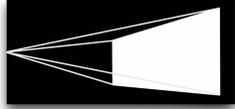


CINEMA D'EUROPA



MEDIA SALLES

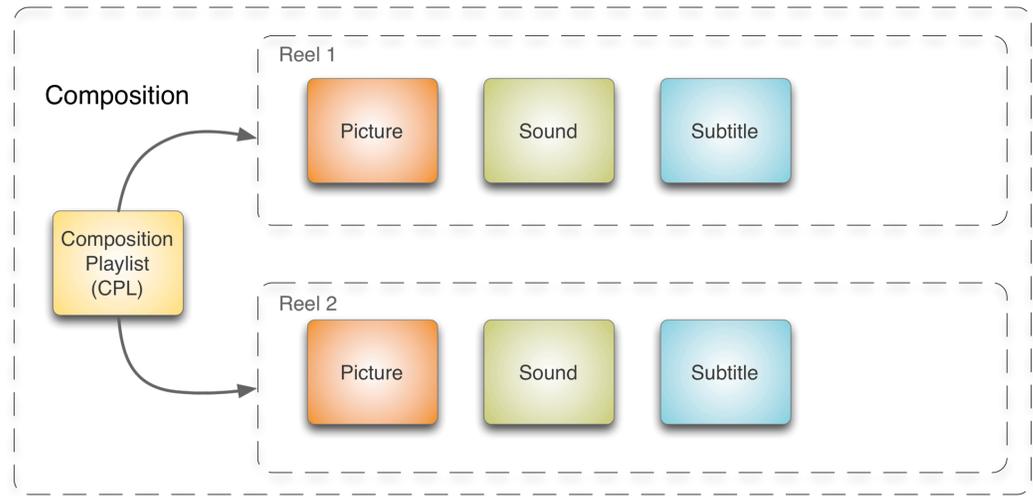
# The Digital Cinema Composition, Security Key Management, And Accessibility

Michael Karagosian  
August 2013



I'm Michael Karagosian, president of MKPE Consulting in Los Angeles. I've been engaged in developing business and technology in the cinema industry for over 30 years, and since 1999 have played an active role in the development and rollout of digital cinema. I led the technology effort within NATO for 11 years, and drove the standards that we now have for accessibility in cinema content. I also organized and led the development of the concepts behind the Digital Cinema Package, in conjunction with a select and fantastic team of industry professionals. In this presentation, I will review how the Digital Cinema Composition is organized, and how security key management, including the KDM, works. These concepts will provide you with an understanding how the accessible content is delivered as part of the digital distribution in an open, non-proprietary manner. I'll also review the open protocols developed for interoperability with 3rd party closed caption systems, and will highlight the competitive closed caption products that have emerged.

## It Starts With The Composition

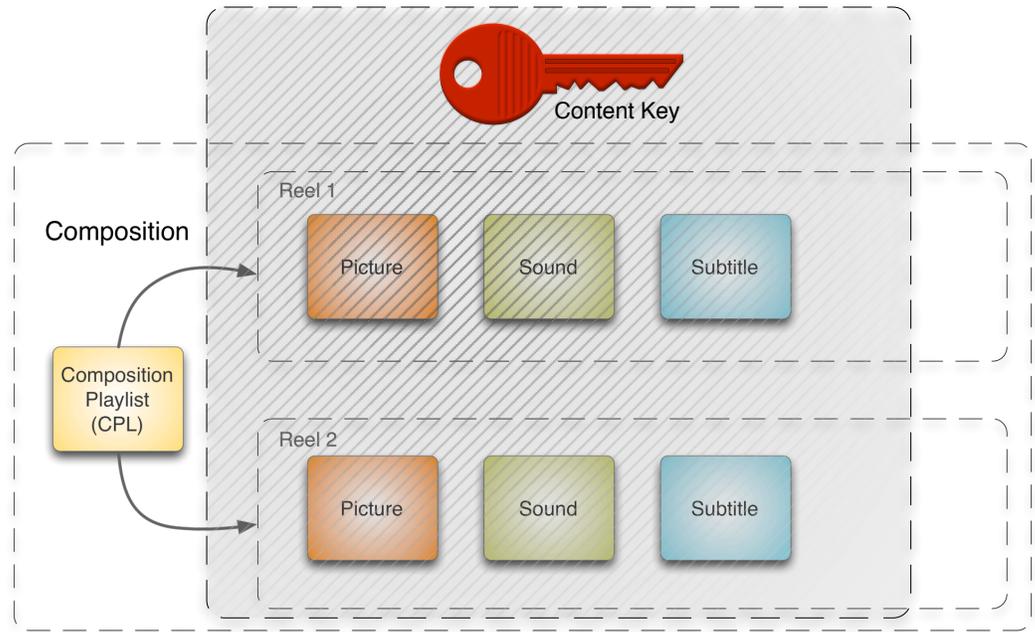


mkpe

The concepts behind the Digital Cinema Package were developed to efficiently preserve director's intent in the cinema distribution. The package needed to support multiple languages, and to be efficient, we wanted to encourage the reusability of very large picture files and the substitution of language-related files, such as sound and captions. To do this, we needed to avoid the methods used by broadcasters where picture and sound are interleaved in files and streams, and instead create something brand new. The result is the structure we call the Composition. A Composition is a complete work, such as a movie, a trailer, or an advertisement.

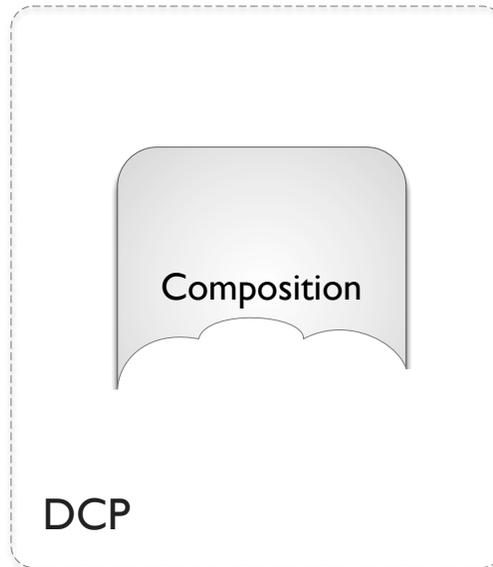
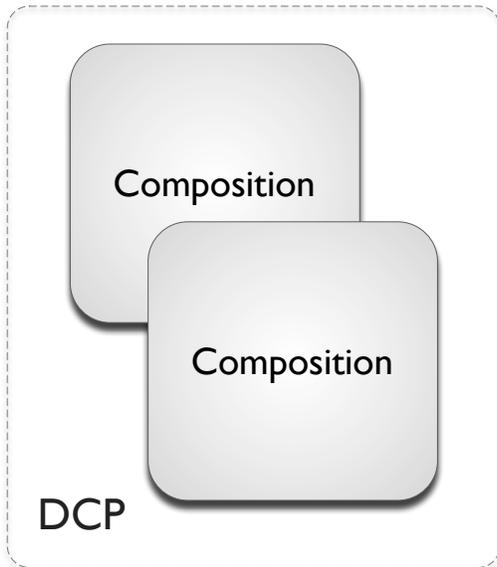
The Composition consists of many files. Each file contains only one essence type, which means that picture is stored in one file, and sound in another. Files are organized temporally in blocks of time. We call these Digital Reels, because the concept mimics that of the film reel. But while film reels strive to be of a similar length of time, digital reels can be of any length, from seconds to hours. Further, there is no restriction on the number of Digital Reels in a Composition. The Composition was designed to be highly extensible. By this I mean that we knew that the demands on content would grow beyond what we could then predict, so the Composition was designed so that additional forms of content could be added without breaking backwards compatibility.

# Encrypted Composition



The Composition can be encrypted, file by file. If encrypted, each encrypted file in each reel requires a separate encryption key, and there is a limit of 256 security encryption keys that can be used in a Composition. (The drawing only shows one content key to simplify the illustration.) The content owner has full control over which files it wants to encrypt. The Composition Playlist, or CPL, is an XML file that instructs the playback system the order in which to decrypt and play the files.

## DCP: Digital Cinema Package

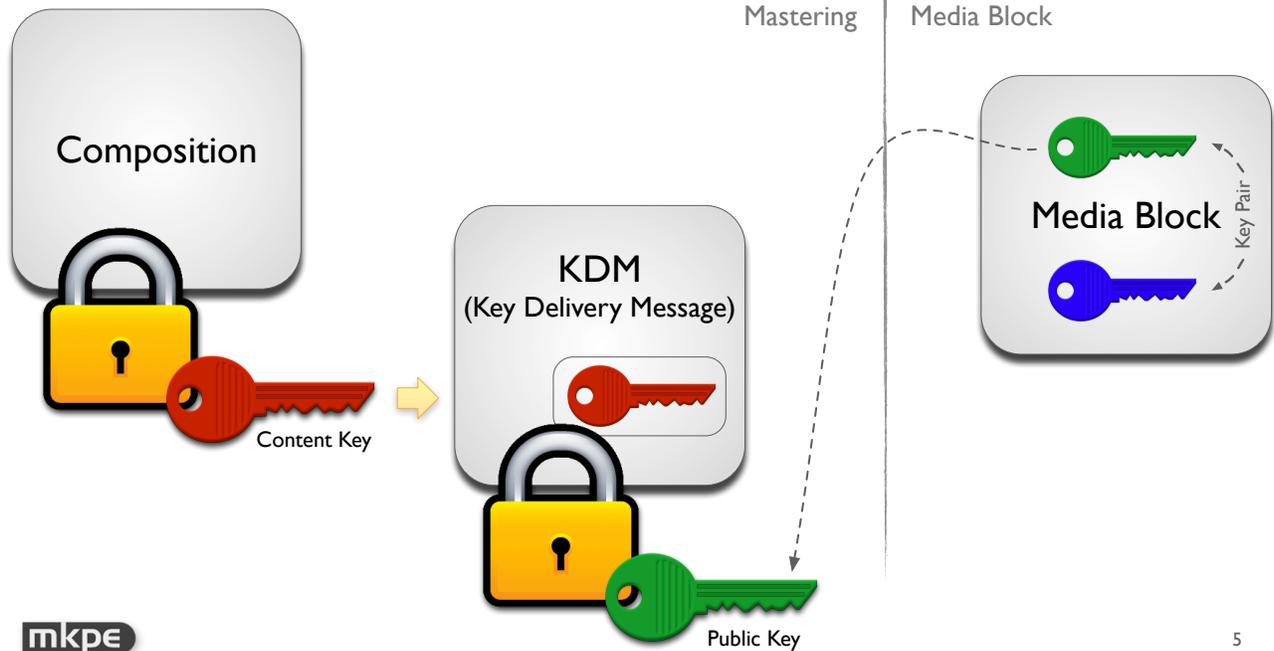


Every  
Version  
of an  
Encrypted  
Composition  
Requires a  
Unique  
KDM

The vocabulary used in the industry, however, is not Composition, but “DCP,” which can be confusing to users. While movies are stored as Compositions, we talk about sending a “DCP” to the cinema. DCP stands for Digital Cinema Package. The DCP is a tool developed for distribution, and is a level above the Composition. A DCP can contain one or more Compositions, or it can contain a partial Composition. Note that every version of the Composition requires a unique KDM.

There are two components when managing digital cinema content. The first is that the right DCP must be sent to each site. Often, multiple Compositions are sent and the exhibitor must choose the right one to show. The more difficult problem is sending the right security keys for each site.

# Security Key Management



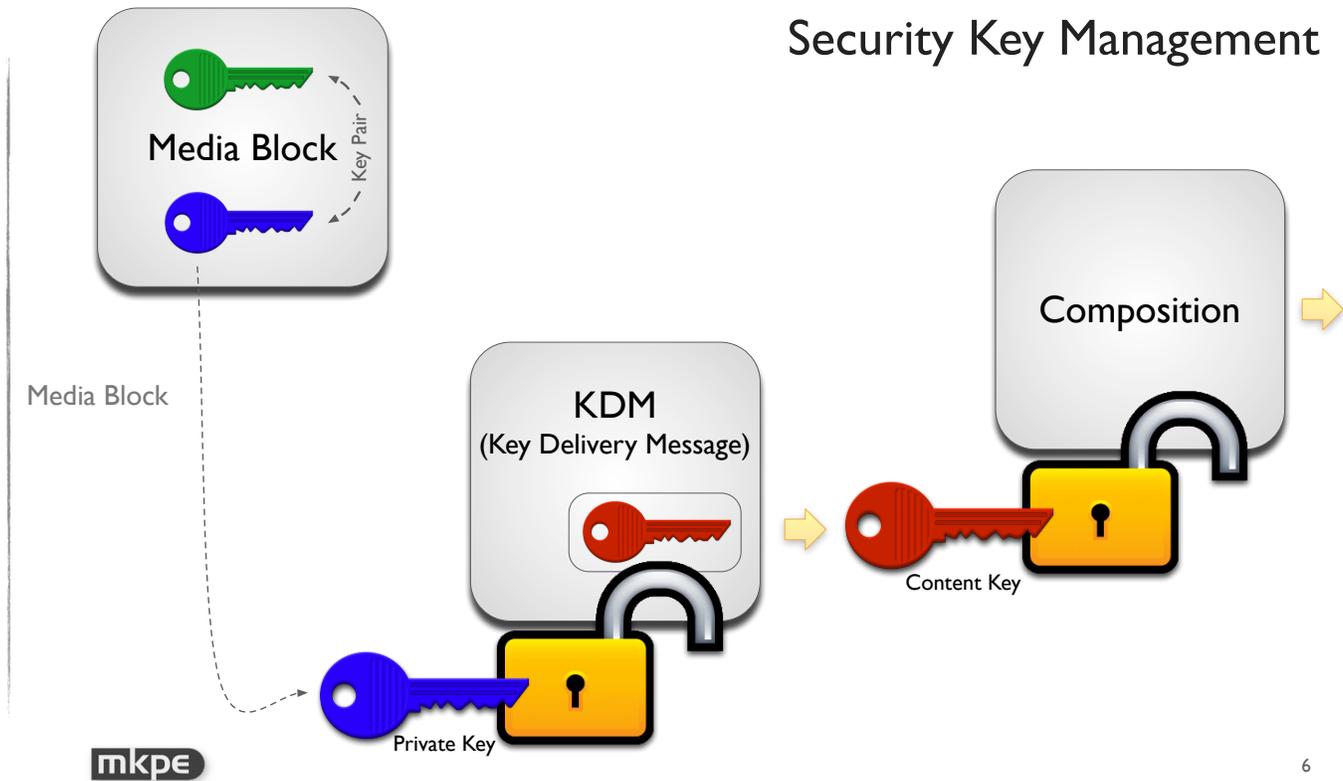
Film has no parallel to digital encryption, and as a result, security key management is a new concept, and has further to evolve before we can call it a mature concept. It is with security key management that most problems occur in exhibition.

When securing files in a Composition, they are “locked” with a “symmetrical” key, which I refer to here as a “Content Key” (red key). Symmetrical means that the identical key that is used to encrypt a file is also used to decrypt the file. When a Composition is widely distributed in a region, the same encrypted set of Composition files can be sent everywhere, without thought as to how the files will be decrypted.

However, to playback the encrypted file, a decryption key is needed. We don’t want to expose the red “Content Key,” because it could be posted to the Internet, defeating the security of the content. To protect the Content Key, it is encrypted, or “locked,” in separate file called a Key Delivery Message, or KDM. The KDM is a small file, and can be emailed if necessary. Each KDM is uniquely created to allow only one digital cinema Media Block to play the Composition. (The Media Block decrypts, decompresses, and plays the Composition.)

The Media Block utilizes asymmetrical encryption, where a “Public Key” and a “Private Key” comprise an asymmetrical “Key Pair.” The “Public Key” (green key) sent to the KDM maker, who uses it to encrypt the Content Key in the KDM. The “Private Key” in the Media Block is the only key that can decrypt the KDM. Private Keys are encoded in secure silicon, and cannot be seen by human eyes.

## Security Key Management



When the KDM is delivered to the Media Block, the Private Key (blue key) decrypts it, and exposes the Content Key (red key). The Content Key can then be used to decrypt the Composition. These tasks are all performed in physically secure section of the Media Block. A major portion of the DCI specification addresses how these secure processes are to be handled.

# Security Key Management Workflow - FLM

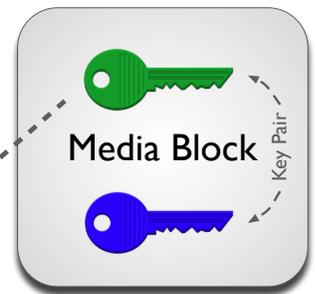


mkpe

Mastering

Cinema

FLM-X



As in any work environment, we have workflow issues in the exhibition of digital movies. Media blocks move around or can be replaced on a moment's notice. It takes a lot of care to make sure that the right KDMs are present in the cinema so that the movie plays.

As digital cinema matures, a concept called the Facility List Message, or FLM, is being put to work. The FLM carries the Public Key (green key) from the cinema to the KDM maker so that the correct KDM can be made for that Media Block. A communication method called FLM-X is used to collect the FLM, where the KDM maker "pulls" the FLM from the cinema.

# Security Key Management Workflow - TKR



mkpe

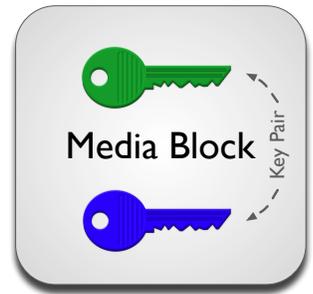
Mastering

Cinema

TKR  
(Theater Key Retrieval)



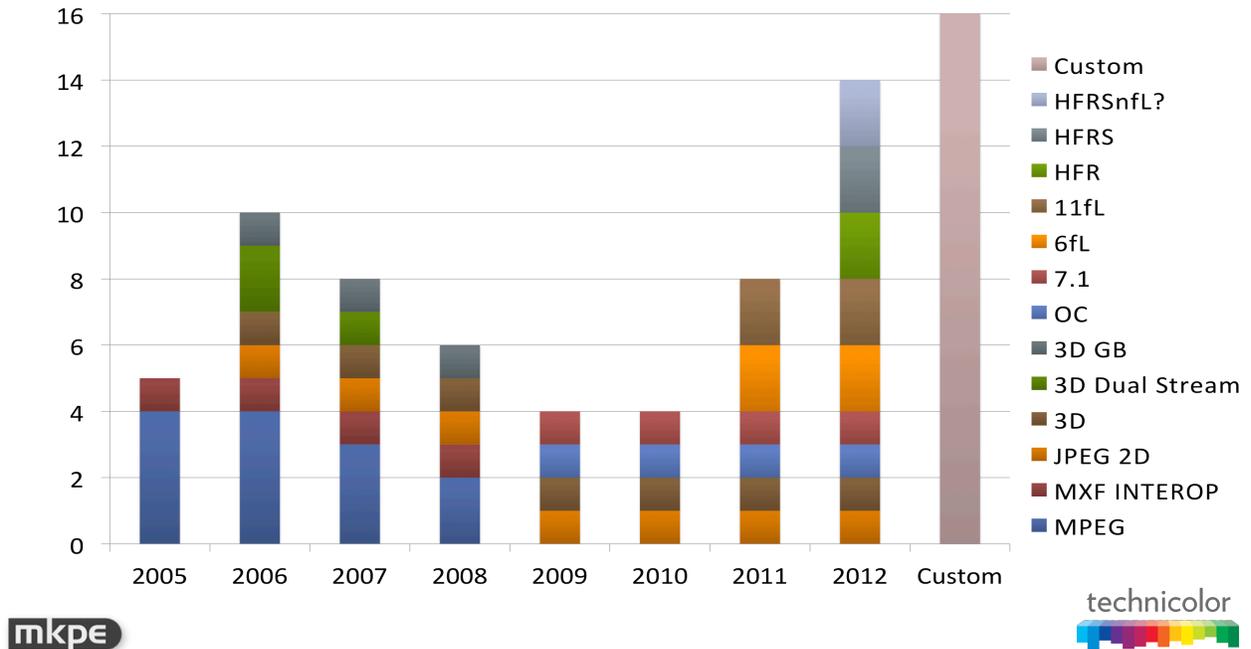
CPL  
(Composition  
Play List)



8

Once the KDM is created, it needs to be sent to the right location. To accomplish this, a method has been devised called Theatre Key Retrieval (TKR) to allow the Media Block to pull the correct KDM from a data center. This is a relatively new concept, but is very promising.

# The Content Management Problem



Improvements in security key management, such as FLM and TKR, are needed because Distributors and Exhibitors are burdened with an ever-increasing number of versions of digital cinema content. The graph shown was presented by Technicolor in a presentation to illustrate the problem of multiple versions of content.



## Automating Content Management

We're Not There Yet

While the digital distribution of movies has reduced the cost of physical distribution of movie content, it has multiplied the number of content management problems faced by distributors and exhibitors. Digital content presents the possibility of highly automating the distribution process, reducing costs to both distributors and exhibitors. But to enable this, standards are needed to insure interoperability among competitive providers of software and hardware systems. So far, no one is pursuing such standards.

## Accessibility



mkpe

Now let's talk about accessibility, and how accessibility is improved in digital cinema over film. I'll explain how extensibility in the Composition enables accessibility in digital cinema content in a manner that was not possible with film.

Visually-Impaired Narrative  
aka Descriptive Narration  
(VI-N)



A narrative dialog track for  
those who have difficulty with  
sight

Hearing Impaired Audio  
(HI)



An enhanced sound track for  
those who have difficulty  
hearing

Closed Captions  
(CC)

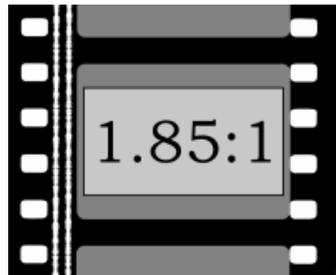


Visual presentation of caption  
text for those who cannot  
hear or hear well

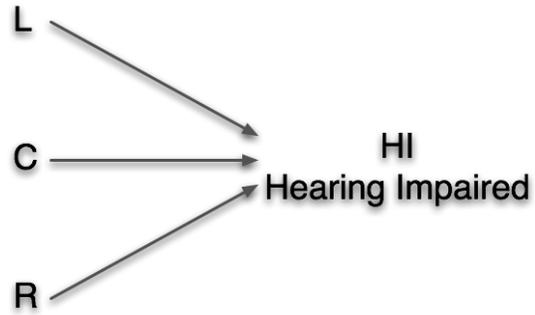
**mkpe**

Some definitions will be useful.

# Hearing Impaired (HI) - How It Used To Be



Stereo  
Sound



Signal Summed in Audio Processor



Some history. With film, the Hearing Impaired audio channel, or HI audio, was synthesized by the audio processor.

# Visually Impaired Narrative (VI-N) *also known as Descriptive Narration* - How It Used To Be



With Film, VI-N was only possible with DTS

mkpe

With film, the Visually Impaired Narrative channel, known as VI-N, or Description Narration, was only available with the Accessibility Disc for DTS systems.



Closed  
Captions  
began...

Rear  
Window®  
Captioning  
System

mkpe

For the audibly impaired, captions can be placed on-screen. However, audiences in the US, and perhaps elsewhere, prefer to NOT have captions on-screen. The Rear Window closed caption system was originally introduced for film.



## Rear Window<sup>®</sup> Captioning System

Rear Window had a  
monopoly in film

mkpe

Rear Window utilizes a transparent reflector, reflecting text emitted from a digital sign on the rear wall of the auditorium.

Due to the degree of patents and licenses associated with Rear Window, it enjoyed a monopoly in film.

## Accessibility in Digital Cinema is Based On Open Technology

- Open distribution
- Open interoperability

Openness allows a competitive product environment to emerge, reducing costs to both distributors and exhibitors.



mkpe

Digital cinema opens up closed captions. There are no licenses associated with closed caption content in digital cinema, and all systems support an open protocol for 3rd party closed caption systems.

# HI & VI-N With Interop DCP

Container Channel	Configuration			General Loudspeaker Position
	5.1	7.1 SDDS	7.1 DS	
1	L	L	L	Left
2	R	R	R	Right
3	C	C	C	Center
4	LFE	LFE	LFE	Low frequency effects
5	Ls	Ls	Lss	Left surround (or left side surround)
6	Rc	Rs	Rss	Right surround (or right side surround)
7		HI		Hearing impaired (with emphasis on dialog)
8		VI-N		Visually impaired narrative (audio description)
9	--	Lc		Left center
10	--	Rc	--	Right center
11	--	--	Lrs	Left rear surround
12	--	--	Rrs	Right rear surround
13		Motion Data		Synchronous signal (currently used by D-Box)
14	--	--	--	Unused at this time
15	--	--	--	Unused at this time
16	--	--	--	Unused at this time



In digital cinema, HI and VI-N audio are delivered in the Composition. This is very simple with Interop DCP. No special equipment is needed to retrieve HI and VI-N audio.

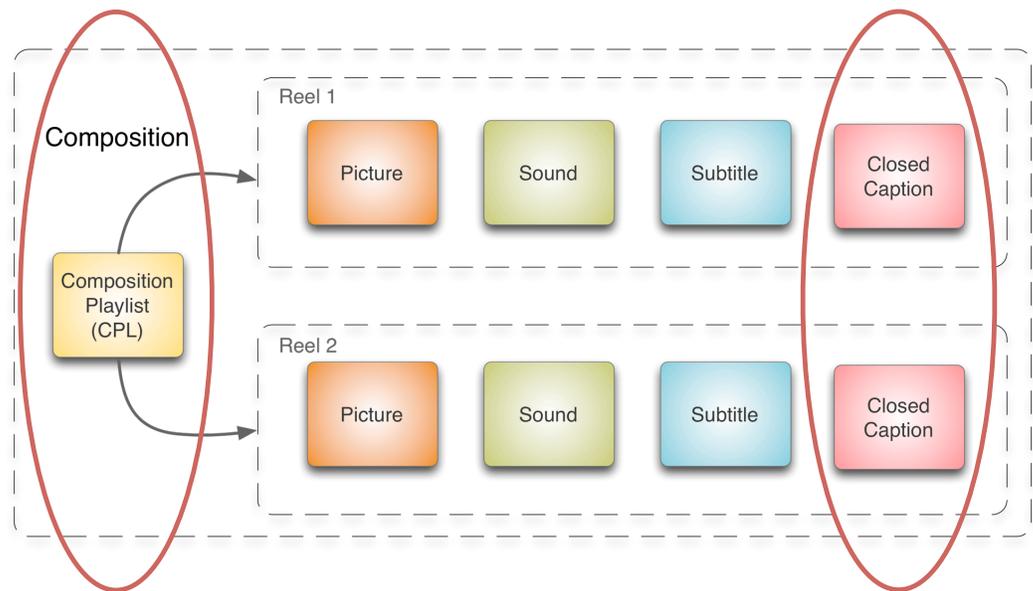
# HI & VI-N With SMPTE DCP



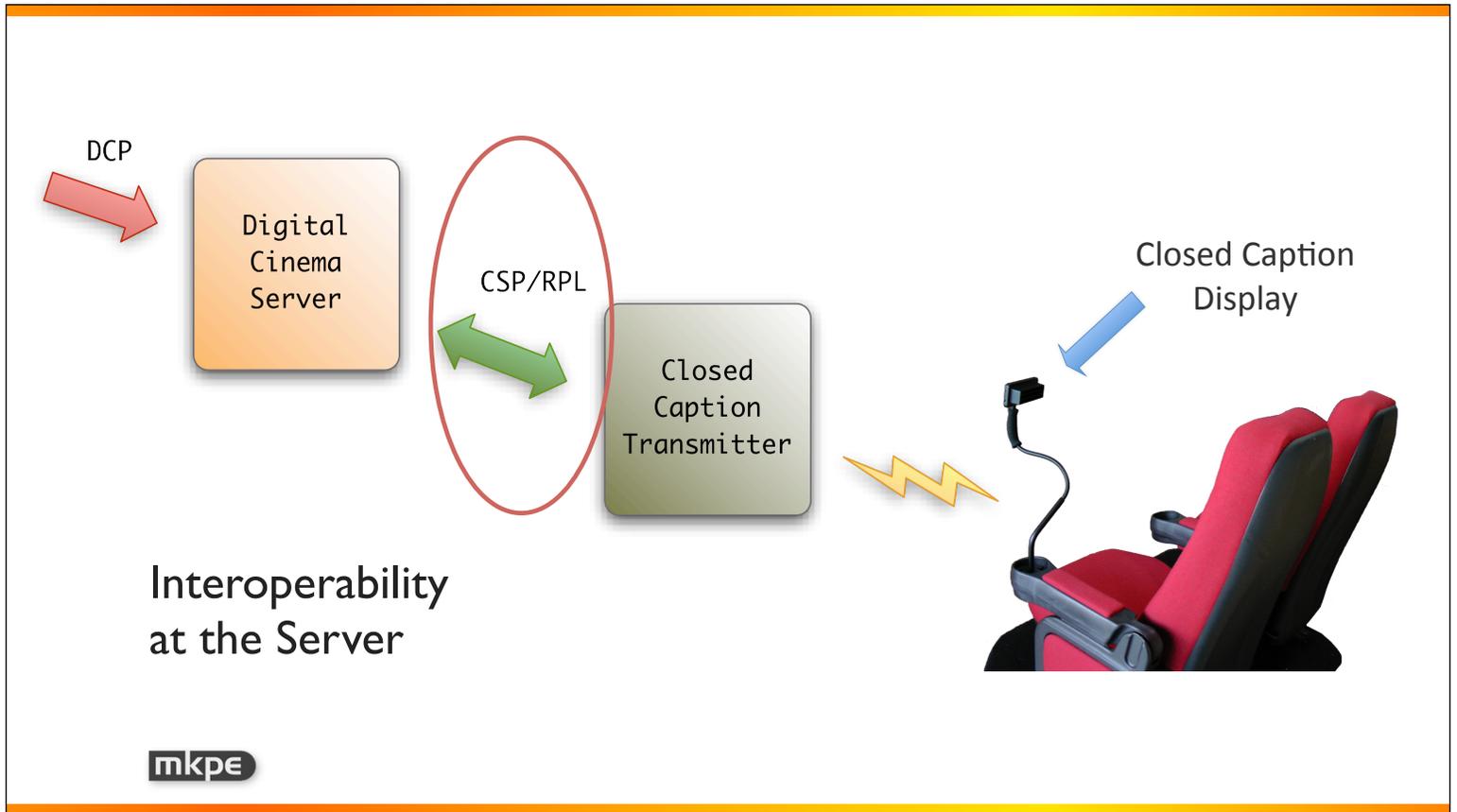
Container Channel	Interop DCP (This is how cinemas are wired)	SMPTE DCP 5.1	SMPTE DCP 6.1	SMPTE DCP 7.1 SDDS	SMPTE DCP 7.1 DS	SMPTE DCP Channel Labeling
1	Left	Left	Left	Left	Left	Channels Can Be In Any Order
2	Right	Right	Right	Right	Right	
3	Center	Center	Center	Center	Center	
4	LFE	LFE	LFE	LFE	LFE	
5	Left Surround	Left Surround	Left Surround	Left Surround	Left Side Surround	
6	Right Surround	Right Surround	Right Surround	Right Surround	Right Side Surround	
7	Hearing Impaired	Hearing Impaired	Center Surround	Left Center	Left Rear Surround	
8	Visually Impaired Narrative	Visually Impaired Narrative	---	Right Center	Right Rear Surround	
9	Left Center	---	Hearing Impaired	Hearing Impaired	Hearing Impaired	
10	Right Center	---	Visually Impaired Narrative	Visually Impaired Narrative	Visually Impaired Narrative	
11	Left Side Surround	---	---	---	---	
12	Right Side Surround	---	---	---	---	
13	Motion Data	---	---	---	---	
14	---	---	---	---	---	
15	---	---	---	---	---	
16	---	---	---	---	---	

But it becomes more complex with SMPTE DCP. SMPTE DCP assumes that the media block will correctly route the audio channels to the correct output. However, DCI compliance testing does not test for this. If your server does not route audio, it will lead to problems with SMPTE DCP distributions.

# Closed Captions in the Composition



Back to the Composition, closed captions were introduced into distribution by adding a new file type to the Composition, and by extending the CPL. Note that DCI compliance testing does not test for the ability to read a closed caption track file.



To allow 3rd party closed caption displays to connect to the digital cinema server, a new communication tool was invented, called the CSP/RPL protocol. CSP stands for Content Synchronization Protocol, and RPL stands for Resource Presentation List. All servers sold today support CSP/RPL. However, note that DCI compliance testing does not test for CSP/RPL.



mkpe



The introduction of open closed caption track files and the CSP/RPL protocol has led to the introduction of competitive accessibility products. USL makes infrared-driven HI / VI-N audio and closed caption products.

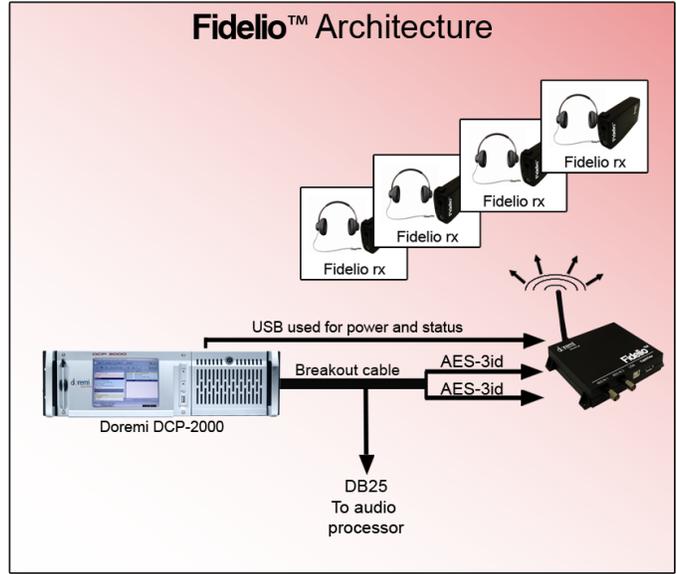


Doremi makes a closed caption display called Captiview driven by an industrial wireless protocol standardized by IEEE.

doremi™



mkpe



Doremi also makes the Fidelio system for HI / VI-N audio, also driven by an industrial wireless protocol standardized by IEEE.



**SONY**



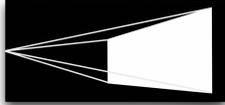
**mkpe**

Sony makes closed caption glasses, that prints text in front of the audience member's eyes. The glasses are driven wirelessly, and the transmitter / receiver also supports HI / VI-N audio.



Some developers have introduced closed caption products using off-the-shelf tablets and smart phones as the display. These products do not utilize the standardized mechanisms for the delivery of closed captions. Studios have expressed concern over the introduction of devices with video cameras in the cinema.

CINEMA D'EUROPA



MEDIA SALLES

Michael Karagosian  
MKPE Consulting LLC  
Calabasas, CA USA  
michael.karagosian@mkpe.com  
[mkpereport.com](http://mkpereport.com)  
[mkpe.com](http://mkpe.com)



\$40 Discount Coupon - 1 free month - for mkpeReport: MEDIA-SALLES-2013

