Sistemi Collaborativi e di Protezione (SCP)

Corso di Laurea in Ingegneria

Part 1a (2013) – ***sistemi di protezione***

Prof. Paolo Nesi

Department of Information Engineering

University of Florence

Via S. Marta 3, 50139, Firenze, Italy

tel: +39-055-4796523, fax: +39-055-4796363

DISIT Lab

http://www.disit.dinfo.unifi.it/

paolo.nesi@unifi.it http://www.dsi.unifi.it/~nesi

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Example of Microsoft Windows Media

Content Services Aspects

- **Scalability**:
  - From few to millions of transactions per hours
  - From few to millions of subscribed users
  - From few to millions of different content items
- **Availability and**
  - High reliability of the service, no or few interruptions
- **Accessibility:**
  - Accessibility of the service, broadcast/cellular coverage
  - User accessibility aspects
- ***Other aspects discussed in the course***
  - ***Privacy of the customers***
  - ***Intellectually property management and protection, IPMP***
  - ***Multichannel distribution***
  - ***Interoperability of content on devices***

Architectures

A. Content/good *distribution*

B. Content/good *production and management*

C. Content/good *Protection and Security*

D. Content/good *Modeling and Processing*

A) Content distribution models

- **Download, P2P download, …:**
  - 1:N: one sender N receivers/users
  - N copies, propagation of seeding/sources sites
  - Network costs from O(N) → O(1)
- **Broadcast Streaming (e.g., MPEG2-TS)**:
  - 1:N: one sender N receivers/users
  - N users that play the same content at the same time
  - Network costs O(1)
  - DVB-T, DVB-S, DVB-H, DVB-SH
- **VOD, progressive download, P2P streaming/progressive:**
  - 1:1 stream processes, one sender process for each receiver/user, that play the same content a different time
  - Network costs O(N) -→ may be going to O(1) if ….

B) Content production and management

- Content Processing:
  - adaptation,
  - production,
  - formatting,
  - packing, etc.

- Scalability GRID for content processing:
  - UGC management
  - Indexing for search,
  - production on demand,
  - massive production
  - transcoding

C) Content Protection and Security, aspects

- CP: Copy Protection
- CAS: Conditional Access Systems
- DRM: Digital Rights Management
- Based on technologies such as
  - **Certification** of: content, users, devices, etc.
  - **Authentication** of: users, actors, devices, etc.
  - **Signature** of: content, DLL, EXE, ..
  - **Identification** of: content, users, devices, etc.
  - **Watermark** and **fingerprint** of: content, descriptors, ...any....
  - **Coding** and Encryption of: .....everything.....

D) Content Modeling and Processing

- **The content model impacts on:**
  - **Format: XML, binary**
  - **Content gathering and ingestion**
  - **Production and production-process definition**
    - Workflow Management systems
    - Cooperative work
  - **CMS, DMS, Content/Media Management Systems**
    - Database management systems
    - query support, distributed queries, etc.
  - **Content description for**
    - Search, classification/indexing, retrieval
  - **Content protection for enforcing respect of**
    - IPR: CAS, DRM, ...
  - **programme/guide production**
    - EPG, GuidePlus, ShowView, TVAnytime, etc.

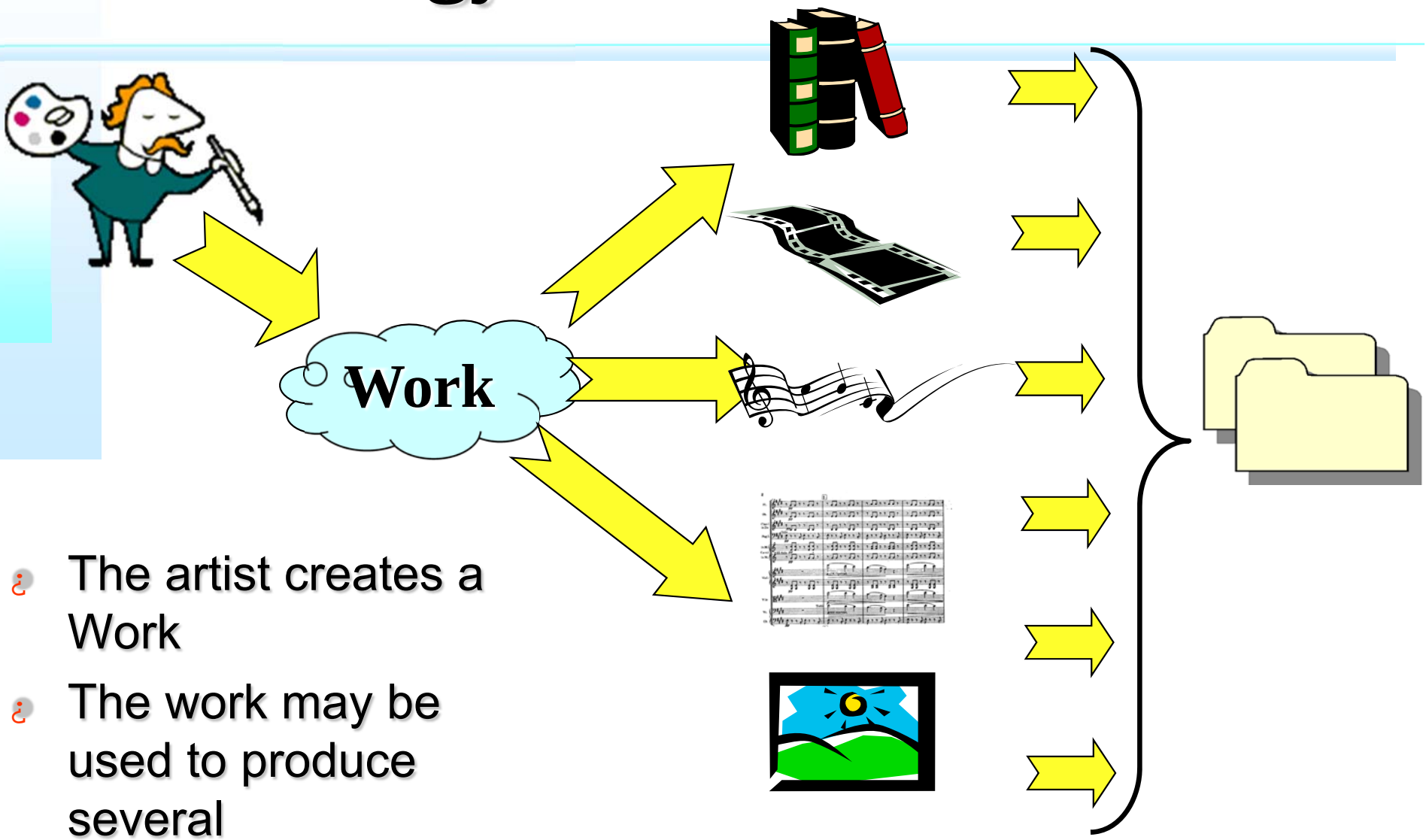
Acronyms and Definitions

- IPR: Intellectually Property Right
- CA: Certification Authority, chain of certificates
- TPM: Technological Protection Model
- FTA: Fault Tolerance Architectures
- VOD: video on demand
- PPP: pay per play
- PPV: pay per view
- VOIP: voice over IP
- TS: Transport Stream
- EPG: electronic program guide
- Etc.

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Example of Microsoft Windows Media

Terminology



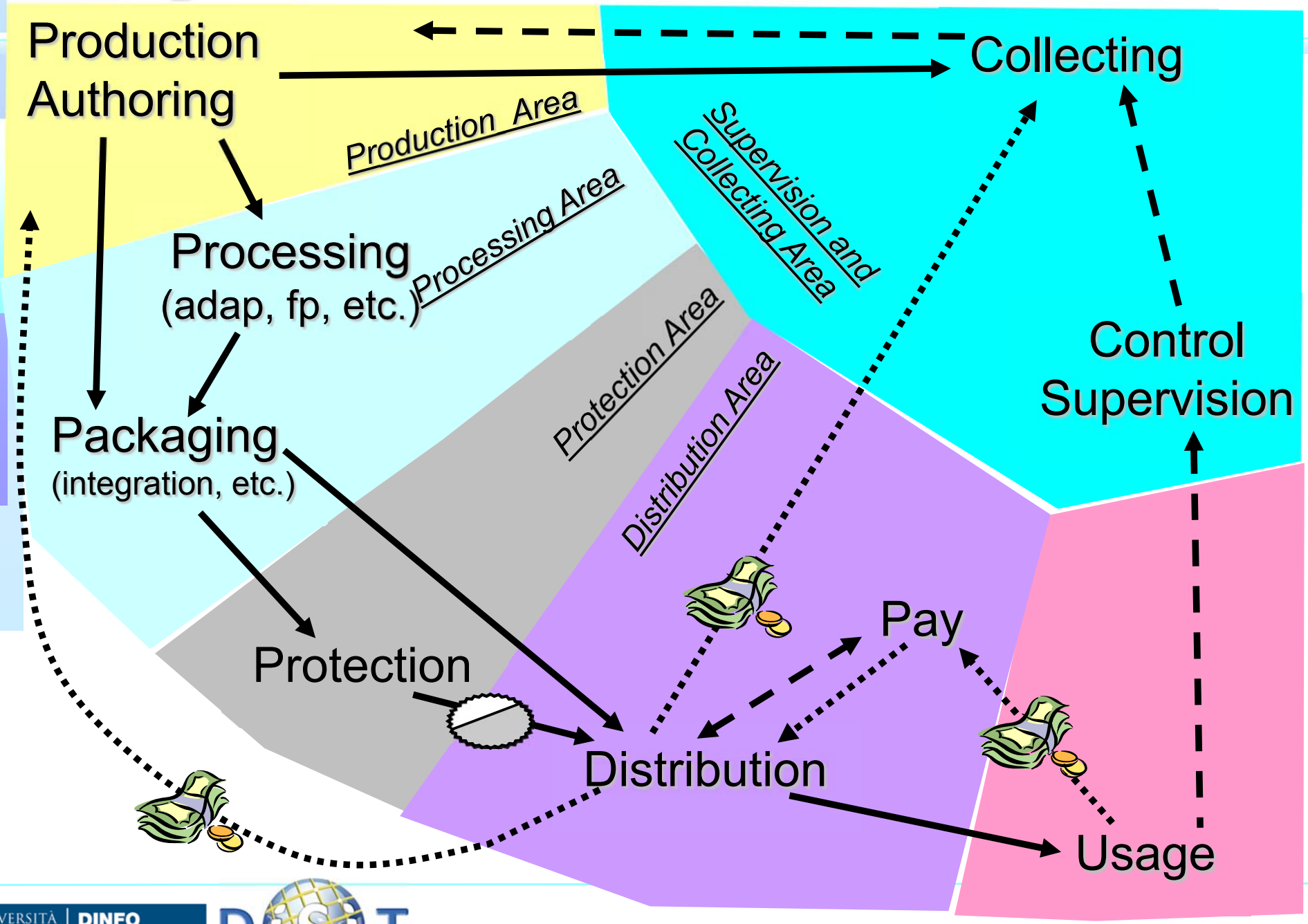
- The artist creates a Work
- The work may be used to produce several manifestations

Manifestations **Resources**

Some Actors of the value chain, “definitions”

- **Right/Content Owners**, artists, etc.
  - who has the rights on the initial work, non digital
- **Content Producers**, Publishers
  - Who is producing the manifestations of the work, define its rights, may produce the digital resources or not, etc.
- **Content Integrators**, aggregators
  - Who is Integration/aggregation: resources + metadata ++ , added value, etc., may be add other rights, etc.
- **Content Distributors**,
  - Who is distributing digital content
- **Final Users**,
  - Who is using (or should use) the digital content on behalf of the rights obtained
- **Users**, in general
  - All the above actors that use in some way content on the basis of the rights obtained

Simplified Traditional value chain



Traditional value chain Issues

- **Producers**
  - Does not protected the content
- **Protection** performed before production
  - By the distributor
  - By a specialized third party
- **Since B2B areas** are (production, licensing, integration, etc.):
  - Considered trusted
  - Based on paper contracts
  - Contracts are produced on the basis of a limited and not standard terminology, so that they are not easy interpreted and transported on other media, or channels, etc.
  - Recently in Digital with XML, with DDEX

Traditional value chain Issues

- **Monitoring about what is done** on the content rights on the:
  - Authors, integrators and producers cannot verify what has been sold, they may ask to each single
    - Distributor (via reports, see DDEX, MPEG-21, etc.)
      - managing one or more channel
    - Collecting Society, e.g.: SIAE, SGAE, ...
      - Managing one or more territorial area and rights type
    - Etc.
- **The distributors**:
  - Controls the selling of content depending on the business model:
    - Pay per play, monthly subscription, etc.
  - In some cases do not control/verify the exploitation of each single right but only the access to the content.
    - High complexity of keeping under control all the user actions, user behaviour, action logs, event reporting, etc.

E-Commerce Services Aspects

- **Business Model (who is going to pay, which is the flow of money)**
  - how/who/when to give money for some goods/service ?
  - How is created the revenue stream ?
  - Subscription, Pay per play, etc..
- **Transaction Models**
  - technical aspects of business transaction
    - Security: certification, smartcards, etc.
    - Mission Critical Applications
- **Subproblems: payment solution**
  - Accounting: for example in phone bill
  - Banking: for example on your bank account
  - Micropayments: for direct payment, small amounts
  - Model: prepaid or post paid
  - Cards: Prepaid cards, Credit Card, temp cards, etc.

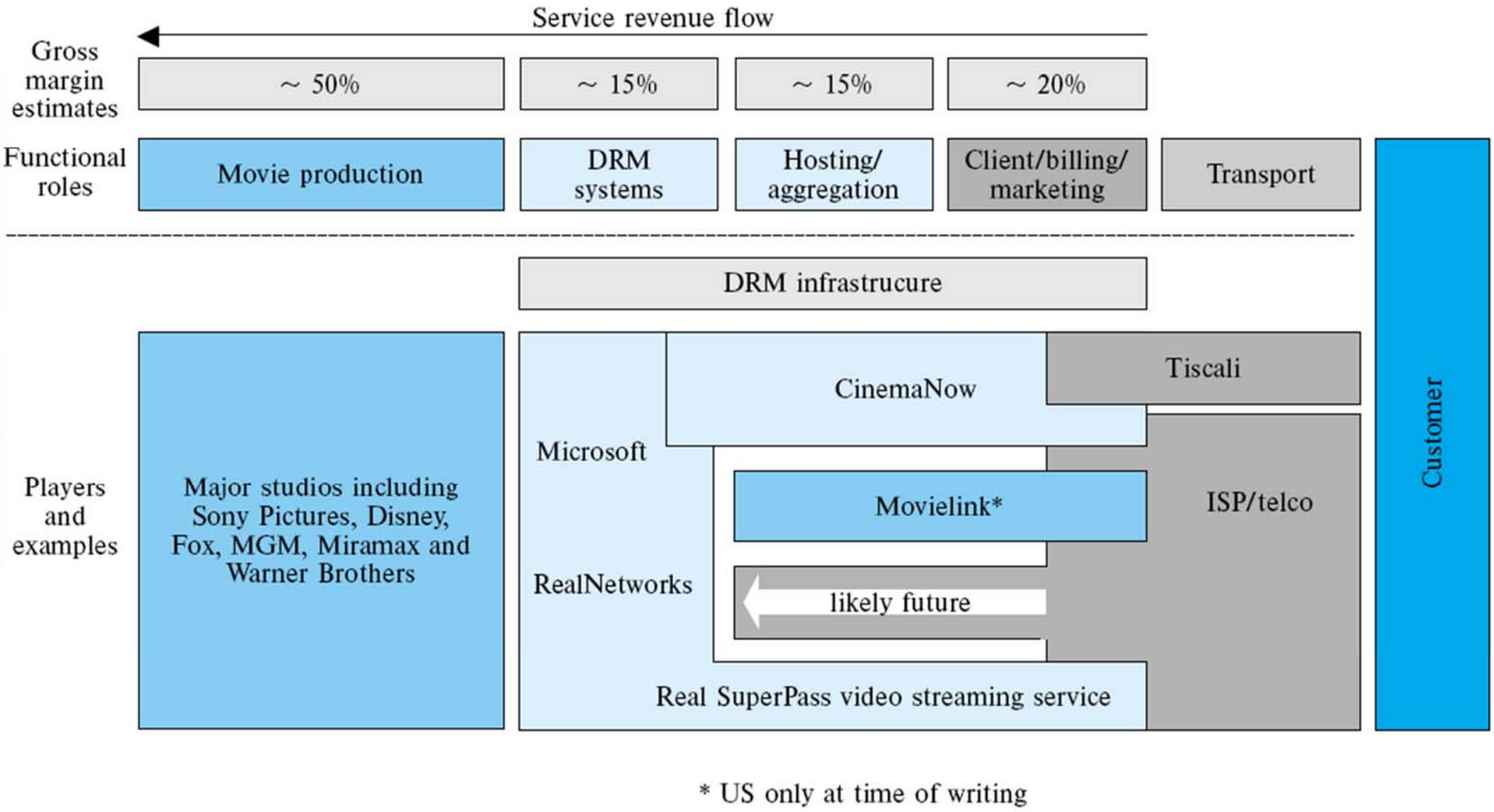
Business Models

- Are business models
  - Monthly subscription to get all videos of channel, for example SKY
  - Generic subscription to have in your monthly bill a price for each item you buy, for example Pay per Play
  - Prepaid card: to pay in advance a certain credit that is consumed every time you buy an item, for example the prepaid cards of Mediaset on DVB-T/DTT
  - Etc.

Classification of Transaction Models

- **B2B:** Business to Business
  - Among digital good: producer, publishers, integrator, resellers, distributors, etc.
  - Each of them add a value and thus charge to final prince of the digital good, …
- **B2C:** Business to Consumer
  - From distributors to consumers
  - The final part of the value chain
- **C2C:** Consumer to Consumer
  - File and good sharing
  - UGC (User Generated Content) sharing
  - Recently IPR management
- **B2B2C**
  - Integrated B2B to B2C

Ex: Broadband VOD value chain



Source EITO2005

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Example of Microsoft Windows Media

Copy Protection solution

- **Naturally digital items can be freely copied**
  - The copy is a feature of the operating system, file system
  - The operating system cannot be typically controlled
  - Microsoft is going to enforce more control on the Operating System

- **CP Solution**: prevents the Copy of digital content
  - Programs: hardware key
  - Holes in FD
  - Special formatting in CDs/DVDs
  - Etc.

Utilizzo della crittografia

- Encryption è il processo che codifica un messaggio in modo da nasconderne il contenuto
- Si basano sull'uso di parametri segreti chiamati *chiavi*
- Si dividono in due classi fondamentali
  - Chiavi segrete condivise *(secret-key)*
  - Coppie di chiavi pubblica/privata *(public-key)*
- Segretezza e integrità
- Autenticazione
- Firma digitale

Algortimi di crittografia

- Un messaggio si dice criptato quando il mittente applica alcune regole per trasformare il testo originale (*plaintext*) in un altro testo (*ciphertext*)

$$E(K_1, M) = \{M\}_K$$

- Il ricevente deve conoscere la trasformazione inversa per ritrasformare il *ciphertext* nel messaggio originale

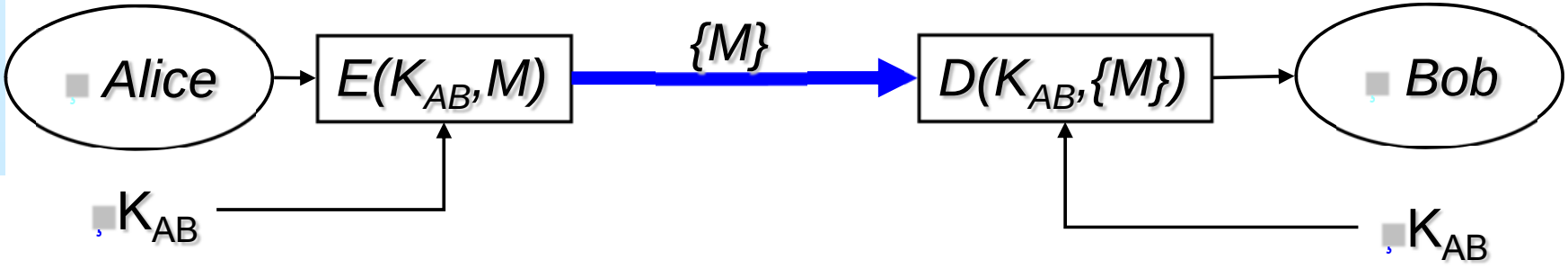
$$D(K_2, \{M\}_K) = M$$

$K_1 = K_2$ **simmetrico**

$K_1 != K_2$ **asimmetrico**

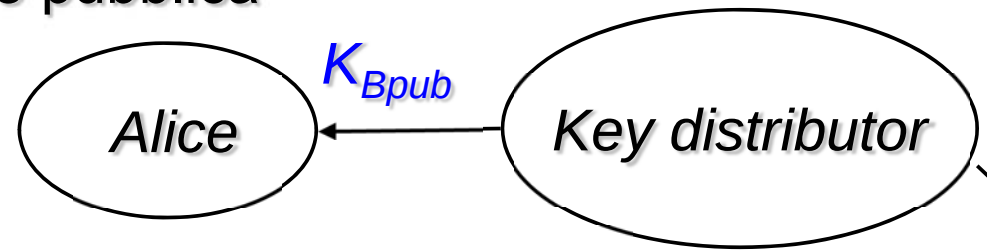
Scenario 1: secret communication

- Alice vuole inviare alcune informazioni segretamente a Bob
  - $\{M\}=E(K_{AB},M)$
- Alice e Bob conoscono entrambi la chiave segreta K_{AB}
- La comunicazione è segreta finchè K_{AB} non è compromessa

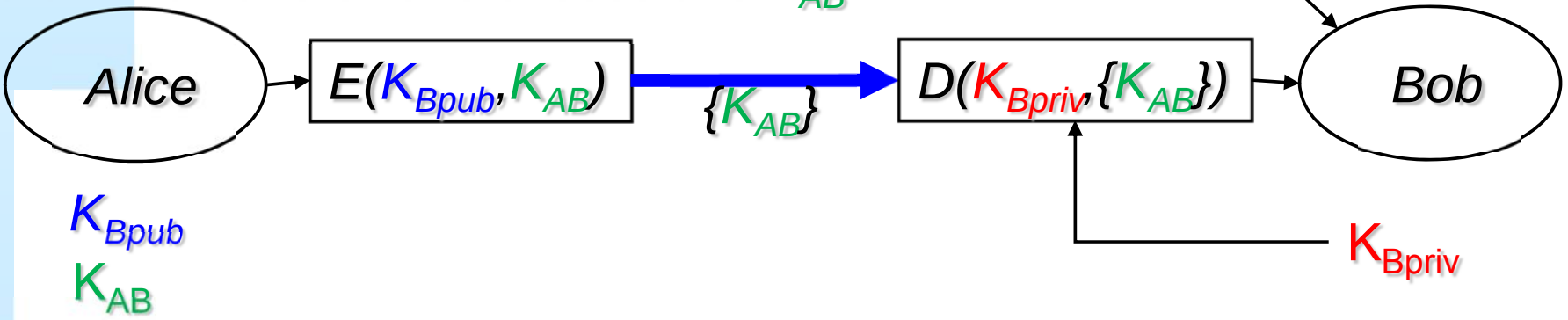


Scenario 3: authenticated with public-key

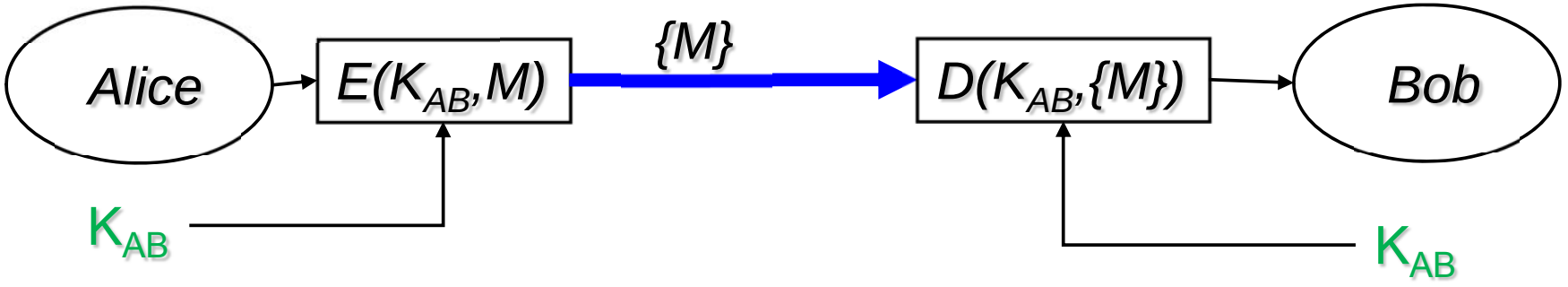
- Richiesta chiave pubblica



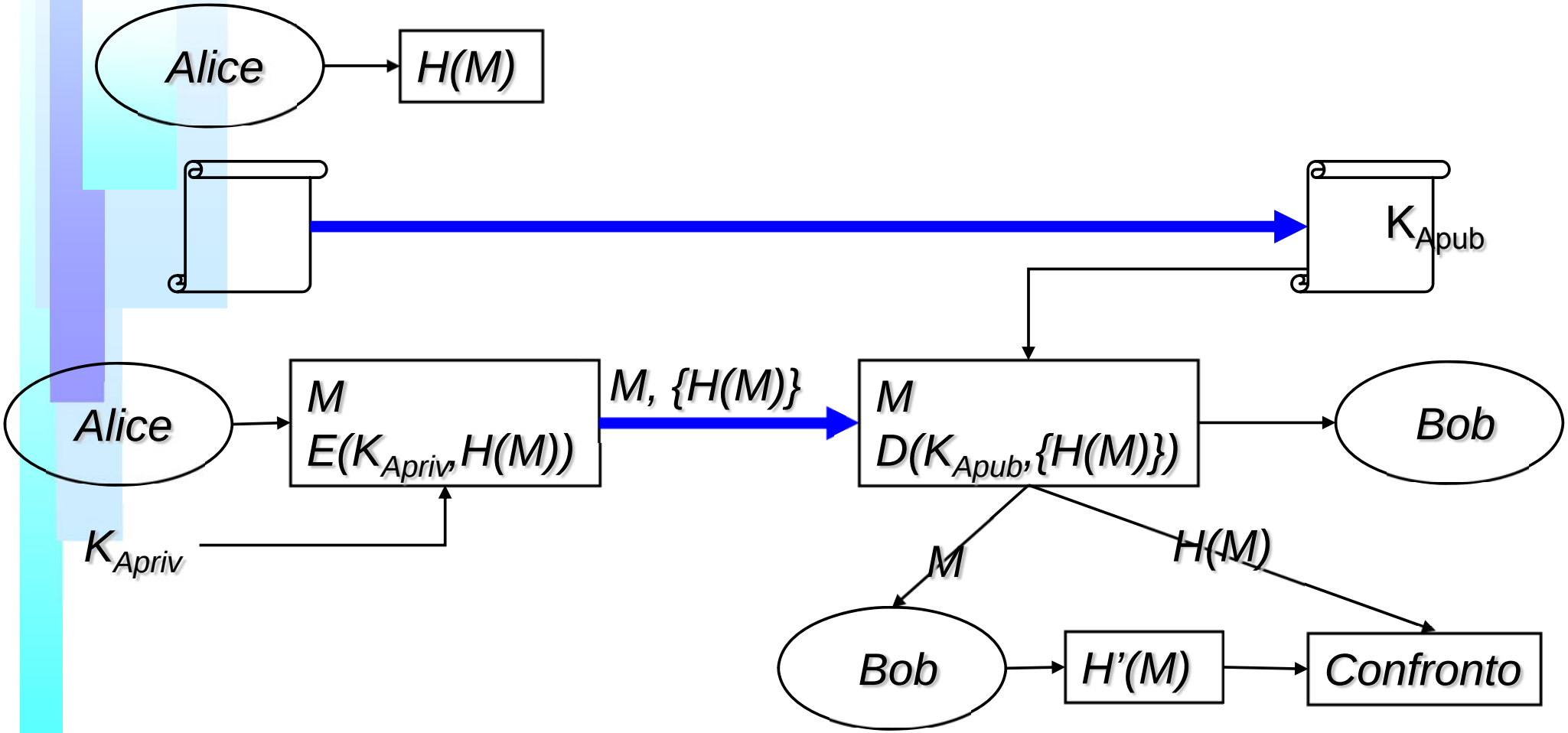
- Determinazione chiave di sessione K_{AB}



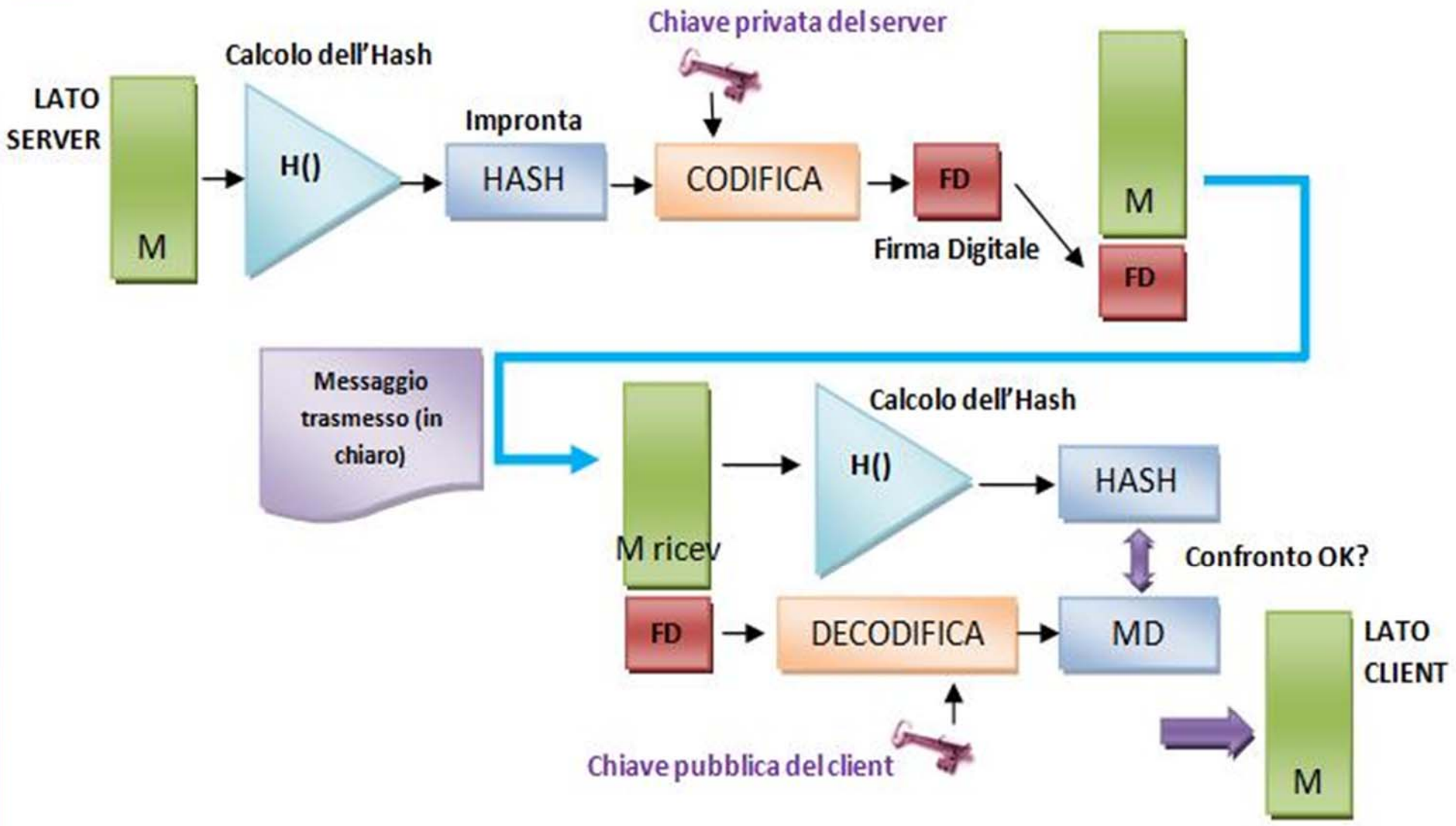
- Cumunicazione sicura



Scenario 4: digital signature

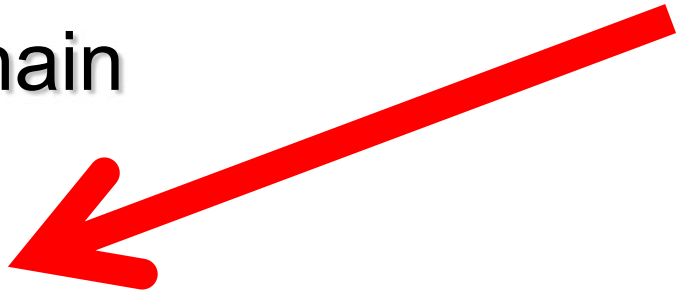


Digital Signature



Part 1: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Example of Microsoft Windows Media



CAS: Conditional Access Systems

- **Systems that controls the access to the content**
  - Typically used on streaming towards STB/Decoders
  - Copy is assumed not possible since the content is not stored locally and neither accessible to the final user.

- **For PC:**
  - Partially suitable for open platforms such as PC
    - ➔On PC: SSL, HTTPS, etc.
  - Temporary storage of smaller content on the disk, may be encrypted
- **For STB:**
  - The most interesting and diffuse solution

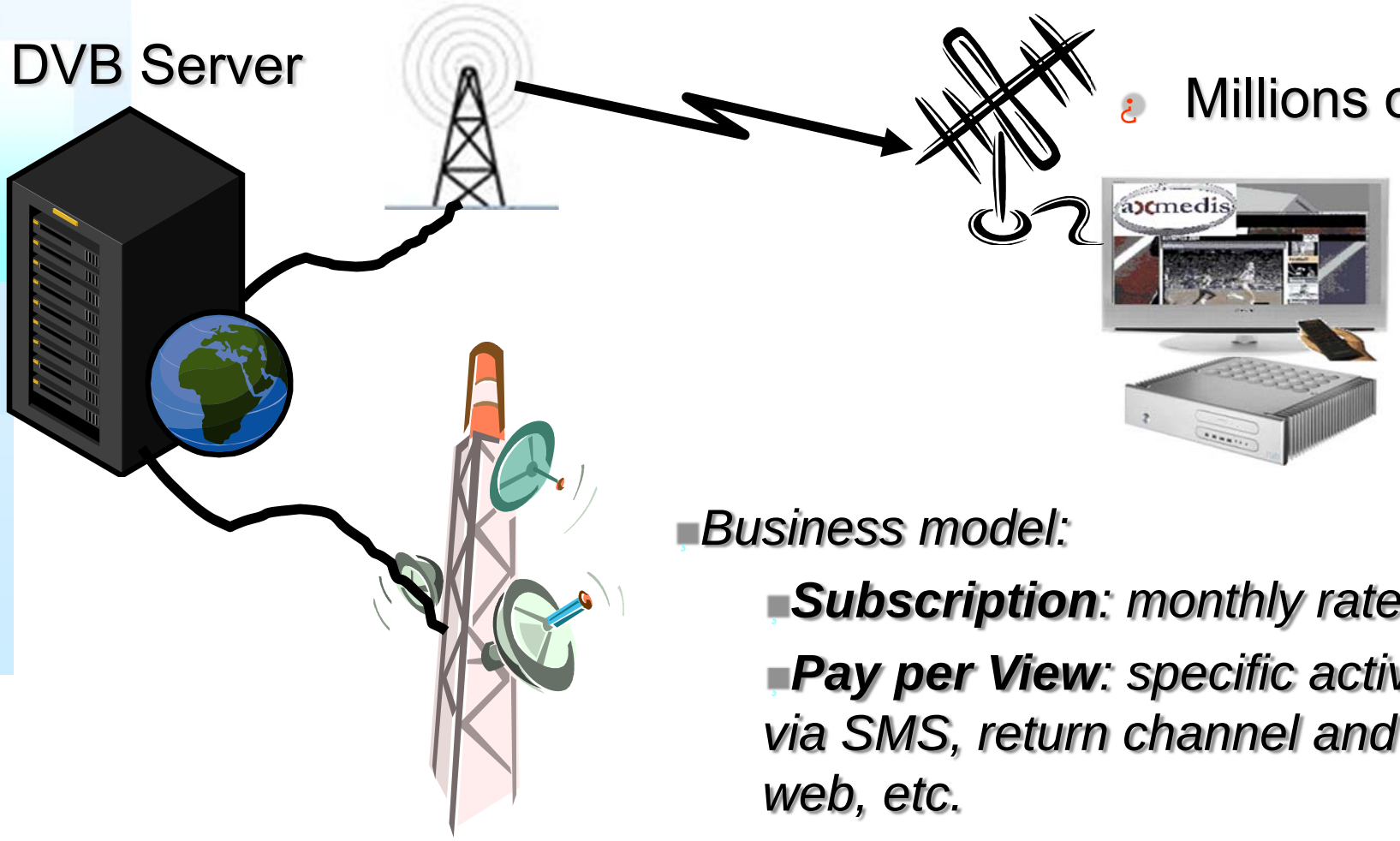
CAS: Conditional Access Systems

- **Systems that controls the access to the content for STB**
  - Streaming towards STB/Decoders
    - DVB-T, DVB-S, DVB standards for CAS
  - Copy is assumed not possible since the content is not locally stored and accessible to the final user. Recently can be temporary stored, see MySky.

- **Protection and solution**
  - Streaming in broadcast
  - Adoption of MPEG-2 TS (other models such as RTSP)
  - *For example*: Irdeto, Nagravision, NDS
  - Key distributed into the stream, accessible with another key
  - Adoption of SmartCard for some business models
  - Adoption of the Return Channel for some business models

DVB-T/DVB-S

- DVB Server
- Millions of STBs



- *Business model:*
  - ***Subscription**: monthly rate*
  - ***Pay per View**: specific activation via SMS, return channel and GUI, web, etc.*

La televisione digitale terrestre ....

Un po' di storia

1991 Nasce l'**European Launching Group** [ELG]

09/1993 Il **MoU** (Memorandum of Understanding): nascita del **DVB Project** (Digital Video Broadcasting)

11/1993 **MPEG-2 (ISO/IEC 13818-2)** viene approvato dall'**ISO**

10/1996 Il **MoU** viene rivisto e integrato con l'**interattività** e l'**accesso condizionato.**

1/2000 Approvata la piattaform mhp

5/2001 Parte la fase **DVB 2.0**

Il sistema DVB terrestre (DVB-T)....

Set Top Box (STB)

La Multimedia Home Platform (MHP)…

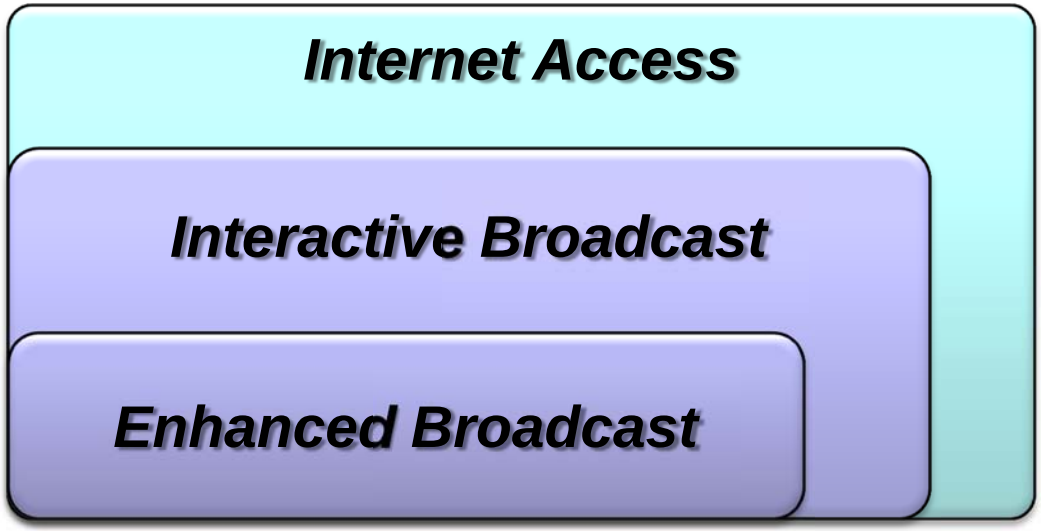
La piattaforma DVB-MHP

MHP 1.0 nel luglio 2000, MPH 1.1 nel giugno 2003

Indipendenza dall'ambiente HW e SW

Approccio a livelli per le API MHP

I Profili

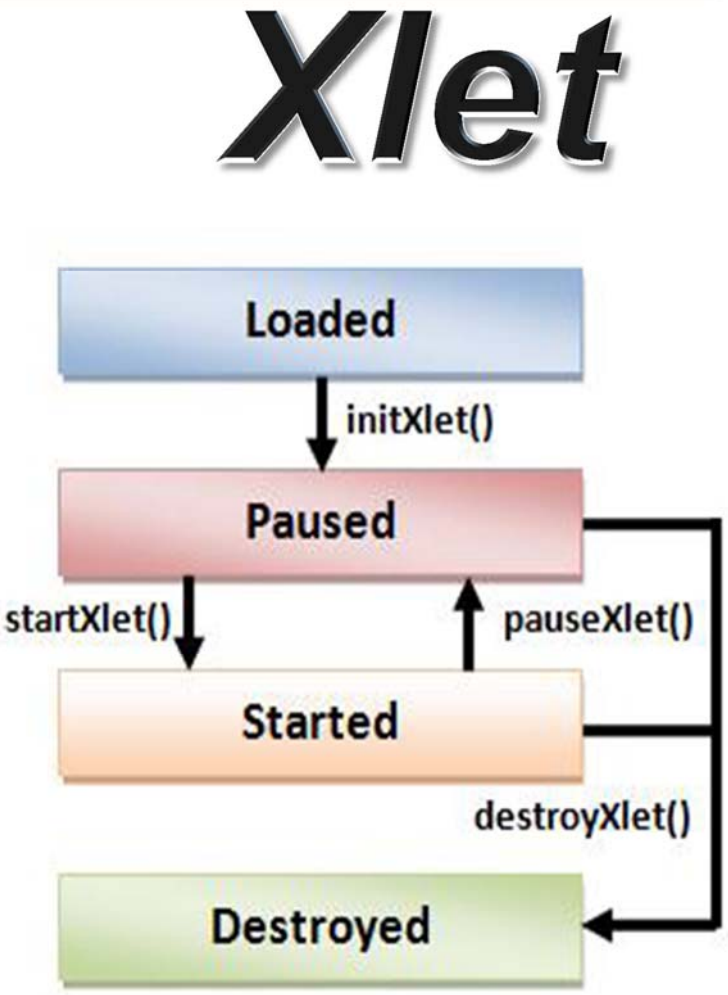


Il digitale terrestre e Java....

Le applicazioni MHP

- Java Virtual Machine (JVM)
- API Java Media Framework (JMF)
- API JavaTV
- Astrazione dalle specifiche HW
- Nessun vincolo con lo standard DVB
- Xlet vs Applet
- L'interfaccia **Xlet**
- La classe **java.tv.XletContext**
- L'interfaccia grafica

Java.awt.* **java.havi.ui.*** **org.dvb.ui.*** **org.dvb.event**

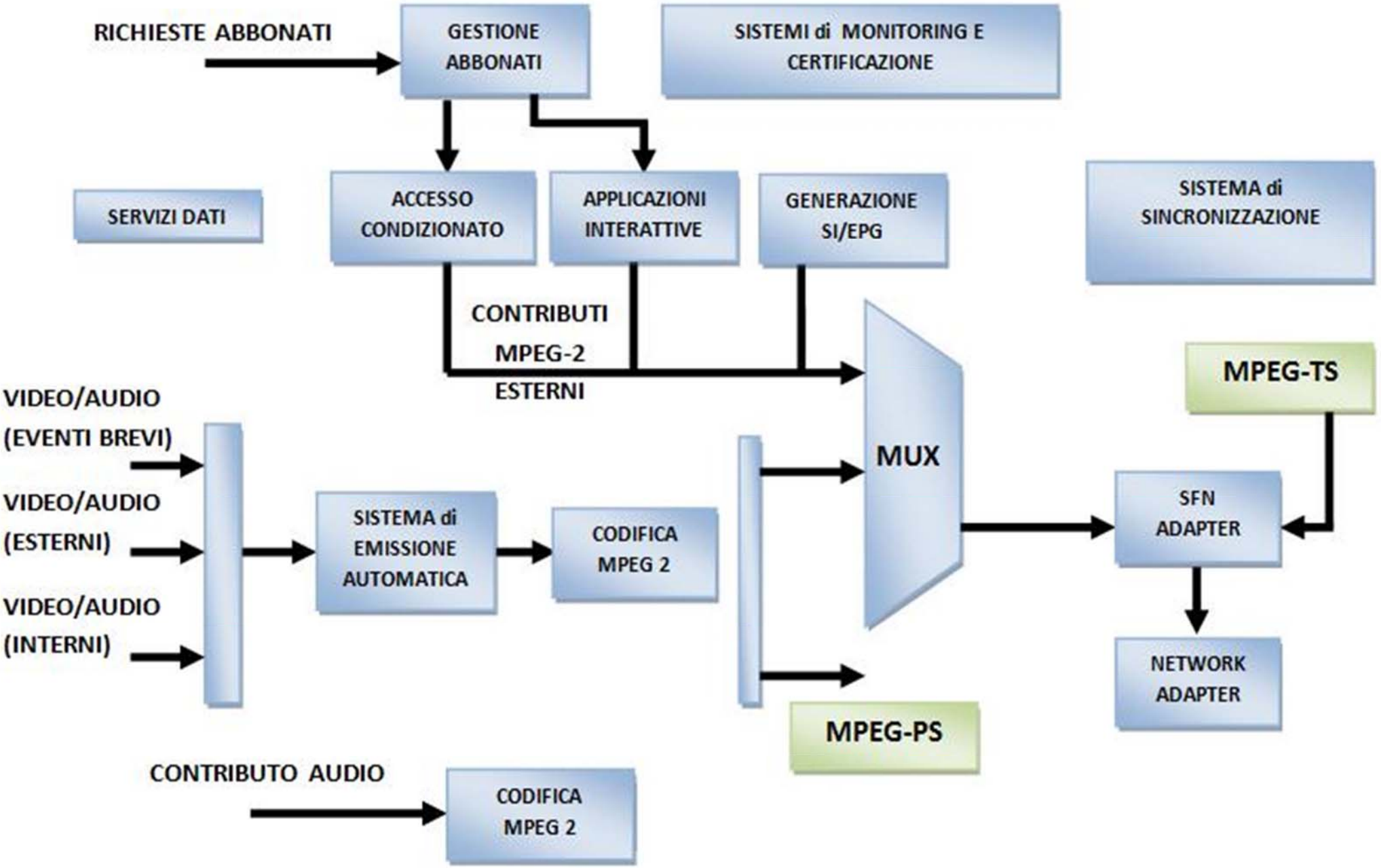


I meccanismi di trasmissione....

MPEG2-DVB System

- Il Program Stream (PS)
- Il Transport Stream (TS)
- La Program Service Information (PSI)
  - Program Association Table (PAT)
  - Program Map Table (PMT)
  - Conditional Access Table (CAT)
  - Newtork Information Table (NIT)

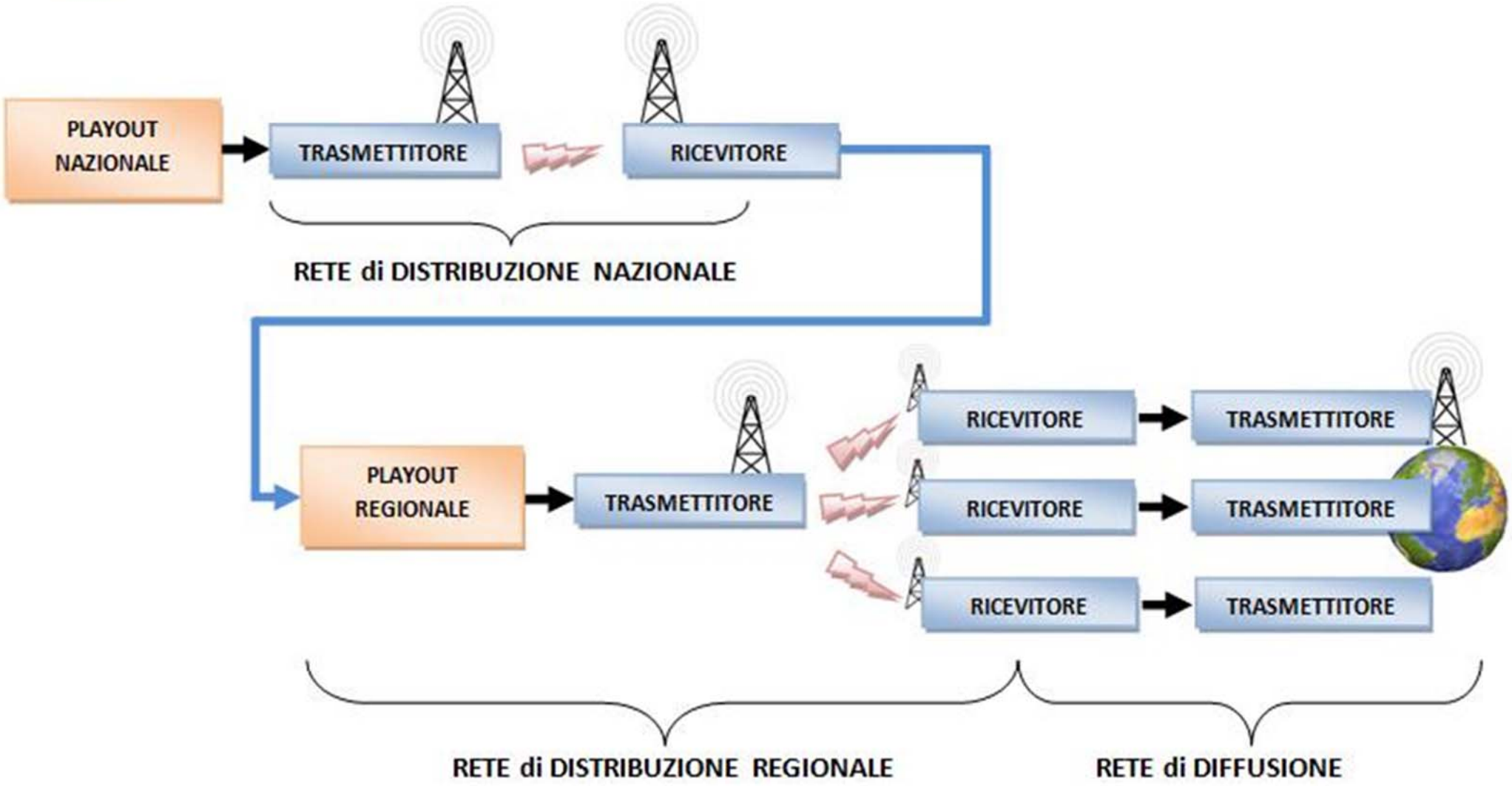
DVB-T Server Side



MPEG2-TS e DVB-T

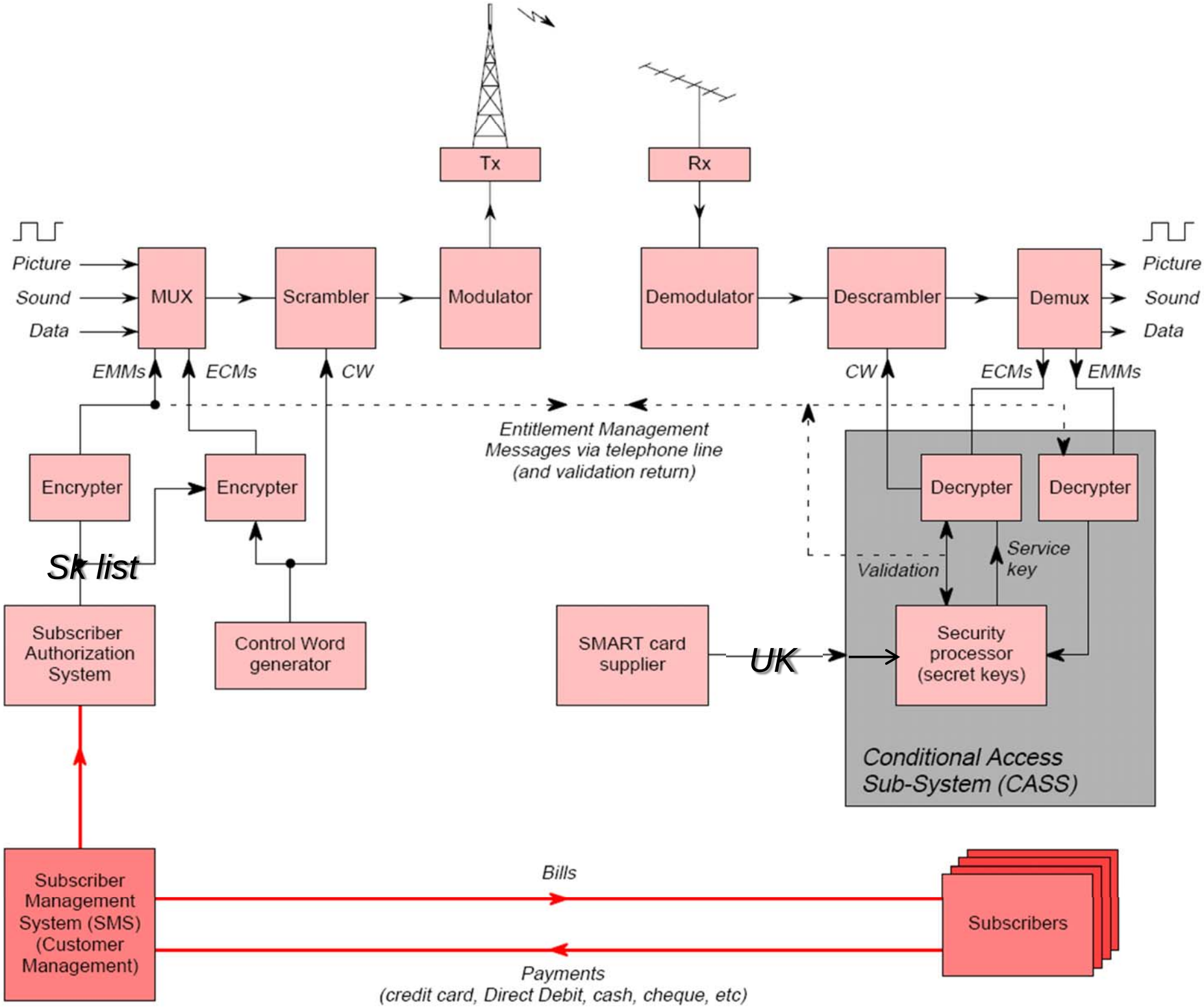
- Il Program Stream, PS, integra nel tempo I vari programmi producendo uno stream integrato
- Il MUX di program integra contenuti di vario tipo nello stesso Stream producendo un TS
  - Program stream, info di CAS, XLET application, EPG
  - Questo puo' essere integrato con quello di altri canali:
  - Ogni TS puo' avere vari PS, cioe' vari canali al suo interno
- Il MUX viene trasmesso su una sola frequenza e puo' pertanto essere ricevuto tutto insieme dal tuner.
  - MUX Canale satellitare: 34-38 Mb/s ≈ 8 programmi
  - MUX Canale terrestre: 20-24 Mb/s ≈ 4 programmi
- La selezione del singolo canale avviene tramite una demux che seleziona I pacchetti del canale dal PS.

Distribuzione



CAS protezione

- Cifrare il TS da lato Server per poi abilitare lato client solo quelli che stipulano un contratto,
  - E pertanto solo questi ottengono una licenza
- La cifratura avviene tipicamente con algoritmi standard (scrambling) e vengono cambiate le chiavi molto spesso.
- Oltre a questo, nel TS vengono anche inviate alcune info che possono essere usate per recuperare la chiave di decifratura.
- La chiave non viene inviata in chiaro per ovvi motivi.


Tx
Rx
Picture
Sound
Data
MUX
Scrambler
Modulator
Demodulator
Descrambler
Demux
Picture
Sound
Data
EMMs
ECMs
CW
CW
ECMs
EMMs
Entitlement Management
Messages via telephone line
(and validation return)
Encrypter
Encrypter
Decrypter
Decrypter
Sk list
Validation
Service
key
Subscriber
Authorization
System
Control Word
generator
SMART card
supplier
UK
Security
processor
(secret keys)
Conditional Access
Sub-System (CASS)
Subscriber
Management
System (SMS)
(Customer
Management)
Bills
Subscribers
Payments
(credit card, Direct Debit, cash, cheque, etc)

Sistema di Chiavi

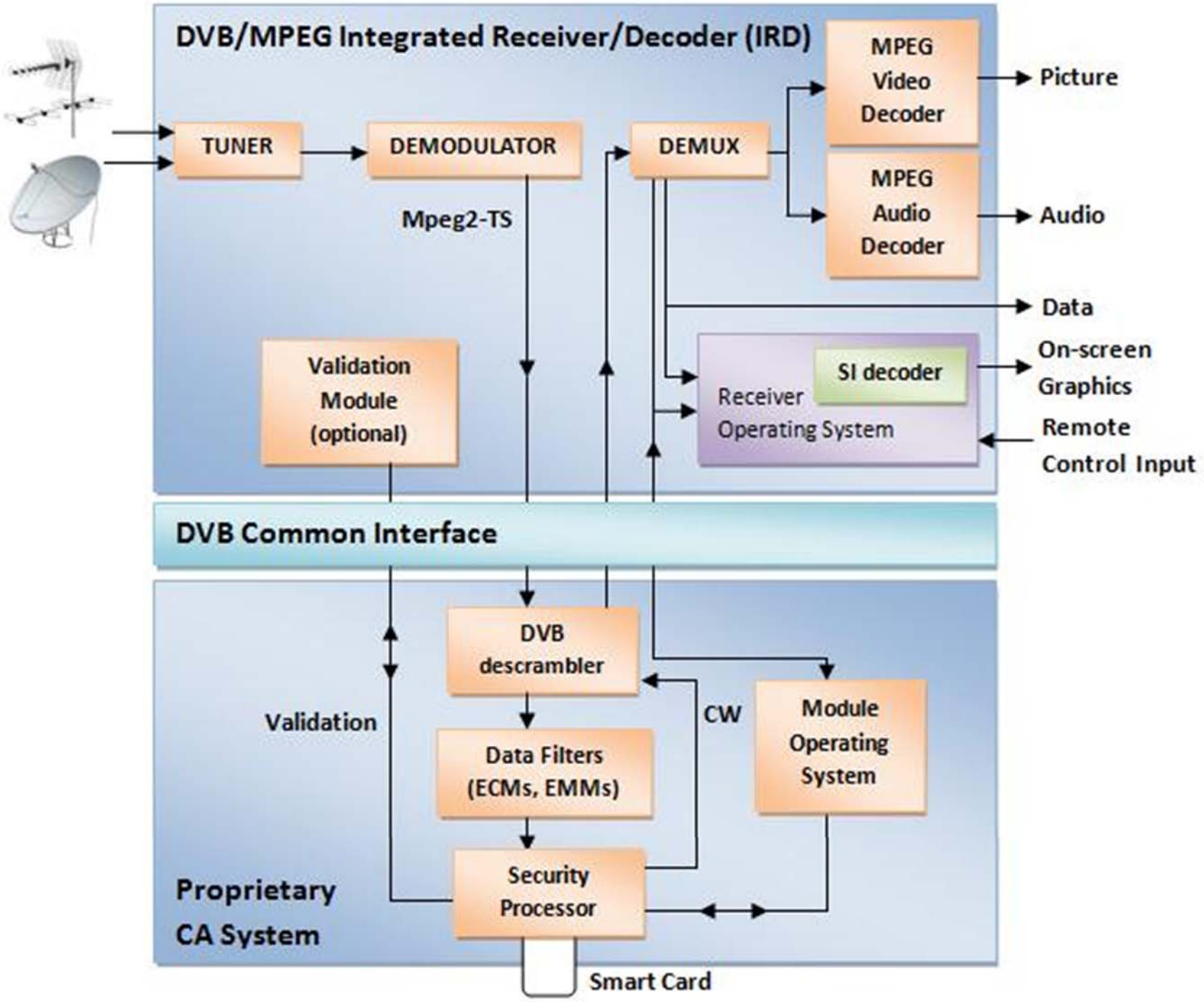
- **CW: Control word**, chiave utilizzata per cifrare il flusso digitale
- **SK: Service Key**, serie di chiavi,
  - una per ogni servizio/canale contenuto nello stream,
  - Per ogni SK viene creato un oggetto cifrato **chiamanto ECM**
- **UK, User key**, permette all'utente di ottenere la SK, decrypt.
  - Ogni utente ha un UK diversa,
  - Per esempio nascosta in una SMARTCARD
- **ECM: Entitlement Control Message**, ECM(SK,CW)={CW}
  - viene inviata in broadcast
  - contiene la CW cryptata tramite la SK
- **EMM, Entitled Management Message**, EMM(UK, SK)={SK}
  - viene inviato in broadcast
  - contiene una SK encrypted che puo' essere decifrata solo con una UK (come quella usata per encription)

- **Client side:**
  1. arriva un EMM per un certo servizio i dallo stream che viene passato al SecProcessor che ha la UK (user key)
  2. Il SecProcessor produce la SK(i) (service key) usando la sua UK se possibile, cioe' se abbonato al servizio
  3. Questa SK(i) (ve ne sono n, una per ogni servizio/canale) viene usata per estrarre la CW (i) da ECM (i)
  4. CW(i) viene usato per decriptare il ProgStream/servizio (i)
- **Server side**:
  1. Le CW per ogni servizio i sono generate in modo periodico
  2. SK(i) (n elementi) sono generate per ogni servizio i degli n
  3. SK(i) viene usata per codificare CW(i) into ECM(i) del servizio i
  4. La User List viene usata per codificare le n SK(i) into m EMM (I,u), un EMM per ogni servizio e per ogni utente, u.

- **ECMn** = { per ogni servizio i si ha SKi, ECM i = Encrip (CWt, SKi) }
  - Con: i di *n; d*ove: *n* e' il numero di oggetti/servizi
  - CW t cambia nel tempo
  - n ECM, uno per ogni SK
  - complessita' O(n)
  - Invio ogni 2 secondi, in anticipo
  - I servizi possono essere canali diversi, PS diversi

- **EMMm** = { per ogni utente j di m: EMM j,i = Encrip (SKi, UKj) }
  - Con: j di m; dove: m e' il numero di utenti
  - Con: i di n; dove: *n* e' il numero di oggetti/servizi
  - m EMM, uno per ogni servizio i-esimo SK (Service Key si trova dentro la EMM e viene decripted tramite la UK)
  - complessita' O(mn)
  - Invio ogni 10 secondi, in anticipo

The Decoder


DVB/MPEG Integrated Receiver/Decoder (IRD)
TUNER
DEMODULATOR
DEMUX
MPEG Video Decoder
MPEG Audio Decoder
Picture
Audio
Mpeg2-TS
Data
Validation Module (optional)
SI decoder
Receiver Operating System
On-screen Graphics
Remote Control Input
DVB Common Interface
DVB descrambler
Validation
CW
Module Operating System
Data Filters (ECMs, EMMs)
Security Processor
Proprietary CA System
Smart Card

Effectiveness of Protection, and example

- The cards have to be very hard to be cloned, but they are standards. So that additional features are added to make them different from the standard one.
- The keys are periodically changed, period is very short.

- **Attack**:
  - Substitute the smartCARD with one capable to extract the key and make it accessible to other decoders in the same house or via internet (on internet other users may use this key in their ad hoc smart card).
- **Defense**:
  - Detection of non correct cards measuring several aspects: patterns, temperature as a function of workload, identification of the electronic circuit contained, etc.

EPG, Electronic Program Guide

- There are several standards
  - **TvAnyTime** adopted by BBC: (limited channels)
    - accessible via specific private services
  - **SKY** model and service (many channels)
    - Publically accessible via web in XML
  - **GuidePlus** (many channels)
    - broadcasted via a terrestrial channel not digital MTV now in Italy.

- Once obtained the program description via EPG it is possible to know:
  - starting time, ending time
  - additional metadata and descriptors
  - Etc.

Pros and Cons of DVB CAS

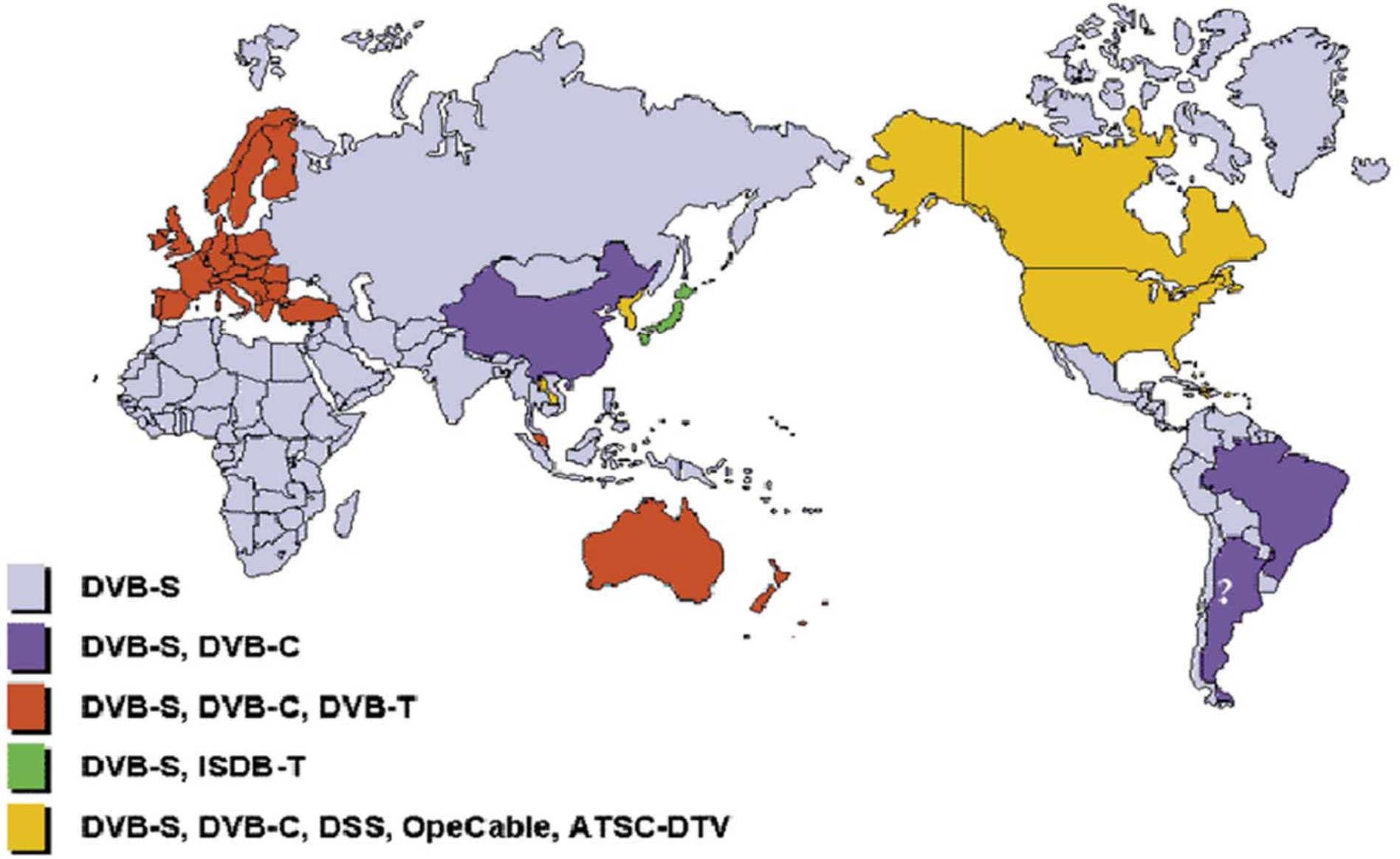
Pros:

- Cheap for the distributor, 1 sender N RX, if DVB-T or S
- Final user privacy respected depending on the business model to get the smartcard
- Suitable for S, T and H and SH: see DVB-H

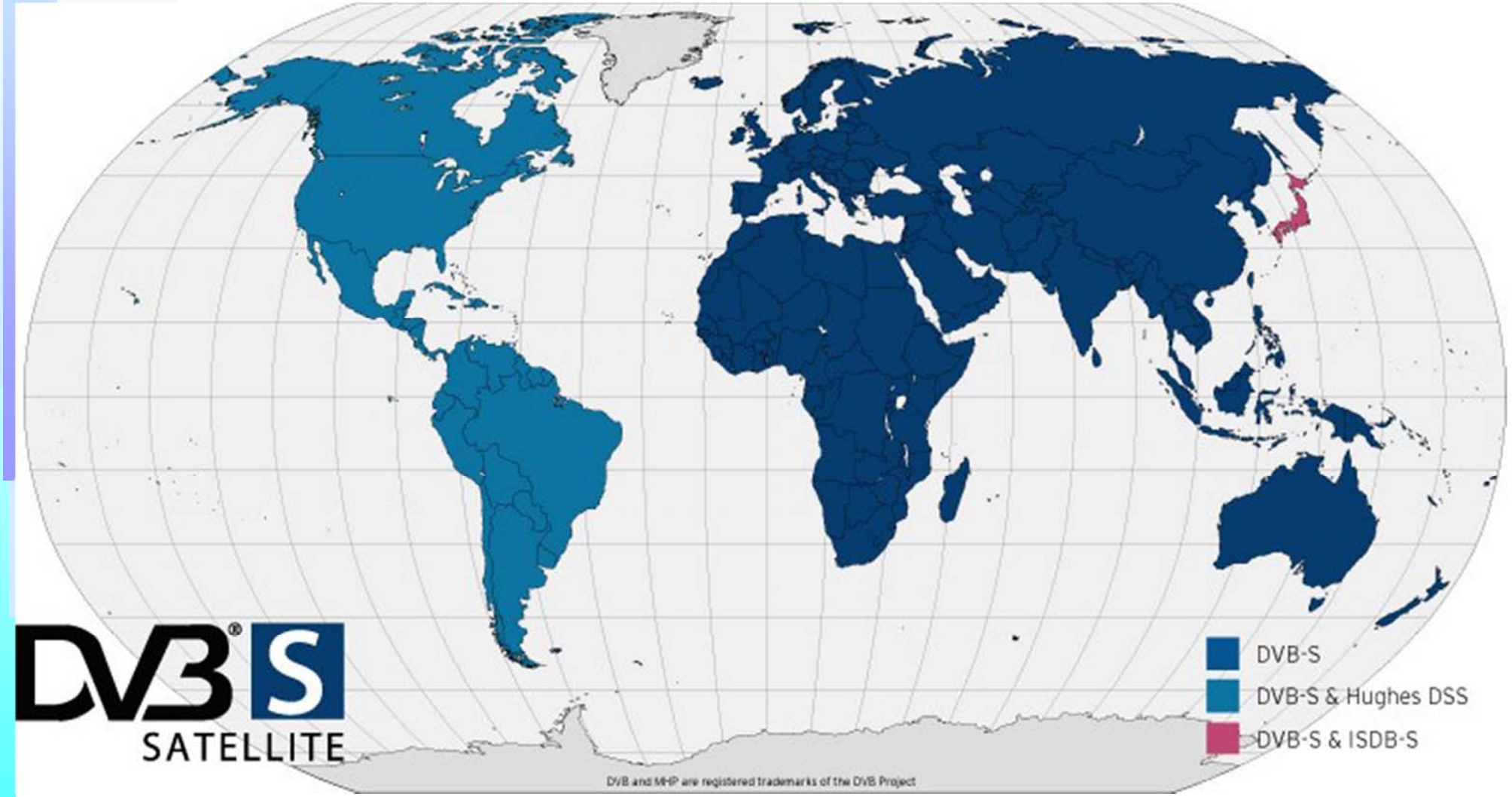
Cons:

- Cost of the decoder
- Cost of the cards
- Hardly replicable on PC
- High costs for VOD, Video on demand.
- High costs for DVB-H, DVB-SH
- Limited rights on the content
  - now recording, but with locked STB!
  - only one TV!
  - Even if one has paid cannot see again the video 10 times in the rest of its life!

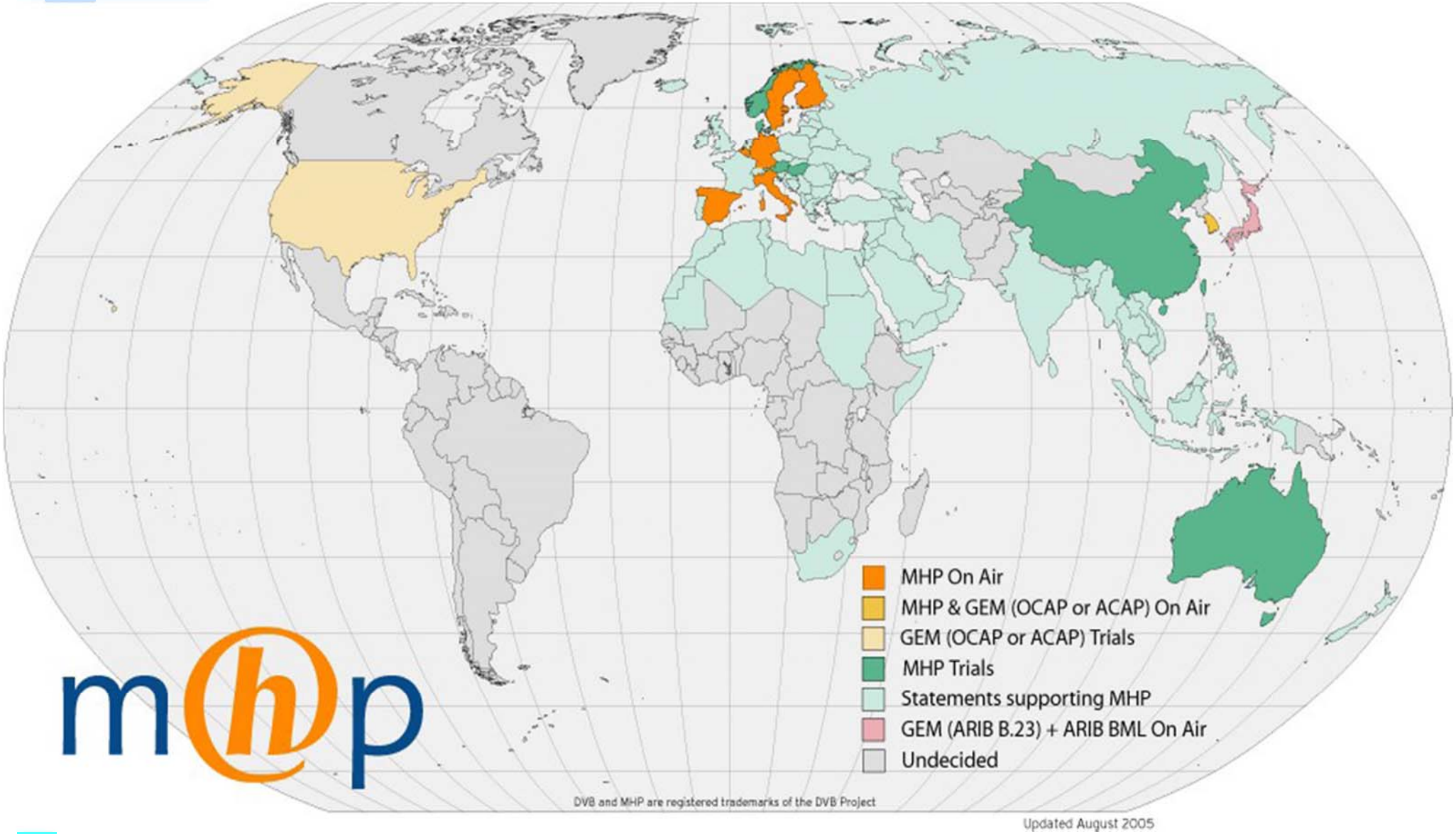
Standard Digital TV



DVB-S



DVB S SATELLITE


MHP On Air
MHP & GEM (OCAP or ACAP) On Air
GEM (OCAP or ACAP) Trials
MHP Trials
Statements supporting MHP
GEM (ARIB B.23) + ARIB BML On Air
Undecided
DVB and MHP are registered trademarks of the DVB Project
Updated August 2005

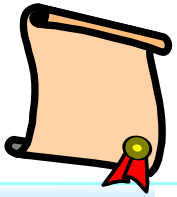
References

- http://www.dvb.org
- http://www.mhp.org
- http://www.interactivetvweb.org/
- http://www.etsi.org
- http://erg.abdn.ac.uk/research/future-net/digitalvideo/
- http://www.dgtvi.it
- Memorandum of Understanding http://www.dvb.org/documents/mou2001.pdf
- List of DVB Members, http://www.dvb.org/index.php?id=27
- DVB Worldwide http://www.dvb.org/index.php?id=228

Part 1a: sistemi di protezione

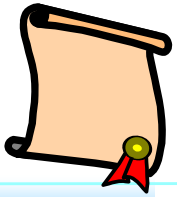
- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Example of Microsoft Windows Media

Rights Management



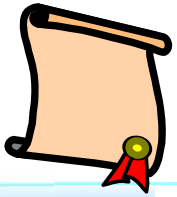
- **DRM**: Digital Rights Management
  - general term many times abused, confused, ...
- Management of Digital Rights
  - Limited to the management of rights of digital content ? → NO!!!
- **Digital Management of Rights → YES!!!**
  - More correct and reasonable
  - Management of both rights for original *works* and related *manifestations*, digital *resources*, etc.
  - in many solutions DRM is not intended in this way

Digital Rights Management



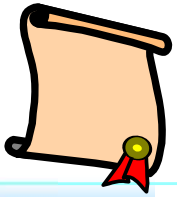
- **DRM: Digital Rights Management**
  - A set of technologies and solution to cope with Digital Management of Rights
- 1st generation of DRM were covering:
  - security and encryption
  - prevent non authorized copying, i.e., CP solutions
- **2nd generation of DRM covers:**
  - Content: description, identification, trading, protection,
  - monitoring, and tracking of all forms of rights usages over contents, including management of rights holders relationships

Aim of …… Digital Rights Management



- To allow exploiting digital content functionalities (rights) in a controlled manner
  - To who has been **authenticated/certified**
  - To do what (are the rights) is defined in a formal **license**
  - **Verifying/Control/Supervise** if the above conditions and others are respected
  - By using technologies to **protect content** (e.g., encryption, fingerprint, watermark, etc.)
- Cons:
  - Registration of users (in some case can be relaxed)
  - Authentic. of users and/or tools/terminal/devices
  - Control of users
- *It has to be supported by a set of additional technical solutions*

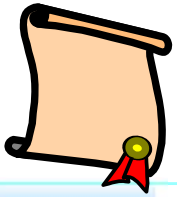
Motivations for Digital Rights Management



- Prevent the rights exploitation to who has not acquired the rights
  - from some rights owner or authorized reseller
- Verifying/Control if the allowed rights are respected:
  - In the whole value chain or at least at the end users
- Support/adoption of protection solution to
  - Enforce the rights control on the players and tools by which the users are accessing to the content.

- **Recently**, strongly rejected by the final users since most the DRM solutions also enforce some limitations with respect to the TRU (traditional rights usages):
  - Cracking the DRM solutions
  - Redistributing the content violating the IPR via P2P, Social Network, direct contacts, etc.

Motivations for Digital Rights Management

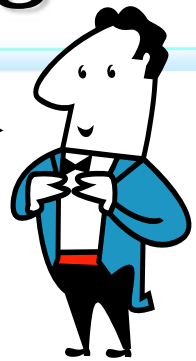


- The **collection of money/revenues (creation of revenue streams)** related to the exploitation of rights is traditionally/partially covered by Collecting Societies (clearing houses)

- **Collecting Societies**
  - Are Focussed on one or more rights types
    - thus, one or more for each Country/area
  - Guarantee/protect the interests of the content/rights owners
  - Are territorially distributed, while in Europe some liberalisation has been performed, permitting in some measure the competitions among different European CS

- They are some common agreement among the majors Collecting Societies in Europe: SIAE, SGAE, SAGEMA, etc.

Simple protection with Key sending



Selling Server

License Production

License distribution and player/device verification and supervision

Ask for the License

Content deprotection and rights exploitation

Get the content

Content Packaging, Protection

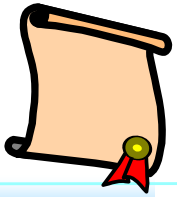
content

Distribution Server

Production and distribution

Player device

What Should be the DRM



- To allow exploiting the (digital) content functionalities (rights) in a controlled/supervised manner
  - To who has been **authenticated/certified**
  - To do what (are the rights) is defined in a formal **license**
  - By using technologies to **protect content** (e.g., encryption, fingerprint, watermark, etc.)
  - **Verifying/Control/Supervise** if the above conditions and other issues are respected,
    - including the *possibility of keep trace of the activity performed by the users and reporting/using them to the distributors* (this part is disputable since for the privacy)

Technical issues behind the DRM

- **Digital Encryption/decryption**
  - DRM may use strong encryption (# bits) never been cracked
- **Digital signatures**
  - content may be digitally signed to prevent tampering
  - license has to be digitally signed, etc.
  - event reporting has to be digitally signed, etc.
- **Unique identification of elements:**
  - Users, Content Objects, devices/players, ...
  - Distributors and rights, ...
- **Authentication and certification of users and devices**
  - To prevent compromised players or non trusting users to receive or distribute other content, ….
  - Black list of devices, licenses, users, etc.

Technical issues behind the DRM

- **Separation of licenses from content**
  - licenses should be kept separate from content
  - The license formalises what can be done by a given user on a given content
  - thus content can be protected once for all and widely distributed via any kind of channel including P2P
- **Revocation of User, User ID**
  - The user that has violated the solution is black listed, banned.
  - He cannot exploit any right on content !!, may be too strong..
- **Revocation of licenses, via License ID**
  - Revocation of rights authorization, for that content-right
  - various ways to prevent players from exploiting content
- **Revocation of Content, via Content ID**
  - Content with the listed IDs cannot be played on players.
- **Revocation of Player, Player ID**
  - Players with the listed IDs cannot be used to open protected content, lost of certification.

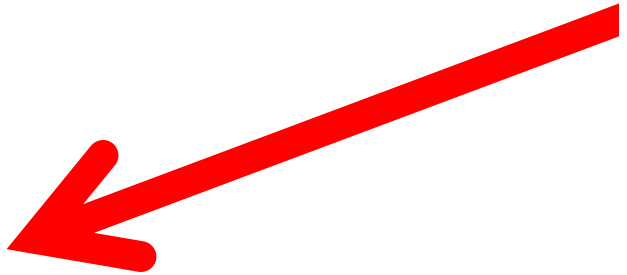
Single Channel Distribution value chain Issues

- The content protection is performed before distribution
- The B2B areas are (production, integration, etc.):
  - Considered trusted, based on paper contracts
- The authors, integrators and producers cannot verify and keep direct trace of the exploited rights.

- **The single channel distributor**:
  - Establishes the business model(s) for the channel:
    - pay per play, subscription, ……etc….
    - produce licenses for each person/device, content, etc.
  - sale the content and produce the Bill: pay per, subscription,..
  - has a limited control on the exploitation of rights
  - Direct relationships with content producers and CS
  - Etc.

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Example of Microsoft Windows Media

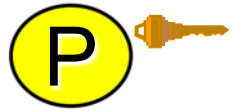


Content Elements

- **Content Packaging to contain the following information**
  - Metadata + semantic descriptors ……
  - Digital Resources: items, digital essences, ……
  - Protection Information: (how to prot/deprot the content)…..
  - License: ……..who can use, when, how, etc...

- **The Package should allow to be**
  - Protected
  - Streamed (so called real-time) and/or downloaded, ….
  - Shared on P2P, etc..
  - Ported on physical supports,
  - Adapted, etc..
  - Coded in binary and/or XML, etc.
  - etc.

Content Elements of the package

- **Metadata:** *Metadata*
  - Identification information, unique ID, distributor ID, etc.
  - Classification information also for indexing: Dublin core, etc.
  - Semantic Descriptors, MPEG-7, for indexing, etc.
  - References to Owner, to distributor, etc.
  - Etc.
- **Digital Resources:** *Resource*
  - Any digital information: images, doc, txt, video, game, application, file, audio, etc.
  - Hierarchy of digital resources
- **Protection Information:** *Prot-Info Model* → 

  - What has to be done to access at a given information/resource
  - Tools used, their parameters, etc.
- **License:** *License Model* → 

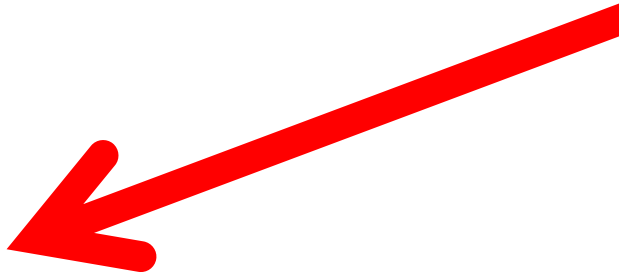
  - Which rights are provided, who is the recipient, conditions, etc.

Packing Content vs other aspects

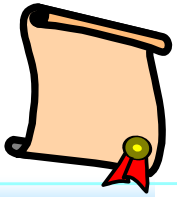
- The **package** may contains several information: metadata, info, several files, etc. →
  - Cross media content
  - hierarchical content and structure
- The **package** to be protected has to encoded in some file and format. For example to be encrypted with some algorithm
  - Protection by ignorance (algorithm and key)
  - Protection by complexity
- The **key** has to reach the player only via specific protected channels
  - If the key is reached and the algorithm is known the protection is violated
- The **player** has to **enforce** the protection and has to provide a precise semantics for the rights
- The **license** is a description of the conditions under which the key can be taken, passed, used to/by the player

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Example of Microsoft Windows Media



License formal language

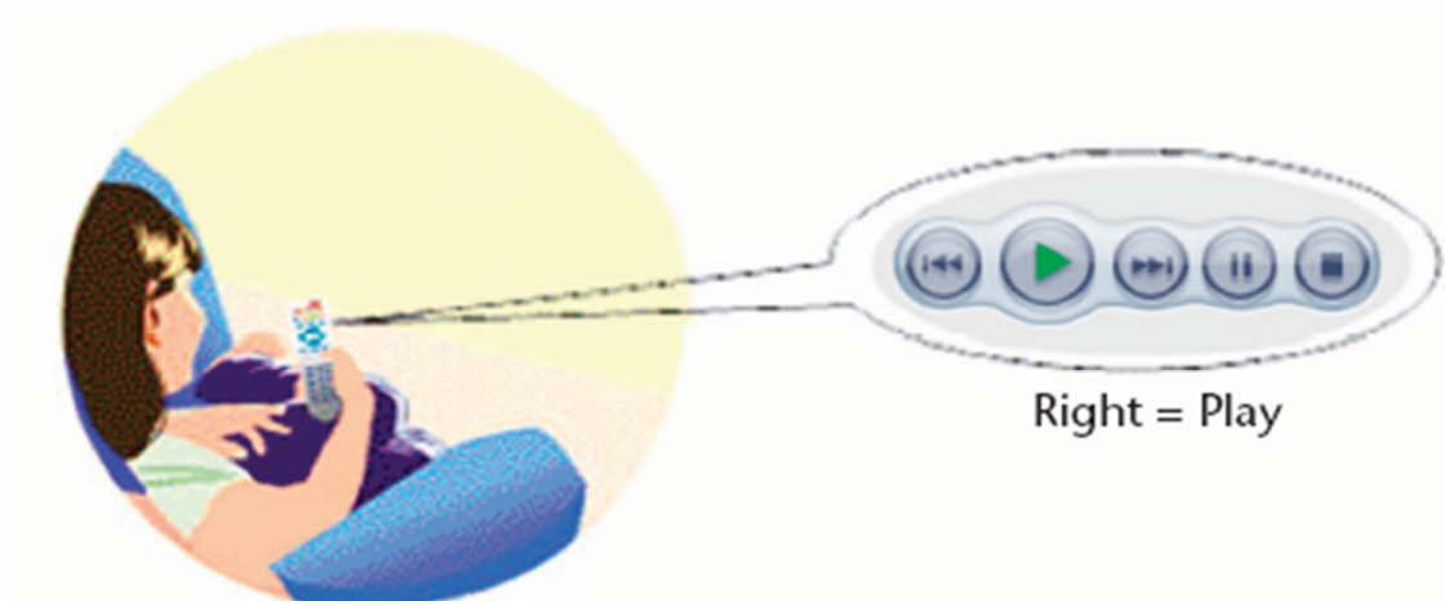


- **XrML 2.0:** eXtensible rights Markup Langua
  - http://www.xrml.org/
  - General purpose
  - ContentGuard, Nov. 2001, Microsoft
  - Derived from DPRL
  - Usato come base per MPEG-21
- **Windows Media DRM**
  - Derived from XrML
- **MPEG-21:**
  - REL: Rights Expression Language
    - Derived from XrML
  - RDD: Rights Data Dictionary
- **OMA ODRL:** Open Digital Rights Management
  - Expression language for mobiles
  - In some way simpler than MPEG-21 REL

An example of statement

Condition = November 2003

Resource = Ocean Wilds



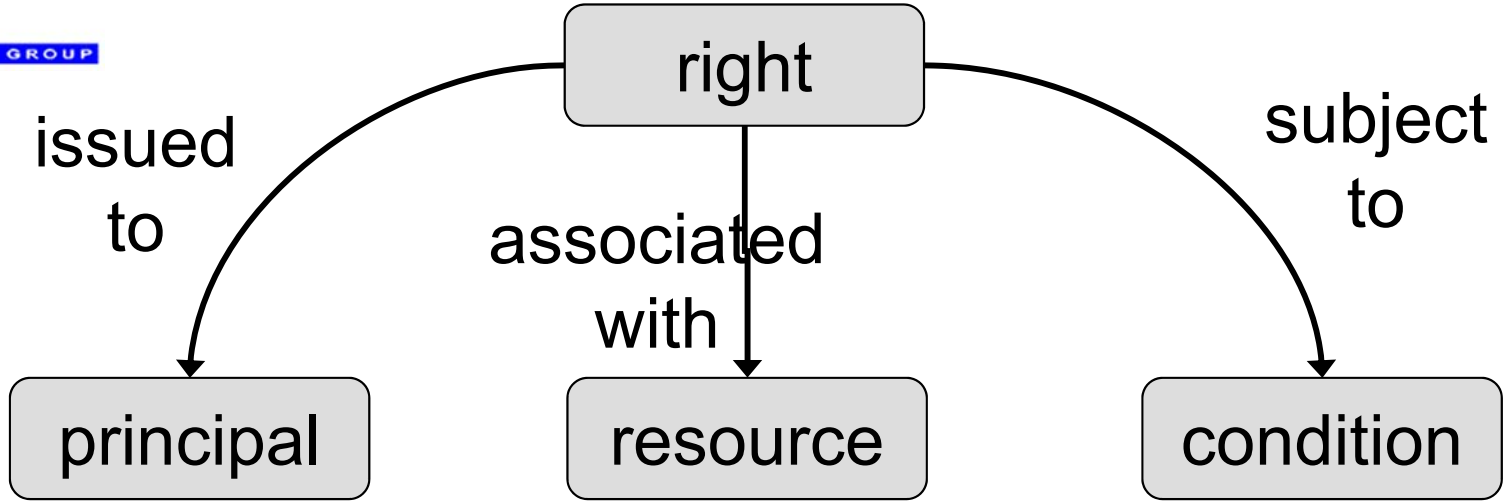
Right = Play

- Rosy can Play 3 times the Ocean Wilds in November 2003.

MPEG-21 — REL, Rights Expression Language

- **REL is** a machine-readable language, XML
  - to declare rights and permissions
  - uses terms defined in the Rights Data Dictionary, RDD
- **REL allows to define licenses** that give specific permissions to Users to perform certain actions on certain resources, given that certain conditions are met
  - Grants can also allow Users to delegate authority to others
- **Systems and device have to**
  - parse and validate the REL formalizations
  - check permissions before any further action is done
- **REL licenses** are wrapped into MPEG-21 Digital Items when the object is governed
- **MPEG-21 DID parser** is responsible for discovering and identifying where to gather licenses

REL data model



- REL grant formalization consists of
  - principal to whom grant is issued
  - rights the grant specifies
  - resource to which right in grant applies
  - condition to be met before grant can be exercised

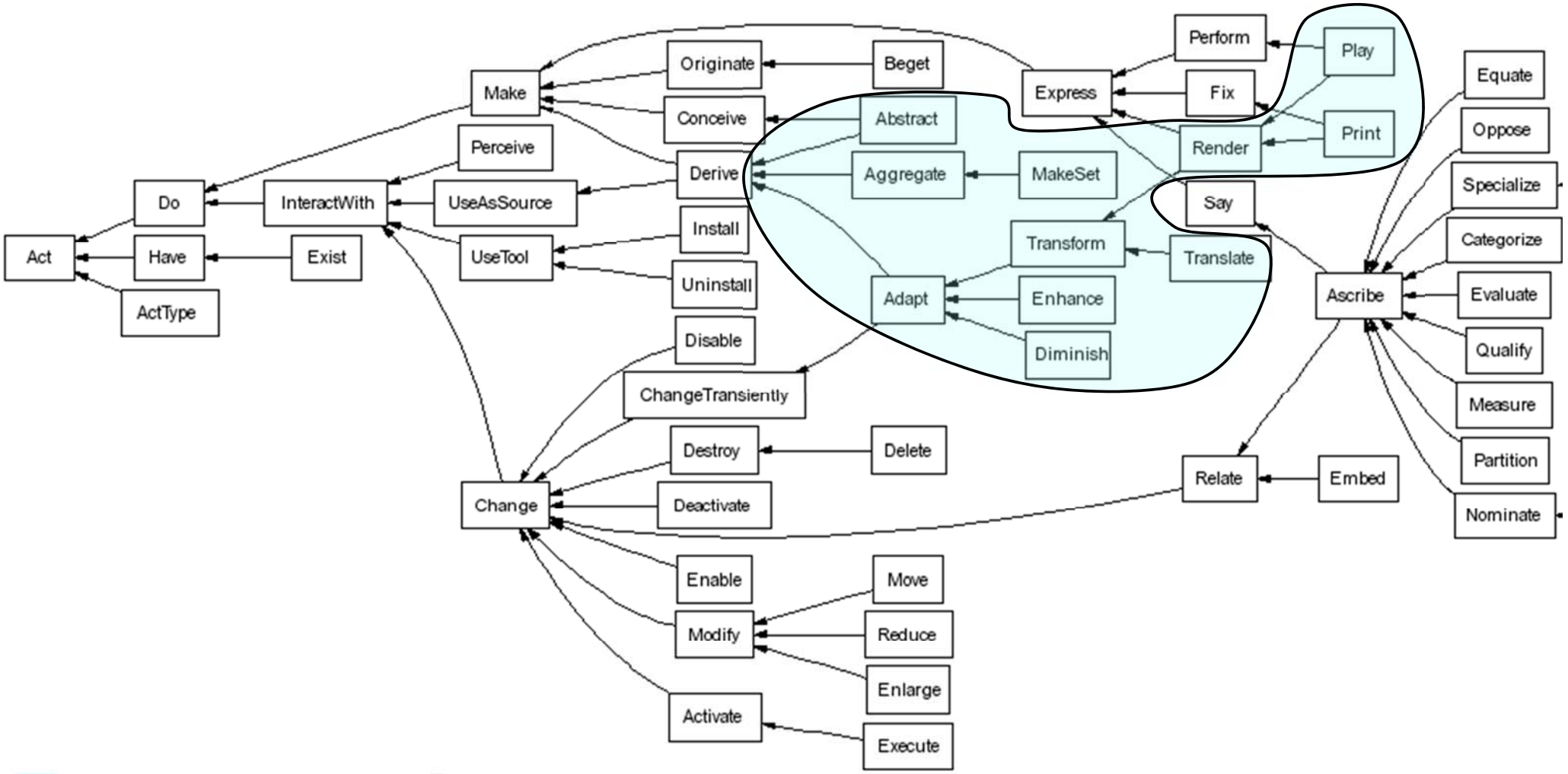
REL – Principal and Rights

- **Principal**: Party to whom a grant conveys usage rights.
  - authentication mechanism by which the principal can prove its identity.
  - a principal that must present multiple credentials, all of them must be simultaneously valid, to be authenticated.
- **Right**:
  - Action or activity that a principal may perform using a resource under some condition.
- **Resource**:
  - Object/content to which the principal can be granted a right.
- **Condition**:
  - Terms under which rights can be exercised.

- **MPEG REL provides** a right element to encapsulate information about rights and provides a set of commonly used, specific rights, notably rights relating to other rights, such as issue, revoke and obtain.
  - Extensions to MPEG REL could define rights appropriate to using specific types of resource.
  - For instance, the MPEG REL content extension defines rights appropriate to using digital works (e.g., play and print)

RDDOnto (Garcia, Delgado, 2007)

- Example: *Act* hierarchy.



Possible values for terms

- **Principal**
  - AllPrincipals and KeyHolder
- **Rights**
  - Issue, Obtain, PossesProperty and Revoke
- **Resources**
  - DigitalResource, Revocable and ServiceReference
- **Conditions**
  - AllConditions, ExerciseMechanism, ExistsRight, Fullfiler, PrerequisiteRight, RevocationFreshness, ValidityInterval
    - CallForCondition
    - ExerciseLimit
    - FeeFlat
    - FeeMetered
    - FeePerInterval
    - FeePerUse
    - FeePerUsePrePay
    - SeekAproval
    - Territory
    - TrackQuery
    - TrackReport
    - TransferControl
    - ValidityIntervalFloating
    - ValidityIntervalStartsNow
    - ValidityTimeMetered
    - ValidityTimePeriodic

- Examples of Rights
  - Adapt
  - Delete
  - Diminish
  - Embed
  - Enhance
  - Enlarge
  - Execute
  - Install
  - Modify
  - Move
  - Play
  - Print
  - Reduce
  - Uninstall

Esempi di Licenze: creator to distrib

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- License model for giving right adapt to the distributor -->
<r:license xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" xmlns:mx="urn:mpeg:mpeg21:2003:01-REL-
    MX-NS" xmlns:r="urn:mpeg:mpeg21:2003:01-REL-R-NS" xmlns:sx="urn:mpeg:mpeg21:2003:01-REL-
    SX-NS" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:mpeg:mpeg21:2003:01-REL-R-NS ../schemas/rel-r.xsd
    urn:mpeg:mpeg21:2003:01-REL-SX-NS ../schemas/rel-sx.xsd urn:mpeg:mpeg21:2003:01-REL-MX-NS
    ../schemas/rel-mx.xsd">
    <r:grantGroup>
    <r:grant>  <r:keyHolder>  <r:info><dsig:KeyName>AXDID:Distributor</dsig:KeyName> </r:info>
               </r:keyHolder>
               <mx:adapt/>
                <mx:diReference><mx:identifier>AXOID:Identifier</mx:identifier> </mx:diReference>
          </r:grant>
    </r:grantGroup>
    <!--The license is issued by the creator.-->
    <r:issuer> <r:keyHolder> <r:info> <dsig:KeyName>AXCID:Creator</dsig:KeyName></r:info>
          </r:keyHolder>
    </r:issuer>
</r:license>
```

```
<r:grantGroup>
        <r:grant><r:keyHolder><r:info><dsig:KeyName>AXDID:Distributor</dsig:KeyName></r:info>
                </r:keyHolder>
                <r:issue/>
        <r:grantGroup>
                <r:grant>
                <mx:play/>
                <mx:diReference>      <mx:identifier>AXOID:Identifier</mx:identifier>
                </mx:diReference>
                <sx:feePerUse  xmlns:iso="urn:mpeg21:2003:01-REL-SX-NS:2003:currency">
                        <sx:rate>   <sx:amount>1.00</sx:amount>
                                <sx:currency>iso:EUR</sx:currency>
                        </sx:rate>
                </sx:feePerUse>
                </r:grant>
        </r:grantGroup>
        </r:grant>
</r:grantGroup>
<!--The license is issued by the Creator-->
<r:issuer><r:keyHolder>
        <r:info><dsig:KeyName>AXCID:Creator</dsig:KeyName></r:info></r:keyHolder>
</r:issuer>
```

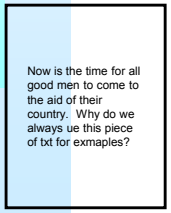
Riferimenti

- **CAS**
  - Irdeto: http://www.irdeto.com/
  - Nagravision: http://www.nagravision.com/
  - NDS: http://www.nds.com/
- **DRM**
  - MPEG-21: http://www.dsi.unifi.it/~nesi/DISIT-Introduction-to-MPEG-21-v1-0.pdf
  - AXMEDIS DRM for dummies: a full round into the content protection, production of licenses, etc.
  - http://www.axmedis.org
  - http://www.axmedis.org/documenti/view_documenti.php?doc_id=3964

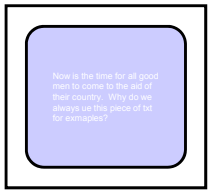
Rights Models: Types of Rights

Render Rights

Print



View



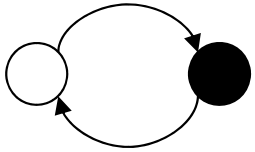
Play

Transport Rights

Copy

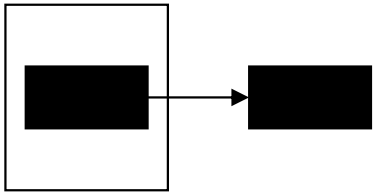
Move

Loan

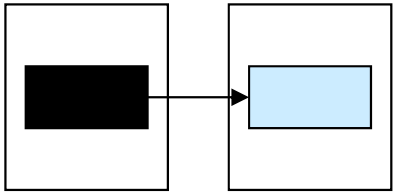


Derivative Work Rights

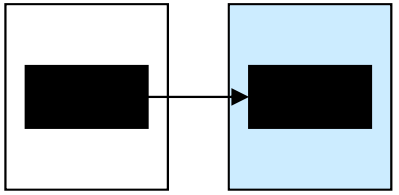
Extract



Edit

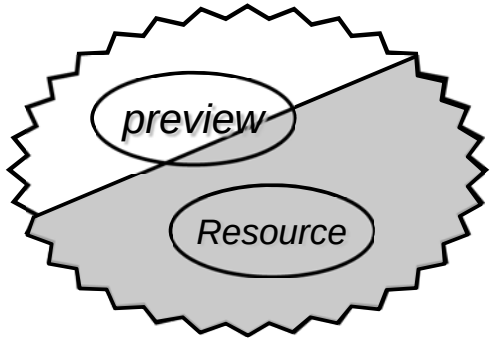


Embed

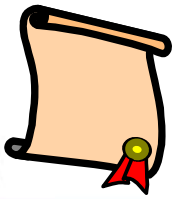


Business Rules, a way to formalize allowed rights

- Exploitation Models (contracts from the consumers to the provider are aligned to the exploitation model):
  - Subscription to a collection or service, per months, per year, etc.
    - All you can eat, per month, etc.
    - Pay per minute all you can eat
  - Pay per
    - rent, use, play, print, etc.
    - stream, download, etc…
    - burning the CD
    - copy the object
    - moving the object
    - passing the object to a different device/friend
    - building a collection
  - Preview without paying
  - Try and buy, e.g., 30 gg try, …
- Etc.

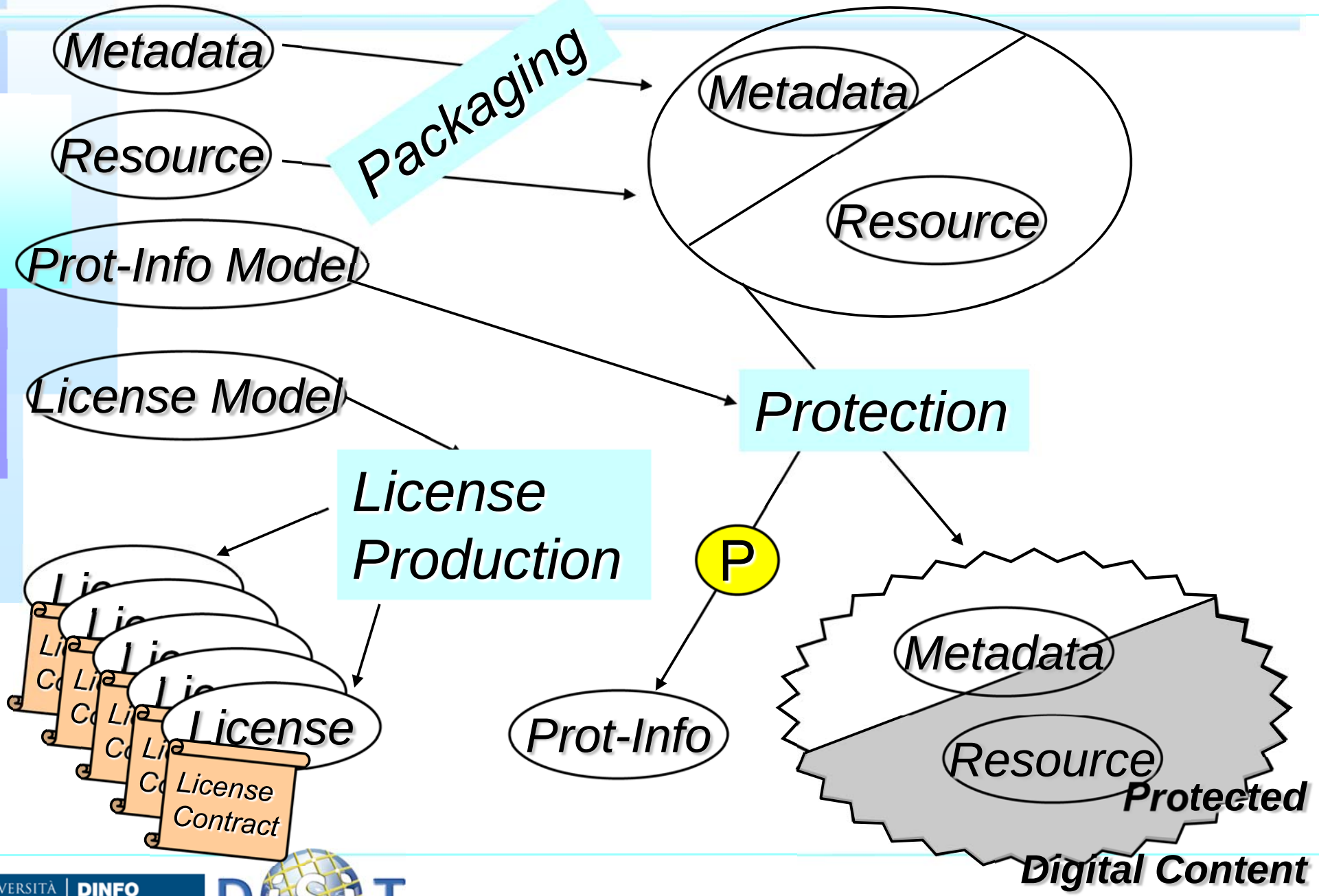


Business Rules, a way to formalize allowed rights

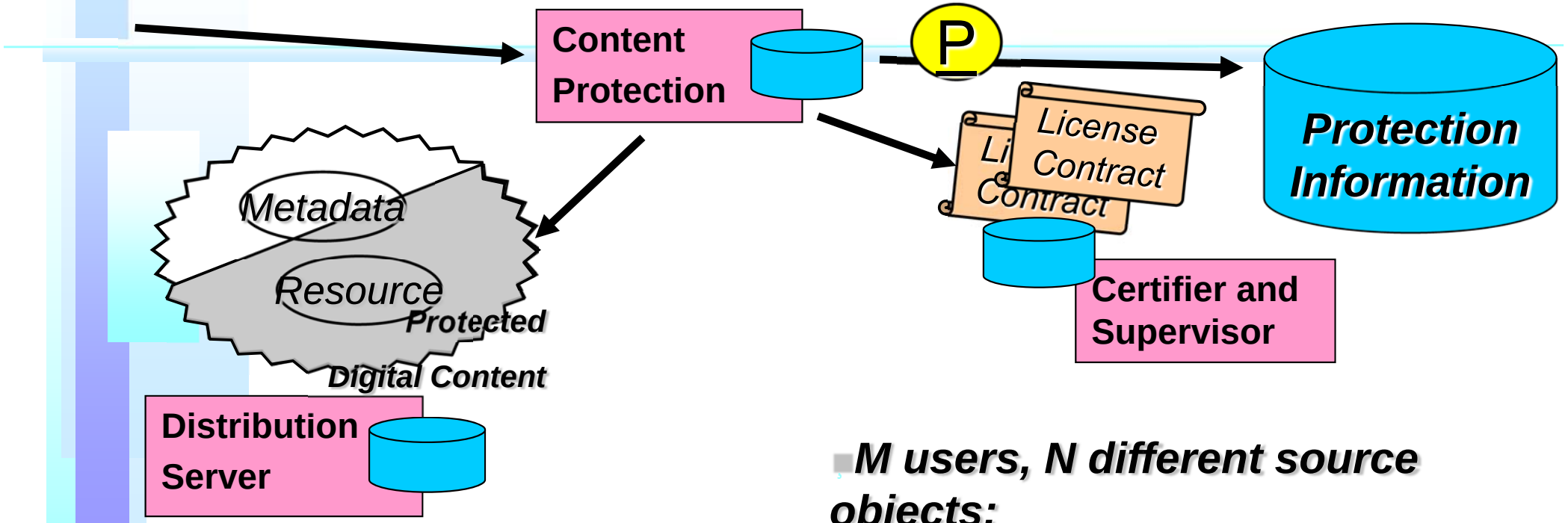


- It may be based on limiting
  - Number of times you can do an action, and usage
  - in a temporal window for the exploitation of any rights
    - renting
  - in a space
    - regional area or
    - domain (set of computers, etc.)
  - The usage according to the user profile:
    - impaired,
    - student,
    - Archival
    - etc.

Packaging and Protection, Open Model



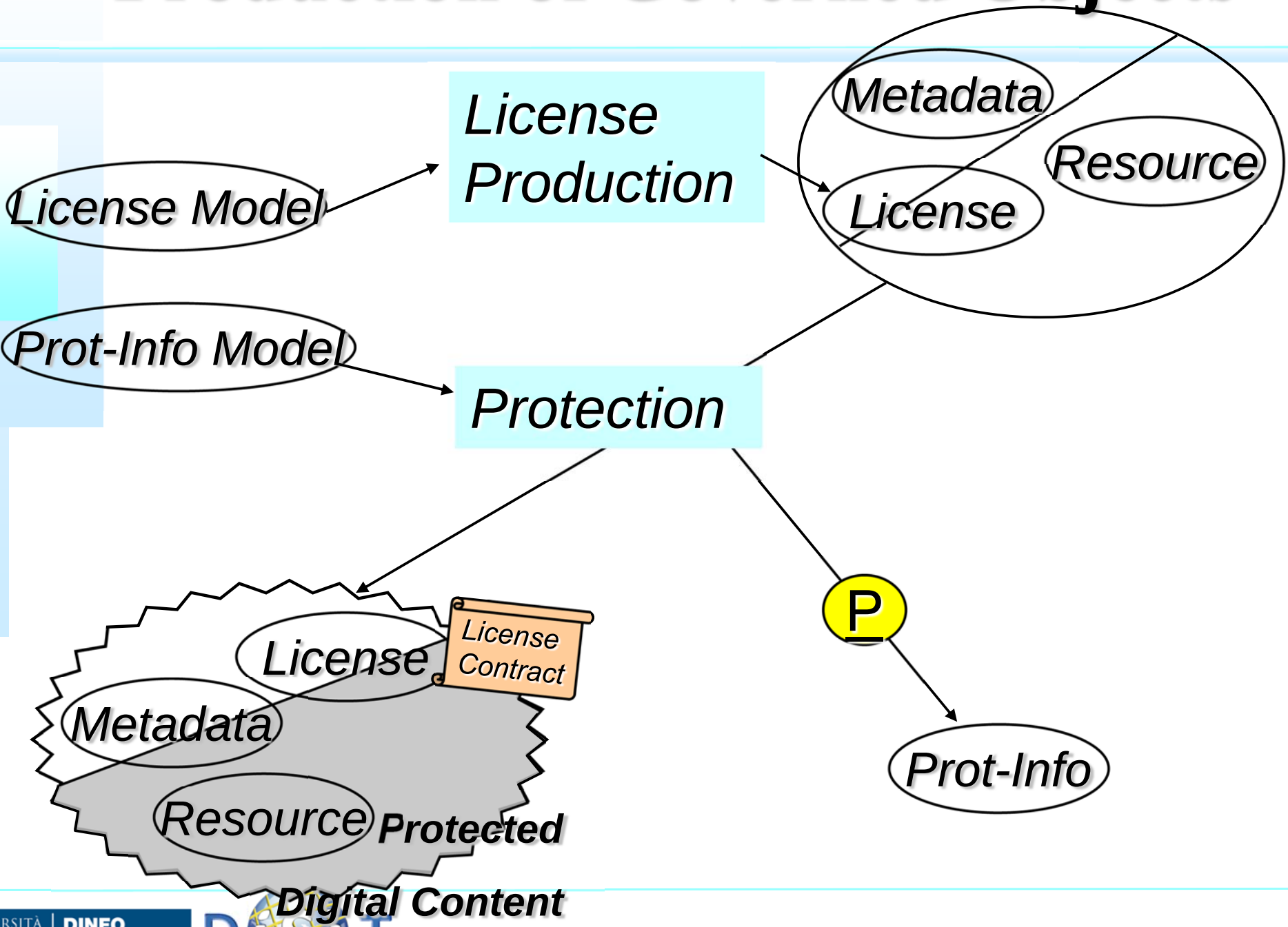
General Architecture of content business



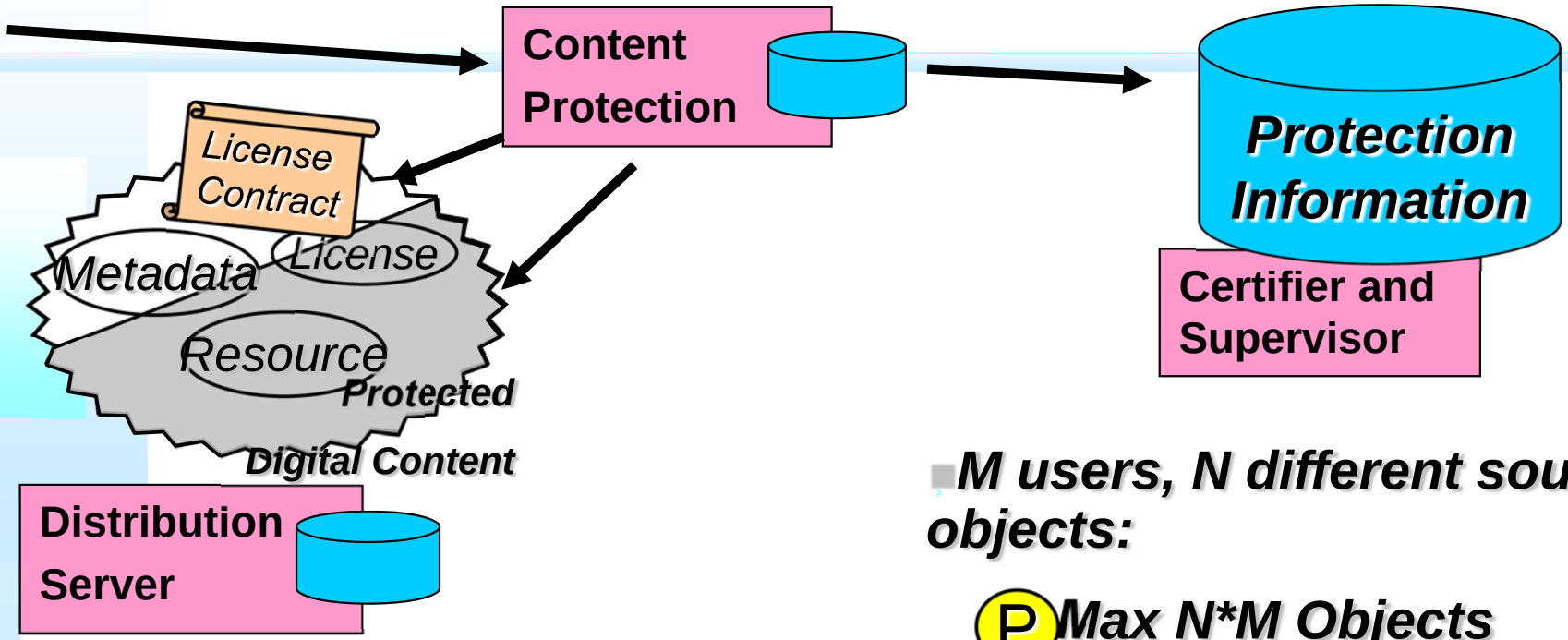
- *Pros:*
  - *Simple distribution*
  - *P2P supported*
- *Cons:*
  - *3 servers*
  - *Many Licenses*

- *M users, N different source objects:*
  - *N Objects protected only once*
  - *N protection info*
  - *M*N licenses maximum since each of them may be interested to have all objects*

Production of Governed Objects



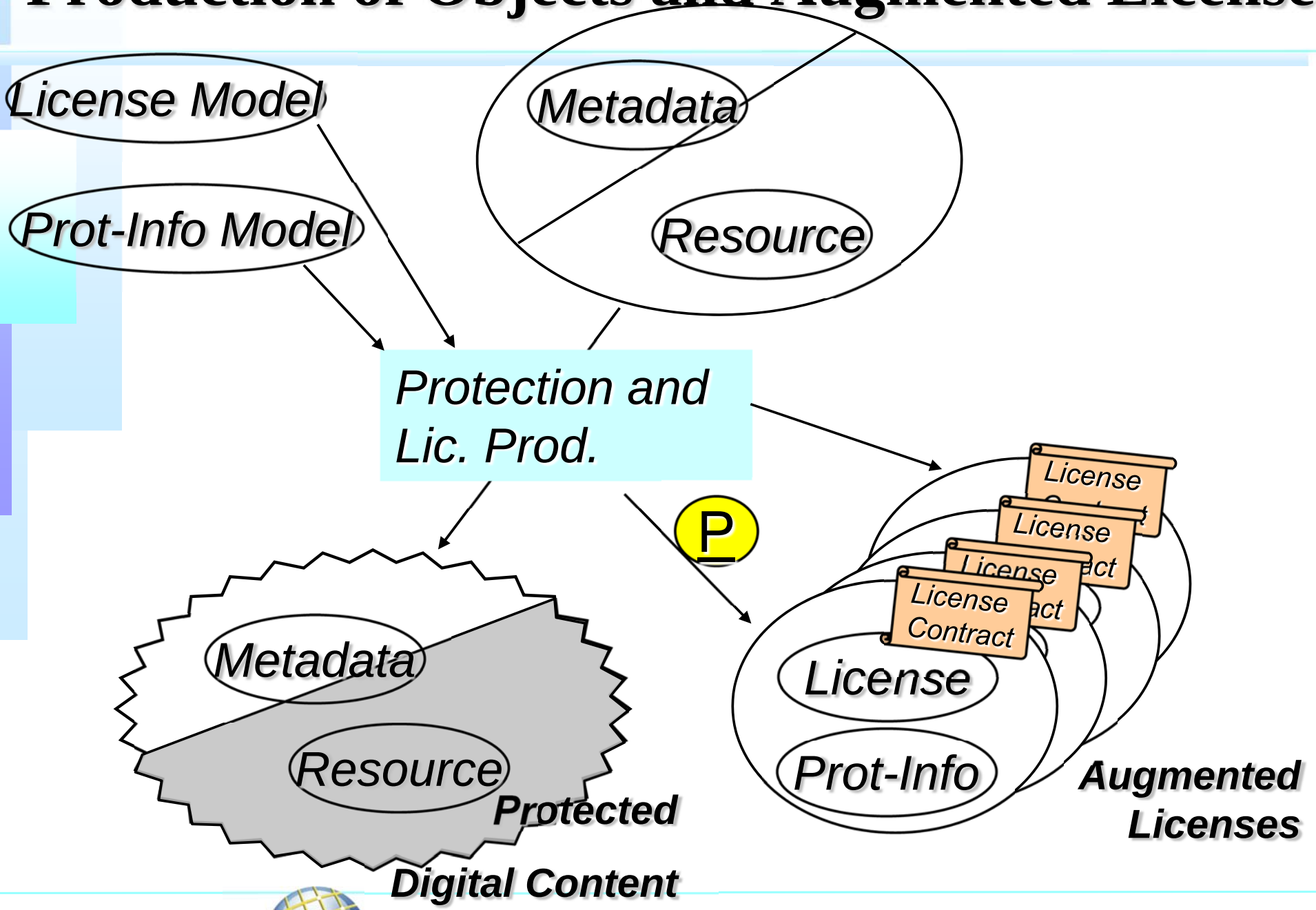
General Architecture of content business



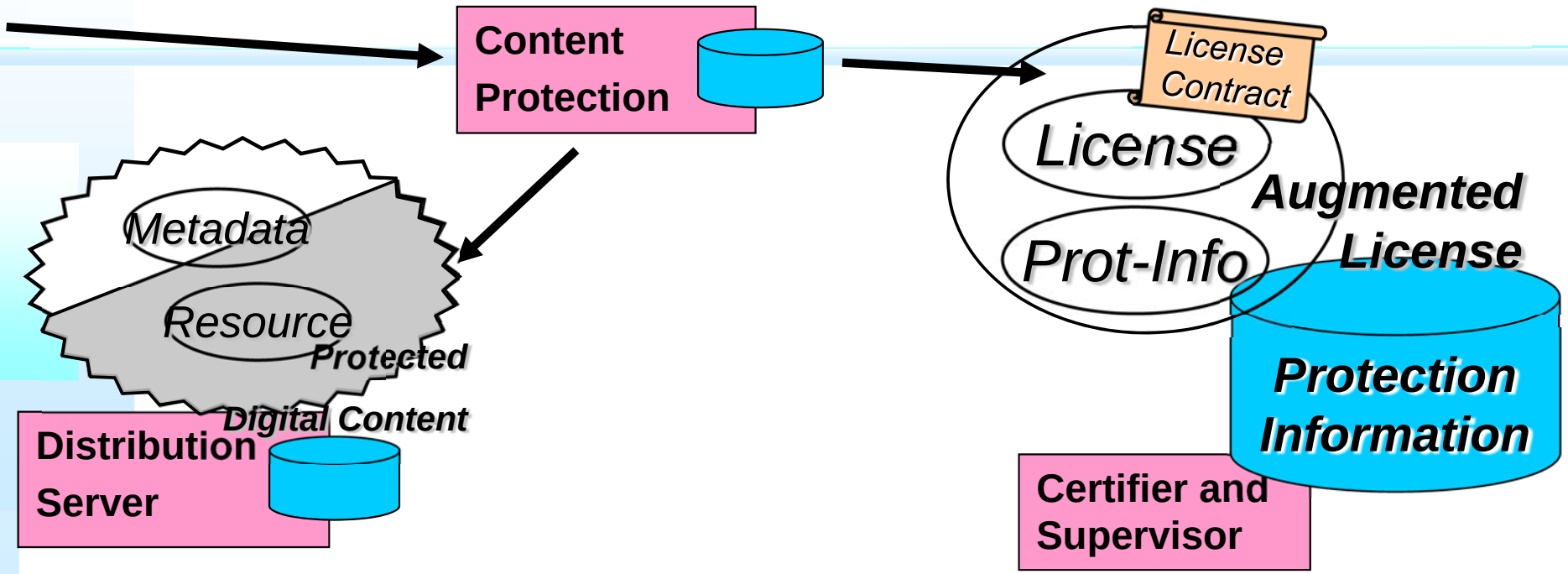
- *Pros:*
  - *Simple distribution, 2 servers*
- *Cons:*
  - *P2P non supported*
  - *Too many different objects, too much space*

- *M users, N different source objects:*
  - P *Max N*M Objects protected, that is for all the N Objects M different protected-licensed versions have to be produced*
  - P *N*M protection info*

Production of Objects and Augmented License



General Architecture of content business



- *Pros:*
  - *Simple distribution, 2 servers*
  - *P2P supported*
- *Cons:*
  - *Many information outside*
  - *Diff users have the same protection inform*

- *M users, N different source objects:*
  - *N Objects protected*
  - *N protection information*
  - *N*M protection info included into licenses*

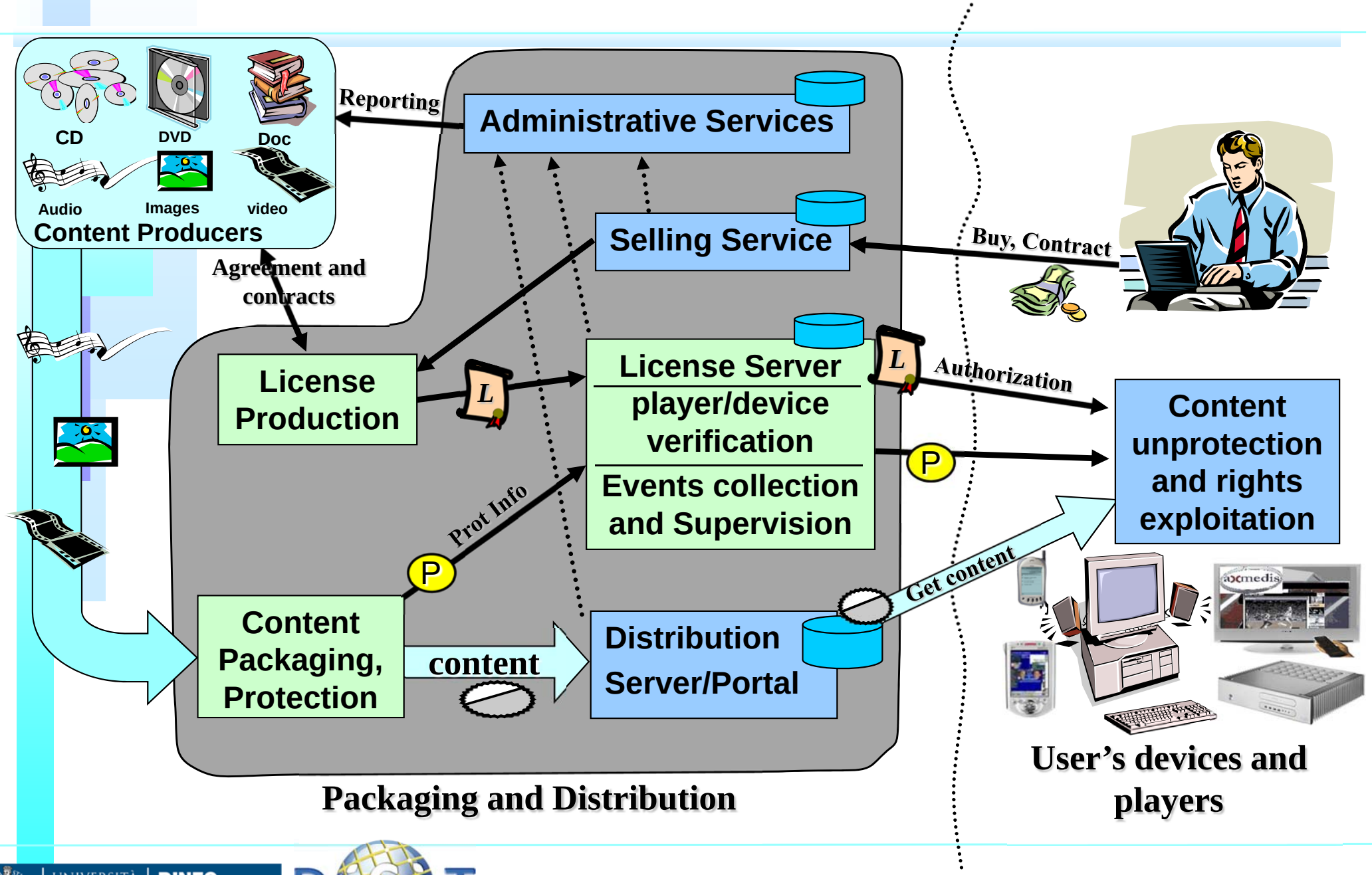
Some Considerations

- **Open Model**:
  - Supporting P2P
  - The volume of Objects is acceptable
  - The elements can be independently manipulated
    - Licenses can be changed, reissued
  - Suitable for B2B and B2C
- **Governed Object**:
  - The user may see what can be done on the objects on the basis of their license
  - the same object with different licenses implies
    - to produce too many objects
- **Augmented License:**
  - Supporting P2P
  - The license ha to include the same protection information
  - The objects can be substituted independently
    - Licenses can be changed, reissued

Open Model vs Augmented License

- **Pros** of **Open Model vs the Augmented License**
  - If the protected objects are used for producing several different more complex objects:
    - They are reused in the B2B area for different productions
    - Since the Protection Information is stored only once and not in every license, this implies to
      - have a more precise control of the black list, and
      - avoid duplications
  - Better for hierarchical nested protected and non prot objects
  - Thus the Open model is better for the B2B
- **Pros** of **Augmented License vs the Open Model**
  - Simpler management for the servers
  - Higher number of licenses
  - Suitable for simpler objects, non nesting protected objects
  - May be better for B2C

Based model for DRM



Different kinds of Packages

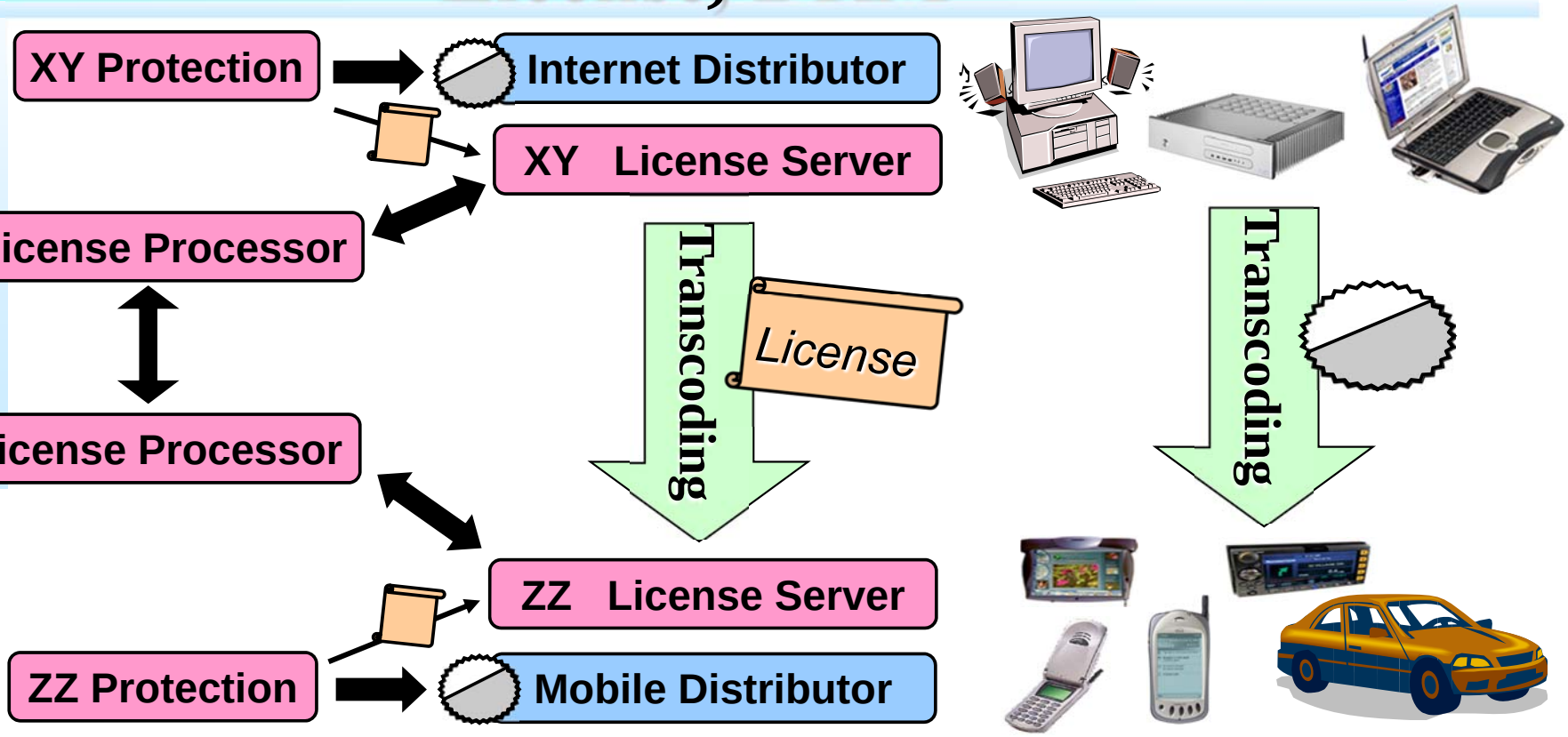
	Package	Protection	Which Files	Distribution models	Annotations	Metadata custom + descriptors
MPEG-21	Xml	Yes/DRM	any	Yes/DIS	(Yes)	Yes
MPEG-4	Yes (xml/bin)	Yes/CAS	Audio video	Yes/Stream	No	No
MXF	Yes (xml/bin)	No	Audio video	Download	No	Yes/No
SCORM/IMS	Yes (xml/bin)	Yes /CAS	any	Download	No	Yes
AXMEDIS	Yes (xml/bin)	Yes /DRM	any	Yes all	(Yes)	Yes
ZIP	Bin	Yes (pwd, CAS)	any	Download	No	No
NewsML	Yes (xml/bin)	Yes (Zip, Pwd, cas)	any	Download	No	Yes

DRM interoperability

- **iDRM: interoperable DRM means:**
  - Content that once under DRM can be moved/used from one device to another ?
- **But HOW ??**
  - Content that can be protected with multiple DRM on the same File? Different DRM enabled players use the same file.
  - Content that can be protected with multiple DRM with several files? Different DRM enabled players use different files.

- **For DMP:** iDRM means that there is only one DRM, and it is a standard for all. This is almost impossible today.
- **For DREAM, AXMEDIS**, etc.: iDRM means that multiple DRM can be applied on content and players may be used.

Es: Convergence, the Interoperable License, DRM



- When interoperable content in terms of format passes from two devices supporting different DRM models and licenses
- License needs to be transcribed and rights semantics preserved
- License chain processing need to be interoperable
- Two single channels DRM are typically disjoined

Major Related Organisations

- **Standardisation Bodies for elements**
  - MPEG (Motion Picture Expert Group), ISO
  - OMA (Open Mobile Alliance)
  - MI3P (ID and licensing aspects)
  - OASIS (Organisation for advancement in Structured Information Standards)
  - DVB (TV-AnyTime, DVB-T, DVB-H, DVB-S, ……)
  - W3C
- **Associations/organization:**
  - OeB (Open eBook Forum)
  - CRF (Content Reference Forum)
  - WIPO (World Intellectual Property Organization)
  - RIAA (Recording Industry Association of America)
  - WS-I (Web Services Interoperability Organisation)
  - ISMA (Internet Streaming Media Alliance)
  - CC (Creative Commons)
- **Projects on Architecture and Value chain solutions**
  - AXMEDIS Project, research and development project
  - DMP (Digital Media Project), standardisation project
  - Etc.

Example of Content Distributors web sites

- Apple i-Tune
  - Audio, video distribution, Proprietary DRM
- FastWeb
  - IPTV, Finsiel, NDS
- SKY (OpenSky), EUTELSAT
  - Video, MPEG4, Smart CARD
- TISCALI portali
  - Audio tracks and videos, Windows Media DRM
- DTT, DVB-T: MHP (MPEG-2 + Java)
  - Mediaset, La-7, RAI, ….., Smart Card: IRDETO, NAGRAVISION
- BuyMusic.com
  - SDMI, Windows Media DRM
- Real Networks
- ROXIO, Napster
  - Windows Media DRM
- Warner Music UK is using the **Share!**
  - Windows Media DRM
- Musicmatch.com
  - Windows Media DRM

Technologies and standards

- **Technologies for content protection**
  - Apple I-Tune
  - Media Commerce Suite of Real Network
  - EMMS of IBM
  - Liquid Audio
  - DMD secure
  - Sealed Media
  - Intertrust
  - Adobe, mainly limited to documents

- **DRM solutions**
  - Microsoft Windows Media, DRM
    - → XrML, Content Guard, related to MPEG-21
  - OMA DRM, Open Mobile Association
  - AXMEDIS/MPEG-21
    - → MPEG-21 smaller cases

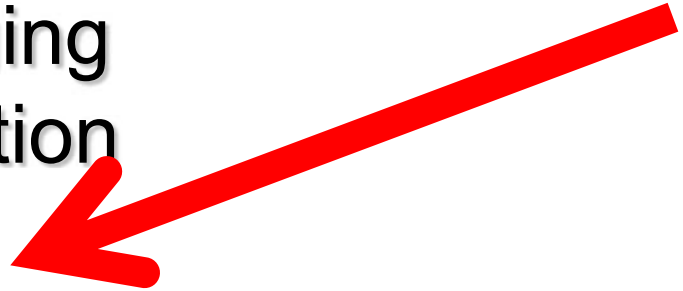
Considerations

Model	privacy	Security level	TRU satisfaction	Suitable for Mobile	Suitable for UGC
CP	Yes	Low	Low	High	High
CAS/STB	Yes/No	Medium	Low	High	no
CAS/PC	Yes/No	Low	Low	High	no
DRM	No/yes	none	High	Medium	Medium
DRM+TPM	No/yes	High		Medium	Medium

- *TRU: traditional rights usage*
- *UGC: user generated content*
- *TPM: technological protection model*

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Example of Microsoft Windows Media



Creative Commons, CC

- Nel commercio elettronico e' necessario includere anche alcune slide relative alle licenze CC.
- Fino ad ora abbiamo visto tecnologia al servizio della protezione della proprieta' intellettuale
- CC mette a disposizione degli strumenti, dei formalismi legali che possono essere o meno adottati da chi pubblica i propri contenuti
- Questi sono license formalizzate:
  - **Struttura della Licenza CC:**
    - Legal Code: testo legale che la descrive
    - Commons Deed: short description della licenza
    - Digital Code: metadati da associare

    (see S. Aliprandi, 2005, 2006…)

http://www.copyleft-italia.it/cc/brochureCCv2.pdf

Creative Commons, CC

- ***Le licenze CC***
  - Nate in USA
  - Sono state adattate alla legislazione nazionale di diversi stati e anche a livello europeo
    - specialmente per contenuti generati dagli utenti e in ambito culturale
    - Questo permette in un certo qual modo di avere una trascodifica fra le questioni legali nazionali e quelle di altre nazioni, ma solo per certe questioni.
  - Licenze CC ipotizzano uno share, copyleft
- E' stato fatta una codifica delle licenze CC in MPEG-21 REL
  - Non e' vero l'opposto, tutte le licenze che si possono formalizzare in MPEG-21 non hanno una controparte in CC

Le tre forme delle licenze

Ogni licenza Creative Commons si manifesta sotto tre forme differenti. La licenza vera e propria è detta **Legal Code**: è un testo piuttosto denso di concetti giuridici, abbastanza lungo e tendenzialmente comprensibile a coloro che hanno una formazione di tipo giuridico. E' questa la licenza che verrà esaminata dal giudice qualora emergesse una controversia legale sull'uso dell'opera licenziata. Tuttavia, Creative Commons ha pensato anche di riassumere i concetti essenziali delle licenze in versioni sintetiche (i cosiddetti **Commons Deed**) facili da capire anche per i semplici utenti e contraddistinti da efficaci *visuals*. Inoltre, ogni licenza è convertibile in alcune righe di linguaggio informatico (il cosiddetto **Digital Code**) che fungono da *metadati*, ovvero da informazioni digitali che permettono ai motori di ricerca di individuare e riconoscere correttamente l'opera che li contiene.

Traduzione e adattamento

L'ente statunitense Creative Commons ha affidato ad alcuni gruppi di lavoro (dislocati nei vari paesi che hanno aderito al progetto) il compito di effettuare il ***porting*** delle licenze: cioè, non una semplice traduzione linguistica delle licenze, ma una traduzione ragionata, in modo che le licenze potessero esplicare gli stessi effetti anche in paesi con sistemi giuridici diversi da quello americano. L'autore quando sceglie la licenza, infatti, se vuole, può anche indicare una giurisdizione preferenziale, cioè il contesto giuridico a cui vuole fare riferimento. In questo modo, alla luce dei principi di diritto internazionale, si cerca di ovviare ad eventuali problemi di interpretazione e di scelta delle fonti normative applicabili al caso concreto.

Come applicare una licenza CC

Il concetto è semplicissimo: poiché il modello tradizionale e standardizzato è quello "tutti i diritti riservati", se vogliamo applicare un modello alternativo dobbiamo segnalarlo esplicitamente. Possiamo ad esempio utilizzare un disclaimer di copyright come quello che trovate nella pagina successiva di questa brochure, in cui indicare con chiarezza chi è il titolare dei diritti d'autore e quale licenza ha scelto per la sua opera. Nient'altro! Non sono necessarie particolari formalità di registazione o certificazione da parte di nessun ente.

Sul sito ufficiale Creative Commons sono poi disponibili informazioni più specifiche per l'inserimento della licenza in versione *digital code* nei file digitali con cui l'opera circolerà.

Come trovare opere sotto licenze CC

In generale è possibile utilizzare lo specifico motore di ricerca che si trova al sito **http://search.creativecommons.org** ;
oppure fare riferimento ad archivi on-line come:

- http://sciencecommons.org/ (letteratura scientifica);
- www.jamendo.com (musica);
- http://ccmixter.org/ (musica, suoni e campionature musicali);
- www.flickr.com/creativecommons (immagini);
- www.spinxpress.com/getmedia (video e contenuti multimediali);
- http://ocw.mit.edu/ (materiale didattico e manualistica);
- commons.wikimedia.org (opere varie).

Per saperne di più...

...oltre a navigare attentamente sui siti ufficiali di Creative Commons e a frequentare le mailing list pubbliche della community (www.creativecommons.it/Liste), potete leggere la voce "Creative Commons" su www.wikipedia.org e le voci ad essa correlate; navigare sul sito www.copyleft-italia.it/cc e leggere le pubblicazioni liberamente scaricabili dal sito www.copyleft-italia.it/pubblicazioni, fra cui si segnalano principalmente:

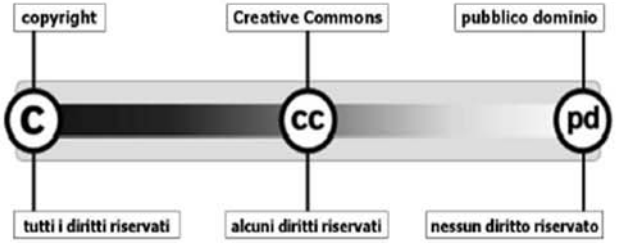
- Aliprandi, Copyleft & opencontent. L'altra faccia del copyright (ed. PrimaOra, 2005);
- Aliprandi (a cura di), Compendio di libertà informatica e cultura open (ed. PrimaOra, 2005);
- Aliprandi, Teoria e pratica del copyleft. Guida all'uso delle licenze opencontent (ed. NDA Press, 2006);
- Aliprandi, Capire il copyright. Percorso guidato nel diritto d'autore (ed. PrimaOra, 2007);
- Lessig, Cultura libera (ed. Apogeo, 2005).

Brochure a scopo divulgativo realizzata da Simone Aliprandi per il Progetto Copyleft-Italia.it nel gennaio 2008. Parte del materiale qui riportato è tratto dai siti ufficiali Creative Commons e dall'opera "Il copyleft in tasca. Vademecum con i concetti base del copyleft" (www.copyleft-italia.it/vademecum).

L'URL originario di questo documento è: www.copyleft-italia.it/cc .

creative commons

un copyright flessibile per opere creative



www.creativecommons.org
www.creativecommons.it

Brochure a scopo divulgativo a cura del Progetto Copyleft-Italia.it

c©pyleft-italia.it
www.copyleft-italia.it

NUOVI MODELLI PER IL DIRITTO D'AUTORE

info@copyleft-italia.it - myspace.com/copyleftitalia

Che cos'è Creative Commons (e cosa non è)

[tratto da www.creativecommons.it/cosa-fa-cc]

Le Creative Commons Public Licenses (CCPL) sono delle licenze di diritto d'autore che si basano sul principio de "alcuni diritti riservati". Le CCPL, infatti, rendono semplice, per il titolare dei diritti d'autore, segnalare in maniera chiara che la riproduzione, diffusione e circolazione della propria opera è esplicitamente permessa.

Il funzionamento delle CCPL è reso possibile dal fatto che la legge italiana sul diritto d'autore - così come, in generale, le corrispondenti normative nazionali e internazionali - riconosce al creatore di un'opera dell'ingegno una serie di diritti; allo stesso tempo, la legge permette al titolare di tali diritti di disporne liberamente.

Uno dei modi in cui ciò si può fare è il meccanismo contrattuale della licenza, tramite cui il titolare dei diritti (il cosiddetto "licenziante") concede o meno alcuni diritti alla controparte (il cosiddetto "licenziatario") ovvero qualsiasi fruitore dell'opera. E` importante sottolineare come le CCPL, e in generale tutte le licenze di diritto d'autore, non siano la fonte dei diritti in oggetto: è grazie alla legge che tali diritti sorgono. Le CCPL sono solo uno strumento tramite cui il titolare dei diritti concede determinati permessi ai licenziatari.

Tali permessi sono flessibili e possono essere vincolati ad alcune condizioni, a seconda del tipo di licenza scelta dall'autore.

Le CCPL sono state create negli Stati Uniti dall'associazione non-profit Creative Commons. Sono state quindi tradotte in italiano e adattate al nostro sistema giuridico da un gruppo di lavoro coordinato dal prof. Marco Ricolfi del Dipartimento di Scienze Giuridiche dell'Università di Torino. Dal gennaio 2005 il referente per Creative Commons Italia è il prof. Juan Carlos De Martin del Dipartimento di Automatica e Informatica del Politecnico di Torino, coadiuvato per le questioni di natura legale dal gruppo di giuristi che ha effettuato l'adattamento originario delle licenze.

Creative Commons Italia promuove l'uso delle licenze Creative Commons e la riflessione sulle motivazioni che hanno portato alla loro creazione, ma non svolge attività di consulenza legale, né di registrazione, archiviazione o catalogazione di opere dell'ingegno, siano esse rilasciate sotto una licenza Creative Commons o meno.

Le licenze Creative Commons

Caratteristiche

[tratto da www.creativecommons.it/Licenze/Spiegazione]

Ogni licenza richiede che il licenziatario:

- ottenga il tuo permesso per fare una qualsiasi delle cose che hai scelto di limitare, per esempio, usi commerciali, o creazione di un'opera derivata;
- mantenga l'indicazione di diritto d'autore intatta su tutte le copie del tuo lavoro;
- faccia un link alla tua licenza dalle copie dell'opera;
- non alteri i termini della licenza;
- non usi mezzi tecnologici per impedire ad altri licenziatari di esercitare uno qualsiasi degli usi consentiti dalla legge.

Ogni licenza permette che i licenziatari, a patto che rispettino le tue condizioni:

- copino l'opera;
- distribuiscano l'opera;
- comunichino al pubblico, rappresentino, eseguano, recitino o espongano l'opera in pubblico, ivi inclusa la trasmissione audio digitale dell'opera;
- cambino il formato dell'opera.

Struttura

Le licenze Creative Commons si strutturano idealmente in **due parti**: una prima parte in cui si indicano quali sono le **libertà** che l'autore vuole concedere sulla sua opera; e una seconda parte che chiarisce a quali **condizioni** è possibile utilizzare l'opera.

PRIMA PARTE - Le libertà per l'utente

Tutte le licenze consentono la copia e la distribuzione dell'opera:

Tu sei libero di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare quest'opera.

Alcune licenze consentono anche la modifica dell'opera:

Tu sei libero di modificare quest'opera.

SECONDA PARTE - Le condizioni per l'utilizzo dell'opera

Le licenze Creative Commons si articolano in **quattro clausole base**, che l'autore può scegliere e combinare a seconda delle sue esigenze.

Attribuzione *- Devi riconoscere la paternità dell'opera all'autore originario.* [1]

[1] Questa clausola è presente *di default* in tutte le licenze. Essa indica che, ogni volta che utilizziamo l'opera, dobbiamo segnalare in modo chiaro chi è l'autore.

Non commerciale *- Non puoi utilizzare quest'opera per scopi commerciali.* [2]

[2] Significa che, se distribuiamo copie dell'opera, non possiamo farlo in una maniera tale che sia prevalentemente intesa o diretta al perseguimento di un vantaggio commerciale o di un compenso monetario privato. Per farne tali usi, è necessario chiedere uno specifico permesso all'autore.

Non opere derivate *- Non puoi alterare, trasformare o sviluppare quest'opera.* [3]

[3] Quindi se vogliamo modificare, correggere, tradurre, remixare l'opera, dobbiamo chiedere uno specifico permesso all'autore originario.

Condividi allo stesso modo *- Se alteri, trasformi o sviluppi quest'opera, puoi distribuire l'opera risultante solo per mezzo di una licenza identica a questa.* [4]

[4] Questa clausola (un po' come succede nell'ambito del software libero) garantisce che le libertà concesse dall'autore si mantengano anche su opere derivate da essa (e su quelle derivate dalle derivate, con un effetto a cascata).

Le attuali sei licenze

Attribuzione
Attribuzione-NonOpereDerivate
Attribuzione-NonCommericale-NonOpereDerivate
Attribuzione-NonCommerciale
Attribuzione-NonCommerciale-CondividiAlloStessoModo
Attribuzione-CondividiAlloStessoModo

Ogni Licenza chiede che il Licensiatario

- Ottenga il tuo permesso per fare una qualsiasi delle cose che
  - hai scelto di limitare con la licenza,
  - for example: limitare gli usi commerciali o quelli di opera derivata
- Mantenga l'indicazione di diritto di autore intatta su tutte le copie del tuo lavoro
- Faccia un link alla tua licenza dalle copie dell'opera
- Non alteri i termini della licenza
- Non usi mezzi tecnologici per impedire ad altri licenziatari di esercitare uno qualsiasi degli usi consentiti dalla legge

Ogni licenza CC permette le seguenti azioni a patto che:

i licenziatari rispettino le condizioni della licenza CC assegnata:

- Possono
  - Copiare l'opera;
  - Distribuire l'opera;
  - Comunicare al pubblico, rappresentare, esegure, recitare o esporre l'opera in pubblico, ivi inclusa la trasmissione audio digitale dell'opera;
  - Cambiare il formato dell'opera.

Alcuni marker CC

Liberta' per l'utente

- Sei libero di distribuire, comunicare, rappresentare, eseguire, recitare o esporre l'opera in pubblico, ivi inclusa la trasmissione audio digitale dell'opera;

- Sei libero di modificare questa opera

Condizioni di uso

- Devi riconoscere la paternita' di questa opera
- Per esempio citando e riportanto un link alla sorgente

Licenze Creative Commons

- Offrono 6 diverse articolazioni
  - per artisti, giornalisti, docenti, istituzioni e, in genere, creatori che desiderino **condividere in maniera ampia** le proprie opere secondo il modello **"alcuni diritti riservati"**.

- **Altre condizioni d'uso, il detentore dei diritti puo'**

  - non autorizzare a priori **usi prevalentemente commerciali** dell'opera (opzione *Non commerciale*, acronimo inglese: *NC*)

  - non autorizzare la creazione di **opere derivate** (*Non opere derivate*, acronimo: *ND*); no extract, no aggregate, ..

  - Imporre di rilasciarle **con la stessa licenza dell'opera originaria** (*Condividi allo stesso modo*, acronimo: *SA*, da "Share-Alike").

Le combinazioni di queste scelte generano 6 licenze CC, disponibili anche in versione italiana, come descritto in seguito!

2 of the 6 CC licenses, 1/3

Attribution Non-commercial No Derivatives (by-nc-nd)

- The most restrictive of our six main licenses, allowing redistribution.
- This license is often called the “free advertising” license
- *it allows others to download your works and share them with others as long as they mention you and link back to you*,
- they can’t change them in any way or use them commercially

Attribution Non-commercial Share Alike (by-nc-sa)

- *Let others remix, tweak, and build upon your work non-commercially, as long as they credit you and license their new creations under the identical terms.*
- Others can download and redistribute your work just like the by-nc-nd license, but they can also translate, make remixes, and produce new stories based on your work.
- All new work based on yours will carry the same license, so any derivatives will also be non-commercial in nature.

2 of the 6 CC licenses, 2/3

- **Attribution Non-commercial (by-nc)**
  - Let others remix, tweak, and build upon your work non-commercially, and their new works must also acknowledge you and be non-commercial,
  - they don't have to license their derivative works on the same terms.

- **Attribution No Derivatives (by-nd)**
  - allows for redistribution, commercial and non-commercial,
  - as long as it is passed along unchanged and in whole, with credit to you

2 of the 6 CC licenses, 3/3

Attribution Share Alike (by-sa)

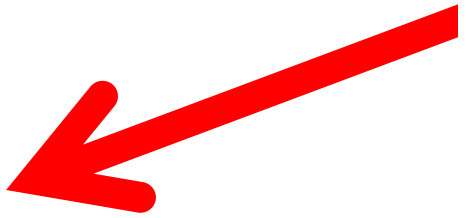
- *lets others remix, tweak, and build upon your work even for commercial reasons, as long as they credit you and license their new creations under the identical terms.*
- This license is often compared to open source software licenses.
- All new works based on yours will carry the same license, so any derivatives will also allow commercial use.

Attribution (by)

- *lets others distribute, remix, tweak, and build upon your work, even commercially, as long as they credit you for the original creation.*
- This is the most accommodating of licenses offered, in terms of what others can do with your works licensed under Attribution.

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Example of Microsoft Windows Media



Windows Media DRM

- **Composto da:**
  - Player (client), Windows Media Player
  - Encoder/packager (content production)
    - Uso di codec vari, MPEG, etc.
  - Server (distribution Server)
  - DRM model
  - Streaming and Download

- **Realizzazione** di soluzioni varie da 2-tier a n-tier
  - Soluzioni basate su cluster di server

Windows Media Ecosystem

Windows Media 9 Series

Business

Content Creation

Processing

Content Packaging

Distribution

License Clearinghouse

Authorization

Web Retailer

- Download
- Streaming

Acquisition

Transaction

Consumer

Portable Devices

Transfer

Home Devic

Sample Applications For WM Technology

- **Consumer Electronics Devices**
  - Portable audio and video players
  - CD and DVD players and burners
  - Digital Media Receivers
  - Mobile Phones
  - Set Top Boxes
- **IC Manufacturers, Technology Suppliers**
  - Chips with WM Codec or DRM built in
  - Ported versions of WM components for OEM use
- **PC Applications**
  - Media Players, Jukeboxes
- **Media Services Infrastructure**
  - Streaming media servers, web servers
  - License Servers (for Digital Rights Management)
  - Content Creation and DRM Encryption Servers

WM Streaming Experience

- **Benefit**
  - Eliminates buffering delays
  - Optimizes the experience
- **Features**
  - Fast Streaming
  - Improved packet recovery techniques
  - Improved multi-bitrate (MBR) audio/video
  - Bandwidth detection improvements
  - Support for standards-based protocols
  - Requires the 9 Series player to obtain benefits

Industrial Strength, scalable

- WMS 9 Series far more scalable than 4.1
  - Greatly improved TCP performance (2x)
  - Greatly improved broadband performance (2x)
  - Dramatically better disk i/o by caching frequently accessed content (2x-8x+)
  - 20,000 streams (using 20 Kbps content) achieved on a single machine
  - 900 Mbps of total throughput (using 1 Mbps content) achieved on a single machine
- Updated load simulation tool on Web

Windows Media Ecosystem

Windows Media 9 Series

Business

Artists
Create intellectual property, digital media content
Windows Media Encoder

License

Solution Providers
Issue Licenses Track Transactions
Windows Media Rights Manager SDK

Consumer

Hardware Vendors
Transfer and Play Protected Media
"PD DRM" *WinCE Platform Builder* *WM DRM for Devices* *WM DRM for Networks*

Processing

Labels, Studios, Publishers, …
Protect Compressed Digital Work
Windows Media Encoder

Authorization

Solution Providers
Host & Distribute Protected Digital Work
Windows Streaming Media Server or Web Server

Transaction

Application Developers
Render Protected Digital Work, Transfer to Devices
Windows Media Format SDK, Windows Media Device Manager

How it works

1. Packaging
2. Rights
3. Distribution
4. License Acquisition
5. License Delivery

Packaging

- Generate Content Header:
  - Key ID
    A String to identify content and generate the KEY
  - License Acquisition URL
    Location that specifies where to get licenses from
  - Individualisation Version
    Minimum Individualisation a player must have to play the content
  - Content ID
    Uniquely identifies the file
  - Additional Attributes
    Provides additional information for packaging and managing file

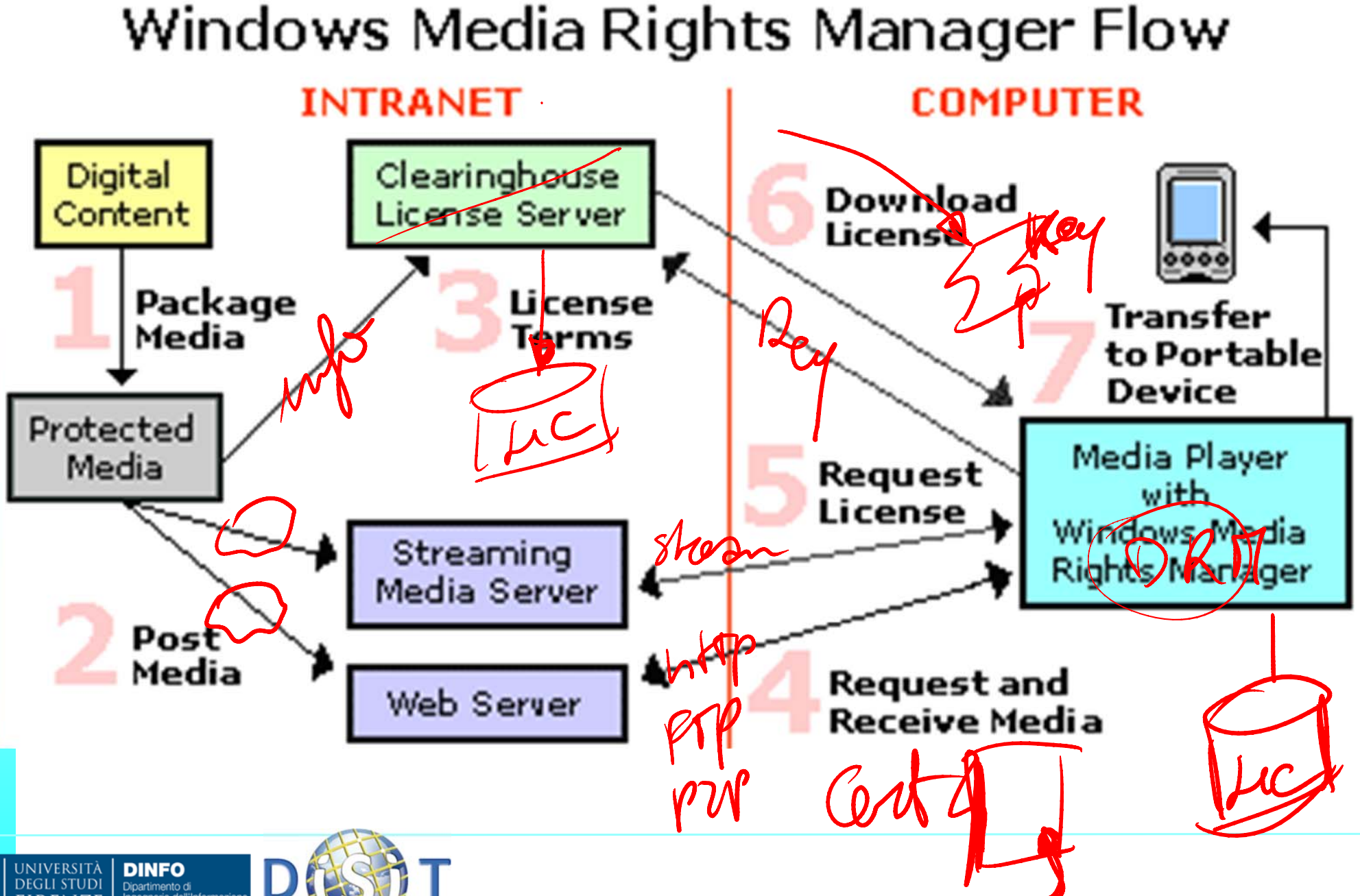
Packaging

- Sign The Header
  - Private Signing Key
    To prevent the header from tampering (Kept secret)
- Generate the KEY
  - Key ID
    Stored in the content header (public)
  - License Key Seed
    Kept secret and not stored in content header (private)
  - Key ID + License Key Seed = KEY
- Encrypt the file using the KEY

Packaging

- Input formats
  - Any input source that can be converted to Windows Media Format
  - WAV
  - AVI
- Output formats (Binary):
  - WMA
  - WMV

Windows Media Rights Manager



Windows Media Rights Manager

Packaging

- Windows Media Rights Manager packages the digital media file.
- The packaged media file has been encrypted and locked with a "key."
  - *This key is stored in an encrypted license, which is distributed separately.*
- Other information is added to the media file, such as the URL where the license can be acquired.
- This packaged digital media file is saved in Windows Media Audio format (with a .wma file name extension) or Windows Media Video format (with a .wmv file name extension).

Windows Media Rights Manager

Establishing a License Server

- The content provider chooses a license clearing house that stores the specific rights or rules of the license and implements the Windows Media Rights Manager license services.
- The role of the *clearing house* is to **authenticate** the consumer's request for a license.
- Digital media files and licenses are distributed and stored separately, making it easier to manage the entire system.

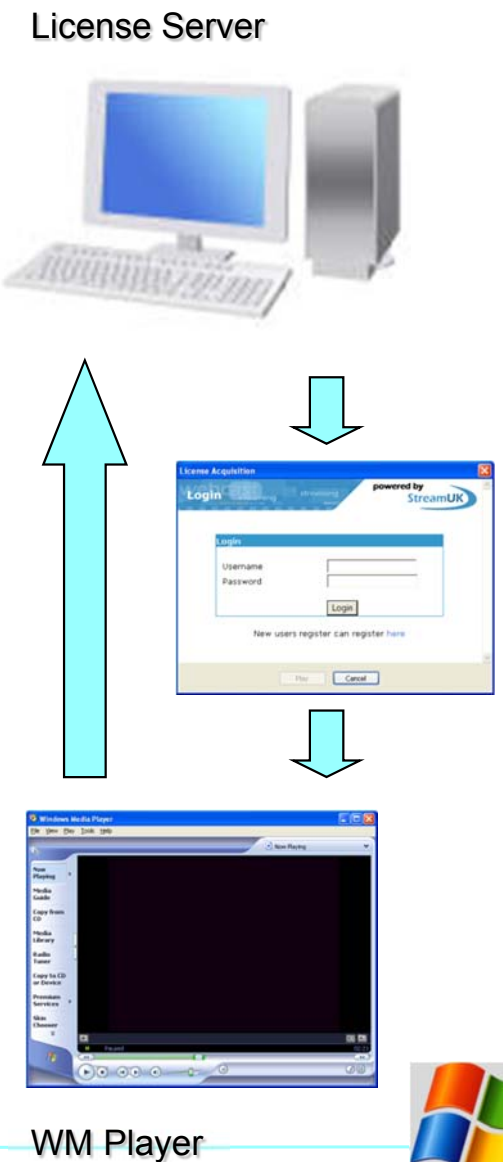
Windows Media Rights Manager

License Acquisition

- To play a packaged digital media file, the consumer must first acquire a license key to unlock the file.
- The process of acquiring a license begins automatically when the consumer attempts to acquire the protected content, acquires a predelivered license, or plays the file for the first time.
- Windows Media Rights Manager either sends the consumer to a registration page where information is requested or payment is required, or "silently" retrieves a license from a clearing house.

License Acquisition

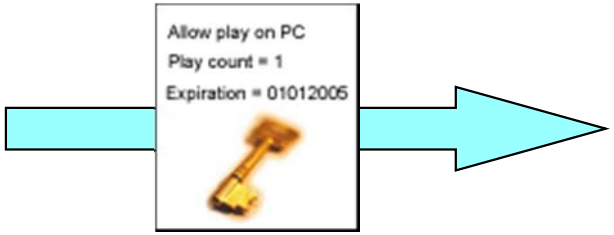
- Process of authenticating user
  Does this user have a right to view the content?
- Depends on business model
- Examples include:
  - Payment
  - Login
  - One time access codes
  - Free, no authentication

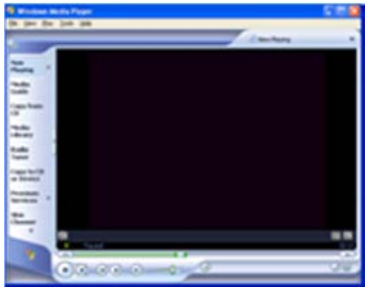


License Delivery

- Get the content
- Verify the content header with the Public Signing Key
- Generate the KEY
  - Get the Key ID from the content header
  - Get the License Key Seed from the system
- Specify the rights for the license, ask it
- Deliver the license containing the KEY and rights

License Server





License Delivery

- A license is delivered ONLY if the user is authorised to view the content

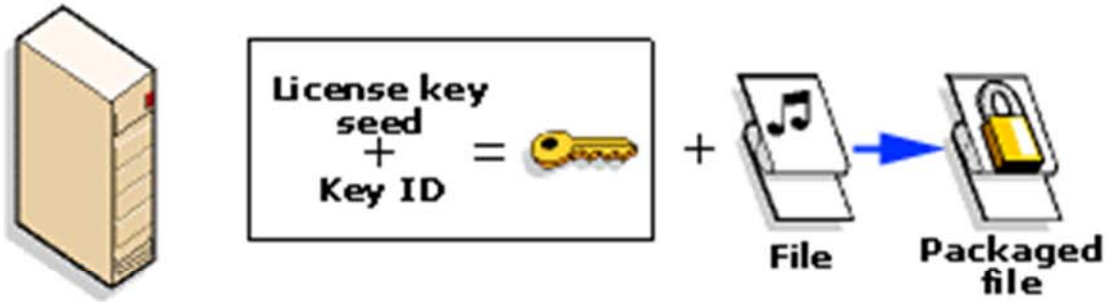
- **Post Delivery:**
  1. Content is distributed first
  2. License delivered second

- **Pre delivery:**
  1. License is delivered first
  2. Content is distributed second

Windows Media Rights Manager

Playing the Media File

- To play the digital media file, the consumer needs a media player that supports Windows Media Rights Manager.
- The consumer can then play the digital media file according to the rules or rights that are included in the license.
- Licenses can have different rights, such as start times and dates, duration, and counted operations.
  - For instance, default rights may allow the consumer to play the digital media file on a specific computer and copy the file to a portable device.
- Licenses, however, are not transferable. If a consumer sends a packaged digital media file to a friend, this friend must acquire his or her own license to play the file.
- This PC-by-PC licensing scheme ensures that the packaged digital media file can only be played by the computer that has been granted the license key for that file.


Content owner
License key seed + Key ID =
+
File
Packaged file


License clearing house
License key seed + Key ID from packaged file =
Windows Media License Service
License


Consumer's player
Packaged file
+
License
Consumer plays music

Microsoft Windows Media Rights Manager License

- license contains the
  - key to unlock the Windows Media file.
  - rights, or rules, that govern the use of the digital media file.
  - (model based on Augmented License)
- content owner sets rights to determine which actions are allowed from minimal control over playback to more restrictive licenses.
- licenses can support different business rules, including:
  - How many times can a file be played.
  - Which devices a file can be played or transferred on. For example, rights can specify if consumers can transfer the file to portable devices that are compliant with the Secure Digital Music Initiative (SDMI).
  - When the user can start playing the file and what is the expiration date.
  - If the file can be transferred to a CD recorder (burner).
  - If the user can back up and restore the license.
  - What security level is required on the client to play the Windows Media file.
  - And many others.

Windows Media DRM?

- Allow Backup Restore
- Allow Burn To CD
- Allow Play On PC
- Allow Transfer To Non SDMI
- Allow Transfer To SDMI
- Begin Date
- Burn To CD Count
- Delete On Clock Roll back
- Disable On Clock Rollback
- Exclude Application
- Expiration After First Use
- Expiration Date
- Expiration On Store
- Minimum App Security
- Minimum Client SDK Security
- Play Count
- PM App Security
- PM Expiration Date
- PM Rights
- Transfer Count

Windows Media DRM?

- **Pay per view**
  - Play count (client side)
- **Rental**
  - Expiration after first use
    Useful for different time zones
  - Expiration on store
    Useful for different time zones
  - Begin & expiration dates
- **Subscription**
  - Begin & expiration dates
- **Controlled distribution of media assets**
  - Can include any of the above

Microsoft License delivering

- **Licenses** can be delivered in different ways and at different times, depending on the business model
  - Can be delivered before or after the content
  - Both possible if downloading
  - Only the first is reasonable in the case of streaming

- **Licenses** can be delivered with or without the consumer being aware of the process using silent or non-silent license delivery.

Consideration on Counting Rights

- **How to arrange the rights counting**
  - **Number of play, print, etc.**
- **Server Side**
  - More secure, and more expensive in terms of server costs,
  - Dependent on the number of licenses, objects and users
    - if we have 1 Million of users and 1 Million of different content objects, we have 10^{12} status records to count the number of plays!! , 1000 Gbyte !!!
- **Client Side**
  - Limit number has to be hidden into the client
    - Thus Less secure
  - Quite cheap with respect to the server solution
  - Adopted by Windows Media DRM

Fine Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Example of Microsoft Windows Media