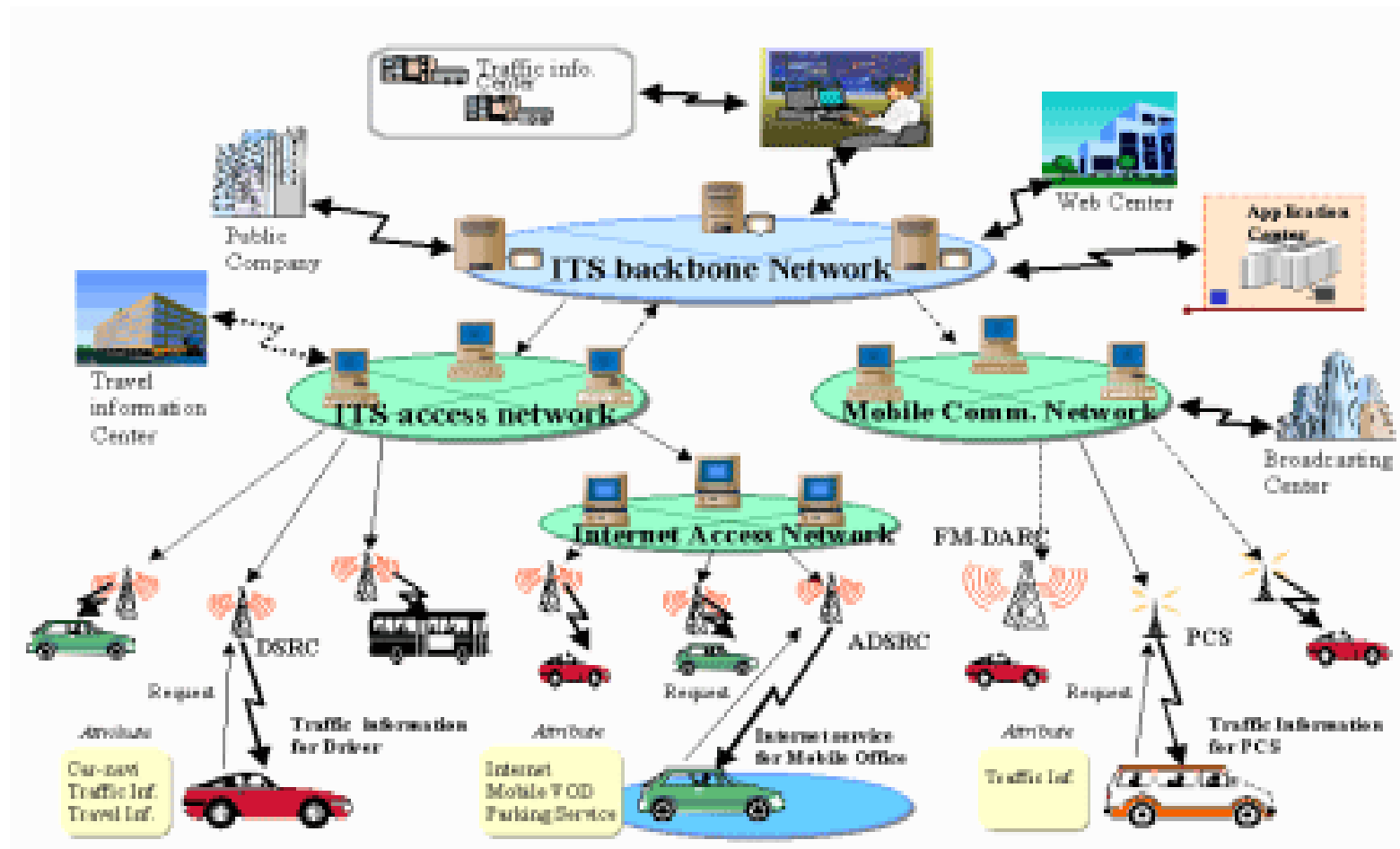
Web2.0 is a new SERVICE INTERFACE to deploy Ubiquitous.

Production Rate

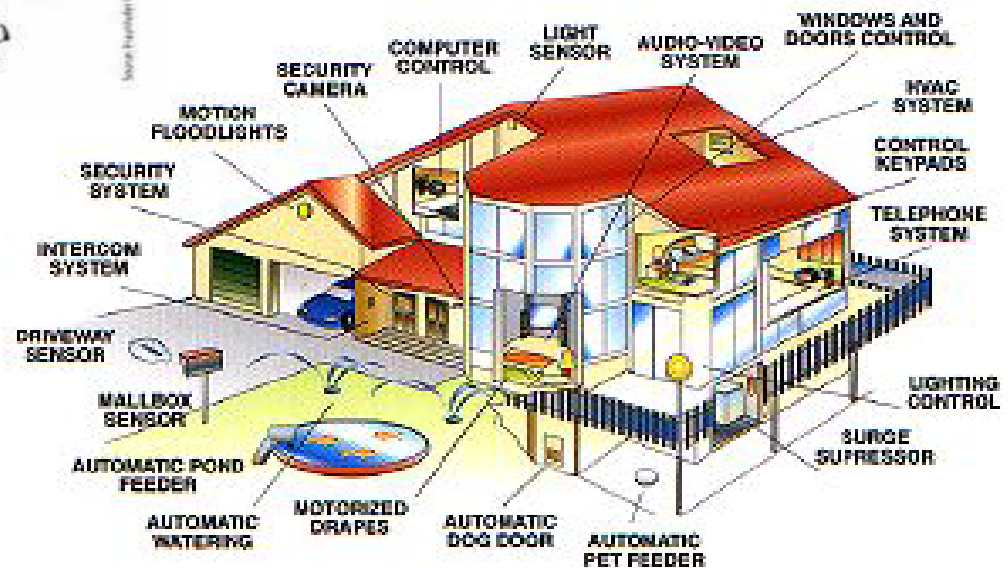


<http://www.ubiq.com/hypertext/weiser>

Internet of THINGS



Future Life & Home



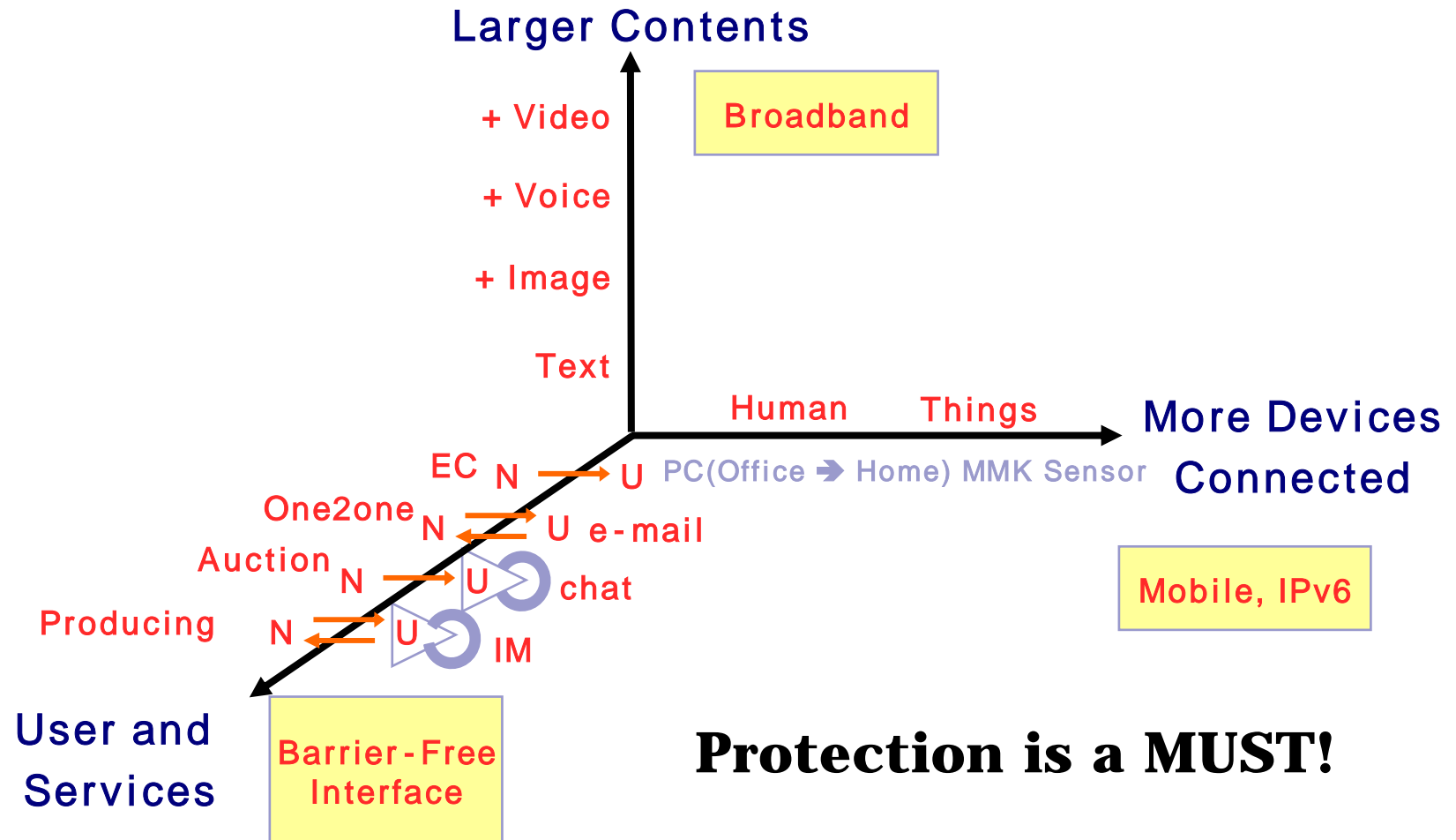


Emerging Platforms and Services

Web2.0 as New Service Creator

- Enhance the use of Web
- One-way to two-way
 - i.e., read-only to read&write
 - Social Computing
 - Prosumer
 - Collective intelligence
 - Long tail (8:2 to 2:8)
- Changes in Media
 - DMB, IPTV, 2-way TV, IPRadio, WiBro
 - Convergence of communications and broadcasting
- UCC
- Mobile Web2.0

Changes in Content Service

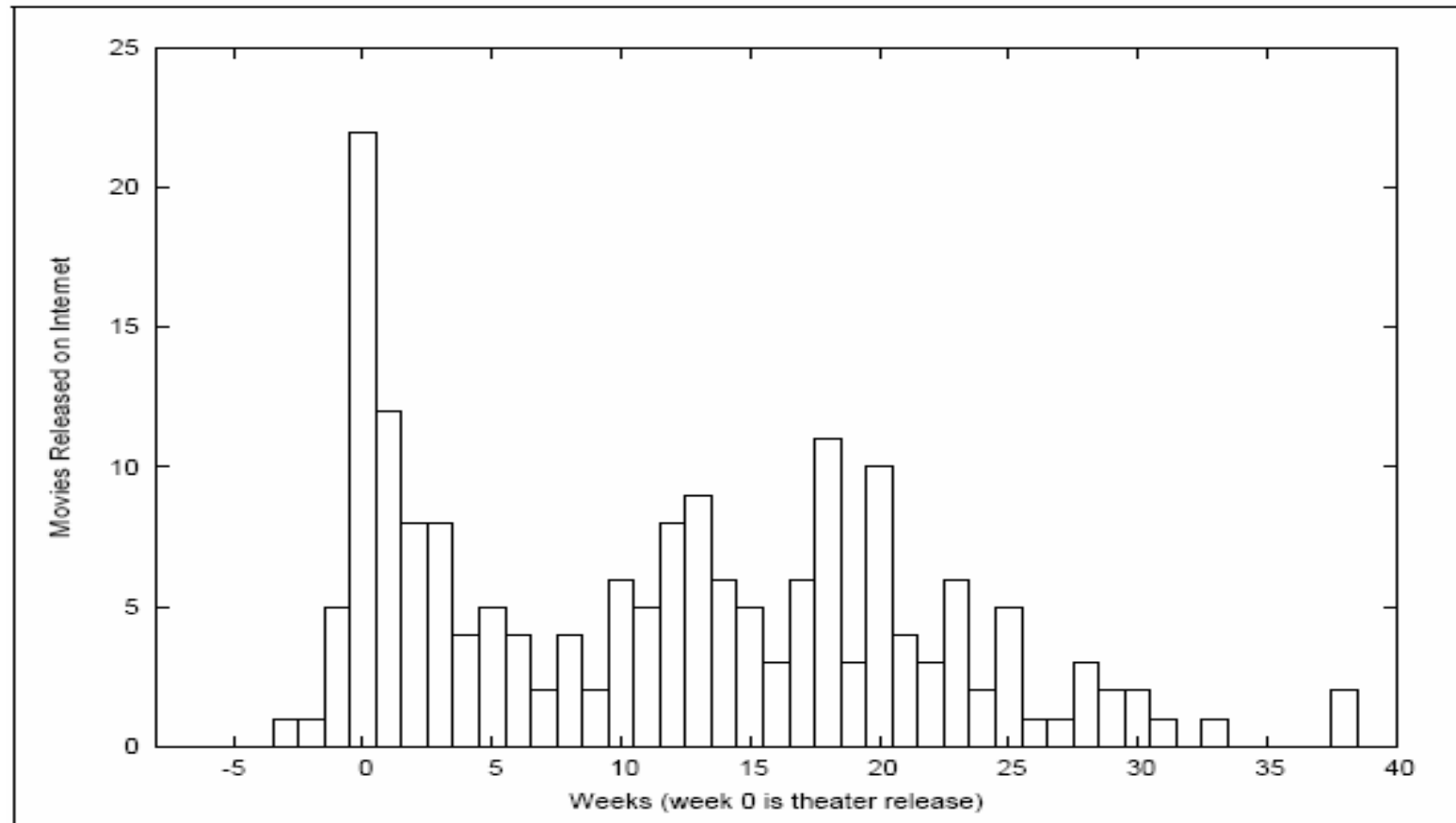




Technology Needed to Protect Contents

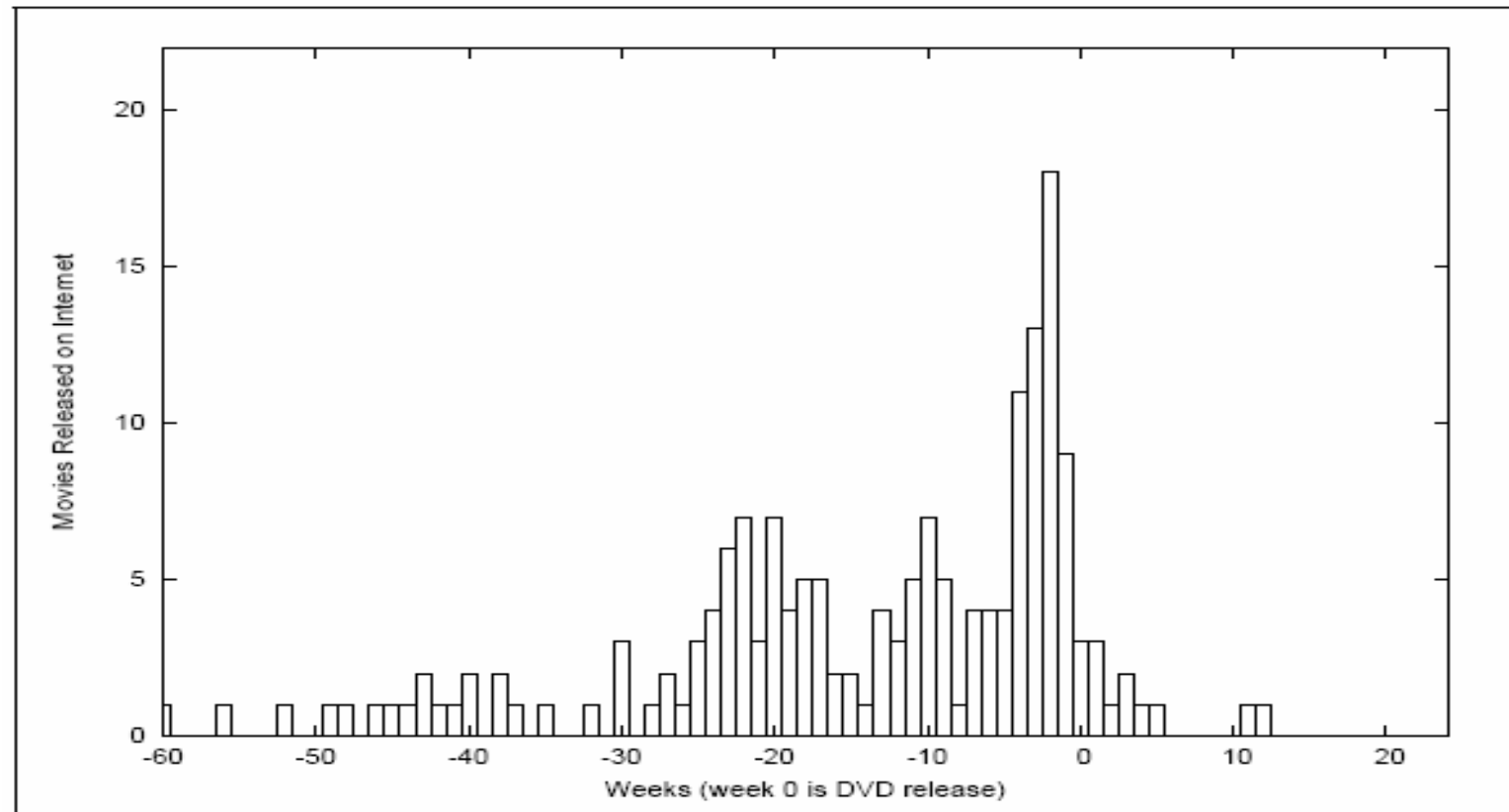
- DRM : Digital Rights Management
- CAS : Conditional Access System

Distribution of theater/Internet release time lags for samples





Distribution of DVD/Internet release time lags for samples



Why DRM?

- Digital World!!
 - More than 60% of contents will be digitized by 2007
- Emerging Digital Content Industry
 - Internet online business, Mobile content service, Digital TV/broadcasting, Home network service
 - World wide : about 35% growth per year
 - Korea : 57% growth per year
 - Web2.0 companies and UCC Industry
 - 47% of Video chips consumed are UCC is USA in 2006
- Digital Convergence makes ALL-in-ONE...
 - Network convergence, Device convergence, Content convergence, Service convergence
 - Society convergence ...
- In Web2.0, multi-right holders, distributed licensing and authentication

Why DRM?

- The necessity for protection of digital contents
 - Features of digital object
 - Possible to copy infinitely
 - Ease of access
 - Possible to reuse and processing
 - Possible to distribute easily and fast
 - Creates illegal copy and distribution problem!
- Drives to a new e-business paradigm
 - Benefits to both service provider and customers
 - “*All-nothing*” to “*all-something-nothing*” service
 - Various pricing model

DRM as a Biz Enabler

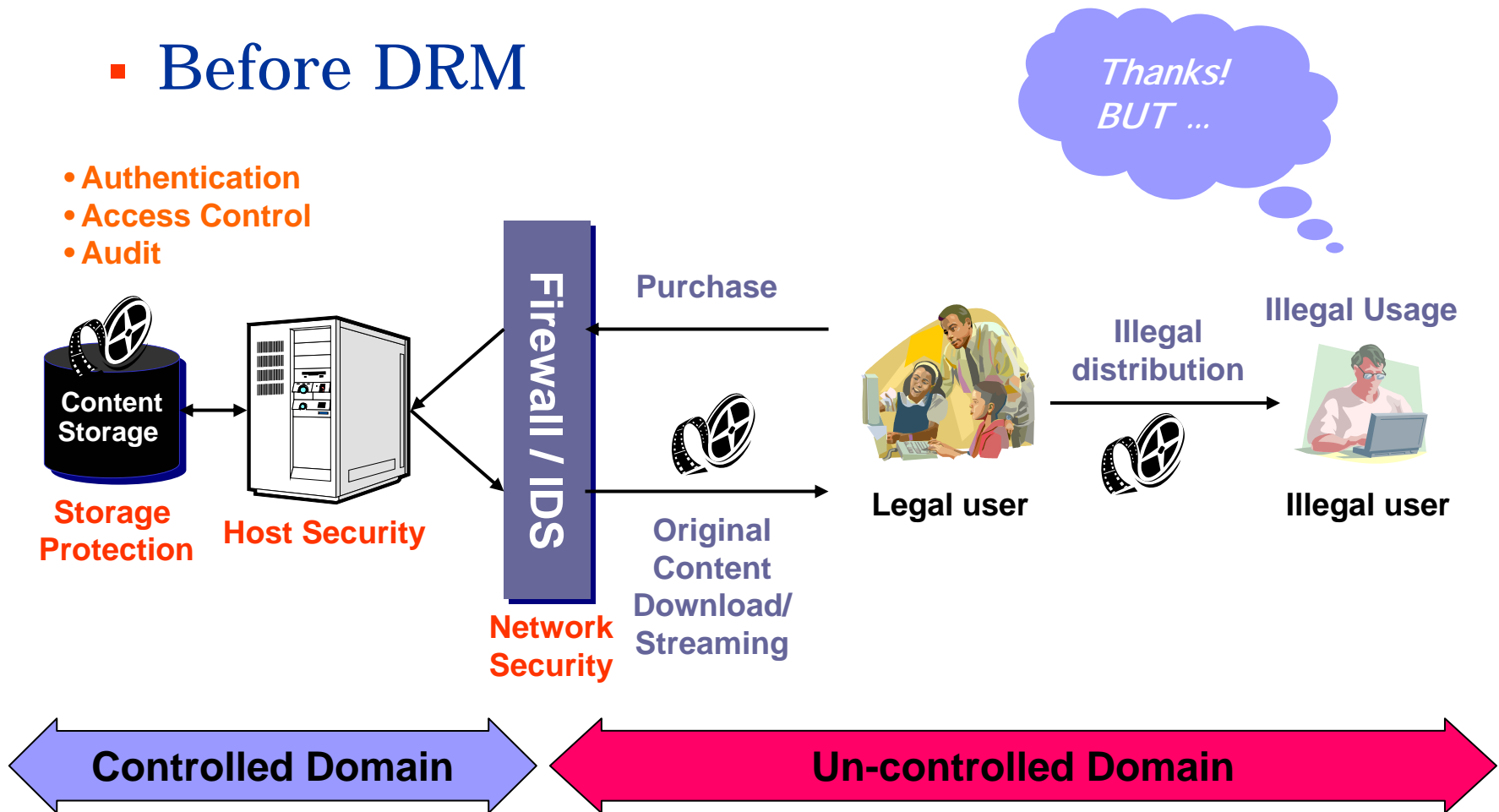
- All-nothing business
 - Buy a *content* in a certain price
 - 50¢ per mp3phone song
- All-something-nothing business
 - Buy a *right* in a variety of prices
 - 50¢ for 3-time play
 - 1.5\$ for 1-week play
 - 2.0\$ ¢ unlimited play
 - 2.5\$ for device transfer option
 - etc.

What is DRM?

- Digital Management of Rights NOT Management of Digital Rights
- 1st generation DRM : copy protection
 - Focused on security and encryption as a means of solving the issue of unauthorized copying
 - Lock the content and limit its distribution to only those who pay
- 2nd generation DRM : usage control
 - Covers the description, identification, trading, protection, monitoring and tracking of all forms of rights usage
- Content-oriented security
 - Content + Protection + Usage rule
 - Provides end-to-end security
 - i.e., persistent protection

What is DRM?

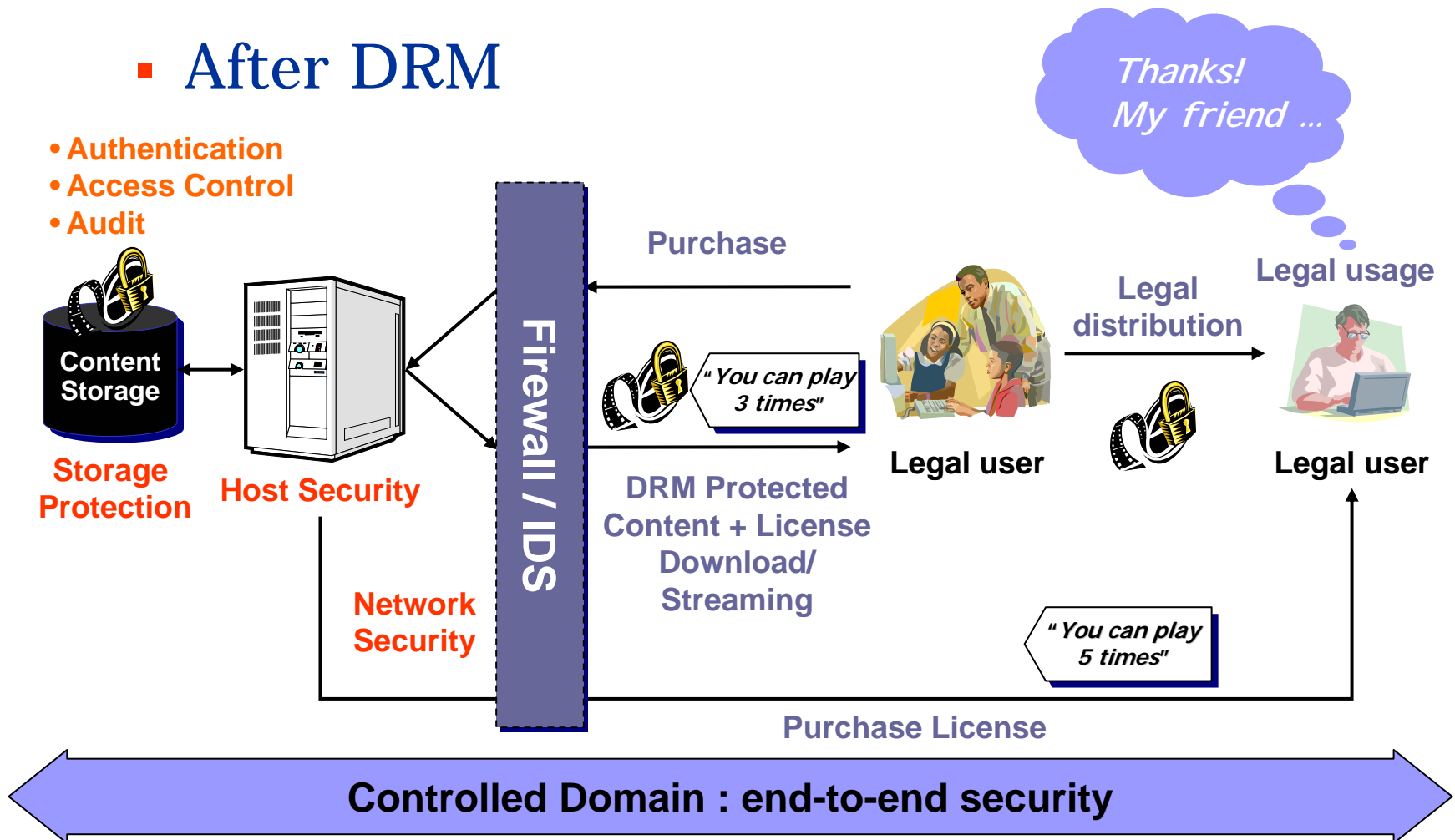
▪ Before DRM



What is DRM?

■ After DRM

- Authentication
- Access Control
- Audit



What is DRM?

"Ten Emerging Technologies That Will Change the World"

The Technology Review Ten

January/February 2001

Brain-Machine Interface	Natural Language Processing
Flexible Transistors	Microphotronics
Data Mining	Untangling Code
Digital Rights Management	Robot Design
Biometrics	Microfluidics

Emerging Technologies That Will Change the World

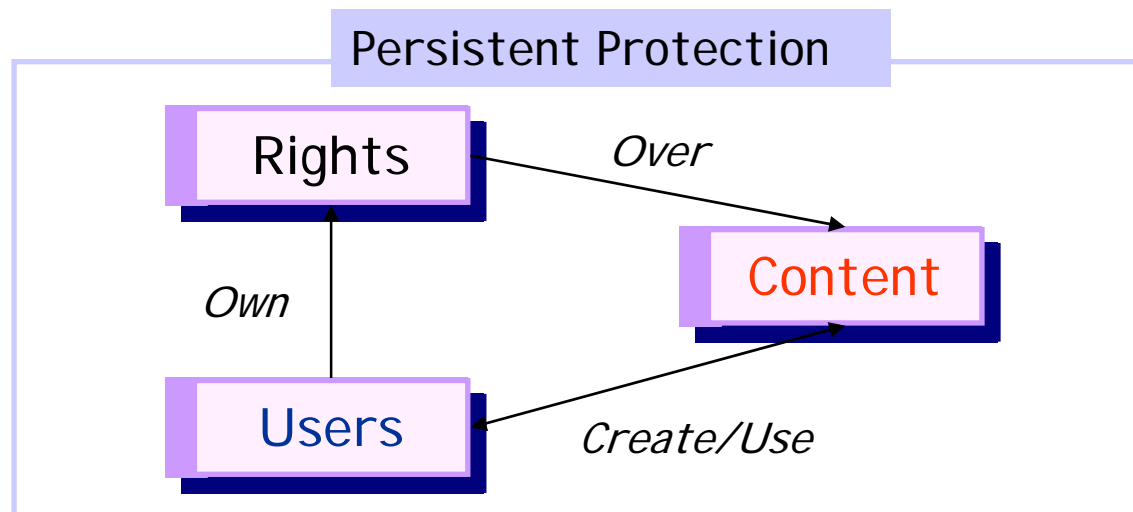
What if you had a crystal ball that foretold the future of technology? Imagine, for example, if you had known in 1990 just how big the Internet was going to be 10 years hence. Sorry, that crystal ball doesn't exist. But in this special issue of Technology Review, we offer you the next best thing: the educated predictions of our editors (made in consultation with some of technology's top experts). We have chosen 10 emerging areas of technology that will soon have a profound impact on the economy and on how we live and work. These advances span information technology, biotechnology and nanotechnology—the core of TR coverage in every issue. All of these areas merit special attention in the decade to come. In each area we've chosen to highlight one innovator who exemplifies the potential and promise of the field. Keep this issue around and see how well our predictions hold up—even without the aid of that crystal ball.



- ✓ Brain-Machine Interfaces
- ✓ Flexible Transistors
- ✓ Data Mining
- ✓ Digital Rights Management
- ✓ Biometrics
- ✓ Natural Language Processing
- ✓ Microphotronics
- ✓ Untangling Code
- ✓ Robot Design
- ✓ Microfluidics

What is DRM?

■ DRM Conceptual Model



- Content: Any type of content at any level of aggregation
- Rights: An expression of the permissions, constraints, and obligations between the users and the content
- Users : Any type of user from a rights holder to an end-user

What is DRM?

■ Benefits of DRM

- Rights holder or e-business side
 - Profit model according to legal distribution of digital contents
 - Proliferation of Internet market or e-Business environment
- Consumer side
 - Possible to purchase easily
 - Possible to choose as one needed
 - Possible to use on-demand

Technology needed for DRM?

■ Protection

- Cryptography
- Key Management
- Secure DB
- Authentication
- Identification
- Watermarking
- Fingerprinting
- Temper Resistance
- Rights Enforcement

■ Language

- Metadata Expression
- Rights Expression
- Content Identifier

■ Key Management

- Symmetric(private) and Asymmetric(public) Cryptosystem
- Hash Algorithm, Digital Signature
- Authentication, Key Distribution, Key Management System

■ Enforcement

- ODRL (Open Digital Rights Language): OMA DRM Rights Expression
- XrML (eXtensible rights Markup Language): MPEG-21 IPMP

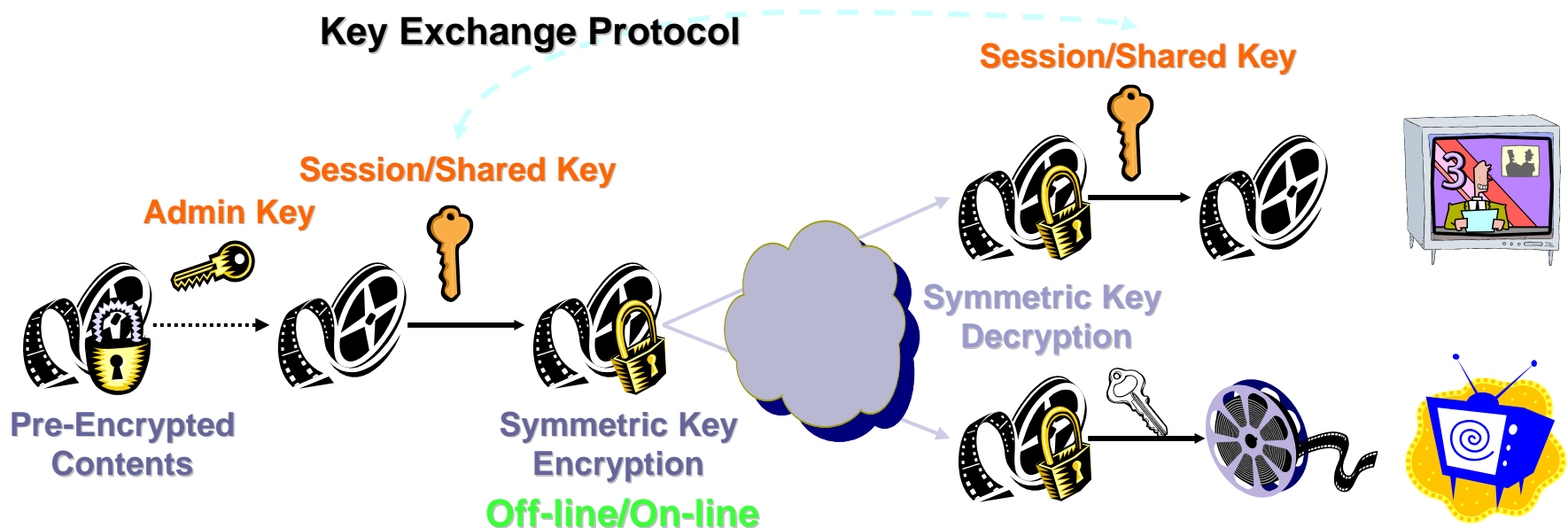
■ Trading

- Billing
- Transaction Reporting (Usage monitoring)
- Clearing House
- Policy Management
- PKI
- Secure Communications

Technology needed for DRM?

■ Key Management

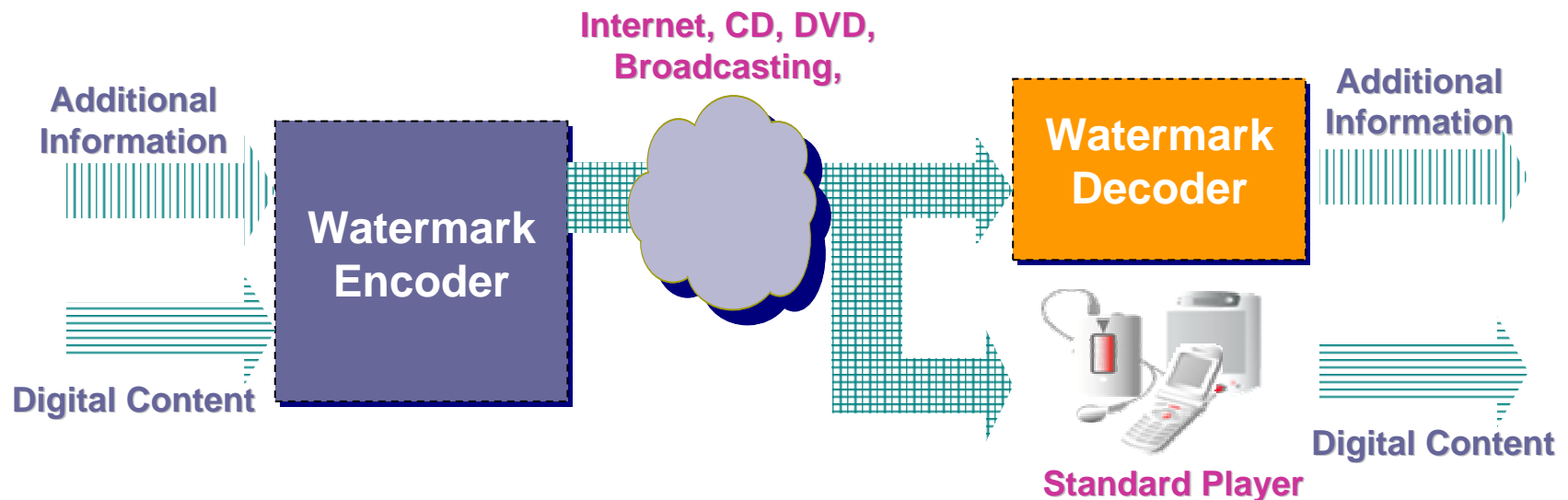
- Symmetric(private) and Asymmetric(public) Cryptosystem
- Hash Algorithm, Digital Signature
- Authentication, Key Distribution, Key Management System



Technology needed for DRM?

■ Watermarking & Finger printing

- Direct embedding of additional information into any digital content including text, image, audio and video
- Information about the origin & recipient (Copyright...)
- No prevention on Copy but allow Tracking



Technology needed for DRM?

■ Right Expression

- A Right Expression Language is a type of policy authorization language through digital value-chain players
- ODRL(Open Digital Rights Language): OMA DRM
- XrML(eXtensible rights Markup Language): MPEG 21

```
<license>
  <grant>
    <cx:print/>
    <cx:digitalWork>
      <cx:locator>
        <nonSecureIndirect URI="http://www.xrml.org/sampleBook.spd"/>
      </cx:locator>
    </cx:digitalWork>
  </grant>
</license>
```

XrML example: "**Anyone** can **print** a book located at <http://www.xrml.com/sampleBook.spd>"

Technology needed for DRM?

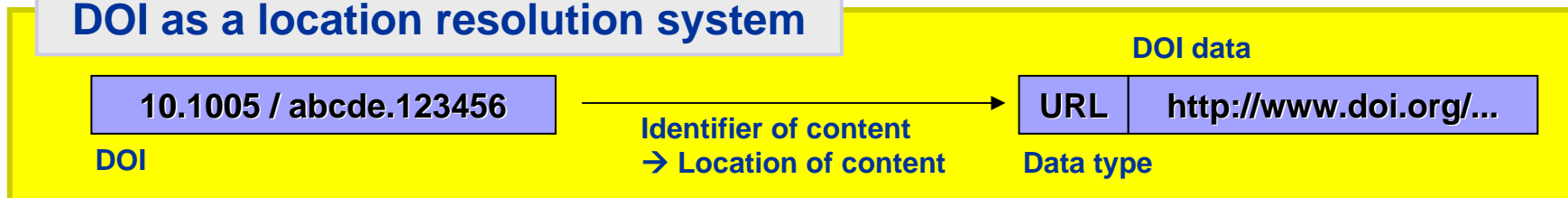
■ Content Identifier

- A unique identifier of a piece of digital content
- Analogue domain: ISBN, ISSN, ISRN, ISMN, ISRC, etc
- Digital domain: DOI, CID, MPEG-21 DII&D, RFID, etc

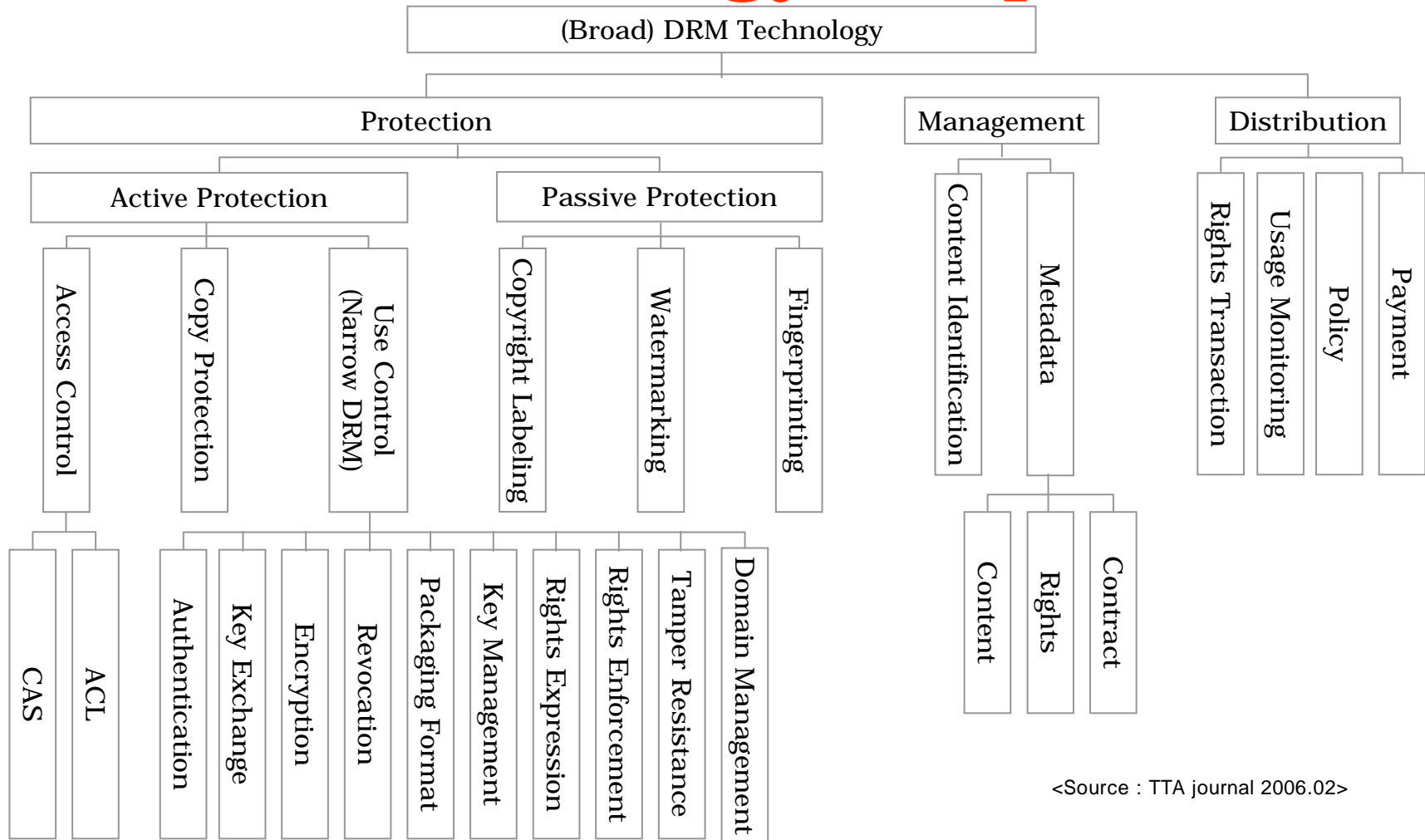
10.1005 / abcde.123456

- **DOI suffix**: Item identifier; any format that the Registrant chooses.
- **DOI prefix(10.1005)**: DOI Registrant String that is assigned to an organization that wishes to register DOIs.
- **DOI(10)**: DOI Registration Agency String that distinguish a DOI from any other implementation of the Handle System.

DOI as a location resolution system



DRM Technology Map



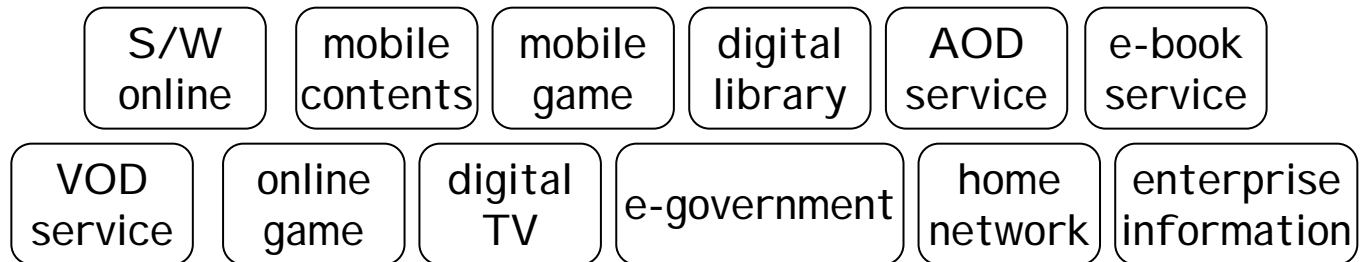
<Source : TTA journal 2006.02>

DRM Applications

User Devices



Commerce & Applications



Contents

music, movie, e-book, photo, document, S/W, game

Communication

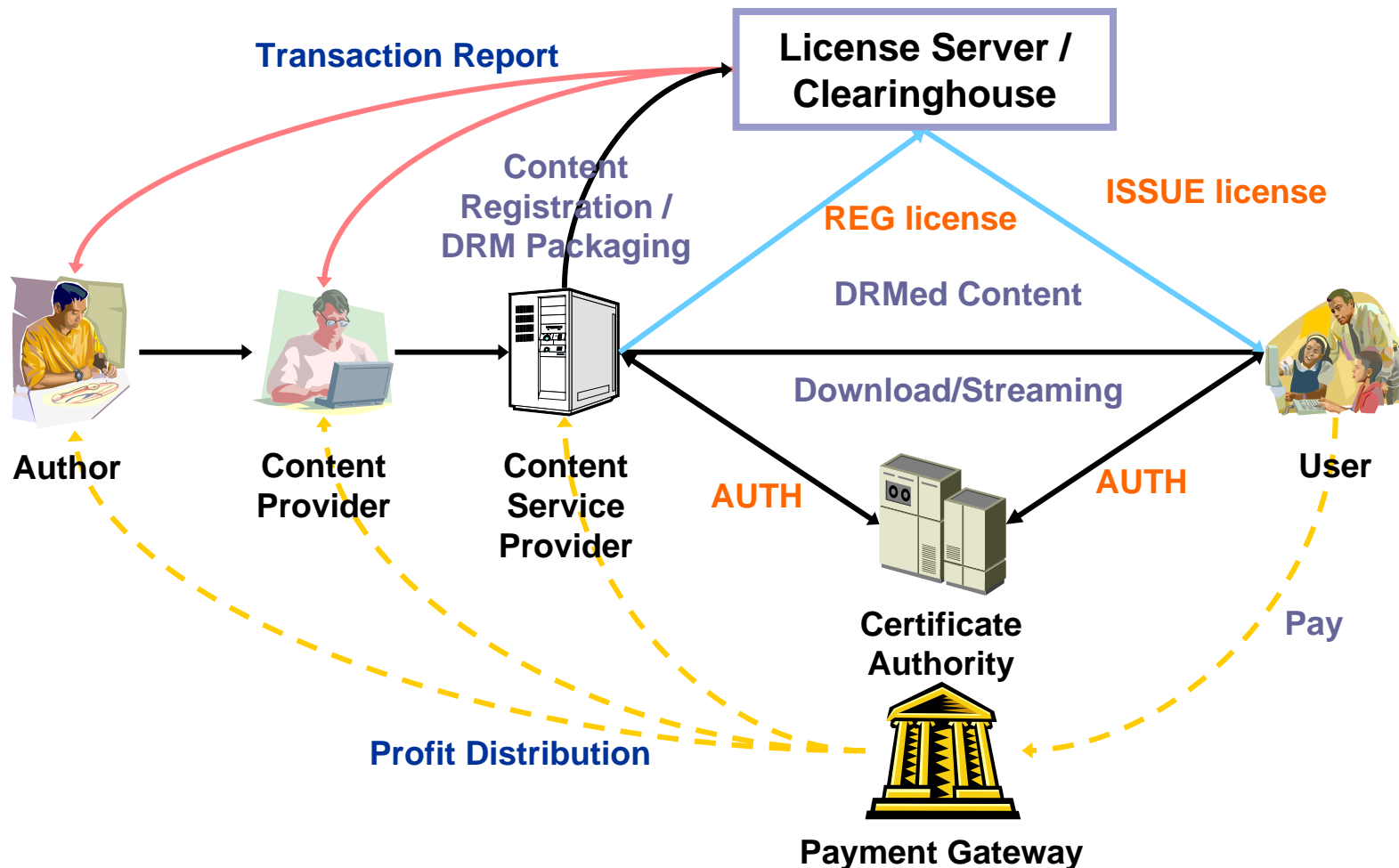
Wired/Wireless Internet

Mobile Communications

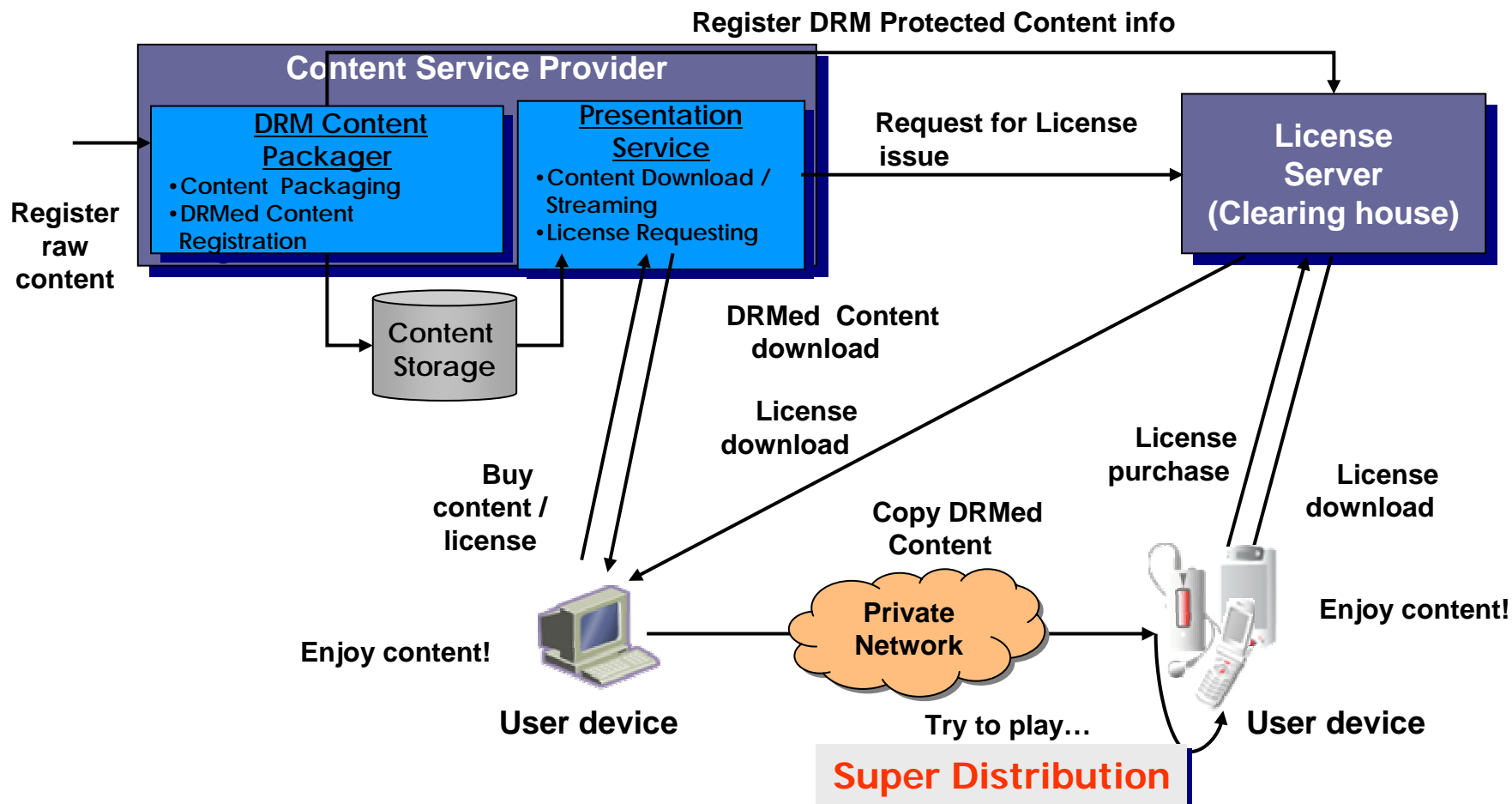
Digital Broadcasting

Satellite Broadcasting

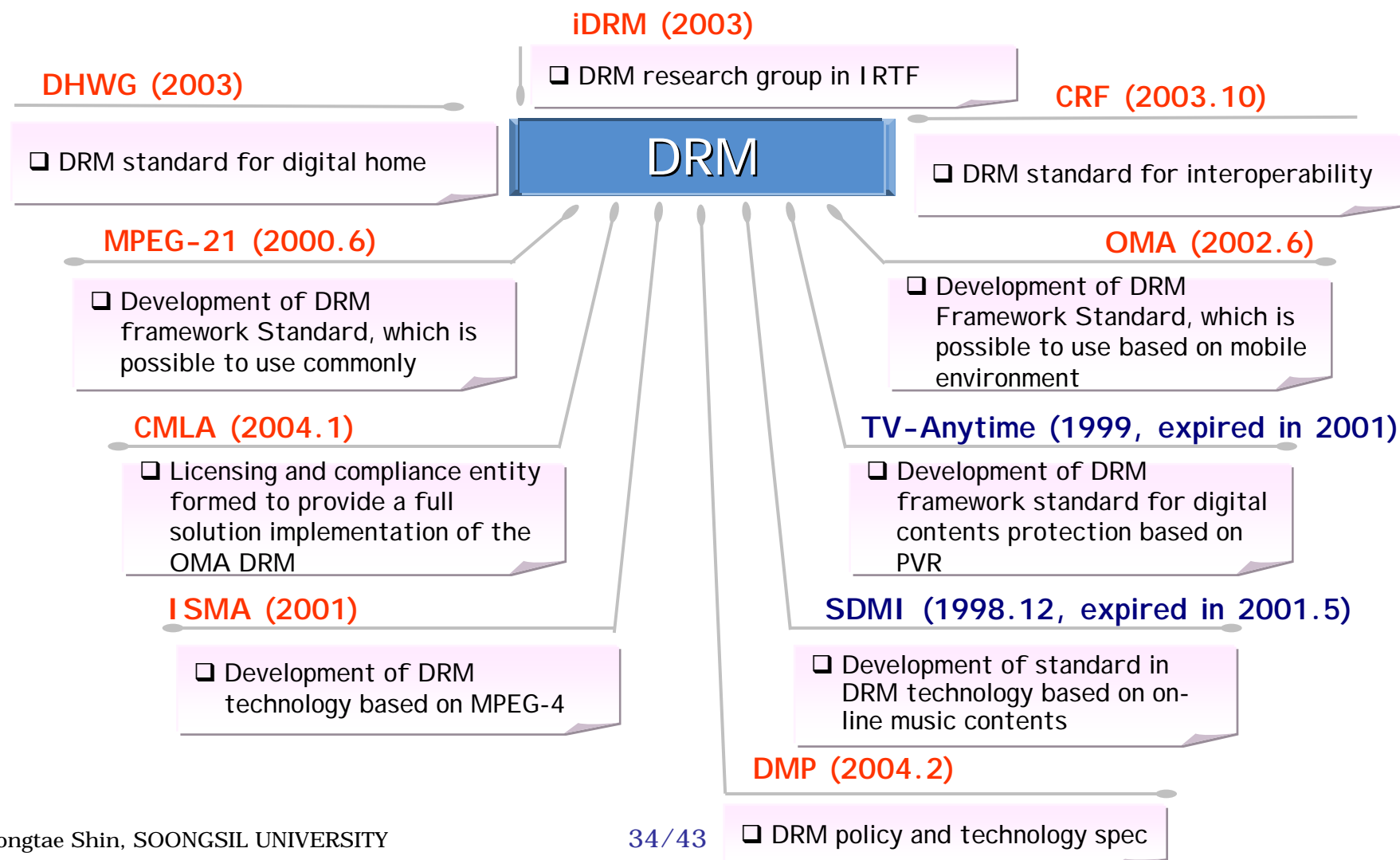
Basic DRM Service Flow (1)



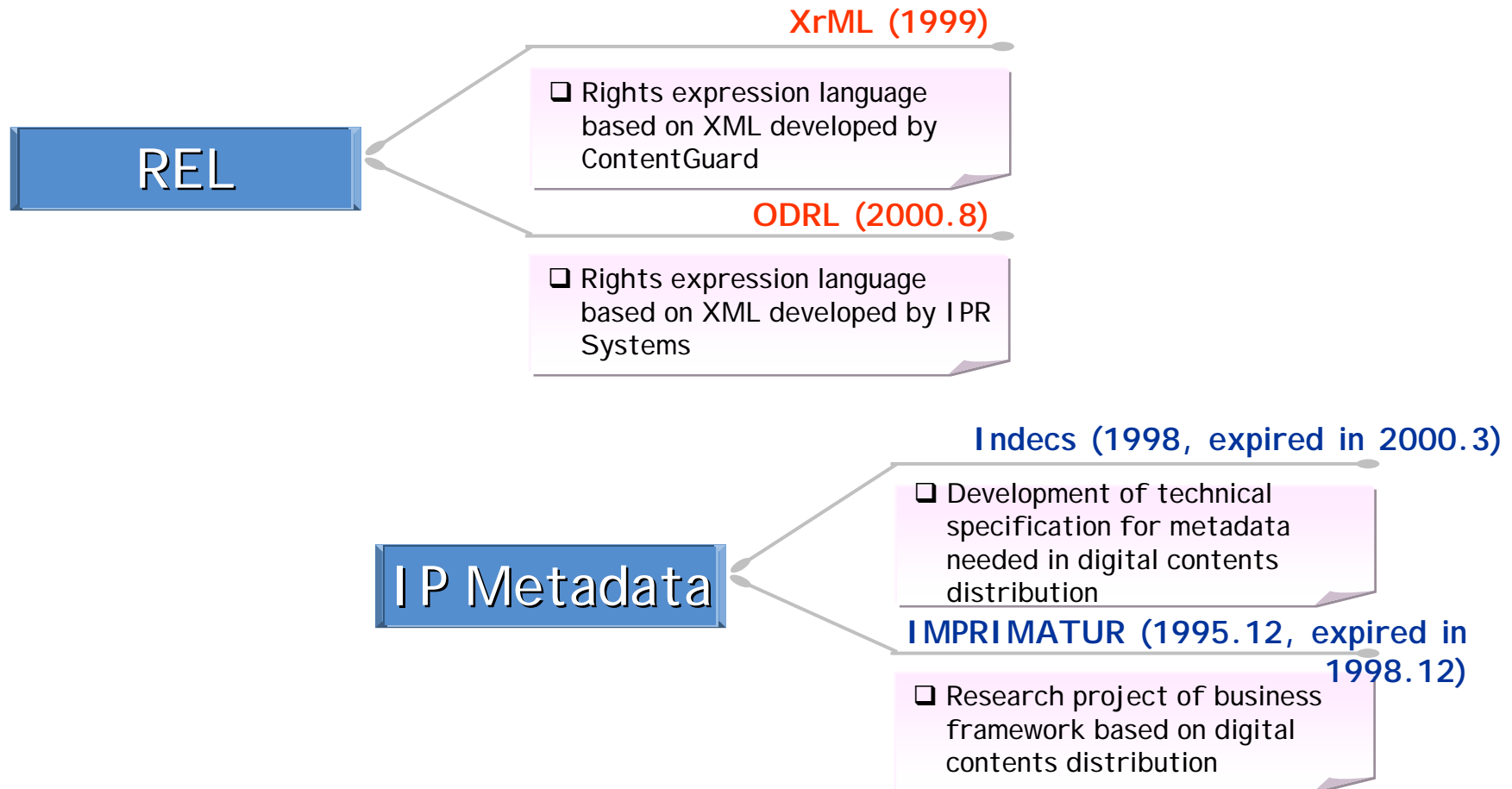
Basic DRM Service Flow (2)



DRM Standard Activity (1)

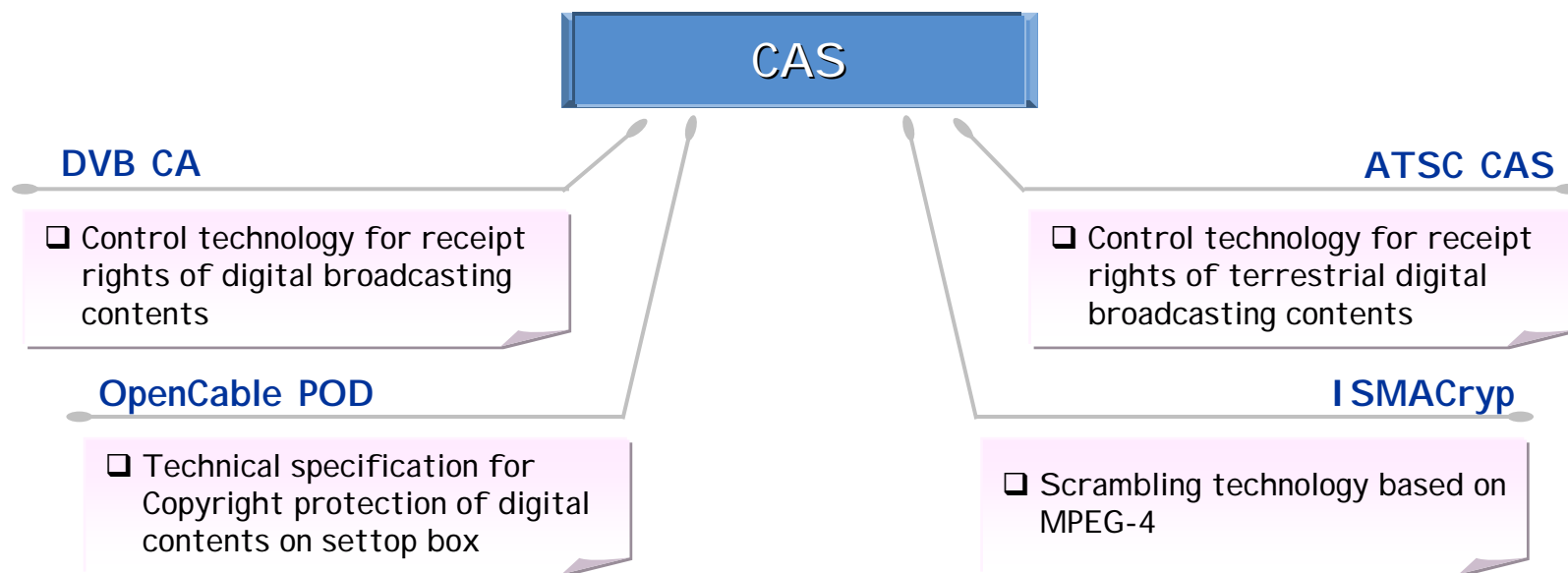


DRM Standard Activity (2)

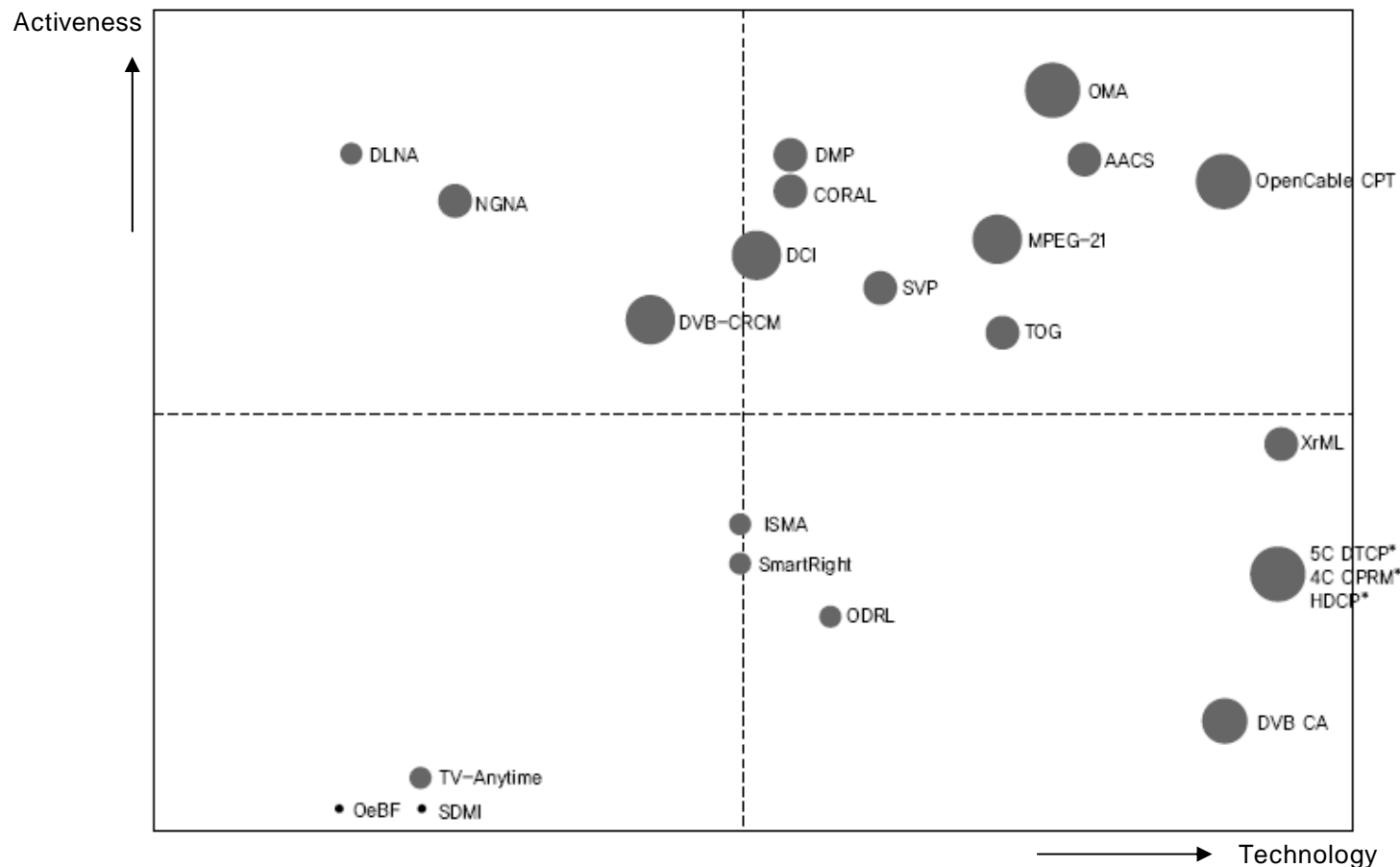


DRM Standard Activity (3)

■ CAS (Conditional Access System) – as DRM subset

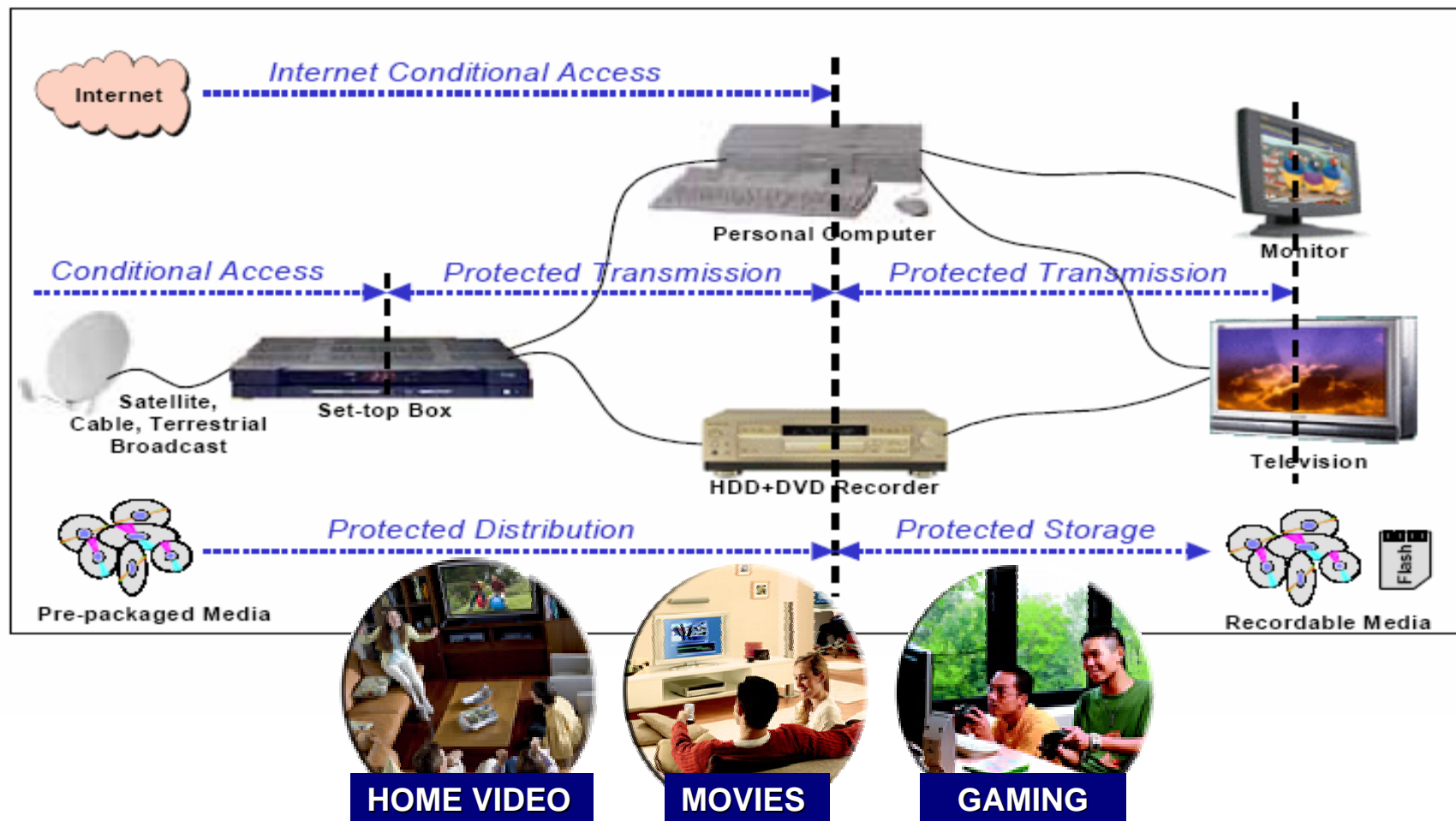


DRM Standard Activity (4)

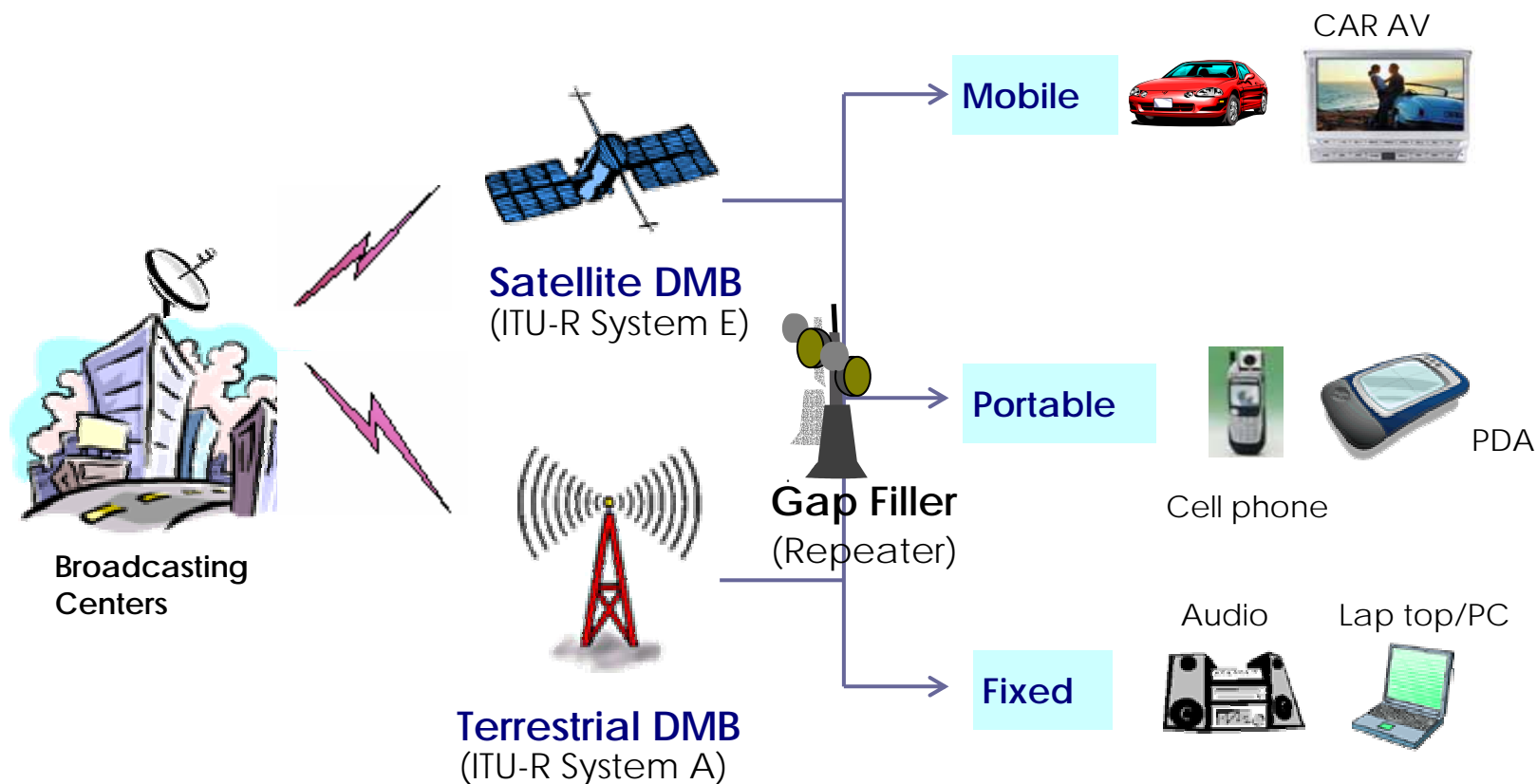


<Source : TTA journal 2006.02>

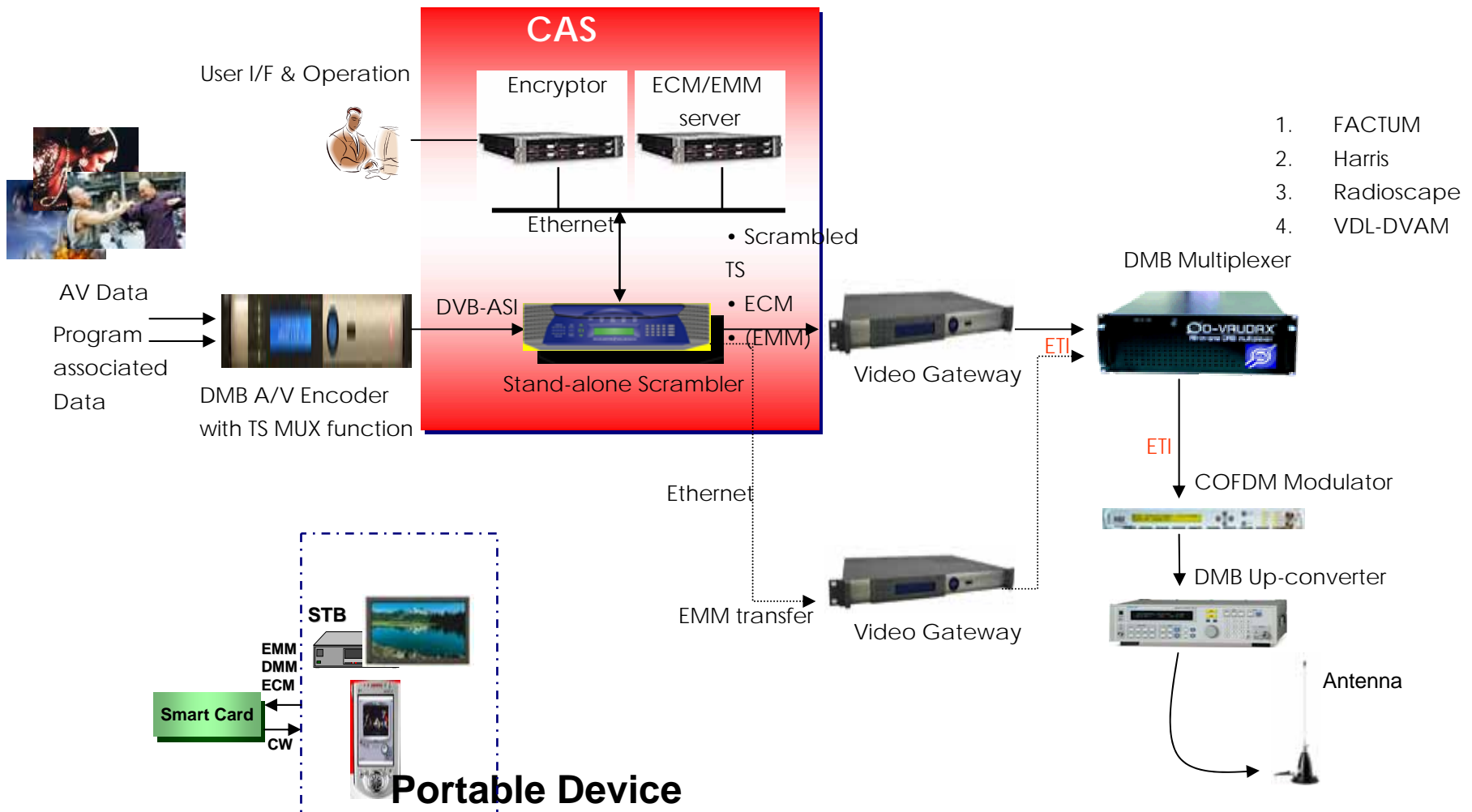
Use of DRM in Digital Home



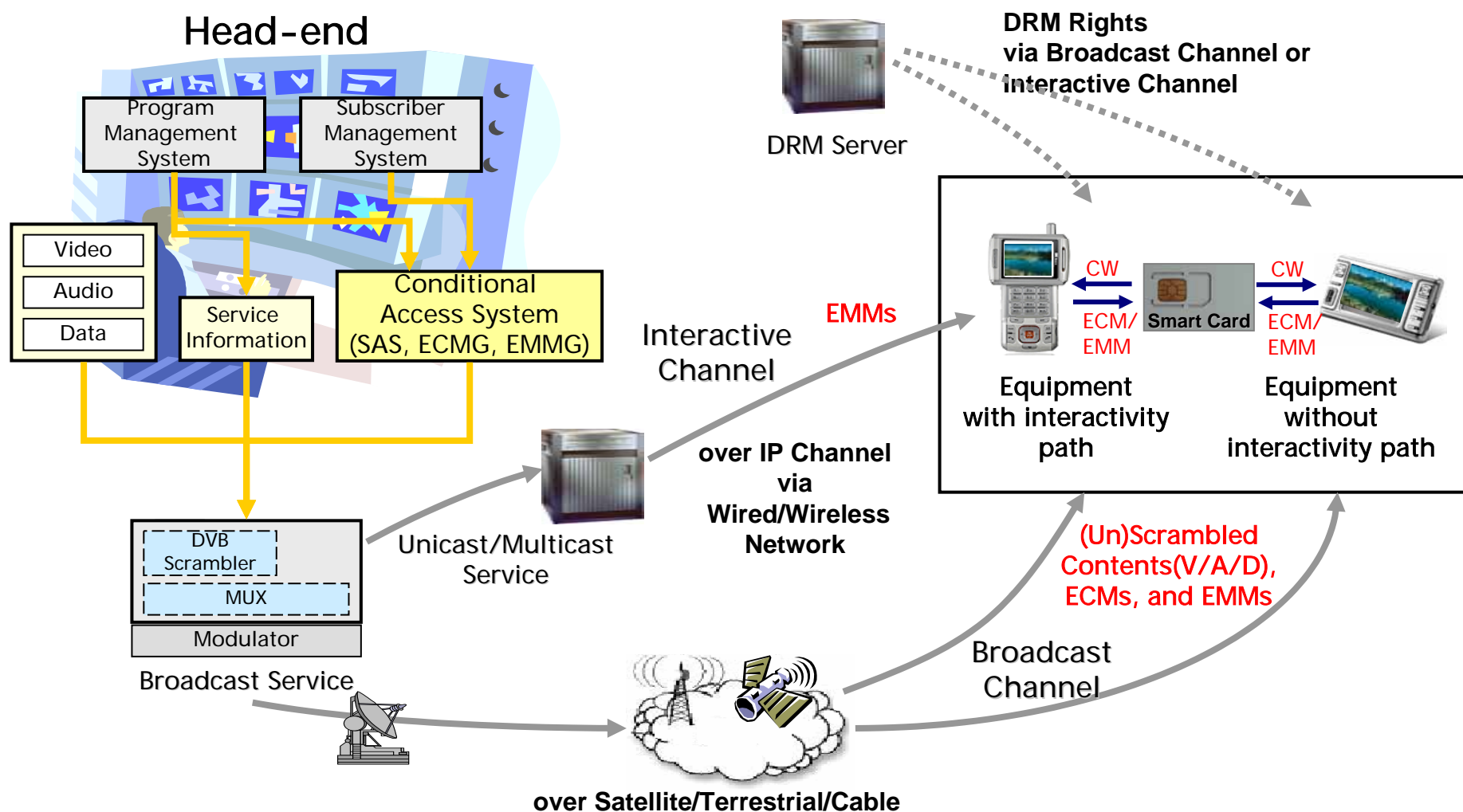
Digital Multimedia Broadcasting (DMB)



CAS



Use of DRM+CAS in IPTV



Conclusion

■ After 2007

- Cross-Platform : Proprietary DRM → Interoperable DRM
- Multi-level Rights
- Combat piracy (defensive) to New Business Model (offensive)
 - Pricing as you use
- Merge of DRM and CAS technology
- Distributed licensing and authentication
- Miss use of digital contents
- Standardization : “*de jure*” vs. “*de facto*”
- DRM for Web 2.0 Platform is here but NOT yet
 - Need to define but very complicate

Discussion?

*A journey of a thousand mile
begins with a single step*

...

We just began...