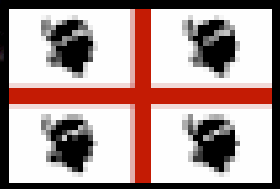
L'ENIGMA DEL DRM

Franco Visintin, SMPTE

Spunti tratti dall'articolo di Eric Grab
"The DRM Conundrum"
SMPTE Journal, 4 April 2004

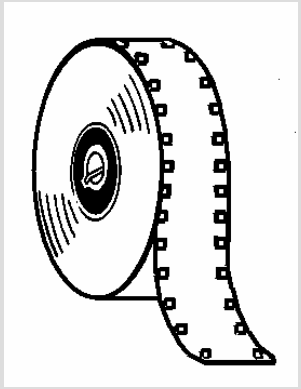


SARDEGNA DISTRICT
Diritto e Tecnologia del
Digital Right Management
19 settembre 2008, Pula (CA)

QUADRO DELLA SITUAZIONE – contenuti e diritti

Molte forme di commercio sono oggi basate sul controllo e sulla vendita di “copie di informazione”.

E’ il commercio dei cosiddetti **contenuti** : audio, video e testi di un film o di un programma TV trasmessi o registrati su un supporto.



Ma i contenuti sono soggetti a **diritti**, volti a difendere la loro proprietà intellettuale.
Sono i diritti di chi ha ideato tali contenuti, cioè i cosiddetti “**diritti di autore**” .

Tali diritti attuano quindi una **difesa dei contenuti**

QUADRO DELLA SITUAZIONE – ieri e oggi

In passato, nel corso dei secoli, i titolari dei "diritti d'autore" hanno tratto vantaggio, nella "difesa dei contenuti", dalle barriere imposte

- dagli elevati costi di copia,
- dal degrado delle opere nella loro copia e diffusione.

Oggi, con l'era digitale,

- i costi di copia sono divenuti quasi insignificanti
- il degrado delle opere copiate inesistente.

QUADRO DELLA SITUAZIONE – il DRM

Quindi, per difendere i diritti d'autore è stato necessario sviluppare tecnologie che erigessero **barriere tecniche** atte a contenere la loro copia.

E' così nato il **Digital Right Management** (**DRM**) , tecnologia volta a gestire i diritti su opere distribuite in forma digitale.

L'ENIGMA DEL DRM

In casi ideali e limitati la "tecnologia della sicurezza" può proteggere e fornire una informazione perfetta.

Ma esiste un ampio gap fra teoria e pratica.

In casi reali e complessi le aspettative riposte nelle tecnologie DRM superano la capacità del sistema, che deve misurarsi con le esigenze della privacy e con gli aspetti autocratici tipici di tali controlli.

Nell'antitesi fra massima sicurezza e massima privacy risiede l'enigma del DRM..

Jean-August Moreau, Edipo e la Sfinge

COMPITI DEL DRM

E’ compito del DRM difendere l’industria dei contenuti (cinema, televisione, supporti registrati)

L’industria dei contenuti (specie il cinema) investe enormi capitali nella creazione e distribuzione dei suoi prodotti.

Le tecnologie digitali, grazie alla loro grande efficienza e versatilità, hanno potuto offrire all’industria del cinema enormi opportunità, ma anche pesanti rischi.

Opportunità : rapida e facile duplicazione dei contenuti, riducendo così costi e tempi di produzione e distribuzione (vedi il successo dei CD e poi dei DVD).

Rischi : la facile duplicazione favorisce la pirateria. L’industria dei contenuti confida dunque nel DRM per ridurre (non certo eliminare) tali rischi

MISURE PRIMARIE DEL DRM - criptaggio

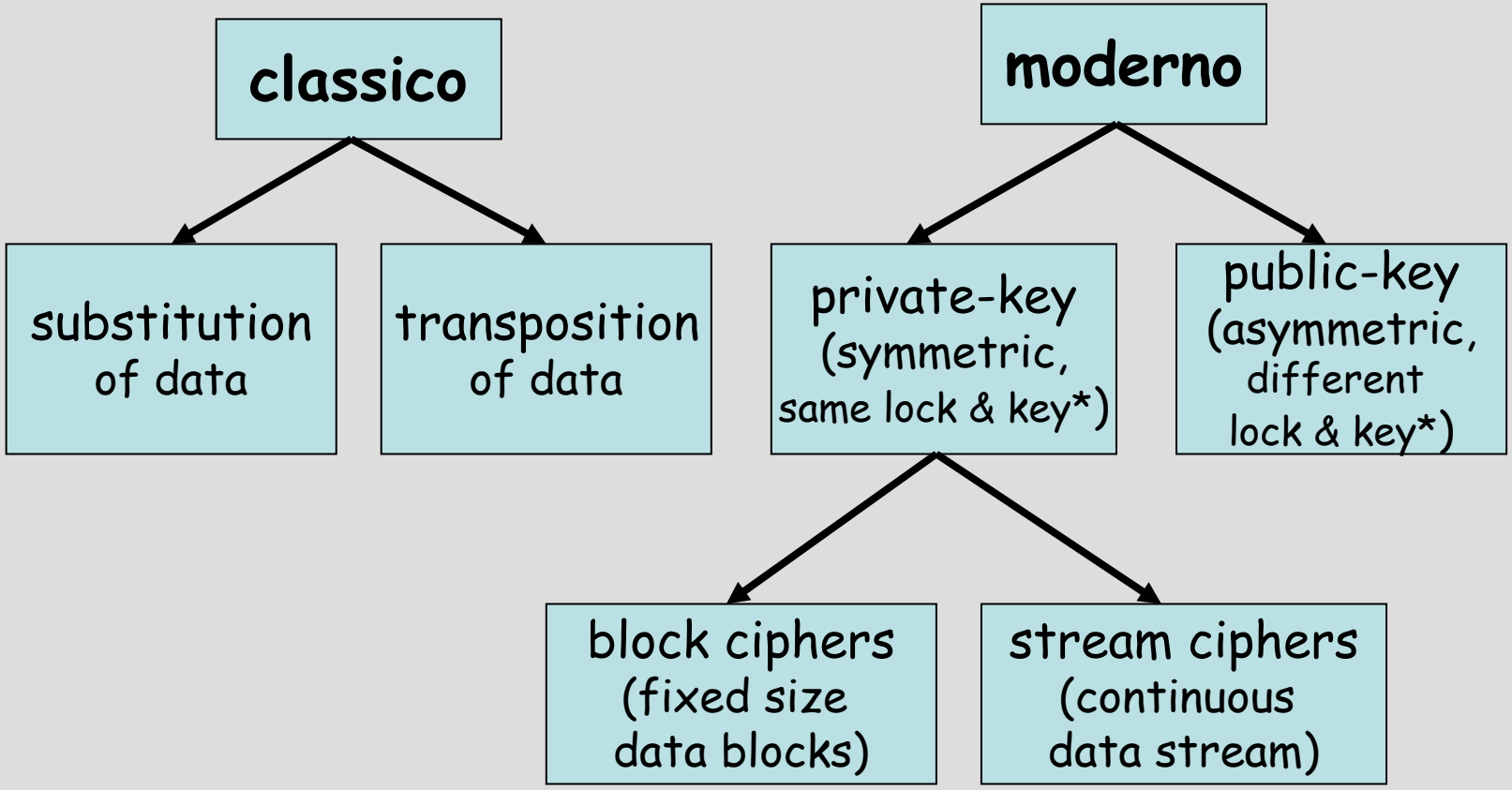
Criptaggio *(encryption)* = sostituzione dei dati digitali o modifica del loro ordine di scorrimento al fine di renderne più difficile la lettura.

La sua forma base prevede: un sistema di chiusura (*lock*) ed una corrispondente chiave per aprirlo (*key*), chiusura e chiave possono essere “simmetriche” o non.
Il rischio consiste nel fatto che una persona non autorizzata venga in possesso della chiave.

Il rischio è ben maggiore se la chiave è “multipla”, potendo conseguire più chiusure. Il possesso non autorizzato della chiave permette in tal caso l’apertura di più contenuti.

Il sistema simmetrico impedisce ad un produttore di mandare lo stesso film a più clienti. Vengono pertanto adottate, caso per caso, soluzioni di compromesso

MISURE PRIMARIE DEL DRM - **criptaggio** (segue)



* lock for encryption, key for decryption

MISURE PRIMARIE DEL DRM - comunicazione autenticata

Ogni utente riceve la chiave dal fornitore dei contenuti.
Nel suo processo di trasferimento, un ladro potrebbe però sostituirsi al destinatario per ricevere la chiave.

Per evitare ciò si impiegano
sistemi di autenticazione della comunicazione
(communication authentication systems)
volti ad accertare l'identità del ricevitore e del distributore prima che la chiave venga consegnata : solo chi ha un permesso appropriato può ottenere la chiave di lettura.

Sono comunque provvedimenti che appesantiscono il sistema rendendolo poco gradito al pubblico.

MISURE PRIMARIE DEL DRM - copy control flags

Un sistema alternativo al criptaggio è l'inserimento nel prodotto inviato di opportuni ed universali "segnali di controllo di copiatura" (***copy control flags***) che danno al prodotto stesso le istruzioni di permesso o meno di copiatura.

E' dunque una "misura di protezione tecnologica" col compito di limitare le possibilità di copiatura o di memorizzazione di tutta o parte dell'opera protetta.

CONTROMISURE DEL DRM

Confidare però nella completa efficacia le misure primarie è illusorio.
Per combattere gli attacchi al contenuto è bene adottare un programma di **contromisure**, che comportano però un piano di investimenti variabile a seconda delle circostanze.

I contenuti possono essere, come accade per altri tipi di merce (si pensi alle confezioni), inventariati e monitorati per controllare la proliferazione di copie non autorizzate.

Soccorre qui quella tecnologia in grado di mimare il riconoscimento umano.

Sono comunque provvedimenti che appesantiscono il sistema .

CONTROMISURE DEL DRM - fingerprinting

fingerprinting (impronta digitale) = consiste nell'usare un mini-campione del contenuto per identificare il tutto.

Il sistema funziona su più fasi.

Prima va eseguito un *database* dei *fingerprint* di tutto il materiale da tenere sotto controllo.

Poi vanno controllati i vari sistemi di distribuzione comparandone i *database* dei *fingerprint*.

Indi il *database* che ne esce va confrontato con quello dei relativi diritti per determinare se la copiatura è autorizzata o meno.

CONTROMISURE DEL DRM - watermarking

Watermarking = permette di inserire, all'interno del contenuto, informazioni che lo autenticano (come la filigrana nella carta moneta).

E' questa una contromisura molto diffusa per rintuzzare attacchi contro il contenuto. Essa consente di rilevare le infrazioni e dove sono avvenute (al pari delle tracce che permettono al detective di individuare il colpevole).

I problemi del marking unico sono simili a quelli del criptaggio unico, ma forse con maggior peso di processamento.
Il contenuto va monitorato seguendo a ritroso il suo percorso fino ad individuare l'autore dell'effrazione.

PROBLEMI SOCIALI E LEGALI

Lo sviluppo tecnico è solo un aspetto dell'enigma del DRM. Un altro sono gli aspetti sociali e legali che, per effetto della tecnologia, vanno estendendo l'influenza del copyright.

APERTURA

I prodotti DRM devono essere in grado di decidere quando e come fornire il contenuto protetto, il tutto in accordo con la legislazione in atto.
Ciò si traduce nella difficoltà di codificare la legislazione entro sistemi informatici.
Un impiego appropriato (*fair use*) delle leggi di copyright deve preoccuparsi di bilanciare il monopolio del copyright con l'interesse pubblico.

PRIVACY

Un sistema DRM è tenuto a identificare il corretto ricevitore di un contenuto protetto. Se il ricevitore si identifica con una persona, la sua privacy è messa a rischio. Esistono però, come per le transazioni di denaro, le "*blind transactions*".

PROBLEMI SOCIALI E LEGALI (segue)

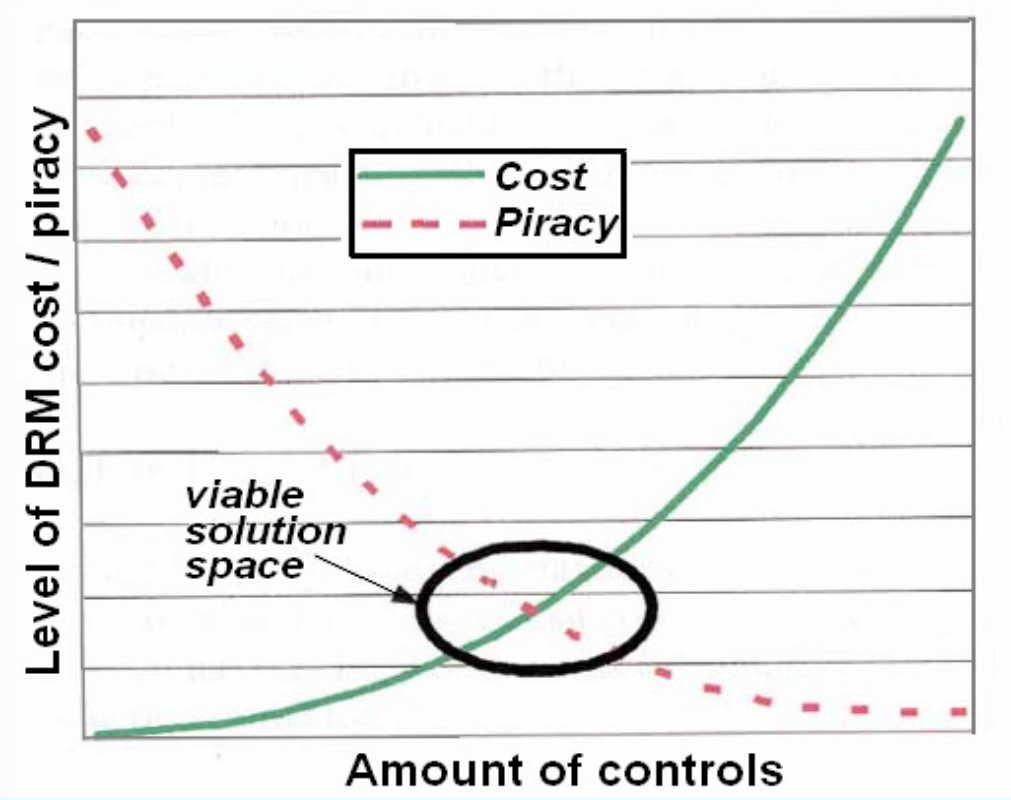
RISCHIO DI POTERE AUTOCRATICO

Il sistema DRM assicura che nessuna copia venga utilizzata al di fuori della volontà del proprietario del contenuto.

Ciò determina però un “potere autocratico”, che paventa visioni orwelliane, ove una piccola elite sarebbe in grado, controllando il flusso informativo, di opprimere una vasta maggioranza della società, e quindi ritardando od anche invertendo il suo progresso.
A tale riguardo la *Free Software Foundation* ha proposto come lettura dell’acronimo DRM le parole *Digital Restrictions Management* .

I sistemi DRM devono quindi, allo stesso tempo, proteggere i diritti di proprietà, ed assicurare la creatività e il continuo progresso, senza creare barriere ingiustificate allo scambio innovativo di idee.

SOLUZIONI REALISTICHE



Ogni sistema DRM dovrà impiegare misure primarie e contromisure, valutando quali sono gli opportuni livelli da adottare per contemperare

- *costi del controllo* e
- *rischio di pirateria*.

La valutazione della qualità dei sistemi DRM dovrebbe quindi essere basata sulla intelligente efficacia delle difese :
sono esse in grado di fermare la copia rapportandosi al livello di effrazione che l'utente medio è in grado di esercitare?

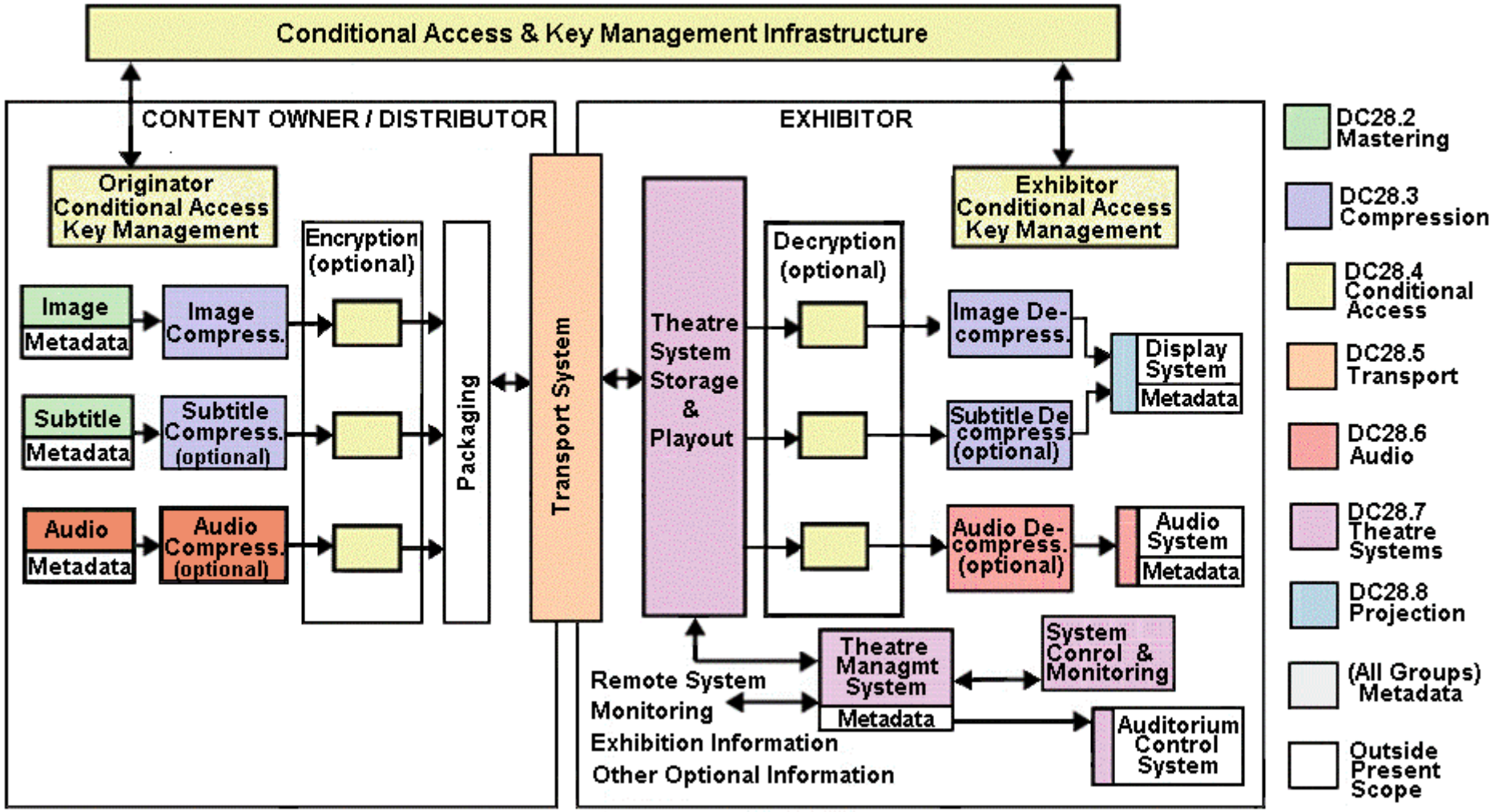
COSA HA FATTO LA SMPTE PER IL DRM

La *Society of Motion Picture and Television Engineers (SMPTE)* è stata creata nel 1916 con lo scopo di sviluppare, attraverso i suoi *Committees* internazionali gli standard industriali e di sostenere l'informazione e la formazione nel campo delle tecniche cinematografiche e di quelle televisive (dal 1950). Conta su più di 10.000 membri distribuiti in 85 paesi e su più di 250 ditte o istituzioni come membri sostenitori.

Nel gennaio 2000 la SMPTE ha creato il **DC28** (**Digital Cinema Technology Committee**) con lo scopo di emettere gli standard per il Cinema Digitale.

In tale ambito è stato creato lo **Study Group DC28-4** col compito di studiare gli opportuni standard per il DRM .

AZIONE DEI GRUPPI DI LAVORO DEL DC28



COSA HA FATTO IL DCI PER IL DRM

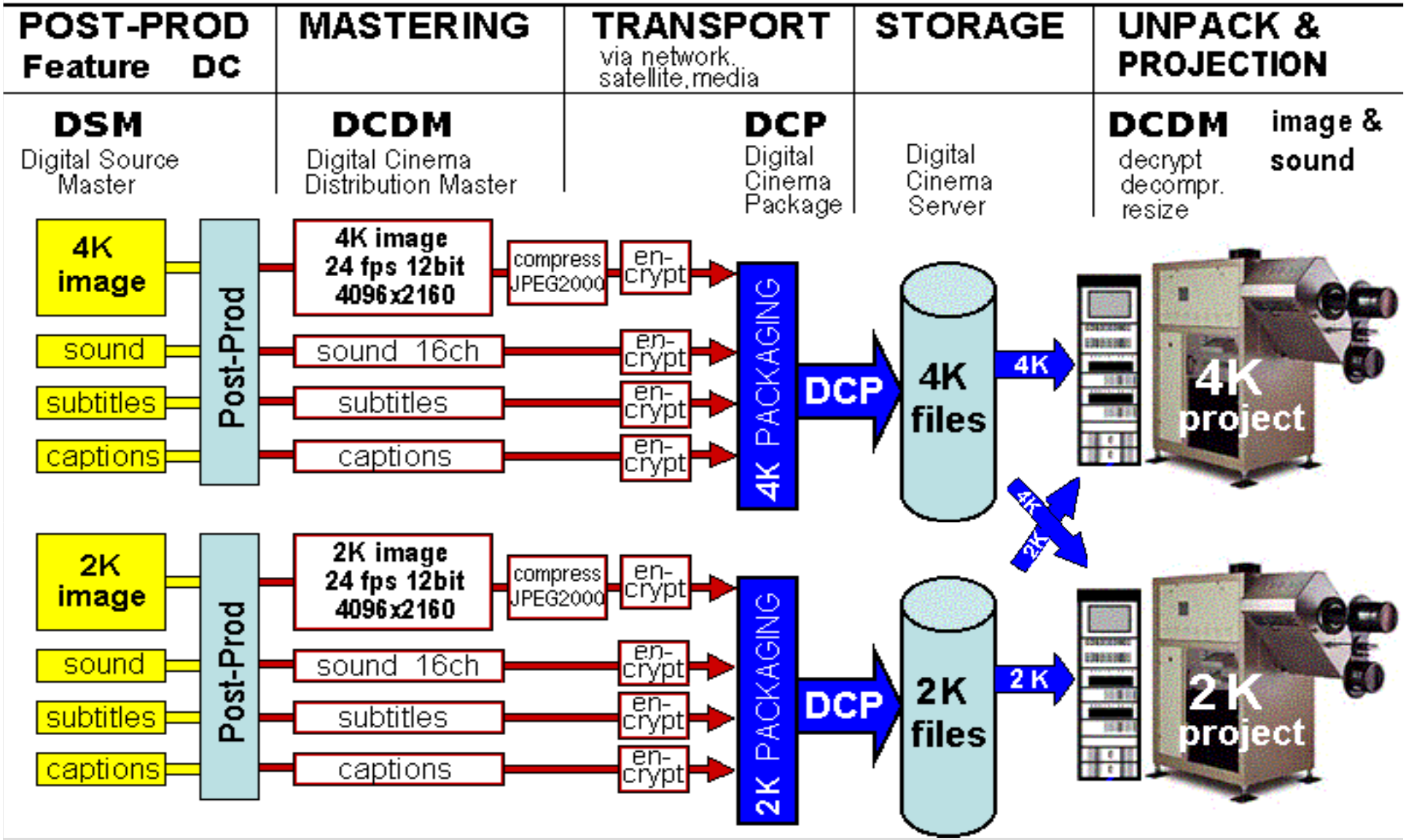
DCI Digital Cinema Initiatives, LLC

Nel 2003 sette major di Hollywood (Disney, Fox, MGM, Paramount Pictures, Sony Pictures Entertainment, Universal, Warner Bros) hanno creano il gruppo di ricerca **DCI** (Digital Cinema Initiatives) con l'intento di emettere le specifiche per il futuro Cinema Digitale.

La DCI prevede, nelle sue ***specifications*** emesse nel luglio 2005, un *Digital Cinema Content Security System*

Lungo questi anni si sono sviluppati intensi contatti fra DCI e SMPTE per pervenire alla definizione degli standard per il Cinema Digitale, includendo fra essi quelli per il DRM.

CATENA DC E DRM SECONDO LE SPECS DCI



COSA STA FACENDO LA SMPTE PER IL DRM

Il lavoro di ricerca e normazione nel settore del Cinema Digitale condotto da *DCI* e *DC-28*, confluisce da questo anno in due nuovi **Technology Committees** creati da **SMPTE** col compito di seguire gli standard del Cinema Digitale nelle loro fasi normative ed applicative :

Essence 10E – creazione e cura (dall'acquisizione alla restituzione) di tutti i "master elements" necessari alla distribuzione dell'*essence* (suoni e immagini) attraverso applicazioni multiple

Digital Cinema Applications 21DC – modifica degli elementi dell'*essence* per poterli fornire a specifiche applicazioni (es. DRM nel cinema digitale)

CONCLUSIONI

Tenendo in conto che

- per distribuzioni di contenuto su larga scala, la tecnologia DRM non potrà mai assicurare o nemmeno approssimare una protezione ideale.

- quando una misura approssima la protezione ideale si manifestano reazioni opposte.

- le contromisure sono limitate e non possono prevenire alcun attacco o minaccia di attacco.

Si dovrà attentamente valutare che le misure adottate non sovra-compensino le potenziali minacce né inducano ad una sovra-ingegnerizzazione dei sistemi.

CONCLUSIONI (segue)

Una efficace strategia del DRM dovrà dunque basarsi su **tecnologie difensive**, non offensive dunque, che riconoscano la costante necessità di

- comprendere i mercati,
- conoscere le forze antagoniste,
- calcolare i rischi della loro azione

Si dovrebbe comunque fare in modo che il contenuto possa essere più facilmente acquistato che rubato :

- le difese del DRM non dovrebbero essere così elevate da proteggere totalmente il mercato.
- gli accessi dei consumatori dovrebbero essere a basso costo, abbondanti e veloci.

Fine