KDM and TKR for Dummies

Jerry Pierce, NATO technology advisor

How security works for digital cinema, what is Key Delivery Message (KDM)? What is Theater Key Retrieval (TKR)? How do they work? Not technically perfect, but close enough.

Introduction

Digital Cinema uses industry standard digital encryption - but really how many of us understand that? Or want to? Well this dummy guide gives a few of the concepts to make a digital cinema security a little less like a magic black box.

The hidden agenda (well I guess it's not that hidden) is to describe an automated way of distributing the keys (KDM) using Theater Key Retrieval (TKR) that will make things easier. Hopefully this will help identify what's needed for TKR and a path to get there from here.

Part 1 - How do Digital Cinema Keys work?

The goal is to send a DCP (Digital Cinema Package - about 250Gbytes worst case – typical would be 140 to 200Gbytes) to a theater and get it there in such a way that no bad person can pirate it. So we want to scramble or encrypt the digital DCP bits so you need a special decoder ring (a key) to enable the movie to play it. This is the magic of encryption - industry standard security - the same that protects your bank account and the ATM cash machine. It is secure enough that we can freely send encrypted DCP's to anyone and guarantee that they can't read them or pirate them. In fact, we can even include the keys in the same package and still guarantee that they can't read them. Pretty cool - how does that work?

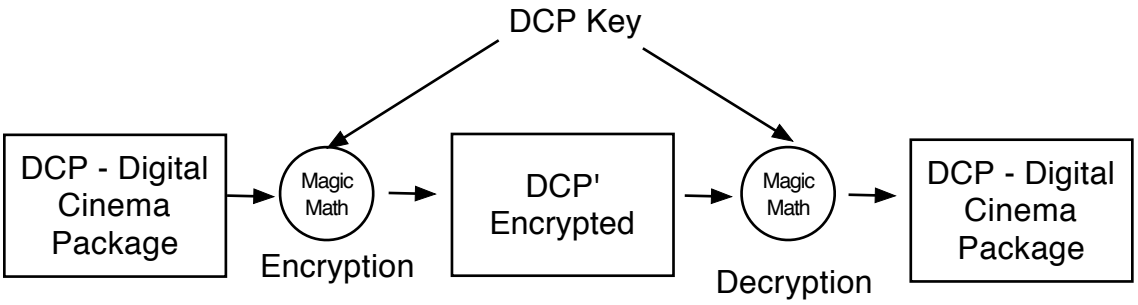


Figure 1 - Simple DCP Encryption

Figure 1 shows that a DCP key (about 1Kbytes) is used to encrypt or scramble the DCP using magic math. The security industry believes that if you get an encrypted file you will NOT be able to decrypt it without the key. But if you do have the DCP key you can easily decrypt the file and recover a copy of the original DCP. So far so good - as

long as you believe in magic math - and in this case you should. Is it worth noting the DCP Key(s) are symmetrical – the SAME key that is used to encrypt the DCP is also used to decrypt the DCP at the theatre. Much like your home key, it locks the front door when you leave and the same key unlocks the front door when you return home.

Well, that's a good start, but if you do this the DCP keys would need very high level of protection (security guards!) - that's not acceptable. But those math/security types have invented a really clever way of protecting a key so that it can be sent in broad daylight! It is called Public Key Infrastructure (PKI) - again very well known (and well used within many industries/governments) and protects bank money and military secrets as well.

It is all about delivering the DCP key. Figure 2 shows the path:

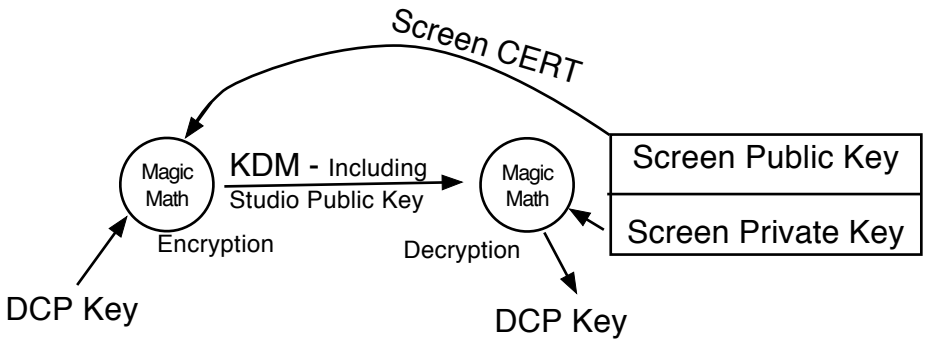


Figure 2 - Simple PKI - Public Key Infrastructure

Here is how it works. Each screen (or server or projector) has two special keys - a Screen Public Key and a Screen Private key. The public keys are just that - public! They can be freely given out, but are useless without the private keys - which are well protected and safe inside the server. The screens share their public keys by giving out the "screen CERT" which is their Public key. Which is why it is necessary for a screen to provide its CERT when it wants a KDM… without providing the cert there is NO KDM!!!!

So the key distributor uses the target Screen Public Key and the DCP Key to create a KDM. The screen server takes the KDM using its own Screen Private key to decode the DCP Key to enable play of the movie.

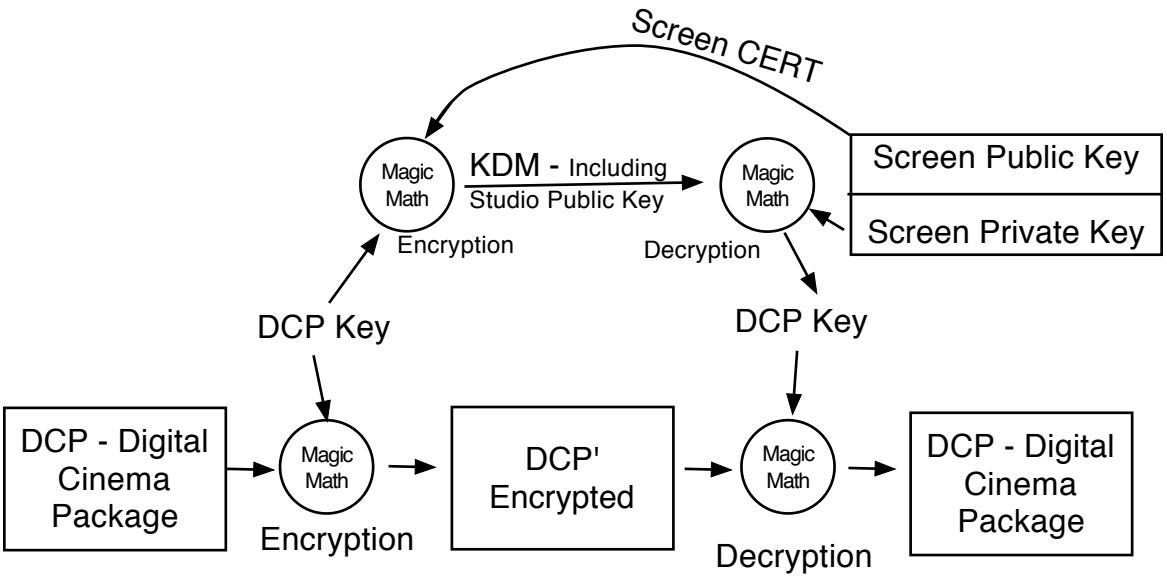
The server does this inside very well protected electronics called the IMB - Integrated Media Block - so that no one can get to the unencrypted DCP Key or the DCP itself or the Screen Private Key. It's really secure!!

So that's the basis of DCP/KDM security. A screen shares its Screen Public Key to a key distributor. The key distributor sends the encrypted DCP out to the screen along with a KDM for that screen. The screen uses the KDM and the Screen Private key to decrypt

the KDM to get the DCP Key and the DCP movie comes magically out for making a wonderful movie on the screen.

For DCP protection it also means each screen/server needs its own private key so it gives better control of distribution. ANYONE can get the encrypted DCP and ANYONE can get the KDMs, but only those with authorized private keys, i.e. the screen/server, can play it.

So the whole picture is:



We send the DCP encrypted on hard drives and over satellite to anyone that MIGHT want to play or book the movie and the KDM is customized for each screen server and sent to that screen server. Pretty clever? I think so.

> *OK, this is a bit simplistic … but the concept is right. Actually the KDM is associated with a CPL (Composition Play List) so if you have a movie CPL for 5.1 audio or 7.1 audio there are two CPL's and therefore will need one KDM for each CPL. Same decryption of the DCP, just more specialized KDMs to make sure the right version is played. The KDM also contains a time window for playback. The server must not allow playback outside that time window. Also there are many "DCP Keys" within a KDM, one DCP key for each encrypted image (reel) track file and one DCP key for each encrypted audio (reel) track file. With SMPTE packages, there will be DCP key(s) for the subtitle files. And with ATMOS ….. you get the idea*
>
> *This just shows that in reality it's more complicated, but not critical to the main theme of KDM for dummies. :)*

Part 2 Delivery of KDMs

in concept, making a KDM is fairly straight forward - you just take the screen CERT (screen public key), the DCP Key for a specific CPL and you have a KDM. Yea, that's too simplistic even for this tutorial.

A KDM facility (a facility that makes and delivers KDM messages) is a very trusted entity. They hold the unprotected DCP key. Something that should be very, very well protected.

The KDM facility needs to keep a good list of all the possible screens and locations. They need the CERTs for each screen server, the owner, and the capabilities of each screen (5.1, 7.1, screen brightness, 3D 2D, HFR, etc.) This list is a Trusted Device List for the KDM facility. They need to have high confidence that these are valid CERTs that go to a real authorized screens. This is not easy.

Next comes the booking. The studio builds a list of which screens / locations are authorized to play the movie and for how long. And the KDM facility needs to know all the screens in a complex since studios send KDMs for all screens in a complex.

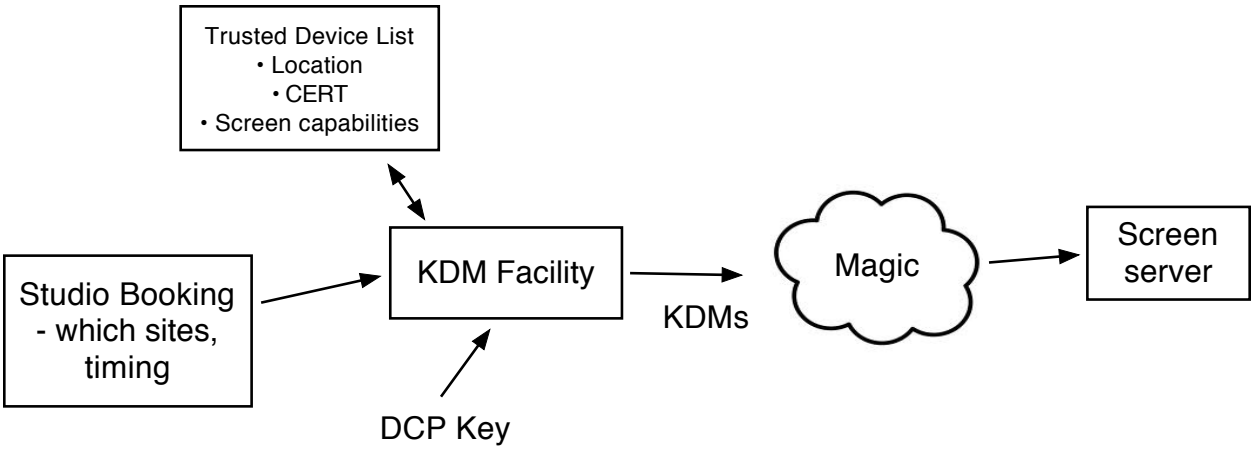


Figure 3 - Simple KDM to theaters

Getting the right keys to the right theaters is a bit more difficult. The KDM facility determines which sites need to play a movie and generates all the keys/KDMs for all the authorized CPLs//screens in the complex. A twenty-plex could get 20 to 60 keys or more!

The most popular way of sending KDMs is through the email system. The KDM facility takes all the keys for a particular site and "zips" them into an attachment to send to the theater manager. The theater manager opens the attachment, unzips the keys and puts them on a USB thumb drive and "sneaker net" the drive to the TMS (Theater Manager

System). The TMS “ingests” the keys and appropriately distributes them to the appropriate servers. Or the theater personnel has to walk the USB thumb drive to each screen (playback server) and ingest the KDM for the specific CPL version (5.1, 7.1, open captions ….)

A variation is to email to the theater chain headquarters and they can distribute the keys via their internal network.

Today MOST KDM deliveries are via email - some variation of this scheme. I believe that between Technicolor and Deluxe they send out over 1 million emails PER MONTH with KDMs! There must be a better way (there is).

There are a number of **drawbacks to email delivery: labor intensive, takes time to get new keys, and network security**. It takes a skilled person to perform the zip and have access to the TMS (would YOU want a non-skilled person having access to your Theater Management System?). If different keys are needed it can take an *act of panic* to get new keys delivered and a whole bunch of running. Finally, it’s never a good idea to allow an USB thumb drive into a TMS - if nothing else for security protocol against possible viruses.

Part 3 - A better way of delivering KDMs - TKR

The first version of the DCI specification required a Fax Modem line into each server! This was for KDM delivery - it did provide direct access for delivery of KDMs, but there were so many problems - getting phone lines into theater booths, unplugging the lines, etc. It has a failure rate of over 15%.

But today every booth has a network between all devices and at some place a bridge to the web. A group of very smart (and nice) folks devised a method of delivery called **“Theater Key Retrieval” (TKR)** that meets a set of very strong criteria for automated key delivery.

Requirements:

1) Fully automated - hands off operation
2) Secure against viruses and threats to current operations
3) Freely available with no licensing costs
4) Easy and FAST to get new keys both for play windows and versions (hands off)
5) The old way of delivery of KDMs must still work so the transition can be seamless

Here is how it works:

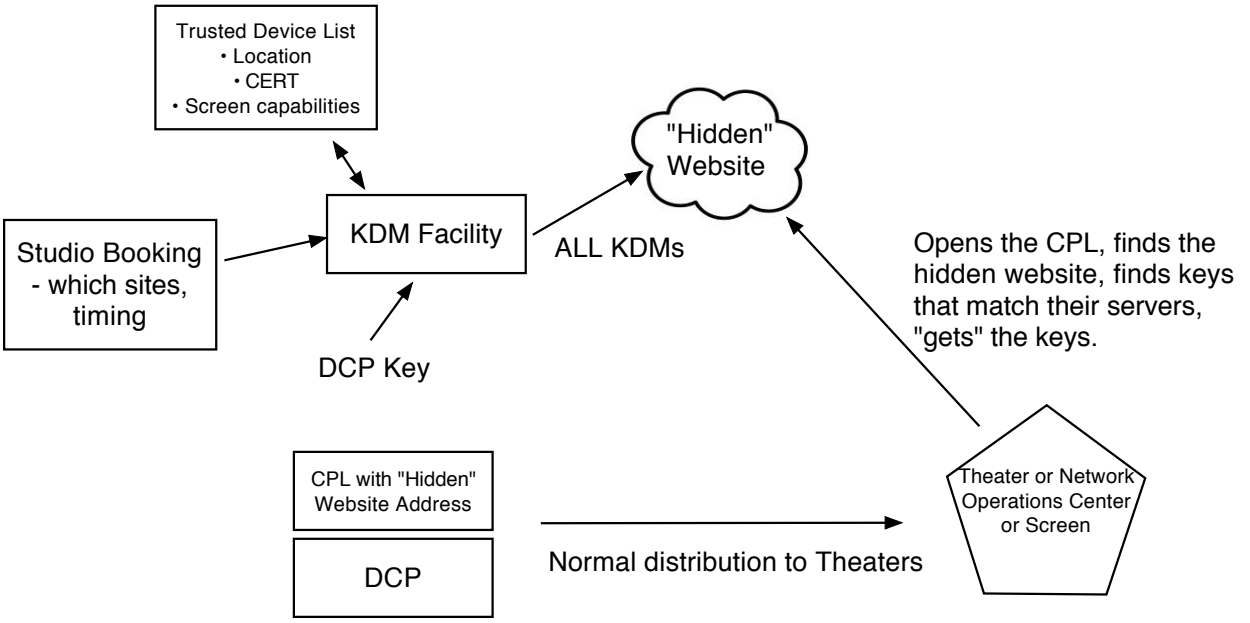


Figure 4 - TKR system

The KDM facility makes a “hidden” website (something like http://www.greatstudio.com/KDM/ 1c326ea0-77fb-11e2-b92a-0800200c9a66 - an address that is not possible to guess). The KDM facility provides this address to the maker of the CPL and the address is included in the CPL. The KDM facility puts ALL the keys for that movie in the hidden website with identification of which KDM goes with which server.

The Theater gets the CPL and finds the address of the hidden website and goes out to find the hidden website and “gets” the KDMs that it needs for its servers.

So the advantages of this approach:

1. The KDMs can be automatically generated (they already are automatically generated) and posted to the hidden website. If you need to “send” a new key, just post a new one and the theater will look for it.
2. The theater is well protected against viruses or someone breaking in the security wall - it is a “get” system and not a “push” to the theater solution.
3. It meets all the requirements specified above.

To make this happen a number of things need to occur.

CPLs need to include the hidden website address. Both Interop-DCP and SMPTE-DCP have been tested and been shown to work (and not cause a problem for software in the field).

Studios need to get on board with using the TKR method of distributing of KDMs. Both Deluxe and Technicolor support this approach and need to be authorized by their studio clients to make it work.

The software in the TMS or servers or Network Operation Center or other centralized KDM distribution architecture needs to use the TKR methodology (of course the email system will still work). This will involve a software change, although many server companies have already written and tested the code (it may be in your server RIGHT NOW). The detail information is posted at http://isdcf.com/papers/ISDCF-Doc8-TheaterKeyRetrieval-TKR-v03.pdf. Also the servers or TMS must have outbound access to the web to access the hidden website in order to retrieve the KDM. Or have the requests relayed through a safe computer accessing the web. Whatever way, this would be easier and more secure than using the email and USB delivery service that is being used now.

Jerry@jerrypierce.org