European Digital Cinema Security White Book

European Digital Cinema Security White Book

Edited by J.-M. Mas Ribés

UCL PRESSES UNIVERSITAIRES DE LOUVAIN

Registration of copyright: D/2007/9964/36
ISBN: 978-2-87463-090-3

Printed in Belgium

Distribution: www.i6doc.com, on-line university publishers.

This book is available on order from bookshops or at:

CIACO University Distributors
Grand-Place, 7
1348 Louvain-la-Neuve, Belgium
Phone: 32 10 47 33 78
Fax: 32 10 45 73 50
e-mail: duc@ciaco.com

Table of Contents

Acknowledgements

This book results from the work of the Enhanced Digital Cinema (EDcine) project established by the European Commission in the context of the Networked Audio Visual line of the 6th framework of IST (Information Society and Technology).

The world of digital cinema has been led by Hollywood initiatives. The Digital Cinema Initiative (DCI) is under standardisation by a subgroup of the Society of Moving Pictures and Television Engineers, namely the DC28.

EDcine was launched in this environment to maintain the European industrial leading edge in the field and to develop new tools and best practices beyond the Digital Cinema Initiative (DCI). Economic, cultural and technical aspects are more complex in Europe. There is a clear need to go beyond DCI.

In its initial functional analysis, EDcine included end-user groups, such as small production studios, local post-production facilities, small and big distribution networks from large multiplexes to small arthouse cinemas, and cinema archives.

It was then deemed necessary to settle the key digital cinema security questions in a “White Book”.

The authors of this book would like to thank the whole EDcine consortium and its project officer, Georgia Efthymiopoulou, for the fruitful discussions which were held during the consortium meetings. We would also like to thank all the associated partners and practitioners from the world of cinema for their useful input.

Foreword

The Shannon model of digital communications is very appealing: the move from analogue to digital allows a compromise between compression rate and quality, and allows communication to be made resilient to error. Digitisation is also an effective means to migrate towards secret communications by establishing ciphered communications. The digital cinema communication chain follows the classical model of compression, ciphering and error protection. The ongoing progress in electronics makes a real-time flexible hardware implementation of the whole chain achievable at the high rates required for digital cinema.

Electronic circuits do not solve all the open issues for the deployment of digital technology. Among others are the security models and tools for key distribution, the audit of content use and the deployment of trusted hardware. This is the topic of this book. Such issues are at the frontier of technology and business models.

For this reason, the landscape of digital cinema is described in the first part of this book. Afterwards, a functional model of digital cinema is proposed, inspired by many interviews with European cinema stakeholders. A security model is derived and analysed using a formal method.

The book concludes with some recommendations for the security of digital cinema in Europe.

Executive Summary

A white book is an authoritative publication whose purpose is to educate stakeholders and to help them make decisions. The "European Digital Cinema Security White Book" deals with different security aspects in the field of digital cinema in Europe.

Security is a difficult area in that it cuts across many different levels, from legal, financial and organisational to systems design, implementation and testing. In security, one requires a global view of all the aspects surrounding a specific issue in order to define an appropriate solution.

In this white book, we cover many of the different areas which have an impact on security and its design and implementation in digital cinema systems. Although the focus is on Europe, most of the contents apply to other markets.

The book begins with a general introduction to digital cinema and security (Chapter 1). The chapter covers the recent history of digital cinema and its financial and technical aspects, as well as including an introduction to general security principles.

Europe is a highly fragmented market in the area of cinema. This contrasts with the homogeneity of the American market. In Chapter 2, we analyse the European market and its different facets, specificities and uniqueness.

The transition to digital cinema is already changing the industry as we know it, and will undoubtedly continue to do so. Chapter 3 analyses these changes with respect to the players in the cinema chain from production to exhibition, and the relationships between them.

When designing security systems – and digital cinema is no exception – one needs to fully understand the organisation in which they are going to operate. In Chapter 4, we model the European digital industry as an organisation, with its own

processes and players. This model is then used to identify the functional requirements and security constraints of a security system which protects digital films, end to end.

Today, there are two organisations working on digital cinema standards in general, as well as on security: SMPTE and DCI. In Chapter 5, we provide a detailed description of the SMPTE standards and DCI specifications which are currently available, and also cover work in progress.

DCI and SMPTE partially define a security system and architecture for digital cinema. A very important part of security engineering is the analysis of the threats a system must protect itself against and the measures in place to mitigate them. Although threat analysis is usually performed on an existing system (which is not the case in digital cinema), in Chapter 6 we base the analysis on the architecture of a system compliant with DCI and SMPTE.

With the transition to digital having just begun, and with technology, standards and financial models being created mostly from a Hollywood standpoint, there is still a long way to go for Europe. Chapter 7 discusses the specific European needs in digital cinema and provides a roadmap for new developments.

Europe is a multicultural, open and independent market, with its own priorities and needs with regard to digital cinema. We conclude this book with a list of 10 recommendations aimed at maintaining the same richness and freedom of content in digital as in 35mm.

Authors and Contributors

We would like to thank all the people that have made this white book a reality. These include EDcine project partners who have written chapters or sections of this book, as well as the many people from the cinema industry who participated in the EDcine "*Digital Cinema Survey*" (results available on the project website). The survey was conducted among European cinema professionals in order to gather their views, concerns and expectations regarding digital cinema. Valuable information was gathered, which has helped provide us with an idea of what digital cinema represents to European professionals, and of the possibilities at this point.

Author List

Séverine Baudry	severine.baudry@thomson.net
Pedro Correa	pedro.correa@uclouvain.be
Didier Doyen	didier.doyen@thomson.net
Benoit Macq	benoit.macq@uclouvain.be
Yves Maetz	yves.maetz@thomson.net
Olivier de Marneffe	olivier.demarneffe@uclouvain.be
JoanMa Mas Ribés	joanma.mas@gmail.com
Philippe Nguyen	philippe.nguyeng@fr.thalesgroup.com
Jean-François Nivart	jf.nivart@intopix.com
Ingo Wolf	wolfi@t-systems.com

List of Interviewed Cinema Professionals

Louis-Philippe Capelle	*Hoverlord Digital Post Production* (Belgium)
Philippe GrandClaudon	*XDC* (Belgium)
Montserrat Guiu	*Cinemes Guiu* (Spain)
Jukka-Pekka Laakso	*Pirkanmaa Film Centre* (Finland)
Antoine Vanderbergh	*Foxority Filmarena* (The Netherlands)

Chapter 1
Introduction to Digital Cinema and Security

The term **digital cinema** refers to digital technology used in the process of producing, distributing and projecting motion pictures. However, this definition – although simple and elegant – does not include all the aspects and complexities that hide behind the notion digital cinema [IDC].

To start with, **cinema** can be defined as the art of presenting motion pictures on "the big screen". Going to the cinema has both social and cultural dimensions. Social because most people go to the cinema with friends or family; and cultural because it is a means of enjoying a form of art. But what makes the *cinema-going experience* an experience, is the big screen, with an image and audio quality found nowhere else. Cinema is about quality.

When we add the adjective **digital** to cinema, it is implied that the quality experienced by a cinema-goer is at least equal to that of 35mm first-run films. Therefore, the above definition should read: digital technology used in the process of producing, distributing and projecting motion pictures such that the quality experienced by the audience is equal to or higher than a first-run 35mm version of the same motion picture.

It is important to note that the cinematic industry as a whole – from production to exhibition – relies on both the social dimension and the quality offered in cinemas, which cannot be experienced on TV, DVD or in top-of-the-line home cinemas.

Quality is an important part of the business model of the cinema industry. Until the advent of the DVD, cinema release was the main source of revenue for films. However, the source of revenues has shifted since the late 1990s, and today, cinema release accounts for around 20% of the total revenues generated by a film; DVD sales and rental generate over 50%[1] of a film's revenue, while TV (pay-per-view, pay-TV and terrestrial broadcast) account for less than 30% (see also [FVA] and [FIR]). The whole film industry depends economically on the release windows in place. Release windows define the point in time when films are released on the various media with respect to their release on the big screen.

The fact that cinemas are moving towards digital technology for receiving, storing and projecting content opens the door to the possibility of projecting other types of content, i.e. films which are not first-run films and are already available in digital form. These "other" types of content are called *alternative content*, and refer to anything other than digital cinema. This includes sports events, music concerts, opera, theatre and other cultural events, publicity, documentaries and archived content. Quality requirements may be different on a case-per-case basis; for instance, independent and low-budget productions or short films may be presented using lower quality (resolution and/or contrast) projectors.

So what term should we use to denote the production, distribution and projection of alternative content shown in cinemas? Industry does not have such a clear definition of the "other stuff" projected in cinemas which has lesser quality requirements than first-run films. It is usually referred to as *alternative entertainment*, *electronic cinema* or simply *alternative content*.

[1] Source: UK Film Council's "Statistical Yearbook 2006/2007", Chapter 13 [SYB]

Today, digital cinema and alternative entertainment are seen as two different classes of cinema presentation. There has been great effort on behalf of the film industry to create new digital cinema standards in terms of image and sound quality, image compression, content packaging and security. Furthermore, as regards financing, distributors will make great savings with the transition to digital since there is no longer a need for 35mm prints; on the other hand, exhibitors need to bear the cost of buying expensive new equipment. In addition, exhibitors are struggling with a decline in the number of cinema-goers. The transition to digital requires the implementation of financing models for exhibitor equipment, of which several alternatives exist today.

On the other hand, there has been no effort on behalf of the industry in terms of the standardisation of alternative entertainment or electronic cinema. Digital TV standards and infrastructure providing a *good enough* quality for the distribution and projection of alternative content already exist. As regards financing, equipment costs much less than digital cinema equipment (around €80K for 2K digital cinema projector and server versus €20K for 1.3K alternative entertainment projector and server).

Due to this cost factor, even until late 2005, when the final version of digital cinema specifications was published by the major studios and the US started producing digital cinema systems, most digital projection systems worldwide were what we call electronic cinema systems. However, in future, when most of the cinemas in Europe and worldwide are digital (i.e. as in digital cinema), it will still be possible to use the same systems for alternative entertainment. From an economic and management point of view, it will be less expensive to exploit a single system, with one projector per screen and a single infrastructure, than to duplicate everything and to use two

parallel systems, i.e. one for digital cinema and one for alternative entertainment.

The Long Transition to Digital

Digital technology in the cinema industry was first introduced in film post-production with digital intermediates: the process of scanning film, correcting colour and manipulating image, and then recording back onto film. Film scanners and recorders whose quality was sufficient enough to produce images that could be inter-cut with regular film appeared in the 1970s, and improved significantly in the late 1980s and early 1990s. However, it was not until 2000 with *O Brother, Where Art Thou?* and *Chicken Run* that the digital intermediate process was used for an entire first-run film. Before that, film scanners and recorders were too slow and the size of images too big for computing capacities at the time [TAN].

As regards exhibition, the first projector able to light up a large cinema screen dates back to the early 1990s, when the Hughes/JVC ILA (Image Light Amplifier) projector became available. The image quality offered by this projector was far from that of 35mm film projectors. Furthermore, due to maintenance and alignment issues, it was impossible to use it in the cinema environment.

DLP (digital light processing) technology was developed by Texas Instruments back in 1987. The technology evolved over 12 years in terms of resolution and contrast until the first DLP-based projector for cinema was demonstrated in 1999. This first-generation DLP cinema projector had a wider colour space than television, a contrast ratio of 1000:1, and a resolution of 1280x1024. With DLP technology, the image is created by microscopic mirrors laid out in a matrix on a semiconductor chip. These mirrors can be repositioned rapidly to reflect light either through the lens or away from it. The

rapid repositioning of the mirrors allows the intensity of the light going out through the lens to be graduated, from white (mirror in *on* position) to black (mirror in *off* position). DLP cinema projectors use three arrays of mirrors (or chips) and a prism to split light from the lamp into each primary colour of light.

DLP technology proved appropriate for cinema projection, in terms of resolution, colour depth and contrast ratio. Furthermore, it was consistent, stable, reliable and without maintenance issues in the exhibition environment.

The availability of DLP technology marked the beginning of digital cinema. From a purely technological point of view, this piece of equipment – the cinema projector – was the only one missing in order to have a full digital chain, from post-production and distribution to the presentation of motion pictures in a cinema environment.

Having addressed the issue of projection technology, it was time to move forward and examine all other aspects of digital cinema. Since 2000, many technology companies, standardisation bodies and industry groups have been working on solving the other issues related to digital cinema, and the new ones which continue to arise. Digital cinema is still in a state of evolution.

Motivating Factors

Cinema has evolved very little in its 100 years of existence. First came audio, then colour motion pictures, and finally digital audio. But these are improvements rather than a radical evolution. So what are the motivating factors behind the evolution towards digital?

The main motivation for the transition to digital in cinema is economics [MOF]. Releasing a film requires the distribution of 35mm reels to each cinema which shows the film within the

first 2 to 4 weeks. It is not unusual for a first release to require 4000 different prints in the US only. Furthermore, the lifespan of a reel is between 50 and 100 presentations, after which the quality of the reel degrades due to scratches on the film.

A film print today costs between €750 and €1125 (1000 to 1500 USD). If, instead of film, hard disks are used to distribute films in digital form, the economy is between €600 and €1000 per print. And by reusing the hard disks – which have a lifespan of several years – the economy is even greater. Other means, such as network-based delivery, whether dedicated or shared, and satellite, once the number of digital cinema rollouts reaches a significant number, may provide even cheaper alternatives to media-based distribution.

This difference in the cost of the duplication process between film and digital has interesting and motivating side effects. First, it would be possible to release a film worldwide on the same day, which would greatly reduce the impact of piracy. The high risk of copying and distributing a film illegally would probably not pay off economically if a film were already available in cinemas.

For all other content (films, documentaries or shorts) which is not a big production and thus cannot afford a major investment in the number of prints, another advantage is the possibility of reaching a much wider audience. In some cases, the number of film prints for a given content does not reach 10. With digital, content can be distributed to a larger number of locations at the same time.

There is another driving factor for the transition to digital which is intrinsic to information in digital form: film quality does not degrade over time. Films are thus more manageable and are easy to copy, destroy and archive. Cinema can take

advantage of all the experience in information management gained by IT.

And last but not the least, with cinemas making the transition to digital – whether digital as in *digital cinema*, or digital as in *alternative entertainment* – there is a possibility of presenting new forms of content in cinemas and generating an extra source of revenue. Sporting events such as the Champions League or the World Football Cup, live or recorded music concerts, or cultural events such as opera or theatre, have relevant audiences.

Push Backs in Digital Cinema

Although there are important and interesting motivating factors that are pushing digital cinema forward, there are also other factors that are preventing it from advancing at a faster pace. Of these factors, the most important are: standardisation and interoperability which, as we will see in next subsection, are only partially addressed today; security, management and equipment certification, which will be covered extensively in this white book; and a fair and working financial model for cost savings and digital equipment investment needs.

The financing of digital cinema equipment is a big and complex issue. On the one hand, the studios and distribution companies will enjoy huge cost savings with the transition to digital.

On the other, there are the cinemas and exhibitors, which have been suffering in recent years from a decline in cinema-goers and from increased competition from technology in the form of home cinemas, DVD, HD-DVD and Blue-Ray. In the United States, big cinema chains have still not amortised the investment they made in the 1990s in multiplexes, whereas in Europe, small cinemas are facing stiffer competition from multiplexes.

Compared to 35mm equipment, the digital counterpart is 4 to 6 times more expensive. Furthermore, a digital installation – or some parts of it – may become technologically obsolete within 5 years, whereas with a 35mm projector, the investment lasts at least 15 to 20 years. To make things worse, the maintenance costs of a digital system are uncertain but expected to be higher, in addition to the need to recycle cinema operators with the new systems. Overall, exhibitors see the investment in digital equipment as too big and too risky, with a vague long-term return on investment [MOF].

For a wide rollout of digital cinema installations, both in the United States and Europe, some kind of co-financing model or subsidy to exhibitors needs to be in place.

In the United States, since the beginning of digital cinema, there have been several efforts to propose such co-financing, from studios and distributors to exhibitors. In 2001, Technicolor pushed its own digital cinema plan, which was later abandoned due to pressure from the American association NATO (National Association of Theatre Owners).

Since 2006, the United States has adopted the virtual print fee (VPF) model, accepted by both studios and exhibitors. Antitrust legislation in the US prevents any direct investment from studios/distributors to exhibitors. The VPF model is based on the existence of an independent party – the digital cinema providers – which, on one hand, signs distribution agreements with studios for digital content, and on the other, finances and pays for digital equipment in cinemas. Studios agree to pay the providers a fee which is proportional to the cost savings they have with digital distribution. Exhibitors, in turn, continue to pay per digital *print* as they would do per 35mm print, but to the equipment provider.

Christie/AIX, Technicolor and Ars Media Alliance all have plans which follow the VPF model, and the initial agreements reached with exhibitor chains have prompted an initial first

wave of digital cinema installations. If all arrangements are fruitful, they would account for 20,000 of the 35,000 screens in the United States.

However, in Europe things are quite different, making it more difficult to implement the VPF model [FJF]. Europe is a diverse market, with significant cultural differences and economic factors contributing to rollout complexity. In Europe there are more than 800 distributors, and a mix of Hollywood and European productions as well as content from other parts of the world [FJE]. The proportion of big multiplexes compared to small- or medium-sized cinemas is lower than in the US, making 35mm prints more crossed-over between cinemas. This means that digital print savings have to be spread across multiple cinemas.

The business in each country also varies greatly depending on the degree of involvement of each government. In Europe, cinema is seen as part of culture, and therefore governments are willing to support it. In Norway, for instance, the government has promised to finance 40% of the costs of the equipment. In the United Kingdom, the majority of the Film Council's digital initiative funding was provided by the government.

Standardization Efforts

In the context of digital cinema, the words "*DCI*", "*SMPTE*" and "*compliant*" often appear together. It is important, however, to clarify exactly what they mean.

The *Society of Motion Picture and Television Engineers* is an international professional association, based in the US, of engineers working in the motion picture and video industries. It is an internationally recognised standards developing organisation, with over 400 standards, recommended practices and engineering guidelines for television, motion pictures, digital cinema, audio and medical imaging.

Digital Cinema Initiatives is a consortium of Hollywood studios formed to establish a standard architecture for digital cinema systems. Its primary purpose is to develop a specification that describes a common open standard for digital cinema that can be adopted by all distributors, studios and vendors. Due to its relationship with Hollywood, conformance to DCI is considered to be a requirement by any equipment manufacturer targeting the digital cinema market.

SMPTE Standards

In January 2000, the first open meeting of the SMPTE's DC28 Digital Cinema Technology Committee was held. DC28 originally created seven different study groups in the areas of mastering, compression, conditional access, transport and delivery, audio, cinema systems and projection. The purpose of the groups was to uncover and discuss the many issues that faced the full deployment of digital cinema.

Today, after more than 7 years and several internal reorganisations, the SMPTE DC28 Technology has 3 working groups covering mastering, distribution and exhibition. These are the groups working on standards, recommended practices and engineering guidelines for digital cinema. Furthermore, there are also 2 study groups for stereoscopic vision and the support of additional framerates.

As of today, the SMPTE has published 14 standards, 2 engineering guides and one recommended practice for digital cinema (see Illustration 1). There are 10 more standards and 6 recommended practices in different stages of the ballot process, and around 10 more draft documents. All together, this makes more than 40 standards, recommended practices and engineering guidelines covering different aspects of digital cinema mastering, distribution and exhibition.

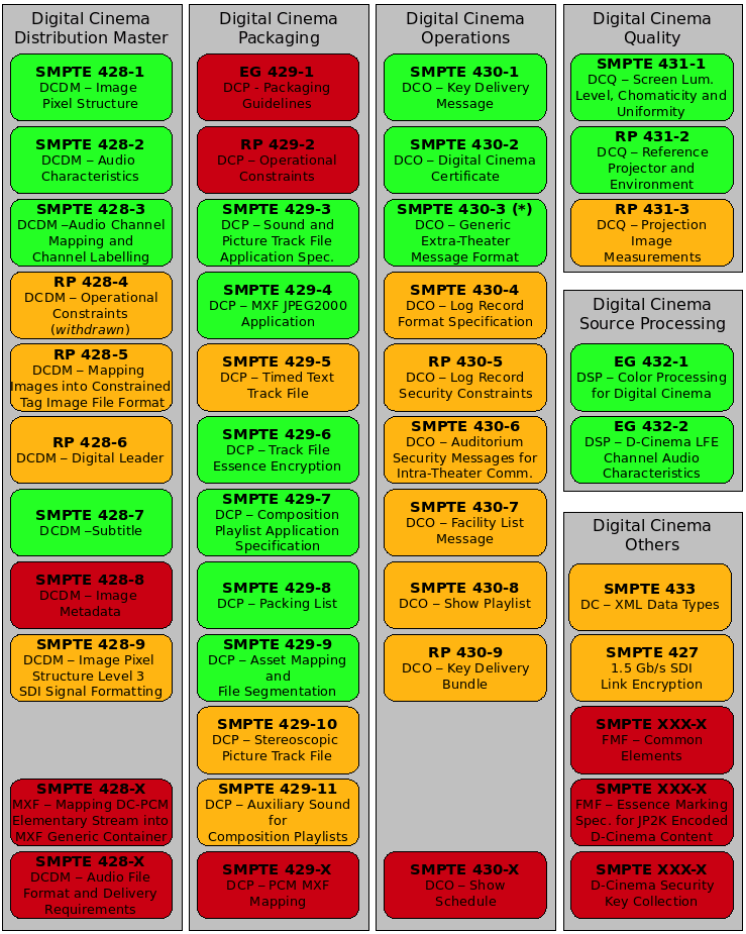


Illustration 1: SMPTE DC28 Digital Cinema Standards (SMPTE), Recommended Practices (RP) and Engineering Guides (EG). Green boxes indicate published documents, orange boxes indicate those in ballot process, and red boxes indicate those in draft process. **(*)** *indicates that an addendum to the document is in the process of approval.*

DCI Specifications

Digital Cinema Initiatives, LLC. ([DCI]) was an entity created in March 2002 as a joint venture of the 7 major Hollywood

studios, namely Disney, Fox, Metro-Goldwyn-Mayer[2], Paramount Pictures, Sony Pictures Entertainment, Universal Studios and Warner Bros. Studios. The goal of DCI was to "*establish and document specifications for an open architecture for digital cinema components that ensures a uniform and high level of technical performance, reliability and quality control*" [DCI].

The main reason for the existence of DCI [FJE], when SMPTE's DC28 digital cinema working group had already been active for over 2 years, was to accelerate the adoption of digital cinema by issuing a set of specifications that would later turn into SMPTE standards. Precisely, the process of creating an industry standard is a long one. In order to accelerate this process, and thus the development of digital cinema equipment and deployment of digital cinema installations, Hollywood studios gathered a group of industry and technology experts to work on the specifications. Once parts of the work were complete, they were submitted to SMPTE DC28 for evaluation, approval and standardisation.

The document "DCI Digital Cinema System Specification version 1.1" [DCI] provides requirements and specifications for parts of the system that are not (yet) covered by standards from the SMPTE or other standardisation bodies (ISO[3], IETF[4] and others). These are:

- Digital Cinema Distribution Master (DCDM): a collection of files whose function is to provide and interchange standard for digital cinema presentations. The DCDM is composed of image, audio and subtitle files (both subpicture and timed text)

[2] Metro-Goldwyn-Mayer withdrew as a member of DCI in May 2005, prior to the publication of version 1.0 of "DCI Digital System Specification".

[3] International Standards Organisation [http://www.iso.org]

[4] Internet Engineering Task Force [http://www.ietf.org]

- Compression: DCI specifies the use of the JPEG2000 [JP2] compression standard (*ISO/IEC 15444-1*). DCI defines the valid resolutions and framerates for DCI-compliant systems: 2K (2048x1080) at 24 and 48 fps, and 4K (4096x2160) at 24fps.
- Packaging: the packaging container is Material eXchange Format (MXF) [MXW], which is defined by a set of SMPTE standards. DCI defines both the organisation of content files and its security within the MXF container.
- Theatre Systems: sets requirements and specifications for both the equipment required for a cinema presentation in a cinema auditorium, and its architecture. This is covered later in this chapter.
- Projection Systems: defines requirements, interfaces and performance specifications for digital cinema projectors.
- Security: defines both the security architecture and the cinema systems architecture, implementation requirements and trust management. This is covered in this chapter.

After publishing version 1.0 of its specifications, DCI accomplished its goals and closed its doors. Physically, DCI no longer exists: there are no offices, employees or assets. However, DCI continues to exist as a legal entity, with administrative and technical oversight being split between two studios every year. Member studios continue to meet whenever required. DCI specifications continue to evolve and changes to the specifications are published.

SMPTE or DCI (or...)?

With all these digital cinema specifications and standards from two different organisations, the question for manufacturers and stakeholders is raised as to what a device or system will implement or comply with.

DCI specifications provide an extensive outline for system architecture and requirements expected by the Hollywood

studios. The label "DCI Compliant" is seen as a *must-have* in order for a device or system to make it to market. Many manufacturers and system providers today claim to be DCI compliant. However, this is only a marketing message without grounds. Only very recently, DCI published a digital cinema validation and compliance test plan (see [CTP]) and no devices or systems have been validated yet. In fact, there are no organisations which have been accredited to perform the tests detailed by the compliance test plan.

DCI references some of the published SMPTE standards, but the effort within SMPTE continues and many documents are still in ballot or draft process. There is a consensus in the industry that DCI specifications are not enough to achieve device and system interoperability. This is expected to be defined by SMPTE standards.

So now, the question is raised as to what will happen in the near future, as more standards are published and the DCI compliance test plan becomes outdated. And what will happen in the not-so-near future, when new technologies become available?

To further complicate matters, DCI compliance is voluntary, and different studios may require different so-called "levels" of compliance. As quoted from "*DCI Digital Cinema System Specification, version 1.1*" [DCI], Notice on page ii, "... *[this document] is intended solely as a guide for companies interested in developing products, which can be compatible with other products, developed using this document. Each DCI member company shall decide independently the extent to which they will utilize, or required adherence to, these specifications*".

As regards SMPTE, things do not look any better. To start with, work is still ongoing and there is no clear view as to when it will reach the desired device interoperability. Even if it were the case already today, there are no testing and

validation procedures for SMPTE standards, and therefore no ways to claim compliance and interoperability.

DCI and SMPTE are not the only organisations active in digital cinema. At European level there is the European Digital Cinema Forum (EDCF, see [EDC]). The EDCF is an industry organisation aimed at promoting discussions and exchange of digital cinema resources among industry members It is not their goal to issue specifications or standards.

There is also the Inter-Society Digital Cinema Forum (ISDCF, see [ISD]) whose mission is to explore all methods of distribution of digital cinema packages and key delivery messages to cinemas worldwide, to recommend technologies within each class of distribution for common acceptable solutions, and to provide information regarding these technologies to the digital cinema community. Until now, however, ISDCF has only one active group working on KDM delivery to cinemas.

Europe

Knowing that the biggest motivating factor for the transition to digital is economic, one understands that the driving force behind the efforts for this transition is, or rather, has been, the United States. Hollywood studios invest billions of dollars every year in the film-making business. The potential reduction in costs of duplicating and distributing films in digital form is enormous. For this reason, the big studios have made huge investments from a financial and human resources point of view, in efforts such as DCI and SMPTE.

The European context is very different to that of the US. Cinema production in Europe is small compared to that of the US, both in the number of films produced per year, and in the average budget per film. Furthermore, in Europe, cinema is considered a cultural good rather than a profitable business.

Cinema production in Europe is highly subsidised by both governments and the European Union.

In Europe, the motivating factor for the transition to digital is cultural rather than financial. European productions and other specialised or non-mainstream films suffer from limited distribution. Distribution agreements for these films are negotiated regionally, country by country. The uncertainty of whether a film will be a success makes distributors keep tight control of the investment they make in both promotion and duplication. The reduced number of 35mm prints also leads to a reduced distribution and availability of non-Hollywood films on European screens.

A transition to digital of European cinemas would solve this limited availability of European and non-mainstream films on European screens.

In 2005, the United Kingdom Film Council launched its Digital Screen Network. It is a £11.5 million government-backed initiative aimed at equipping over 200 cinemas across the UK with DLP projectors. Participating cinemas guarantee to show a specified number of specialised films a week, including foreign language films, in return for the installation and maintenance of equipment.

In the standardisation area as well, Europe has been a follower. There have been no significant initiatives in Europe with regard to standardisation. Rather, cinema professionals and European digital cinema equipment manufacturers have participated and contributed to SMPTE and DCI. After all, these are the standards and specifications that any system must implement in order to play Hollywood content. And US films (most being Hollywood productions) enjoy a market share of between 65 and 85% of the films shown in Europe [MED], depending on the country.

However, DCI specifications, and to a lesser degree, SMPTE standards, have been drafted based on Hollywood

requirements. These standards and specifications define the technology to be used in cinemas, both in the US and across the globe. Systems deployed in Europe also comply with them.

But Europe also differs from the US in many aspects. Now that the early adopters have initiated a rollout of digital cinema installations across Europe, it is time for Europe to start addressing its specificity. This does not mean that Europe should now start creating new independent digital cinema standards; rather, Europe needs to make sure that the use of these standards guarantees accessibility to digital cinema installations of all types of content.

Digital Cinema Today

According to a recent report by cinema analyst Dodoma Research (see [HSD]), half of the screens worldwide will be digital by 2013. This year has seen an explosion in digital conversion, with 4,627 screens switching to digital by September 2007. This represents 5% of the world's total. It is important to note, however, that while Europe and the US deploy DCI-compliant systems (in terms of image resolution and projector luminance), other markets, such as India and China, deploy *e-cinema*[5] systems.

While penetration is deepest in the US, where 78% of the world's digital screens exist, the UK and South Korea come in second and third place. In Europe, around 50% of the screens in Luxembourg and Belgium have already transitioned to digital, thanks to the push by exhibition circuits.

Historically, the first e-cinema systems were deployed for testing purposes in 1999 (see Illustration 2[6]). Until 2004, the number of e-cinema systems, mostly deployed in Latin America and Asia, clearly outnumbered d-cinema systems.

[5] E-cinema resolution ranges between 1.3K and 1.4K, while compression is typically MPEG-2 and MPEG-4 AVC (H.264)

[6] Source: D-Cinema Today http://www.dcinematoday.com/

With the publication of DCI specifications, 2005 marked the wide rollout of d-cinema systems, which already outnumbered e-cinema systems. Since then, the number of d-cinema systems has more than doubled yearly.

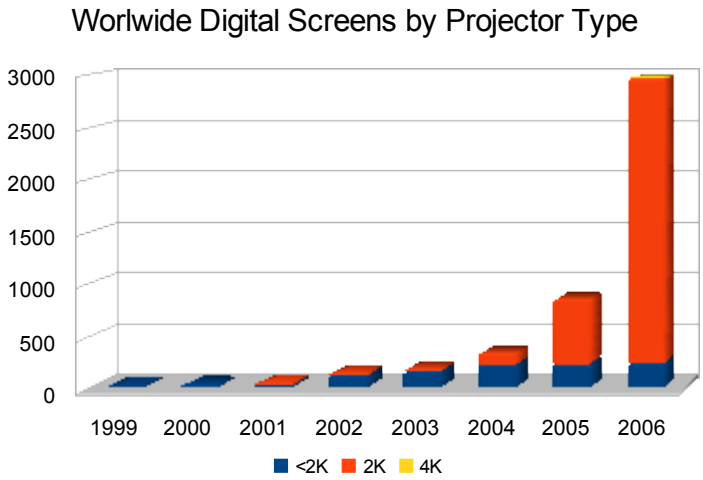


Illustration 2: Number of screens converted to digital worldwide, from 1999 to 2006.

Looking at the number of digital screens and the number of digitally equipped facilities, North America is clearly the leader in both categories (see Illustration 3 and Illustration 4), particularly the US. Europe comes second both in the number of screens and cinemas with at least one digital screen, followed by Asia and Pacific regions, with Latin America far behind. Africa is not even mentioned, having only 2 installations.

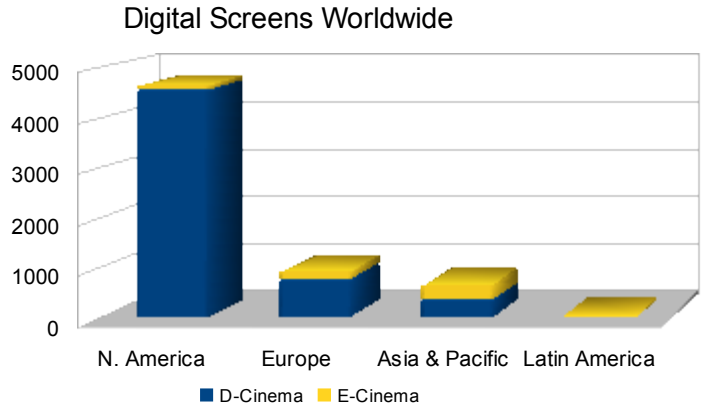


Illustration 3: Number of D-Cinema and E-Cinema screens worldwide by region as of December 2007.

There is however, a significant regional difference in how digital cinema systems are rolled out. In North America, cinemas equip several screens at the same time (with an average of 5.7 digital screens per facility), while in Europe and Asia, only one or two screens are digital per facility (averaging 1.6 and 1.7 respectively).

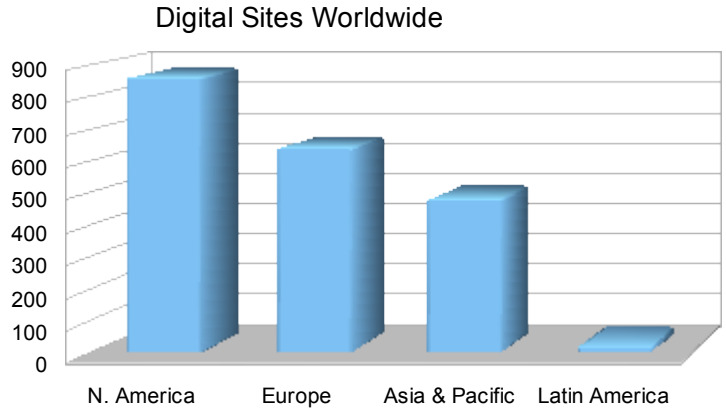


Illustration 4: Number of sites with at least one digital screen worldwide as of December 2007. Data includes both d-cinema and e-cinema systems.

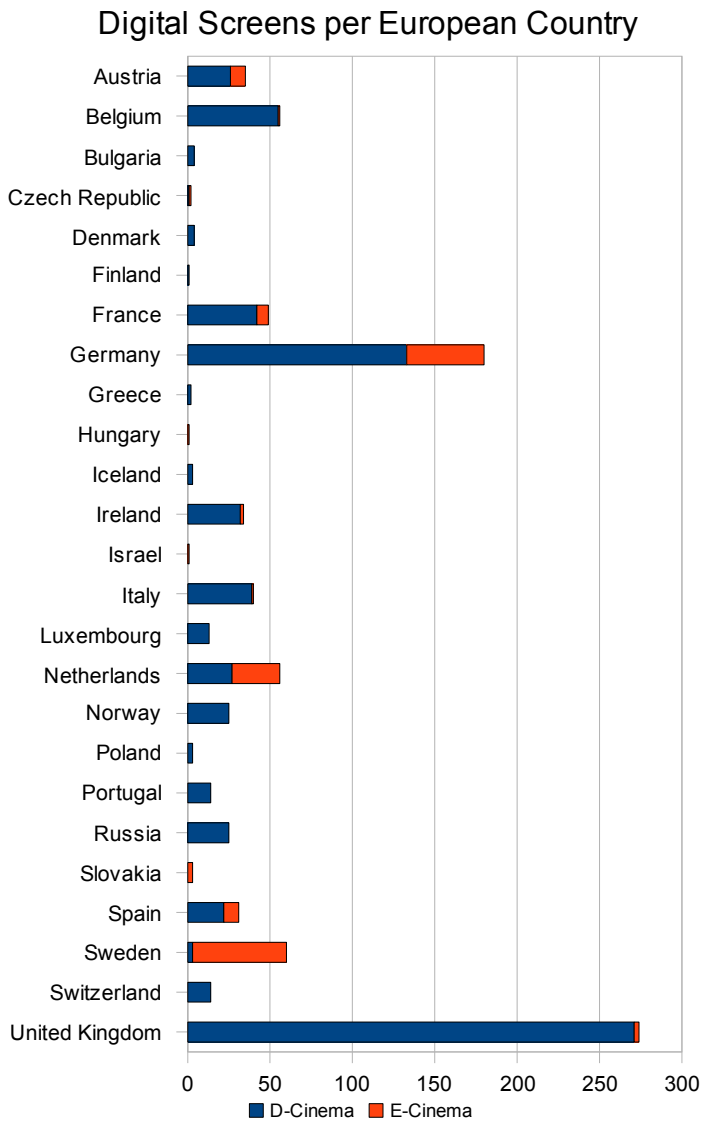


Illustration 5: Number of screens equipped with digital projection systems, both d-cinema *and* e-cinema*, per European country.*

Digital and Security in the Film Industry

Security is the condition of being protected against damage or loss [SEC]. In the digital world, security engineering is the field of engineering dealing with development of detailed engineering designs for security systems and for the security of spaces. It is similar to systems engineering in that its motivation is to make a system meet requirements, but with the added dimension of enforcing a security policy [SEN].

For this reason it involves aspects of computer engineering cryptography, and software development, but also of social science, psychology and economics, as well as physics, chemistry, mathematics and architecture.

Technological advances, mainly in the field of computers and computer systems, have allowed the creation of far more complex systems, with new and complex security problems. Because these systems cut across many different areas, security engineers need to consider the mathematical and physical properties of systems, as well as potential attacks on and from the people who use or are part of these systems. Secure systems have to resist not only technical attacks, but also coercion, fraud and deception.

In IT[7], information security means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

Security is about risk management. In information security, risk management is defined as the process of identifying vulnerabilities and threats to the information resources used by an organisation in achieving business objectives, and deciding what countermeasures, if any, to take in order to reduce risk to

[7] Information Technology is the study, design, development, support or management of computer-based information systems, particularly software applications and computer hardware.

an acceptable level, based on the value of the information resource to the organisation [ISE].

There are two important elements in this definition. Firstly, risk management is an ongoing iterative process. The business environment is constantly changing, and new threats and vulnerabilities emerge every day. Secondly, the choice of countermeasures used to manage or mitigate risk must strike a balance between productivity, cost, effectiveness and value of the asset being protected.

"*The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts*" — Eugene H. Spafford[8].

In other words, given enough resources, any security systems can be compromised or broken. However, in general, *a system is considered secure if the cost of breaking it exceeds the potential benefit of breaking it*.

Digital Cinema, Security and Economics

In the film-making industry, content is the main asset to be protected. Film piracy is perceived as the biggest threat to the industry. Content piracy results in loss of revenue generated by the content. Thus, it is the economic loss, rather than the cost of making a film, that we should consider as the value of the asset we are protecting.

However, estimating economic loss due to piracy in the cinema industry is a very complex and controversial issue. Different stakeholders and industry observers have different positions on the issue.

[8] Eugene H. Spafford is director of the Purdue Center for Education and Research in Information Assurance and Security.

Typically, industry reports backed by Hollywood producers and studios calculate the impact of piracy by estimating the number of pirated copies in the market (both from peer-to-peer illegal sharing networks and illegal DVD copying), and the value of those copies in the market. Like with any estimation, the resulting value strongly depends on the methodology used and assumptions made.

Typically, industry reports backed by Hollywood producers and studios calculate the impact of piracy by estimating the number of pirated copies on the market (both from peer-to-peer illegal sharing networks and illegal DVD copying), and the value of these copies on the market. As with any estimation, the resulting value strongly depends on the methodology used and assumptions made.

It is important to distinguish between piracy occurring before or during cinema release, which causes a loss in box office sales (our concern in this book), and that occurring after DVD release, which causes a loss in DVD sales.

Critics of these reports claim the figures are overblown and alarmist, and put forth several arguments countering and downplaying the impact of piracy in the industry.

A first argument is that the impact of piracy on ticket sales is minimal. They recognise the fact that cinema-going is, above all else, a social event people enjoy with friends and family. Cinema-goers pay for the experience of enjoying a film on the big screen. There are numerous examples supporting this argument. In 2005 someone leaked the studio print of the latest instalment of the *Star Wars* saga before its cinema release. However, despite the film being widely available on illegal peer-to-peer networks, the film did amazingly well in cinemas and generated impressive revenues [SWD]. Recent examples include *Sicko* by Michael Moore [SIC], and *The Simpsons' Movie* [SIM], which, despite being available for download before cinema release, did not hurt the box office. And the list

goes on. In fact, after years of reports and studies claiming year-by-year increases in film piracy, 2007 had the biggest box office summer ever in the United States [BSE]. It is then difficult to believe that the figures presented in these reports are accurate.

These data support another argument against the accuracy and realism of these reports, based on the fact that studies on piracy in the film-making industry only focus on the negative impact piracy has in terms of loss in generated revenue. However, they do not recognise piracy as a free promotional channel. This is the case for big-budget films that invest significant amounts of money in promotion, and is especially true for films with small budgets, as seen in the European cinema industry and, in general, non-Hollywood content.

Independent film-makers are starting to recognise this, and some go as far as "thanking pirates for stealing their film" [TFS]. Eric Wilkinson, producer of the independent film The Man From Earth wrote in an email [NTB], "Our independent movie had next to no advertising budget and very little going for it until somebody ripped one of our DVD screeners and put the movie online for all to download. Most of the feedback from everyone who has downloaded *The Man From Earth* has been overwhelmingly positive. People like our movie and are talking about it on the internet, all thanks to piracy on the net!" In fact, before being available for download, the film occupied the 11,235th position in terms of popularity on IMDb[9]. After 2 weeks, the film was the fifth most popular film, and number one on the lists of most popular independent and science fiction films.

Some industry analysts and economists are realising that the internet and the availability of digital content are shaking the traditional content production and distribution business models

[9] www.imdb.com "The Internet Movie Database", a popular film reviewing and ranking website.

and economics. Recognising that the fight against piracy is a lost battle, with all consumer content protection technologies[10] being broken as they hit the market, some economists are advocating that business models should de adapted and adopted based on the *economics of free* [EOF].

The way the *economics of free* works is actually quite easy and fits with the same basic economics in place. Knocking down the barriers of artificial scarcity opens up tremendous new opportunities – just as knocking down protectionism has helped markets grow by creating new opportunities. The idea here is to start by redefining the market based on the benefits content owners are providing, rather than the specific product they are selling. If the focus is on benefits, then any means of selling these benefits is a good thing. The benefits are then broken down into components that make up the benefits being sold. Every bundle of goods and services that makes up the benefits being sold has components that are scarce as well as components that are infinite. Given that the infinite components are what make the scarce components more valuable at no extra cost, they should be set free. At that point there is every incentive to create more of them and encourage people to get them, by making them easy to share, embed, distribute and promote. And, yet, all the while, one remains aware of exactly what scarce resources these non-scarce goods are tied to, being ready to sell these scarce resources and recognising that the more people who consume the infinite goods, the more valuable the non-scarce resource is.

Business models based on the *economics of free* are already being experimented with in the recording industry, the most notable example being the band *Radiohead* [NYP]. When the band's latest album was released, they told fans they could decide on their price for digital downloads. Then, rather than just offering the content, they also tried to give fans a reason to

[10] DVD's Content Scrambling System (CSS), and HD-DVD and Blu-Ray's Advanced Access Content System (AACS).

buy something else. In this case it was a "discobox", which included the new album both on CD and vinyl, and an additional CD with extra songs, pictures, artwork and lyrics. The move turned out to be a success: direct revenue from CD sales was roughly the same as a major-label CD, they received tons of free publicity, their market share increased enormously and they are signing contracts to perform in big venues that pay better.

With security in digital cinema, much too often we hear the arguments from content owners and producers of big budget films with high levels of investment and promotion. These content owners are in the business of product selling, and thus, it is natural that they invest heavily in system security that protects their business.

However, we must also recognise that for many other content owners, this is not the case. For them, wide availability and distribution of content represents a benefit rather than a loss. We also need to recognise that product selling is not the only economic model that the content industry in general – which digital cinema is a part of – can exploit.

In security, as in many other technological areas, one size does not fit all. Security is a compromise, and if or when the value of the asset being protected is close to zero, as the *economics of free* promotes, then the cost of security will also be very low.

The reader must understand that this section is in no way about defending unauthorised downloads. Piracy is illegal and will by no means be encouraged. This section discusses matters from the perspective of content owners, and explains business models which encourage people to get their content for free. **If done correctly**, they can increase their market share greatly with these new business models.

Security Principles

Independently of the value of the assets a system is protecting and therefore of the level of security a system provides and the cost of breaking it, security engineering must respect some basic security principles. These security principles have been taken from the *OWASP*[11] *Guide* [OPG] and the excellent book entitled *Writing Secure Code* [WSC].

Minimise Attack Surface Area

Every feature in a system or application adds a certain amount of risk to the overall system. The aim for secure development is to reduce the overall risk, and reducing the surface area is a way to achieve this.

Secure Defaults

Many times security restricts functionality. There are many configurations possible to deliver a system to the costumer or user which balance security and functionality. By default, however, the system should be delivered configured for security. It should be up to the user or customer to reduce security if they are allowed to do so.

Least Privilege

Each and every component of a system must have the least amount of privileges required to perform its business processes. This encompasses user rights and resource permissions such as CPU limits, memory, file systems or networks.

External Systems are Insecure

Many organisations utilise the processing capabilities and systems of third-party partners, who may have different

[11] Open Web Application Security Project, a worldwide free and open community focused on improving the security of application software. See http://www.owasp.org/

security policies. Therefore, implicit trust of externally run systems is not warranted. All external systems should be treated in a similar fashion and assumed to be insecure. In other words, protect your system as if all external systems were insecure.

Defence in Depth

The principle of defence in depth is a corollary of the previous principle and suggests that where one control would be reasonable, more controls that approach risks from different angles are better. Controls, when used in depth, can make severe vulnerabilities extremely difficult to exploit and therefore unlikely to occur.

Another way to read the principle is that any component in a system should be configured for security independently of other components' security configurations.

End-to-Endness

The security of a system boils down to the security of the weakest link. Clearly identify the limits of the security system, and apply the same level of security measures. Failing to do so would be like transporting money in an armoured truck, but then depositing it in a cardboard safe.

Fail Safely

Application and system errors happen all the time. However, little attention is paid to the state in which they fail, and most importantly, the security risks of that state are usually overlooked.

When a component fails, make sure it does so in a state that does not compromise the security of the system.

Separation of Duties

Separation of duties is a key fraud control. As a typical example, someone requesting a computer cannot also sign for

it or receive the computer directly. This prevents the user from requesting many computers and claiming they never arrived.

Do not Trust Security through Obscurity

Security through obscurity is a weak security control, and nearly always fails when it is the only control. This is not to say that keeping secrets is a bad idea, it simply means that the security of key systems should not be reliant upon keeping details hidden.

Simplicity

Attack surface area and simplicity go hand in hand. Certain security engineering fads prefer overly complex approaches to what would otherwise be relatively straightforward and simple code.

Goals

At this stage, those who are not security literate should already have understood that security engineering is a complex and multi-disciplinary field. Security cuts across many different areas and layers, from low-level hardware implementation to high-level organisational structure. These different levels are not independent in terms of security. Precisely, a security decision at one level may have an impact on lower levels, in the same way that a flaw at the lower levels may break a system higher-up. In security, more than in any other engineering field, one cannot confine the work to a specific area. The security engineer needs to view the *big picture* to clearly understand all aspects that have an impact on his or her work.

Digital cinema is very young, and early adopters started equipping cinema auditoriums with DCI-grade digital cinema systems only recently. As regards standardisation, there is a long way to go before standards providing secure inter-device

interoperability are completed. Because of this, rather than a digital cinema security system, we have many independent and partial digital cinema systems. Industry stakeholders and professionals are faced with the need to define and/or adapt business processes and business relationships, and to take decisions that will probably have an impact and consequences in terms of security.

Our goal in this book is to provide industry stakeholders and professionals with a clear and complete view of the security-related issues surrounding digital cinema production, distribution and exhibition. The structure of the book follows a top-down approach, with each chapter covering a different layer. The focus of the book is the European film industry, although most of the material provided here also applies to other markets. Digital cinema is digital cinema around the world, and security knows no geographical borders.

Chapter 2
European Cinema Specificity

Introduction

This chapter presents a short overview of the European cinema industry specificities. It is not intended to present an exhaustive or objective analysis, but rather to highlight some characteristics that could be related to digital cinema.

For a more in-depth approach, interested readers may refer to the Mediasalles yearly report on European cinema figures [MED].

About European Cinema Fragmentation

Let us begin with this simple fact:

While Europe produces around 1,000 films per year, film production in the US is substantially inferior in volume, amounting to 600 films a year. However, this proportion contrasts with the revenue figures: Hollywood obtains 79% of the European film business. Let us discuss some of the possible reasons for this paradox.

American Homogeneity versus European Fragmentation

Most of the major American distributors and cinema chains cover the country from east to west, enabling global distribution agreements across the USA. This helps the industry to achieve a large economy of scale on production and distribution. Language, culture, censorship and applicable laws are also harmonised across the whole country or are only

slightly different between states. All these characteristics help create content which targets large audiences across the USA.

Finally, film direction itself adapts to this situation. The Hollywood marketing machine imposes screenings, audience surveys and consequently film adaptations to suit large audiences and guarantee results.

On the other hand, due to historical, geographical and political reasons, Europe is fragmented into different cultures and a vast number of official languages[12] and regulations. This fragmentation generates major differences between Europe and North America for every aspect of the cinema industry: production, distribution and exhibition.

European Cultures

This fragmented European culture strongly influences its film industry. Statistics indeed show [MED] that European films perform below 10% of the box office bar outside their national market (European films have an average of 20% of their own national market).

The desire to promote local culture pushes European production into a vicious circle. Most films are funded by local governments or organisations, each promoting local culture or targeting local markets. Moreover, European artistic culture pushes for the respect the author's artistic vision. Therefore, films are usually not massively adapted or oriented to meet the expectations of big audiences.

This results in a wide and rich range of art films and only a few pan-European blockbusters.

[12] Fox example, 3 different official languages coexist in Belgium and 4 in Spain.

European Languages

Furthermore, language variety constitutes a major barrier to exportation within European countries.

Dubbing production costs are prohibitive for small export quantities. In consequence, most of the exported copies are burned with subtitles, which avoids having to dedicate expensive copies to a specific language.

European Distribution

Censorship differs by country, adding a localisation cost to film exportation.

Distribution habits, customs and regulations also vary, imposing local representatives, distributors or agents.

European Exhibition

Finally most of the cinema chains are also quite local reinforcing the difficulty to get global agreements across Europe.

All these factors preclude the economy of scale of a large pan-European distribution.

A Pan-European Future?

When will we see the development of a pan-European cinema industry?

Digital cinema could help bypass some of the abovementioned hurdles.

Digital subtitling and soundtrack flexibility costs are negligible compared to the current film processing costs. This could help cross language borders.

In the near future, low-cost encoding and duplication could also empower small producers/directors.

The internet already provides a strong globalisation tool, forcing a harmonisation of laws and regulations.

Finally, the additional security of digital cinema will reassure producers and provide powerful tools against piracy.

Chapter 3
From Celluloid to Digital in Europe

The Cinema Chain

The Players

Any cinema production chain, whether 35mm or digital, looks roughly the same, i.e. with four main players: the producer, the post-producer, the distributor and the exhibitor. We will see later that this basic chain can be broken down into many more intermediate players and that it can also vary according to the technology used and the type of material.

Henceforth, the term **'content'** will refer to full-length films (either fictional or documentaries), unless stated otherwise.

The **'producer'** is the rights holder of the film, and is either the creator of the film, or the production house that has bought the rights.

The term **'post-production'** refers to a multitude of intermediate processes (e.g. transfers to tape, scanning, editing, dust-busting, special effects, etc.) accomplished by many different players (labs and post-production houses). Nowadays, the main post-production steps are:

- **Lab processing**: Since 99% of the material is still shot in 35mm negatives, a first step is needed to develop these films into a film positive.
- **Film-to-tape transfers**: This process transfers the film positive to tapes (e.g. BETA digital or DV Cam).
- **Off-line editing**: This is the main creative step after the shooting, and is often achieved in close collaboration with

the film director. It is aimed at assembling the original filmed footage (known as *rushes*) into a *rough cut* film version, i.e. the film as intended by the director, but still without additional enhancements (such as digital retouches, colorimetry and special effects).

- **Scanning** and **lossless file** transfer: This is the process whereby lossless digital files (i.e. files that have not been digitally compressed) are created from analogue support.
- **Dust-busting**: This digital enhancement technique is aimed at getting rid of dust and speckles resulting from the scanning process.
- **Compositing** and **special effects**: This is another digital enhancement technique aimed at creating effects that were not possible during the shooting. Compositing superimposes different layers (either filmed or computer-generated material) to create a final enhanced scene.
- **Colorimetry**: This process enhances the rough cut by changing lighting and colour throughout the film, either to create an artistic effect or to homogenise lighting in different shots corresponding to the same scene.
- **Title generation**: This step creates the opening and closing credits.
- **Dubbing** and/or **subtitling**: These processes create a synchronised audio or text translation of the film dialogues respectively, in order to be integrated into the film when necessary.
- **Mastering**: This step creates the film *master,* i.e. the final lossless copy of the film to be archived, as well as all the different master versions for different purposes (broadcast and video master tapes, DVD masters, etc.).
- **Disk-to-film transfer** and **printing**: This process is the symmetric of the scanning step. It converts the final digital material into 35mm copies.

These steps can be more or less integrated into single post-production houses, depending on their size (however, dust-busting, compositing and special effects steps are generally achieved in the same facility).

The **'distributor'** is the intermediate player who is the link between the producer and the exhibitor. This player is very often much more than a mere logistic intermediate and embodies the rights holder of the film with regard to the exhibitor. The distributor is therefore one of the two negotiating parties of the exhibition contract. This contract with the exhibitor settles the time-window during which the exhibitor is allowed to play the film. In some cases (e.g. blockbusters for cinema chains), this contract can include additional restrictions, such as the screen used for the film projection.

The **'exhibitor'** is the last player in the chain, whose goal is to project the content to the public.

As we shall see below, these basic definitions can be broken down into different variations.

The Cinema Chain by Pairs

Producer – Post-Producer

The relationship between producer and post-producer is multiple and complex. It is both of a creative and technical nature. The producer interacts with the post-production chain in order both to create the film conceptually (editing, compositing, special effects and colorimetry) and physically (scanning, film transfer, archiving and mastering).

As the cinema business is a "small family business" and as these are the first stages of content creation, these interactions are very much based on trust.

Very often, these players have known each other personally for a very long time, trust each other and sometimes even work only using oral agreements. Moreover, producers often allow post-production companies to have an archived copy of each film in their facilities.

This relation, however, tends to be more rigid as the content budget increases. Furthermore, as this chain tends to be more fragmented into different intermediate players in Europe, this rather informal relationship is often more common in Europe than in the USA.

Changes with Digital Cinema

Changes in the chain when using digital cinema are presented in Illustration 6 below, where the blue steps correspond to analogue steps and the green ones to digital ones.

The first column depicts a full 35mm cinema chain. This chain is very seldom used in modern cinema since there is no possibility to take advantage of a digital intermediate tool of any kind. For example, editing is achieved physically (by cutting and gluing pieces of 35mm film together).

The second chain is the most common nowadays: filming and projection is achieved in 35mm, but most of the intermediate post-processing steps are achieved using digital tools. Scanning and printing steps are thus the links between the digital and analogue world.

The third column represents the short- to medium-term digital cinema chain as it will be deployed initially: shooting the rushes will be the only remaining analogue process in the chain, and once the positive film is scanned, every step will be digital up to the screen (making the printing process obsolete). Note that the mastering process will be changed into a DCP creation process. This DCP creation will include the JPEG2000 file encoding, encryption and multiple layer

(image, audio and subtitles) MXF packaging into the final DCP (see Chapter 5 for more details).

The cinema chain presented on the far right will effectively occur not only when digital cinema will be in place, i.e. when the majority of exhibitors will use digital projectors in their facilities, but also when films will be shot in digital support. At this stage, neither the scanning nor the printing processes will be needed. Note that digital film shooting will occur much later than the digital projection revolution, because this step does not only have to evolve to meet analogue image quality, but will also have to meet other technological specifications such as robustness under aggressive conditions (rain, dust, wind and a high temperature range), long-lasting and light power supplies, and robust, transportable and affordable storage capabilities. In non-compressed 2K footage, files weigh a minimum of 9 megabytes per frame, thus having to reach transfer bitrates of 225 MByte/s, and storage capacities of 2 TBytes per film. It is thus easy to imagine how this issue is still an important challenge.

Changes with the Transition to Digital

The main difference in the producer–post-producer relationship will be positive. With the whole post-production process being simplified, producers (and more importantly small producers) could perceive post-production increasingly as an intermediate step between them and the final copy, rather than a long ‘chain within the chain’ process.

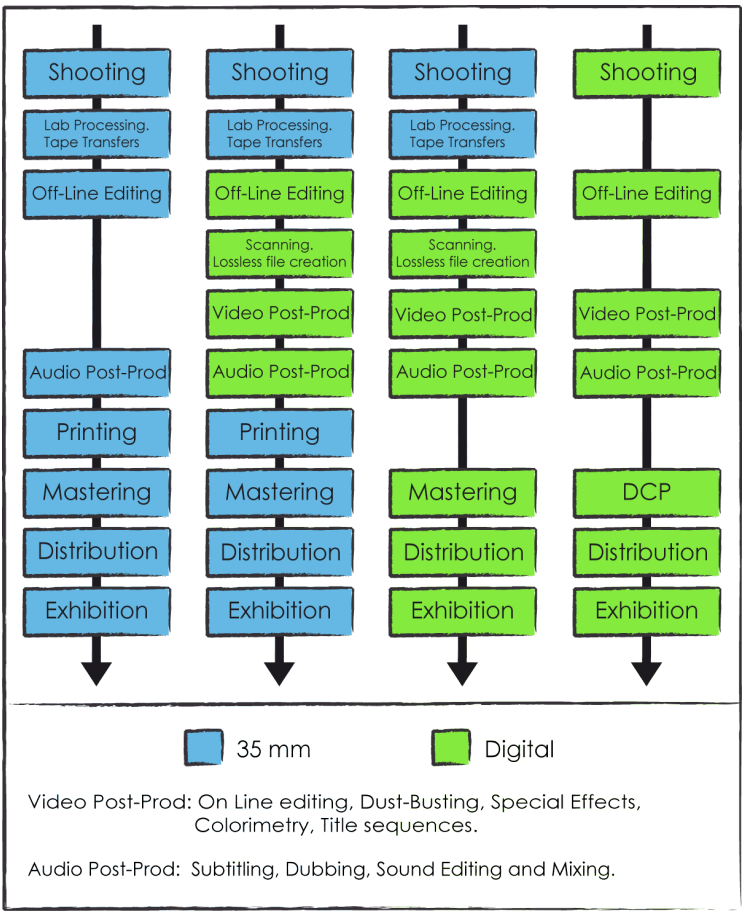


Illustration 6: Progressive changes in film production and distribution chain with the transition to a full digital process

Reducing the post-production chain complexity will not only reduce costs, but it could also have an additional impact with respect to 35mm: as the post-production process shrinks and the final medium becomes easier to produce, producers and exhibitors move closer to one another. This way they could have easier and more direct contact, especially for small-

budget alternative films and, last but not least, alternative content (live concerts, sports, etc.). In some cases, this could allow producers and exhibitors to bypass the distributor intermediary.

Producer – Distributor

As the European cinema model is much more fragmented and heterogeneous than the American model, the producer-distributor relationship can vary in many ways, depending on the production country, grants and budget.

Let us now summarise the relationship in four different scenarios within the scope of this work.

- In the first one, a single player bears the responsibility for both production and distribution. Quite paradoxically, this can occur both for big budget films and for the smallest ones. The former case represents the norm in the Hollywood model (all *big 7* studios are both producers and distributors of their films, and all have European branch offices). The latter case illustrates how a producer, either for economic reasons or for simplicity (because the material will only be distributed to a single country or even a single region) can afford to bypass the services of a distributor company. As stated above, this latter possibility could become easier (and thus more frequent) with digital cinema.
- The second one is the norm in Europe and consists in having a producer get in touch with distribution companies. These contacts can become quickly very rigid and standardised (by societies of authors and the European legal framework on intellectual property).
- The third possibility is to have an additional intermediate player between the producer and the distributor called a *distribution agent* who is in charge of selling the distribution rights. The main advantage of this alternative

is to be able to get in touch with as many distributors as possible through a single contact. This is therefore useful for alternative and independent productions, or for producers with little contact with the European industry (*opera prima* or foreign production with no European branch office, etc.). The main drawback for producers is the additional transaction cost of this agent.

- Finally, an additional alternative has been coming to light more recently: distribution as a service. In this case, the film-maker bears the costs of prints and advertising and subsequently hires a company to provide distribution services, from promotion to the collection of revenues from exhibitors. The film-maker is thus actually renting the distribution system for cinema releases, but pays less for the distribution fee (around 10%-25% of the gross revenue, rather than the classic 40% of the gross revenue). Moreover, "the producer is risking his or her own money, but retains control over the film and continues to have final say in the promotion and costs"[13]. Although this option could be very beneficial to independent and low-budget films, it needs – quite ironically – a substantial amount of upfront cash.

Changes with the Transition to Digital

The changes concerning the distributor role will be discussed in the next section, within the context of the distributor-exhibitor relationship.

With the transition to digital cinema, the relationship between producers and distributors will not be significantly altered, or in any case only indirectly, via changes with other intermediate players (see below, for example, in the section "New Digital Distribution Models", the new post-production–

[13] Peter Broderick, President of Paradigm Consulting, during the 2007 Vancouver International Film Festival Trade Forum

distribution relationship, due to the appearance of new merged digital cinema players).

Distributor – Exhibitor

The relationship between distributors and exhibitors varies greatly depending on the type of cinema. Indeed, even though multiplexes are well established in Europe (about 40% of the exhibition sites [MED]) there is a significant heterogeneity in the types of cinema (the average number of screens in Europe is 2.5 compared to around 10 in the USA [MED]), which means a significant heterogeneity in relationships.

Let us simplify the picture by introducing 2 types of cinema facility: the big cinema chains (multiplexes mainly projecting blockbuster productions) and the alternative cinemas (with 1 or 2 screens and a more balanced play-list of American and European, blockbuster and art-house films, very often projecting only *second-run* copies[14]). There are of course a multitude of other different types of cinema, with between 2 and 8 screens, but these two opposite poles present the most significant differences in their relationship with distributors.

Concerning small cinemas, their relationship with distributors is based much more on trust and is much more flexible than big cinema chains. This could appear quite straightforward, since the revenues they generate are also much lower than those of the big chains. Since these small cinemas are often at the *end of the chain* (either because they use second-run copies of blockbusters, or copies of material that does not need to be released quickly), they do not have the same pressure as first-run facilities to pass the copy on to the next cinema.

[14] Copies that have already been projected a certain number of times (typically between 50 and 100). These copies show clearly how a 35mm degrades with usage, presenting dust, scratches and jittering.

Contracts are very often oral and flexible (they can be modified weekly). Most of the time, the exhibitor has the last word on the number of weeks the cinema will keep the copy. Indeed, since it suits the interests of both the exhibitor and the distributor, and since there is no pressure to give back the copy, the exhibitor will have the last word on the exhibition time-window, holding it as long as spectators keep attending. However, these cinemas are also subject to random supervisions by the distributor company, in order to verify that the weekly attendance figures are accurate.

On the other hand, cinema chains have a very different relationship with their blockbuster distributors, and trust is definitively not part of the equation. Their contracts are all written, rigid and legally robust. These contracts often fix an *a priori* time-window, which is quite rigorous due to the tight schedule of other complexes waiting for the copy. It also fixes the number of screens, shows and even the screen for the film projection (particularly the big screen).

These chains also have weekly reports to be sent to the distributors, and have the same kind of *in situ* supervisions as any other facility. Due to their computerised ticketing infrastructure, very often these complexes have a semi-automatic and formalised way of counting the number of entries and communicating them to the distributors.

Some even say that big cinema chains keep projecting art-house or more alternative films in order to avoid all the abovementioned constraints and to have total freedom as regards how to manage these projections (i.e. time-window, number of screens, size of the screen, etc.). Indeed, these films could introduce additional flexibility into the global equation, either because the chain is a co-producer of the film, or because the distributors do not apply such pressure and supervision with respect to their films.

Finally, big cinema chains can also embody the role of distributor, when handing out the film within their own multiplexes, either as an additional intermediate after the distributor holding the rights or, as presented above, because they are co-producers of the film.

Nowadays, the financial agreements between distributors and exhibitors are mostly based on “revenue-share” deals. This means that the exhibitor will pay the distributor an agreed-upon percentage of the gross revenue of the film. The amount of the share differs from country to country and from studio to studio, but nowadays it is around 40% of the box office gross revenue and can reach 60% (this is the case with blockbusters in Spain for instance, which is the country with the highest revenue-share basis in Europe).

This revenue-share model is the norm nowadays, having been preferred over the years to the previous “flat fee” agreement.

Changes with the Transition to Digital

The distributor-exhibitor relationship is the most prone to change with the digital cinema transition, and even more so for big multiplexes and cinema chains. There is indeed a major change that will tend to shift the negotiating power from the exhibitor to the distributor: with 35mm, exhibitors were in possession of the physical media, whereas in digital cinema, distributors will have the power to create the digital keys and their subsequent time-window. Even though digital keys will still be created and discussed weekly, distributors will then have this additional asset.

Moreover, additional monitoring techniques will be put in place in order to supervise the use of the film: logs will be created for each screen, recording all sensitive data about the screening (name of the film, number of times played, time of projection, etc.).

As long as these two players are concerned, the transition towards DC will therefore, at best, make the former implicit supervision, which was largely based on trust, more explicit. The time-window will also not be based on trust or contracts anymore, but will be technically settled and unalterable.

Pros and Cons with the Transition to Digital

Production

Pros

Since digital cinema will have 35mm final image quality (or even better), and since this quality will not be altered over time, film-makers see digital cinema as an improvement.

The substantial decrease in the cost of producing digital rather than 35mm copies (roughly half the price) is also of the utmost importance for small and independent film-makers.

Finally, material that previously had a very scarce number of copies (sometimes only a single copy) such as archives or documentaries, will also increase their audience as they will have the chance to be shown simultaneously at several different places, with no risk of altering or damaging the copy.

Post – Production

Pros

Post-producers also have a very positive opinion of digital cinema. It will indeed be an extremely good opportunity to ease interaction between intermediate steps. The inclusion of different soundtracks or subtitles will indeed just be an additional digital step, with all the different final creative players working on the visual material.

Cons

The only small issue post-production houses could have concerning digital cinema would be an indirect one. As digital cinema preliminary specifications tend to focus on security, and more specifically on anti-piracy issues related to exhibitors, some voices [BYE] point out the very significant number of illegal copies that come from the production chain itself. This could bring the spotlight on production-related security issues, which could in turn force post-production houses to increase their security measures.

Distributor

Pros

Distributor copies will be cheaper to produce, and will be available in large quantities. Distributors will also have much more control over them, and therefore more negotiation control.

Cons

As explained earlier, by making the whole production chain shorter and the whole transport process easier, digital cinema could very much facilitate contact between producers and exhibitors, allowing the latter to bypass the distributor intermediary regarding some specific content (mainly independent and alternative content).

Their business model will also be the hardest to adapt. Indeed, not only will they have to face a new VPF or VPF-like paradigm[15] to allow the exhibitor's financial transition, but new ways of interacting with the exhibitors will also have to be found. In digital times, for example, distributors will not have tangible reasons for not allowing a film to be played as long as it is deemed necessary by the exhibitor, or for not

[15] See Chapter 1 for more details on VPFs.

allowing a small cinema to have the film at the same time as the big cinema chain next door.

Exhibitor

Pros

Alternative content (e.g. live concerts and sports) will be an additional source of revenue, and will not necessarily have the same business model or same intermediate players as blockbusters.

As mentioned above, the ability to duplicate film material much more easily will benefit creators as well as exhibitors, since they will be able to get hold of very rare material without the risk of altering it.

Generally speaking, a higher number of cheap and unalterable copies could make the distributor-exhibitor relationship more flexible, yet this issue is a very sensitive one and will have to be fine-tuned over time.

Finally, second-run cinemas could have their copies sooner than with the 35mm model, since the copy does not have to go physically from one facility to another, but again this will depend greatly on how the business model is established.

Last but not least, second-run facilities will benefit from having unaltered copies that will therefore no longer seem to be second run.

Cons

Exhibitors could have much less flexibility overall as regards how to manage film projections. Not only will they receive the film with a pre-determined time-window that will automatically disable the film once the deadline has been reached, but the distributor will even have the possibility to link each film to a specific server and therefore to a specific screen in the facility. This latter option is, however, quite

unlikely to occur, due to the fact that the idea of a “set” of trusted servers within the facility has much wider support.

Fixing a *minimum* time-window during which the exhibitor is obliged to air the film – even if it shows disappointing box office figures – is already quite frequent, since it ensures that a certain screen will not show another company's films during that period of time, while promoting the films of their own distribution company. On the other hand, it is both in the distributor's and the exhibitor's interest to get as much of an audience as possible for each film; both parties therefore benefit from extending the time-window as long as the film keeps generating revenue.

Their shows will also be monitored continuously by log reports linked to each server.

The transition to DC will thus increase the distributor’s power of negotiation and supervision control over distributed copies.

Finally, watermarking could put pressure on exhibition facilities to increase their surveillance against camcording.

New Digital Distribution Models

As we have seen above, the cinema chain will change somewhat during the transition to digital cinema. These changes will be both limited, affecting each player individually – e.g. exhibitors having to change equipment or post-producers having to adapt internal processes, etc. – and global, i.e. affecting the chain as a whole.

However, global changes will not be dramatic. As described in the previous section (and Illustration 6 on page 56), only some players (or even processes within players' actions) will be added or removed.

However, the new European Distribution Model will have to take into account:

- The technological implantation (technological changes of each player in the chain).
- The need for new intermediate players in the chain, both financial and technical, in order to make the migration effective.

New players will thus arise in order to tackle these issues separately or jointly (the latter option being more probable).

Some companies (XDC, T-Systems, Arts-Alliance, etc.) are already addressing four tasks in this respect:

- Equipment providers: They supply exhibitors with the necessary equipment for projecting digital, i.e. mainly servers and projectors.
- Financial third-parties: They are also the intermediaries between technical providers, distributors and exhibitors, assuming the role of a 'third-party' investor in the VPF model.
- Service providers: They will provide exhibitors with additional services in order to complete the technical migration (installation, network connection, remote maintenance, staff training, help desk, etc.).
- Content providers: As mentioned above, DCP creation will replace the 35mm copy creation. These types of new business entities, using both their technical assets and their connections with post-producers and distributors, will also assume the role of copy provider.

Since the first task is accomplished in order to help the industry to migrate, it will be the only one to remain for as long as digital cinema finds its way into European customs, disappearing afterwards. The other three roles could nevertheless remain and thus create a new hybrid player, close to post-producers, distributors and exhibitors. These new entities will provide digital cinema services and packaged

(encoded and encrypted) films. These roles will however also be feasible through new distinct intermediate players.

Chapter 4
End-to-End European Digital Cinema Trust Model

Security plays a key role in system development. However, despite this importance, security engineering is still largely independent of the processes of system requirements and system models. Typically, security is included in the system development process *after* the initial system design.

This is a **critical problem**, because security mechanisms then have to be fitted into an existing design that may not be able to accommodate them. Moreover, the design may assume security mechanisms are not necessary, or, on the contrary, force security mechanisms that hinder the operation of the system when it was not necessary. Late analysis of security requirements can also generate conflicts between security needs and functional requirements.

Systems are often compromised not by breaking cryptographic algorithms or protocols, but by exploiting weaknesses in the way they are used. Most security systems have been compromised because the late-design trust model does not match reality.

Consumer DRM is a clear example of this: while consumers perceive they have the “fair-use” right over content they purchase, DRM restricts or eliminates this right. As a result, the customer feels his/her rights have been abused and is then motivated to break the system. The DRM trust model – whereby the content provider considers consumers as trusted – turns out to be false. However, the problem here is not the customer, who is now motivated to break a system that restricts the usage of content they own, but the content provider who imposes restrictions and limits consumers' rights.

With DVD, for instance, this is precisely what happened. "DVD Jon"[16] was motivated to break the protection mechanisms of DVD because 1) he was unable to watch DVD on his FreeBSD[17] computer, and 2) the DVD copy protection mechanism prevents backups of content he had purchased, which is *fair use*.

When security mechanisms are fitted into an existing design or follow a flawed trust model, users try to circumvent these security mechanisms to achieve their goals.

Security requirements reflect a high-level organisational policy regarding the detailed requirements of a specific system. Security analysis and trust modelling need to be integrated into the standard system requirements analysis process. Security requirements can be formulated and integrated into system design at a high level of abstraction. This makes it possible to develop systems and software that are designed with the goal of preventing violations of a security policy.

Introduction

The cinema industry, being a "small family business", can be seen as an organisation, with its goals, policies and relationships among its players. Until recently, this organisation was analogue, with 35mm content, paper or oral distribution contracts, and with film rental agreements reached over the telephone or by fax. The transition to digital content implies that the organisation needs a system supporting the management and distribution of this content. Given the fact that it is 100 years old, this industry already has its well-established trust and business relationships and policies. The security system supporting the transition to digital content

[16] Jon Lech Johansen (November 18th, 1983 in Norway). See [JLJ]

[17] FreeBSD is an open-source, free operating system. For more information, see www.freebsd.org.

must incorporate these into the early requirements gathering and design processes. The goal of this security system is not to replace how relationships are established and agreements are reached and signed, but to support those in the transition to digital.

The fundamental change in the cinema industry with the transition to digital is the migration from 35mm film reels to digital files, i.e. the mechanisms for distributing films. With 35mm reels, the security of film distribution is physical: reels are stored in secure facilities, distributed by trusted transporters, and delivered to known physical locations. With digital content, the security system must emulate and provide the same level of security and trustworthiness to the content distribution process.

Scope and Background

In previous chapters, we analysed the European Cinema industry and how this industry will change with the transition to digital. We identified the different players in the industry, how their relationships are established and agreements signed, the means to control the fulfilment of these agreements, and the different types of content and how it is produced and distributed, from camera to screen. With this clear view of the European cinema industry, we can now build a trust model that will develop requirements and drive the system design.

As we have already explained, the goal in this chapter is to analyse and create a European Digital Cinema System abstract trust model. This model can be further refined to match the precise examples of organisations collaborating in the content distribution process, from post-production to presentation. Working at this abstract level, modelling the industry as it is and works today guarantees that the systems following it will respect and adapt to the business. Risks of security systems whose design is flawed due to integrating security concerns

late in the system design and development process are minimised.

It is important to note that the trust models we present here do not claim to be absolute and to respond to all types of players. With the transition to digital, the responsibilities of each player may change. An example of this, as we have seen in the section “New Digital Distribution Models” in the previous chapter, is the partial role taken by new players as post-producers and distributors.

Trust Modelling

Typically, security engineering begins after the early requirements phase and deals with a series of security services (such as integrity, confidentiality authentication and authorisation) and mechanisms that implement them (such as cryptographic hashes, encryption, user names and passwords, and role-based access control). These mechanisms are then incorporated into the system design phase. However, too often there is a missing step which indicates the need for encryption or access control: what is missing is the capture of high-level security requirements.

Early requirements analysis needs to consider trust relationships, ownership and delegation of authority in addition to the traditional functional requirements. Too often, we observe that, for practical or pragmatic reasons, permissions are delegated to players or staff who are not trusted.

The goal of trust modelling is to analyse the structure of an organisation (roles with their goals and the relationships between them) and map it to roles, agents and functions in the future system.

Introduction to Secure Tropos[18]

Tropos is a software development methodology aimed at describing both the organisational environment of a system and the system itself [BRE]. Tropos adopts the i* modelling framework [EYU], which uses the concepts of *actors*, *goals*, *resources* and *dependencies* to define the obligations of actors (*dependees*) to other actors (*dependers*). An **actor** models an entity that has strategic goals and intentionality within the system of the organisation. An actor represents a physical or software *agent*, as well as a *role* or *position*. A **goal** represents an actor's strategic interests. A **task** represents a means, at an abstract level, of achieving a goal. A **resource** is a physical or informational entity, having no intentionality. A **dependency** between two actors indicates that one actor depends on another in order to achieve a goal, execute some task or deliver a resource.

Secure Tropos Constructs

Secure Tropos extends the original Tropos methodology [GIA] [GIB] [MAS] [MOU] to overcome the limitations of Tropos in providing concepts and processes to capture security requirements and to model trust relationships. Illustration 7 below depicts the top-level constructs in Secure Tropos[19].

A **security constraint** represents a constraint that is related to the security of the system or organisation. A constraint is defined as a restriction related to security issues, such as privacy, integrity, confidentiality or availability, which influence the analysis of the system. **Ownership** indicates that an actor is the legitimate owner of a goal, task or resource.

---

[18] Research on Secure Tropos methodology has been partially financed by the EU-financed projects SENSORIA and SERENITY of the 6th Framework Programme.

[19] All Secure Tropos diagrams have been created with the ST-Tool (version 1.4.04). See http://sesa.dit.unitn.it/sttool/

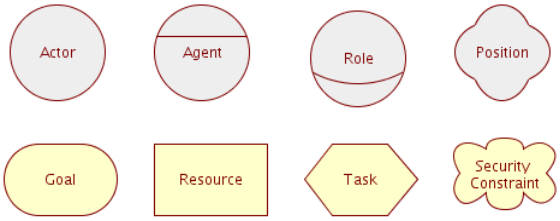


Illustration 7: Top level constructs in Secure Tropos methodology.

Trust of permission between two actors indicates that an actor, *truster*, believes that another actor, *trustee*, will not misuse the permission to achieve a goal, execute a task or access a resource. In these cases trust in centered on an object, which is called *trustum*. In general, by trusting another actor in relation to a trustum, an actor assumes that the trustum is properly used. **Trust of execution** between two actors indicates the belief of one truster that the trustee will achieve a goal, execute a task or deliver a resource. In general, by trusting another actor in relation to a trustum, an actor assumes that the trustum will be delivered.

Delegation of permission between two actors indicates that one actor, called *delegater*, delegates to another actor, *delegatee*, the permission to achieve a goal, execute a task or use a resource. In these cases, delegation is centered around an object, the *delegatum*. **Delegation of execution** between two actors indicates that one delegater delegates to the delegatee the achievement of a goal, execution of a task or provision of a resource.

Illustration 8 below depicts the graphical representation of Tropos dependencies and Secure Tropos trust and delegation relationships.

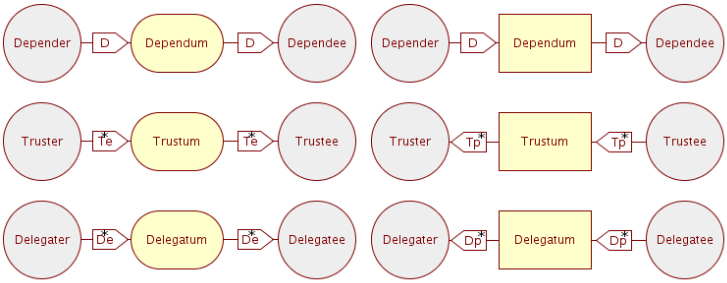


Illustration 8: Dependency relationships in Secure Tropos. A goal dependency and how it translates into trust of execution and delegation of execution, is depicted on the left. Resource dependency and how it is translated into trust of permission and delegation of permission relationships, is depicted on the right.

Secure trust of permission / execution represents that a trust relationship between two actors involves the introduction of a security constraint that must be satisfied either by the truster, the trustee or both, in order for the trust relationship to be valid.

Along the same lines, **secure delegation of permission / execution** represents that a delegation between two actors involves the introduction of a security constraint that must be satisfied either by the delegater, delegatee or both, for the delegation to be valid.

Secure delegations of permission / execution (and also secure trust) are categorised into *delegater secure delegation*, in which the delegater introduces a security constraint for the delegatee to satisfy (see Illustration 9 below), *delegatee secure delegation*, in which the delegatee introduces a security constraint for the delegater to satisfy, and *double secure delegation*, where both the delegater and the delegatee introduce security constraints for the other to satisfy.

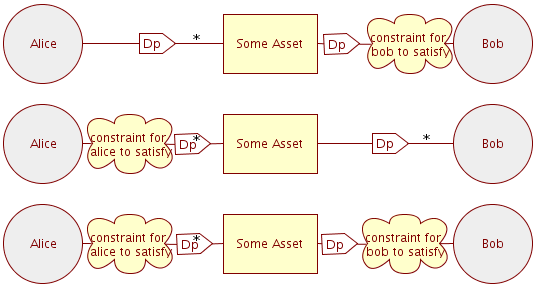


Illustration 9: From top to bottom, graphical representation of Secure Tropos delegater secure delegation*,* delegatee secure delegation*, and* double secure delegation *relationships.*

Secure Tropos Modelling Activities

Secure Tropos defines several modelling activities as part of the methodology process. The initial modelling activity is **actor and dependency modelling**, which is inherited from classical Tropos, and may be used to start the process. Dependency modelling aims at identifying actors and their goals within an organisation, and the dependencies they have with other actors in order to achieve their goals.

Trust modelling consists in identifying actors that trust others actors for goals, tasks and resources, and also actors which own goals, tasks and resources. In the early requirements analysis, the focus is on modelling trust relationships between social actors of the organisational setting. New trust relationships and actors are added to the model as it is refined through iterations. During the late requirements analysis, trust modelling focuses on analysing the trust relationships of the system-to-be actor.

Delegation modelling consists of identifying actors that delegate to other actors the permission or execution of goals, tasks or resources. In particular, in the early requirements analysis, the focus is on modelling delegation relationships between social actors of the organisational setting. New

delegation relationships are added to the model as it is refined through iterations. During the late requirements analysis, delegation modelling focuses on analysing the delegation relationships of the system-to-be actor.

Security constraint modelling extends trust and delegation models by modelling security constraints imposed on the actors and the system, allowing an analysis to be performed by introducing relationships between the security constraints.

All these models use the same notation and constructs for actors, goals, tasks and resources. Essentially, a trust model represents the trust network among actors involved in the system, while the delegation model represents which permissions are effectively delegated by actors, and which actors receive these permissions.

Secure Tropos Process

The overall methodology process defined for Secure Tropos is an iterative one in which the modelling activities presented above are used to produce different kinds of actor and goal diagrams. The diagrams produced in one activity are used as input for other activities. In general the process starts with an actor and dependency model. Trust and delegation relationships are then defined together with any security constraints that might restrict the actors.

During the **early requirements analysis phase**, the goal is to identify the domain stakeholders and model them as social actors, who depend on each other for goals to be achieved, and resources to be provided. By clearly defining these dependencies, it is then possible to state *why*, in addition to *what* and *how*, as regards system functionalities, and to guide the development of the final system. An actor and dependency diagram is produced initially, which is refined after subsequent analysis. This diagram is extended to include the trust and delegation dependencies among actors. This activity will produce a more refined version of the actor diagram in terms

of trust and delegation diagrams, where trust and ownership relationships are analysed along with the delegations among actors. Then, the security constraint modelling activity will further enhance the analysis by identifying and modelling the security constraints of the involved actors.

It is worth mentioning that the analysis process and the application of the modelling activities is quite iterative, meaning that various iterations, leading to refined diagrams, take place before the final version is produced. Moreover, each modelling activity may generate further analysis, since new actors, goals or resources might be discovered. This will start a new iteration of analysis aiming to preserve the consistency of the produced models.

The late requirements analysis phase employs the same modelling activities as in the early requirements analysis. The main difference is that whereas in early requirements analysis, the environment of the system is modelled, during late requirements analysis we model the system-to-be. The system is introduced into the analysis as an actor, which has a number of goals. The diagrams are then adapted then to model the dependencies and relationship between the new system-to-be actor and the existing actors. These dependencies allow us to identify the system requirements, both from a functional and security standpoint. Trust, delegation and security constraint modelling activities then allow the goals and security constraints of the system-to-be to be identified.

European Digital Cinema Model

When the cinema industry was all 35mm, from shooting to post-production and presentation, the security of content was physical: physical media, secured facilities with physical access control, delivery of reels to well-known locations, and staff trusted with handling these reels throughout the chain. Stealing a reel was difficult due to its size and weight; the

investment in film duplicating equipment was (is) very high; and so was (is) the risk of being discovered for any cinema making use of a pirate copy of a film.

With the introduction of digital post-production of content, the low cost of digital media and the wide availability of internet connectivity in recent years has caused film piracy to skyrocket: it is very easy to access a digital file from a server or workstation unnoticed and to compress and copy it onto removable media. Duplicating digital media is straightforward and cheap, and putting a pirate copy on the internet (dedicated servers or illegal peer-to-peer networks) requires very little technical knowledge and costs nothing.

According to a study conducted in 2003 on the origin of copies that were available on illegal peer-to-peer networks [BYE], over 75% of them (out of 285 samples) had been leaked by industry insiders, with copies originating mainly from award or promotional screeners, but also from unfinished post-production. With digital distribution, things can only get worse, since the number of places where film is in clear form increases significantly.

Although studios have already started addressing these issues and are implementing measures to prevent or at least identify the origin of screener leaks, protection of digital content during production, post-production and distribution phases remains widely unaddressed by both the industry, equipment manufacturers and standardisation bodies.

Social vs. Individual Trust

The problem the industry is facing is one of trust: social vs. individual trust (see Illustration 10 below). Social trust is defined at an organisational level between actors or roles: a *Producer* trusts a *Post-Producer* (and more precisely, the role

of *Film Editor* which is part of the *Post-Producer*) to prevent content piracy. This trust is necessary in order for the *Post-Producer* to perform its task. However, at an individual level, the *Producer* should not trust whoever is the *Film Editor* (refer again to [BYE]) to do the same, especially when the risk of being caught is negligible for this individual, and the benefit may be very high.

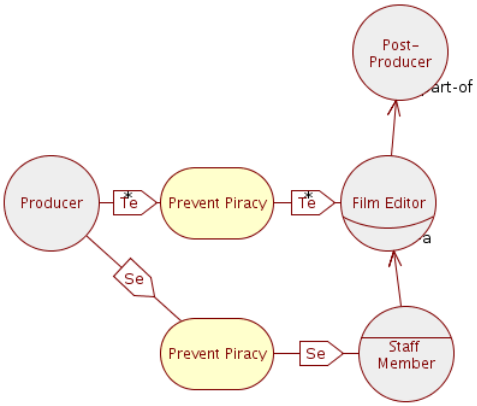


Illustration 10: Social vs. individual (dis)trust. A Film Editor*, part of the* Post-Producer*, is trusted by the* Producer *to* Prevent Piracy*. On the other hand, the individual* Staff Member *who plays the role of* Film Editor*, is not*.

When performing trust modelling, we focus on social trust and dependency relations, since these define the structure of the organisation which should be described explicitly in the requirements phase. Systems designed and implemented following this trust model will support the functional requirements identified, while protecting resources (specifically digital content) and preventing any illegal or unauthorised use.

Early Actor Model

The first activity in the early requirements phase is **actor modelling**. We focus only in the content production, distribution and exhibition processes; that is, we intentionally do not include agreements negotiation, signature and enforcement in our analysis. As explained earlier, it is accepted by industry players that early security systems will manage the protection of the content throughout the cinema chain. Security systems shall follow the "**control loosely & audit tightly**" rule, meaning that players are entitled to manage content, both at distribution and exhibition level, as they have been doing until today, as long as any action is audited and reported back to the content owner.

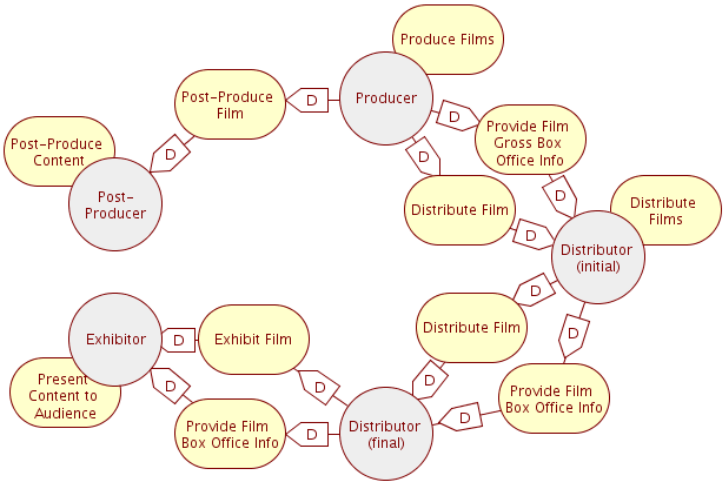


Illustration 11: Early actor dependency model depicts digital cinema actors, and the goal dependencies among them.

Illustration 11 below depicts the "control loosely audit tightly" rule: a *Producer* depends on a *Distributor* for distributing a film, but also for providing accurate box office information detailing the content usage by all *Exhibitors* down the

distribution chain. Note that the illustration shows two *Distributors*, in order to serve as a generalisation. It is precisely not uncommon for a film to go through two or more distributors or distributor agents. By considering a system with two distributors we guarantee that it will be able to accommodate any number of distribution steps.

Refined Trust/Delegation Models

In Secure Tropos, we should now refine the goals identified in the actor dependency diagram in order to further analyse and break them down into sub-goals. However, we will not present this step here, as our aim is to focus on the trust and delegation models, which will help us identify both functional requirements and security constraints.

The requirements modelling process starts by introducing the social relations among actors.

Trust modelling consists in identifying actors who trust other actors for goals and resources, and actors who own goals and resources. These trust relationships are of two different natures: trust of execution of a goal, and trust of permission for a resource. In the early requirements phase, the focus is on the social actors.

On the other hand, **Delegation modelling** consists in identifying actors who delegate the execution of their own goals to other actors, or the permission to access a resource they own or are delegatees of.

Illustration 11 shows that dependencies between actors in the digital cinema chain always happen between two actors, independently of the others. There is a *Producer Post-Producer* dependency; same applies to *Producer Distributor*, *Distributor Distributor*, and *Distributor Exhibitor*. This allows

us to perform the trust and delegation modelling to a pair of actors, independently of the others.

Producer – Post-Producer

The *Post-Production Manager* role, who is part of the *Producer*, sends the digital film dailies to the *Post-Producer*. The *Film Editor* role, who is part of the *Post-Producer*, scans the dailies into digital form and stores them on an image server, thus starting the *Digital Intermediate* process. *Film Editors* and *Quality Control Editors* work on the *Digital Intermediate* until the final *Digital Source Master* is created and returned to the *Producer*. Illustration 12 below shows the trust and ownership model between *Producer* and *Post-Producer.*

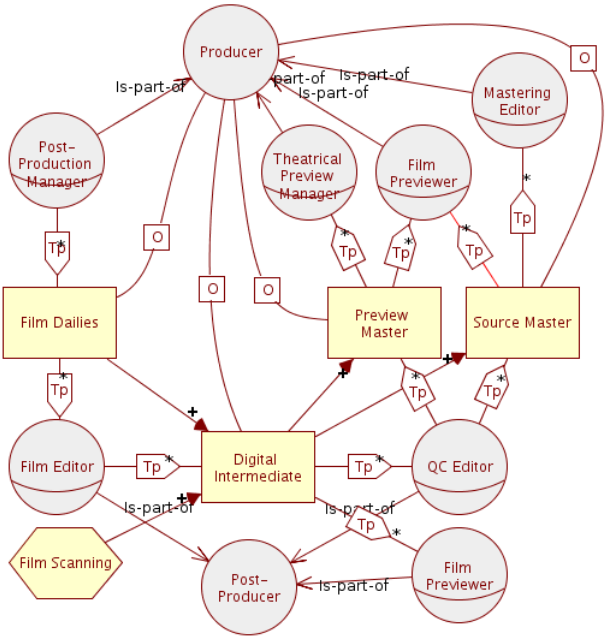


Illustration 12: Refined Producer/Post-Producer trust model. The image shows the actor's specific roles, trust relationships between them, and the ownership of digital assets.

Illustration 13 below shows the delegation model with **security constraints** in the relationships between social roles. For instance, the *Post-Production Manager* will provide the *Film Dailies* of a specific film only to the *Post-Producer* hired to perform this task. The *Film Editor*, in turn, shall take the necessary measures to keep these *Film Dailies* confidential.

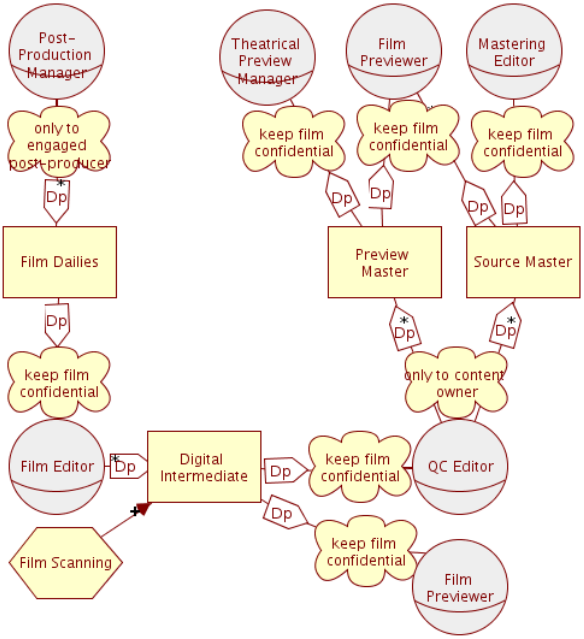


Illustration 13: Refined Producer/Post-Producer Delegation Model with security constraints depicted as soft-goals.

Producer – Distributor

There is a wide range of relationships between *Producer* and *Distributor*, from the permanent ones that the big Hollywood studios have with their own distributors, to relationships established on a per-film basis between an art-house producer and a distribution agent.

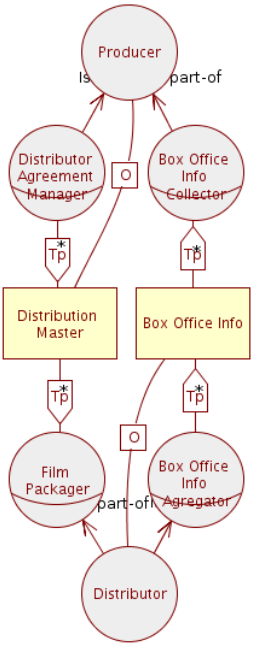


Illustration 14: Trust and ownership model.

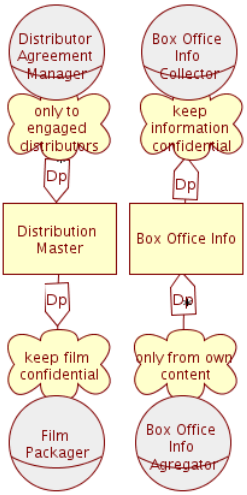


Illustration 15: Delegation model with security constraints.

This variety in the relationships between *Producer* and *Distributor*, however, does not fundamentally change their nature: a producer reaches a distribution agreement with the distributor. Within the context of this agreement, the producer will provide the distributor with a digital cinema distribution master. In turn, the distributor commits itself to collecting box office information from the exhibitors and/or distributors it

signs agreements with. Illustration 14 and Illustration 15 depict the trust and delegation models for this relationship.

One can see in the illustrations that the *Producer* delegates permission over the *Distribution Master* to the *Distributor*, or more precisely to the role of *Film Packager*, who is responsible for creating the Digital Cinema Package.

In the delegation model, we also see the *Box Office Info Aggregator* role, whose goal is to aggregate all the collected box office information and provide it to the *Producer*.

At this point it is important to mention the depth of trust and delegation. Unless stated otherwise, trust and delegation have infinite depth. This means that a *delegatee* of some resource can further delegate this resource, becoming a *delegater*, to some other actor. Although in Secure Tropos the trust and delegation depths can be constrained, this is highly dependent on the actual actors and their relationships, and is thus too detailed for this level of abstraction.

Distributor – Distributor

The relationship between a *Producer* and a *Distributor* offers a wide range of possibilities, yet the relationship between *Distributors* is even wider, especially in Europe where there are roughly 800 distributors. There can be classic distributors that act as intermediaries between producers and exhibitors. There are also the so-called distribution agents that either receive content from a distributor and negotiate agreements with small cinemas, or find other distributors for a small producer. Cinema chains are also distributors from a functional point of view, since they are an intermediary between a distributor and a group of cinemas.

Once again, however, the variety in the nature of the relationships between distributors does not fundamentally change the nature of their relationship. Illustration 16 and

Illustration 17 below show the trust and ownership model and the delegation model with security constraints.

We should note that, especially for low-budget and art-house productions, it is common for the agreements between national distributors from different countries to follow a *fixed-price* model. Since the revenue generated is independent of the audience and number of times the film has been played, there is no transfer of *Box Office Information* between the distributors. In the models, the fact that such transfer appears does not imply that it is mandatory. However, we anticipate that the *fixed-priced* model will disappear with digital distribution; the existence of this model is linked to the high cost of film duplicates and to the impossibility of sending inspectors to cinemas outside their geographical area. Instead of renting a film, the film media are "sold". With the transition to digital, both of these reasons disappear: the duplication cost is negligible, and the security system will keep track of the number of times a film has been played. This will probably cause the *fixed-price* model to disappear too.

The ownership relations in the trust model deserve some clarification. With respect to the *Digital Cinema Package*, the initial distributor is responsible for its creation. This package may be created by different distributors covering different geographical or linguistic areas. It then seems natural to assign ownership to the distributor that creates each different version, although the ultimate owner remains the producer of the film. And with respect to the *Box Office Information*, this is the result of aggregating and possibly filtering box office information originating from several sources, either exhibitors or distributors. Again, the ownership is assigned to the distributor that generates it, even if parts of it are ultimately owned by other actors.

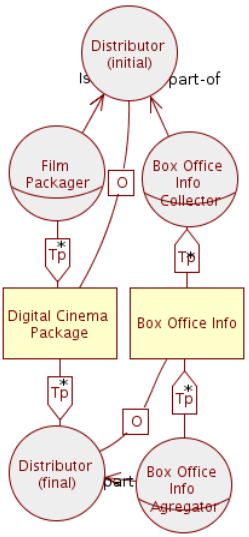


Illustration 16: Trust and ownership model.

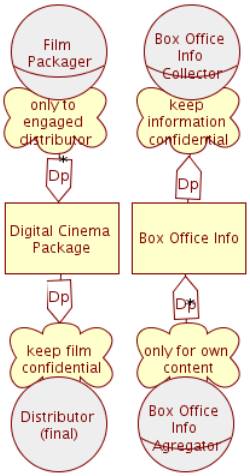


Illustration 17: Delegation model with security constraints.

Distributor – Exhibitor

Contrary to all other cinema actors between whom there is a more or less implicit trust relationship, distributors historically (until today) have not trusted exhibitors to provide accurate film usage and audience information. Exhibitors, in turn, are reluctant towards distributors that want to intervene in their business.

The way to solve this situation was for distributors, with exhibitors' consent, to have inspectors in cinemas who verify the weekly schedule of cinemas, and estimate the size of the audience attending a show. This information is then reported back to the distributor, who correlates it with the one provided by the exhibitor itself. In the case of inconsistencies and disagreements, the distributor may decide to sanction the exhibitor.

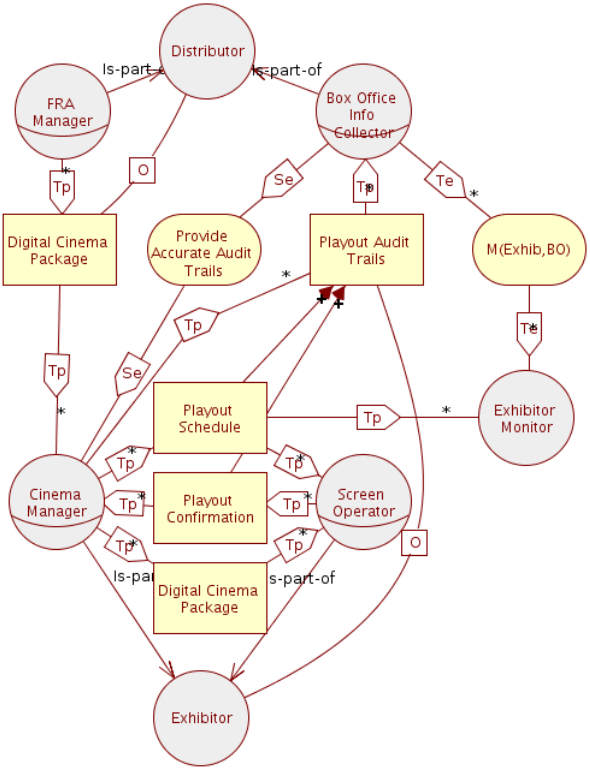


Illustration 18: Trust and ownership model for the distributor exhibitor relationship. The figure also depicts the trust model for film presentation. Note distributor's distrust of the exhibitor to provide accurate audit trails.

This relationship, which includes the cinema inspector, represents a clear example of a situation in which an actor distrusts another for the execution of a goal, but does not have any other option but to delegate it. The only way to make sure the delegatee will not take advantage of the delegatum is through monitoring it.

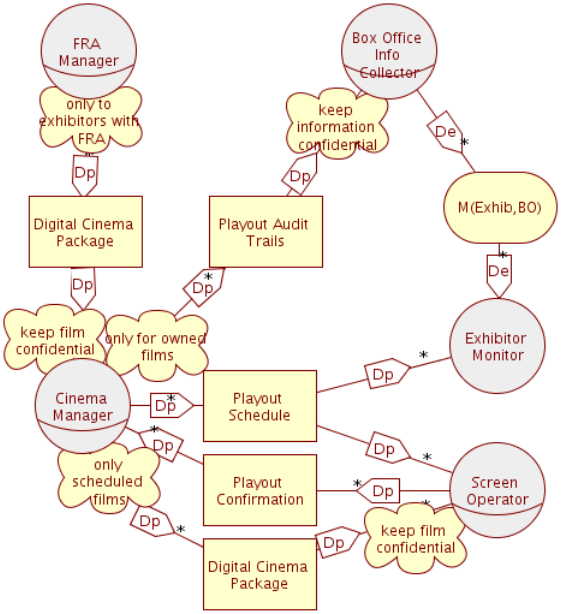


Illustration 19: Delegation model with security constraints. One can also see that the Distributor *delegates the monitoring of the exhibitor to an* Exhibitor Monitor.

Secure Tropos also allows these situations to be modelled (see [GIA] and Illustration 18). The *Distributor* distrusts the *Exhibitor* to provide accurate *Playout Audit Trails*, so a monitoring system is put in place. The *Distributor* now trusts a new actor (*Exhibitor Monitor*) to monitor the *Exhibitor* in providing accurate audit trails. In practical terms, this is achieved by the *Exhibitor Monitor* performing inspections in cinemas and estimating the size of the audience. Later, this information is correlated with the one provided by the *Exhibitor*.

It is worth noting that today it seems quite pointless to have someone performing inspections in cinemas once a week. To start with, cinema schedules are available from many sources

of information, such as the internet, the press and the printed cinema schedule available in all cinemas. Today most cinemas also have computerised ticket selling systems that can be audited to obtain detailed figures regarding audience size per film. We see little interest in an exhibitor faking audit trails when the risk of being caught is high.

The delegation model shown in Illustration 19 also illustrates the relationship in which the *Distributor* distrusts the *Exhibitor*.

Alternative Content

We have focused our trust models and analysis on film content. It is important to note that, at this level of trust modelling, the nature of the content, be it blockbusters, alternative content, publicity and trailers, live and cultural events, or archived material, has little or no significance as regards the resulting models. Differences are mostly related to image compression format and transmission methods.

- Publicity: should be treated like any other content; protected for delivery and storage, usage reported to the publicity distributor.
- Trailers: delivered along with film content. It should be treated in the same way as publicity.
- Live and cultural events: the main difference here is the compression and transmission format (typically MPEG2 over satellite), rather than the trust models themselves.
- Archives: the DCP is created by the archiving organisation, with distribution taking place in the same way as for film content.
- Art-house and alternative productions/distributions: the same trust models as those for “normal” film content apply here.

Digital Cinema Security System Model

In the previous section we presented an organisational model of the European digital cinema content creation, distribution and exhibition processes, and of the audit trails thereof. It is important to highlight that the focus of the model and the system we will study in this section deals only with content and audit trails; establishment of business (and thus trust and delegation) relationships and negotiation of agreements happen outside the system in the same way they do today for 35mm. Whether this is done over the phone, via fax, over the internet or by signing a paper contract does not influence the security system itself.

It is worth calling to mind again that the digital cinema security system follows a *control loosely audit tightly* principle, as agreed by industry stakeholders. In other words, the system controls the access and distribution of cinema content to players with whom an agreement or business relationship exists, and provides the necessary information allowing the verification by the truster that the trustee has honoured this trust relationship.

It is likely that in future, the security system will incorporate some type of digital rights management. This implies shifting the responsibility of expressing and managing rights over content and negotiating agreements from humans today to the system. In order to achieve this goal, one will need to extend the different trust and delegation models to incorporate business relationship establishment and agreement negotiations. This will imply the addition of new actors, goals and resources in the organisational models, and the delegation of new responsibilities (functionality) to the security system. However, the current system model for content and audit management should remain the same.

Transferring Trust to the Digital Cinema System

The definition and management of trust relationships is of critical importance, especially when it refers to security systems. We have seen in the organisational models that actors need to trust other actors in fulfilling goals and using resources correctly (in other words, not abusing). However, when the assets (film content and audit trails) are in digital form, duplicating them is very easy and difficult to detect. Thus, there is a need for a security system to manage access to the digital assets.

When we introduce the security system in the organisational models defined in the previous section, we are transferring trust from actors to the system itself. It then becomes the responsibility of the security system to guarantee that the security constraints identified are fulfilled.

Making Stakeholders Trust DC Systems

However, the question still remains as to what makes a stakeholder trust a security device or system. How can a player be sure that a specific system, manufactured by some more or less well-known manufacturer, complies with some specification and, most importantly, has been designed and implemented with security in mind throughout the development life-cycle?

There is more than just one answer to this question. In most professional sectors, this trust relationship is established on the basis of reputation: for instance, a manufacturer of video editing software earns the reputation of developing trustworthy software if over the years it has had a track record of making bug-free reliable software. Another possibility is observation: one can observe, test and experiment with a system until trust

is built on the fact that the system behaves as expected and desired

However, when we are in the security domain, these approaches are not valid. The reason for this is that security cannot be measured or observed. The fact that a system provides the desired functionality does not imply that it has been designed, developed and tested for security. Security analysis, design and development is a highly specialised and difficult field. The smallest and most insignificant flaw may open the system to all kinds of attack.

In the security domain, for systems that protect high-value assets as is the case for digital cinema, most of the time, devices and systems must be certified by a neutral, specialised third party.

There are several certifications which a device or system can obtain. However, each certification aims at specific goals. For instance:

- **Trusted Computer System Evaluation Criteria** (see [TCS]), also known as the *Orange Book* of computer security, was a United States Department of Defence standard to assess the effectiveness of computer security controls built into a computer system. Originally published in 1983, it was later replaced by the Common Criteria international standard.
- **Common Criteria** is an international standard ISO/IEC 15408 (see [CCP] and [CCW]) to ensure that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.
- The **FIPS 140-2** standard (see [FIP] and [FIW]) specifies the security requirements to be met by a cryptographic module utilised within a security system protecting sensitive information. FIPS 140 does not purport to provide *sufficient* conditions to guarantee that a module

conforming to its requirements is secure, and still less that a system built using such modules is secure.

Another issue that remains to be solved is how this certification is managed within the system and the infrastructure behind the certification process that supports it. There is a wide range of possibilities. Traditionally, this certification happens outside the system itself. For instance, with FIPS 140-2, a test laboratory validates that a certain device model and version from a specific manufacturer complies with the security requirements, both physical and logical, required for each level. If the validation is successful, the test laboratory issues a paper certificate to the manufacturer. In this case, the entire certification process takes place outside the system, and the devices themselves are not aware of it.

Another approach, which is the one taken by SMPTE and DCI, mandates that devices, upon successful validation, should be issued a certificate per device assessing them. This certificate is then attached to the device itself, as part of the system, allowing other devices or players to authenticate the device and assess that it complies with a given security certification standard. If we follow this approach, there is still a question that remains to be answered as to the certification organisation and infrastructure required to support it. In order to illustrate this, we provide a description of two alternatives:

- The **device manufacturer issues certificates** for each device: after obtaining the specific model and version of a validated and certified device, the device manufacturer acts as certification authority for its devices. This flat certification authority solution has the advantage of being closer to the business itself: the device manufacturer is responsible for its own certificates. However, the management of root certificates becomes slightly more

complex, although this is relative given the reduced number of manufacturers of digital cinema devices.

- A **hierarchical certification infrastructure** manages the issuing and revocation of device certificates. The certification infrastructure is composed of a digital cinema specific root certification authority, and a number of levels of surrogate certification authorities. The exact topology and organisation of this infrastructure depends on many factors and falls outside the scope of this chapter. As its main advantage, this option makes the management of root certificates straightforward, since only one is required. However, the whole management of the certification infrastructure is more complex, with new players appearing in the picture, introducing significant changes in an industry that is slow to adopt them.

Between these two approaches, there are still a number of valid alternatives. One needs to make a detailed analysis of the requirements imposed on the infrastructure, as well as national or regional specificities, national regulations and laws, the degree of control of the certificate issuing process, or the acceptance by device manufacturers to assume the responsibility of issuing and managing certificates, just to name a few.

In the rest of this chapter, we simply assume that such a certification infrastructure is in place and that both stakeholders and the devices themselves can assess other devices which have the required certification.

Models with System-to-be Actor

This phase in Secure Tropos corresponds to the *late requirements analysis* phase. In this phase, the *system-to-be* actor (or actors) is introduced as another actor in the existing models. This results in a refinement of some of the dependencies and delegation of some goals or resources from

existing actors to the new *system-to-be* actor. In addition, this refinement of dependencies result in the identification of new dependencies necessary for the *system-to-be* actor in order to achieve the dependencies assigned by system's existing actors.

Producer & Post-Producer Systems

Producers and post-producers started the transition to digital content in the 70s, reaching a full digital production chain in the 90s. For many years, security was not a concern due to the high cost of digital media duplicating hardware, limited bandwidth and availability of internet connections and the non-existence of peer-to-peer illegal sharing networks.

This picture, however, changed dramatically in the late 90s, with wide availability of cheap digital media duplicating hardware and fast internet connections. Film leakages in production and post-production environments have been largely minimised or denied in public by the industry. On the inside, however, measures to fight leakages are being put in place [BYE]. These measures mainly address the physical security of the media in which content is stored, and not the content security itself.

In this section, we will examine cinema content security throughout the production and distribution chain. The big question is, when does raw content start having value as a film? Should film dailies be protected right after scanning? Is it only when the digital source master is created that the film has value? Or is it somewhere in between?

Illustration 20 depicts a refinement of the delegation model from Illustration 13 (on page 84) in production and post-production environments, including the different systems. We have assumed that content is handled by the security systems from the moment film dailies are scanned into digital form. Although we recognise the fact that this assumption may be exaggerated, in doing so we are simplifying the security

system by treating all content in an uniform manner, independently of its stage in the process.

Illustration 20: Delegation model for Producer *and* Post-Producer *relationship, with the newly added* system-to-be *actors. The picture shows how the fulfilment of the security constraints shifts from human actors to the different systems.*

This refined delegation model shows how all security constraints – and the responsibility to respect them – have shifted from human actors to both security *systems-to-be* and those manipulating or accessing content. With the appearance of the security *system-to-be*, there is a new actor associated with it: the *Security Manager*. This is the person or people whose sole responsibility is to maintain the lists of authorised users and systems within the production or post-production environments. Note the delegation of execution of the goal from the security system to the *Security Manager* role. In the likely case in which device certificates are used, the responsibility of the *Security Manager* role would also include checking whether some device has been revoked.

It is worth explaining how, for instance, the *Film Editor*, *Editing System*, and *Post-Producer Security System* interact in order to get the film edited, since it is a pattern that we will often encounter. Let us assume that *Bob* is a *Film Editor* in a post-production facility. In order to be granted access to content, *Bob* will first authenticate himself to the *Post-Producer Security System*. He will then request the security system to grant him access to certain content from an *Editing System*. The security system will validate that *Bob* has the role of *Film Editor* for some content, authenticate the *Editing System* and validate its security profile, and finally grant access specifically to *Bob* on the precise *Editing System.*

Producer & Distributor Systems

The film distribution business in Europe is very complex, especially when compared to the distribution of American blockbusters. In Europe, distribution happens at national level, for any type of cinematographic content. For big productions, studios and producers already have pre-established distribution channels.

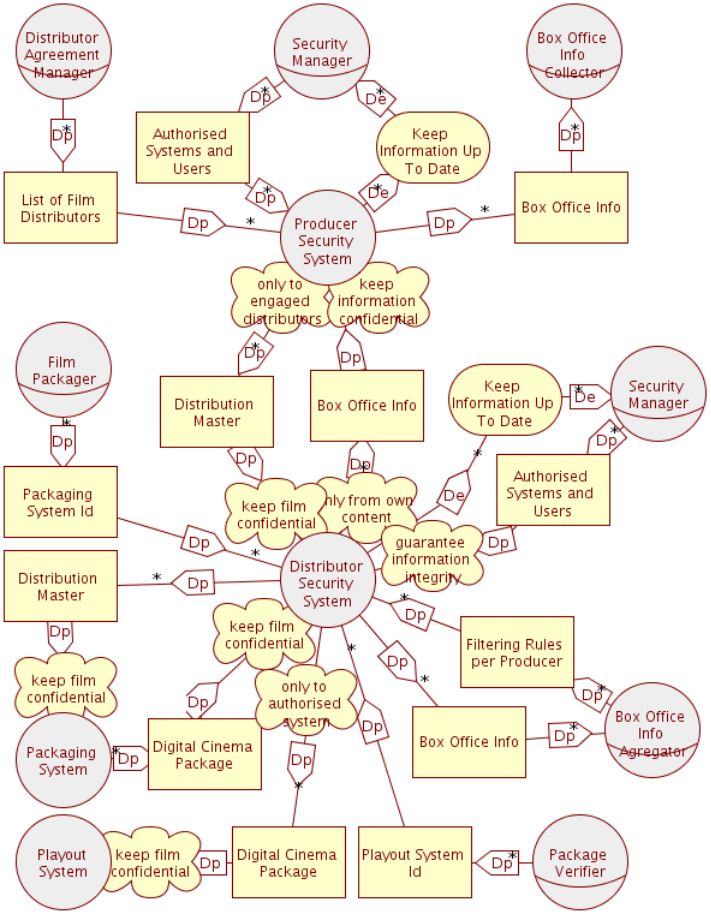


Illustration 21: Refined delegation model between Producer *and* Distributor*, with the newly added* security system-to-be*'s.*

The distribution of films within Europe typically goes through several distributors. Here we refer to the distribution of European content in Europe, although the same applies to independent and international films. Typically, a producer delegates all the rights over a film to a single distributor, who

distributes it nationwide. For intra-European (and international) distribution outside the distributor's area of operation, other distributors need to be found. Illustration 21 depicts the refined delegation model between *Producer* and *Distributor*, with their corresponding security systems. The next subsection deals with the *Distributor – Distributor* relationship and systems.

The illustration shows similar shifts of the security constraints from the human actors with a role in the organisation, to the *system-to-be* actor. Doing so greatly mitigates insider attacks: it is the responsibility of the *Security System* to protect digital content and audit trails, and to control access to them. Human actors in the system can only access content through some system in order to execute their goals. These systems also implement their only security constraint, i.e. to *keep film confidential,* contributing to the protection of content.

Note, for instance, the *Package Verifier* role, which verifies the result of the packaging process. This role supported by the security system is entitled to ask for the presentation of a film to some, previously certified and authorised payout system.

Distributor & Distributor Systems

In Europe as well as in other places, the distribution of films is rarely a one-step process from a distributor to the exhibitor. This also happens with Asian or South-American films, for instance, as well as with independent US productions.

The European digital cinema security system is capable of supporting this multi-stage content distribution. Although this may seem like a whole new set of requirements and security constraints, it is not. When examining the issue in closer detail, one realises that, from the downstream distributor's point of view, receiving content and providing audit trails does not change fundamentally if the distributor is dealing with a producer (as seen in the previous subsection) or another distributor. In the same way, from a distributor's point of view,

providing content to an exhibitor or to another distributor is fundamentally the same process.

Remember that the scope of the security system covers the management and control of access to digital assets (films and audits), while the contracts and agreements regarding these assets are managed outside the system. The level does indeed change significantly depending on whether we are talking about a producer-distributor or a distributor-distributor relationship. However, from a system level, the system functionality and security constraints are basically the same.

Distributor & Exhibitor Systems

The relationship between distributors and exhibitors is more prone to change with the transition to digital. And we are not referring to the fact that content will be distributed in digital form, but to the equilibrium which exists today in basically a relationship of distrust between them (see section “New Digital Distribution Models” in Chapter 3).

With the transition, this equilibrium can easily be broken to the advantage of distributors. With 35mm, once cinemas had the reels, they had some power of negotiation with distributors, whereas with digital content – and especially with authorisations – all negotiation power falls in the distributors' hands.

Illustration 22: Refined delegation model between Distributor *and* Exhibitor*, incorporating the newly added* system-to-be*'s.*

From a security point of view, this is extremely important. Imagine the case of an exhibitor, for whom it is the tenth time a distributor refuses to extend the length of a film rental agreement for whatever reason. This situation motivates the exhibitor to tamper with the system so he can achieve his goal and maximise the number of attendees to the shows.

Illustration 22 above shows the refinement in the delegation model – including the *systems-to-be* – of the relationship between distributor and exhibitor.

According to the model in Illustration 22, in order for a show to take place, the *Cinema Manager* first enters the schedule (for a screen or for the whole cinema) to the *Theatre Management System*. For each show, the *TMS* validates whether all elements of the show are available and have the necessary authorisations. If everything is alright, the *TMS* will control the playout system performing the presentation, while delegating the *Screen Operator* with the task of starting and monitoring the show.

It is worth noting the different sources of logging information. At the *SMS/TMS* level, the log information generated deals with a show, i.e. the different parts which comprise the show and whether all authorisations are alright, or any failed. The *Playout System*, in turn, generates log information for each piece of content it plays.

One could argue that these two levels of logging information are unnecessary, and that logging each usage of content is enough. However, in the same auditorium one can have different playout systems (one for publicity, and the other for trailers and films, for instance); furthermore, in the same show some elements may be protected, while others not. Having a schedule or show level logging makes log consolidation and correlation easier.

Conclusions

In this chapter we have created a trust model of the digital cinema content production, distribution and exhibition "organisational setting". We have argued that most security problems in computer systems and applications today arise from the fact that security considerations are introduced in the system development process at a late stage. By integrating

security at the same moment as functional requirements analysis, we guarantee that security concerns are considered throughout the whole system development process.

After modelling the "organisation", its actors, resources and trust and delegation relationships, we introduced a new actor in the model: the *system-to-be*. By introducing this new actor we have shifted both functional requirements and security constraints from the actor (i.e. human) level to the system level. Later in the system development process, all these security constraints will also be directly incorporated in the system architecture and design.

However, our model is focused only on production, distribution and exhibition of content, and leaves out other aspects that are also important in the security of digital cinema systems and content. Furthermore, we have intentionally remained at an abstract level; however, in some cases it is worth being more precise to have a clearer view. We will be addressing these cases here.

Watermarking and Fingerprinting

"Digital watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages to digital audio, video, or image signals and documents. Such a message is a group of bits describing information pertaining to the signal or to the author of the signal (name, place, etc.)" [DWW].

Watermarking is applied to content by the owner of the content itself in order to identify and authenticate content once it has been distributed.

Fingerprinting uses the same techniques as watermarking. However, fingerprinting is applied to content when it is presented. Typically it inserts information such as time and location in the video stream, and identifies the device that

decoded the content. Fingerprinting is used for forensic reasons to identify the origin of content theft.

Although both of these techniques will likely be used for forensic investigations and thus contribute to the overall security of digital cinema, they are not part of the trust model developed in this chapter. We address both of these technologies later in this book, in Chapter 7.

Anti-Camcording

Camcording a feature film is often presented as the most significant source of piracy, generating the most losses for the industry [POC]. There have been initiatives in the past which are still ongoing today, to create a technology that would degrade the quality of the recorded film or even totally prevent it, while cinema-goers could continue to experience the film at best quality.

Here again, although this technology [JAM] would, when available, help to fight film piracy, it has not been included in the digital cinema models developed in this chapter. The technology is not part of the film production, distribution and presentation processes.

It is worth noting, however, that both the statistics on camcording activities in cinemas (see [MMO] and [MMU]) and the real impact they have on box office revenues [BOS] are highly questionable [YIJ]. First of all, the cinematic industry is bringing in record revenue, despite the increasing availability of films online. Secondly, there is little demand for camcorded films on peer-to-peer sharing networks, with illegal downloaders preferring DVD rips than through-the-air camcordings. And thirdly, camcorded films represent only a small percentage of film piracy [BYE].

In Chapter 7 we provide an introduction and overview of the different technological approaches to camcorder-jamming technologies. On the legal side, there have been and continue

to be laws passed, making in-cinema camcording a felony in the US [CRD], Europe [MMO] and worldwide.

Screeners and Other Distributions

According to [BYE], an important source of piracy and content theft comes from industry insiders having access to finalised film material. We are not referring to content during the production and post-production stages. Once the digital source master is finished, it is common practice to send out copies of the film (mostly on DVD) to executives, critics, screeners or marketing.

Again, since these distributions of content happen outside the digital cinema distribution to cinemas, which is the scope of this chapter, they do not appear in the trust models.

However, it is of critical importance for these distributions to be tightly controlled and secured. It only takes one untrustworthy industry insider with a copy of a film to make it available on illegal peer-to-peer sharing networks. One copy and that is all. Although it would probably have little impact on revenue generated by cinemas and on audience attendance, it would undoubtedly hurt the revenue generated by film rental and purchases.

On the positive side, Hollywood studios are already implementing measures (such as screener DVD fingerprinting, physical access controls, etc.) to mitigate these threats. On the negative side, there is still a long way to go until every single copy is controlled.

Other Logs and Audit Trails

Audit trails and logging information requirements ([DCI]) are centred on the presentation of digital cinema films only. Logging information is generated by the different devices

collaborating in the presentation, for different classes of events. These logs are stored locally in each device until retrieved by some authorised personnel. The goal of these audit trails is for distributors and studios to have a secure record of the use a cinema has made of a film, and whether there have been security incidents before or during presentation.

However, on analysis of the different trust and delegation models presented in this chapter, it is clear that there are also other logs that can be generated. These logs, by themselves or correlated with other logs, would be very helpful in monitoring and controlling the distribution of content and in identifying potential threats or issues at an early stage. For example:

- Distributor management of exhibitors: adding, updating or removing an exhibitor from a distributor's database. These logs would reflect the exhibitors receiving content.
- Generation of entitlements for exhibitors: log the creation of individual entitlements per exhibitor for a given distributor.

Analysing and correlating both logs can help identify a potential rogue (fake) exhibitor, perhaps added by an insider only to be able to generate entitlements that may be decrypted later.

On the other hand, correlating the generation of entitlements with the reception of audit trails from exhibitors would help automate the process of detecting issues with individual exhibitors. If an exhibitor has received an entitlement for film X, but does not report any audit trails for that film, this would mean that something is wrong.

Cryptography, Security and Lack of Transport

In this chapter, we have not used terms such as “AES”, “Public Key Cryptography”, “Encryption” or “Key Management”. This may seem odd when addressing system security, but it is not. As we have already stated, the modelling activities in this chapter are aimed at explaining the need for security measures and policies, but not how to implement them.

If we were to model the 35mm distribution of reels, we would end up with very similar diagrams. For instance, instead of having a *Security System* at the producer and another at the distributor, we could have a *Trusted Transporter*, who would *keep content confidential* and distribute it *only to authorised distributors*.

Along the same lines, a digital source master can be delivered from post-production to production via physical media such as hard disks. The content is digital, but its transport takes place via physical media. Again, the trust and delegation models need little tuning to reflect this behaviour.

Practically speaking, however, content will be encrypted. By encrypting large amounts of data, what we are achieving is the simplification of a problem. Instead of making huge efforts to protect massive amounts of information (digital content), we simplify the problem so that we “only” need to protect a few bytes of information: a cryptographic key.

Systems designed following the models created here will in fact send entitlements (a message containing content keys in such a way that only the intended receiver will be able to access them) instead of digital cinema packages, for instance. Films are supposed to be safe during transport because they are encrypted. The problem of safely transporting a film

between two players is replaced by the problem of safely conveying the content keys to the intended receiver.

Architecture and Design

After a functional and security requirements analysis, the next step in a system development process is the definition of a system architecture and design. However, these phases are not straightforward.

From an architectural point of view, it is difficult to define security and functional components together, and at the same time provide a clear distinction between, for instance, components which are part of the security architecture and those which are part of the functional specification.

From a design point of view, it is difficult to move from a set of security requirements to a design that satisfies these requirements, and to understand the consequences of adopting specific design solutions for such requirements.

Furthermore, it is difficult to obtain empirical evidence of security issues during the design stages. This makes the process of analysing security during the design stage more difficult.

[MOU] is an approach based on Secure Tropos aimed at solving these difficulties by proposing a process for selecting among alternative architectural styles; a pattern-based approach to transform the analysis to design, and a security attack scenarios approach to test the developed solution.

However, this is also an approach. Other approaches exist as well, ranging from RUP-based (Rational Unified Process) to Agile Software Development methodologies.

Chapter 5
Digital Cinema Standards and Specifications

The goal of standards and industry-backed specifications, as is the case for the Society of Motion Pictures Experts (SMPTE, see [SMP]) and the Digital Cinema Initiatives consortium (DCI, see [DCC]), is to promote interoperability between vendors across the system. With standards in place, devices from different manufacturers can cooperate and interact; in theory, a device from a given manufacturer can be replaced by another from a different manufacturer. This effectively opens the market for device and service providers.

In digital cinema, standards and interoperability are considered a critical factor for worldwide rollout of digital cinema systems. The publication of *DCI Digital Cinema System Specification version 1.0* [DCO] in July 2005 marked a milestone in digital cinema. Equipment and device manufacturers now had a set of specifications and standards to comply with.

In this section, we present in some detail the DCI specifications and derived SMPTE standards and work in progress related to security aspects of digital cinema. From these specifications we derive a trust and delegation model like those in the previous chapter, and analyse the system defined, identifying potential issues.

DCI & SMPTE Functional Model

DCI Specifications and SMPTE standards cover to some extend the processes of creating a Digital Cinema Package, which contains a feature (film, trailer or publicity), and the process of playout in cinemas.

The cinema producer provides digital cinema content (image, audio, and subtitles) in uncompressed form to a distributor as a Digital Cinema Distribution Master (DCDM). This master is then transformed into a Digital Cinema Package (DCP) to distribute to Exhibitors.

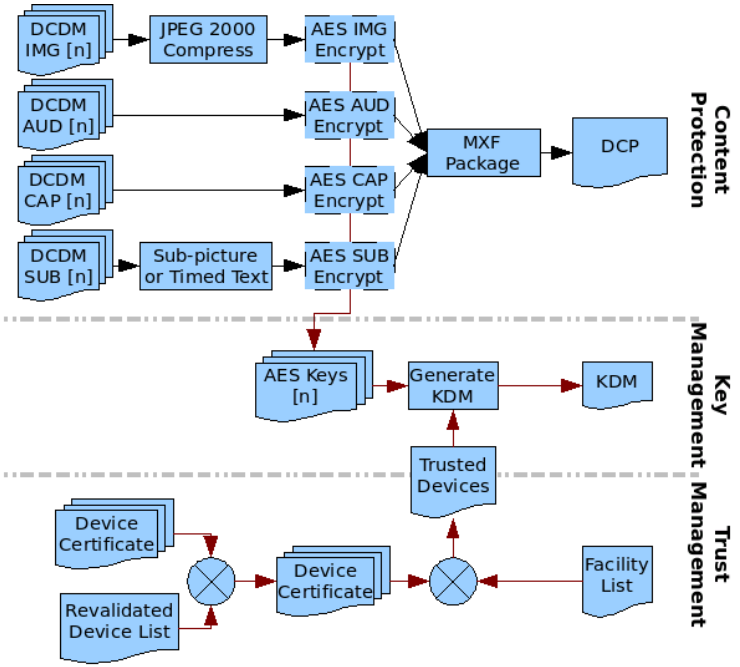


Illustration 23: Functional diagram of the processes for creating a DCP from a Distribution Master, and the process for creating a Key Delivery Message for a specific auditorium. Black arrows indicate content path, red indicate security parameters path.

In the process of creating a Digital Cinema Package (see Illustration 23), image content is compressed using JPEG-2000 [JPW]. Digital content (compressed image, audio

and subtitles[20]) is protected persistently for *confidentiality*, *integrity* and *authenticity*. Content is encrypted [CRY] with one or more symmetric[21] cryptographic keys [SKA] using the Advanced Encryption Standard [AES]. The same key is used to guarantee the *integrity* and *authenticity* of the content using keyed-hash message authentication codes[22]. These properties allow the content to be safely distributed via any transmission channel, whether or not it is secure. These include physical media such as hard disks or DVDs, satellite, computer networks or any combination thereof.

In a separate channel, the content encryption keys for a given film are transmitted to each auditorium authorised to play it in a Key Delivery Message, or KDM. The KDM protects the content encryption keys for *confidentiality*, *integrity* and *authenticity*. The keys are encrypted using a public key[23] (or asymmetric) cryptographic algorithm [PKC], in such a way that only authorised devices will be able to access them with their private key. *Integrity* and *authenticity* are also provided in the message by means of digital signatures [DSI]. The KDM also carries a list of devices that are authorised to access content, the Trusted Device List, matching those in the provided facility list.

The auditorium private keys are assigned to and stored inside the Security Manager, which physically protects it. According to DCI specifications, the Security Manager resides in the Media Block, where content decryption and forensic marking for audio and image take place. This arrangement prevents an

[20] DCI only encrypts image and audio content, while SMPTE supports selective encryption of image, audio and/or subtitles.

[21] In symmetric cryptographic algorithms, the same key is used for encryption and decryption.

[22] Known as HMAC for keyed-Hash Message Authentication Code.

[23] In asymmetric cryptographic algorithms, different keys are used for encryption (public key) and decryption (private key).

attacker from having access to clear text and non-watermarked content.

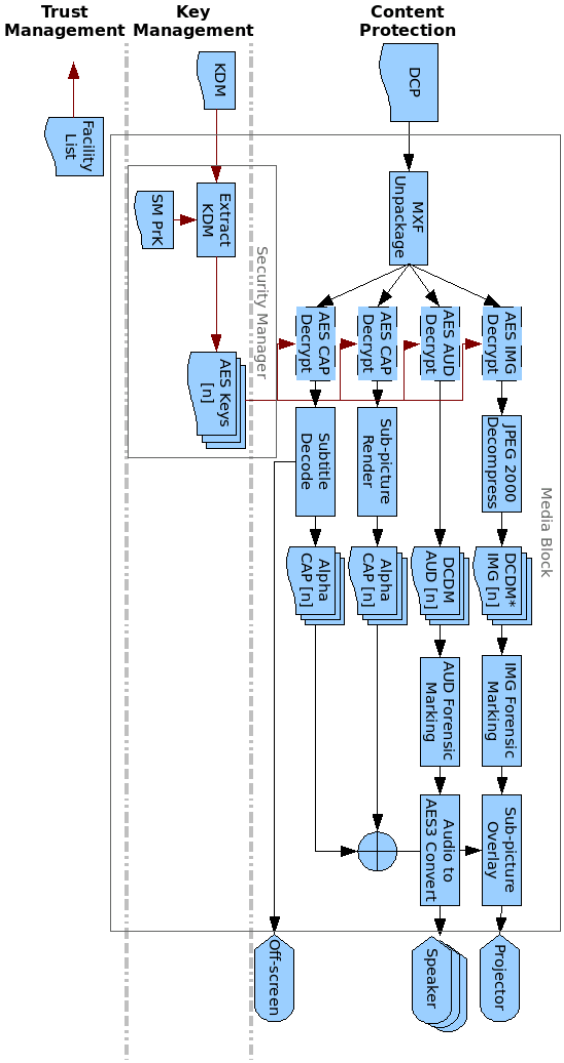


Illustration 24: Functional diagram of the DCP playout process. Arrows in black indicate the content path, while arrows in red indicate the path of security parameters.

At playout (see Illustration 24), content is unpackaged, decrypted (if necessary), watermarked (only DCI mandates it) and send to the projector for playout.

However, in order to play some content, some rules and restrictions must be satisfied. First, only the authorised auditorium will be able to play the film. Also, this must happen within a time window, and only through authorised devices. And last, all devices participating in the presentation must have logging enabled and functioning. All this is verified by the Security Manager prior to authorising the presentation.

The cinema manager is expected to present content honouring the negotiated film rental agreements. The philosophy behind both DCI and SMPTE is "*control loosely, audit tightly*". Thus, instead of enforcing the film rental agreements via some complex DRM system, DCI specifications rely on a secure logging mechanism, so all use of content is reported back to the content owner.

DCI Security Specifications and SMPTE Standards

This whole security process relies on different standards and specifications. Illustration 25 presents the different SMPTE security standards issued by the Digital Cinema working group, and their dependencies[24]. In the illustration, a title starting with *SMPTE* means it is a standard, while those starting with *RP* means they are recommended practice, and *EG* stands for engineering guidelines. Table 1 provides a short description of each of these SMPTE standards and recommended practices.

[24] By "*dependency*" we mean that a document references another. Note that only SMPTE and DCI are considered here.

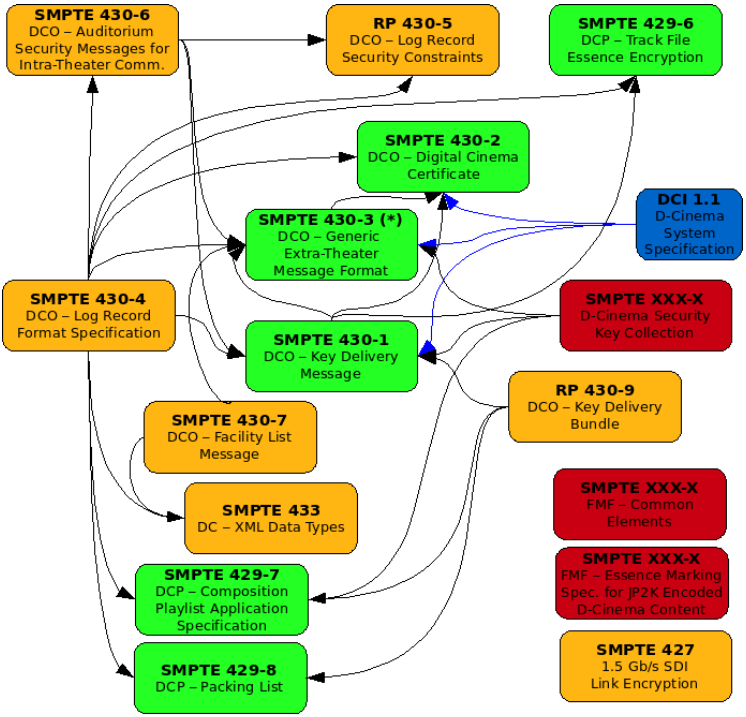


Illustration 25: Dependency diagram of the different SMPTE security standards. The diagram also shows the dependencies between DCI Security Specifications and SMPTE standards (in blue).

It is important to bear in mind that SMPTE focuses on standards to achieve device and system interoperability, without going into the system or device implementing these standards. It leaves manufacturers the freedom to design and implement their systems and devices.

Num.	Type	Group	Description
427*	STD	SDI	Defines a method for providing secure transmission of digital pictures over a transport conforming to SMPTE 292M. The document also defines the metadata for en/decryption synchronisation and message for key management.
429-6	STD	DCP	Specification of the syntax of encrypted D-Cinema non-interleaved MXF frame-wrapped track files and of the reference decryption model. It uses AES encryption algorithm and, optionally, the HMAC-SHA1 integrity check. [429-6]
429-7	STD	DCP	Specifies the structure of a Composition Playlist, which is a self-contained representation of a single complete d-cinema work. They consist of an ordered sequence of reel structures, each referencing a set of track files. [429-7]
429-8	STD	DCP	Specifies the structure of a Packing List, which specifies the contents of a distribution package containing one packing list together with a Composition Playlist and associated assets. [429-8]
430-1	STD	DCO	Specifies a Key Delivery Message structure, which delivers security parameters and usage rights between d-cinema content processing centres. These security parameters are the content keys, validity window, and a list of trusted devices. [430-1]

* Not a published SMPTE standard. Provided only for informational purposes.

Num.	Type	Group	Description
430-2	STD	DCO	Specifies Digital Certificates for use in d-cinema systems. The standard defines both the certificate format and the processing rules associated. [430-2]
430-3	STD	DCO	Specifies a generic Extra-Theater Message format for use with unidirectional communications channels. The ETM specification is a generic XML security wrapper. [430-3]
430-4*	STD	DCO	Specifies the XML structures and schema for individual log records and sequences of records. The specification provides optional authentication of log records and sequences of records.
430-5*	RP	DCO	Specifies classes and types of log events and the associated log records. Defines both system elements and XML structures. These log records are generated by security devices.
430-6*	STD	DCO	Specifies a set of messages, in KLV[25] formatting, for intra-theatre security messaging. It covers time, log and device status querying and link encryption keying.
430-7*	STD	DCO	Specifies the Facility List Message extra-theatre message. The FLM delivers facility information, device certificates and optionally descriptions of a site to KDM distributors and/or content owners.

* Not a published SMPTE standard. Provided only for informational purposes.

[25] Key-Length-Value encoding. See [KLV].

Num.	Type	Group	Description
430-9	RP	DCO	Specifies the Key Delivery Message Bundle extra-theatre message. A KDMb delivers a collection of KDMs and a mapping file for a specific recipient. A recipient may be an exhibitor or circuit, a distributor, or other actor.
433*	STD	DC	Defines the d-cinema specific XML namespaces and data types used by the different d-cinema standards.

Table 1: Overview and short description of the SMPTE's Digital Cinema Security Standards, Recommended Practices and Engineering Guidelines. Note that the table contains both published documents and on-ballot process standards.

DCI, on the other hand, defines the system architecture and provides a long list of requirements for different aspects of systems and devices, while referencing SMPTE standards. In Illustration 25, DCI dependencies with published SMPTE standards are shown as blue arrows.

In the following sections we present these different SMPTE standards and DCI specifications in more detail.

DCI Exhibitor Security Architectures

Neither DCI nor SMPTE define any architecture elements at production, post-production, distribution or mastering level. It is assumed that these are trusted environments, and systems will be secure without the need to specify them. Note however, that this assumption cannot be taken for granted, since most piracy originates precisely from these environments [BYE].

At exhibition level, however, DCI extensively defines the architecture of the different components within a cinema. The

architecture covers both the cinema and auditoriums, as well as the security components. The approach taken by DCI is first to define the architecture of a single auditorium and then to extend it to multi-screen venues. Although this approach may be valid, it carries some issues with it that we will see later in this chapter.

At SMPTE level, nothing is defined regarding exhibitor architectures. However, in order to define standards, the DCI-defined architecture was adopted.

Single Auditorium

At auditorium level, DCI defines four main components from a security point of view (see Illustration 26):

- **Screen Management System**: is the human interface to a single-screen digital cinema system. The SMS provides a user interface to control a single auditorium. From the SMS, cinema staff can manage a show. DCI mandates that users must be authenticated by the SMS. However, DCI does not specify how this process takes place, or the security requirements for the SMS.
- **Storage Server**: stores at least all the content for a given presentation (including trailers and publicity). DCI mandates that the storage capacity per screen must be 1 TByte. Note that a 3-hour feature with 20 minutes of pre-show content takes up to 377 GBytes. The ingest interface is also required to be Gigabit Ethernet [GBE].
- **Digital Cinema Player**: the device containing the media block. The media block (see next section) is the security device responsible for content unpackaging, content decryption, image decompression and audio and video forensic watermarking.
- **Digital Cinema Projector**: transforms the uncompressed digital image into the light on screen. The projector is required to support the different cinema architectures. If

the projector and media block are in physically separate devices, the projector is required to have a projector media block (see next section).

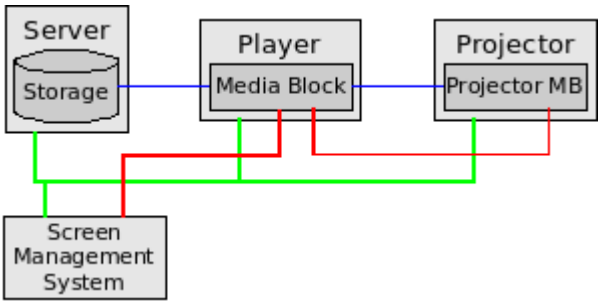


Illustration 26: Security architecture of a Digital Cinema auditorium. The image depicts the 4 basic components within the auditorium: Screen Management System, Storage Server, Player with integrated Media Block, and Projector, with associated Projector Media Block. Blue represents content path, green represent management communications and red security ones.

These auditorium components are defined at a functional level, which does not necessarily match the physical implementation. For instance, the Screen Management System may be integrated into the Player, or the Media Block may be integrated into the Projector itself. One can even have a fully integrated Projector with local storage, a Screen Management System and a Media Block.

Multi-Screen Venue

Going from a single digital screen to multiple digital screens implies, at the very least, a multiplication of the same architecture for each screen. However, since the management of such a system would be cumbersome, content is moved between screens and the whole exhibitor is managed from a central location.

In order to overcome these limitations, DCI proposes new elements for a multiplex:

- **Theatre Management System**: provides a human interface allowing the management of all auditoriums in the venue. In order to achieve this, the TMS talks to the different SMS in the exhibitor.
- **Theatre Management Network**: a dedicated network for control and management. The network is required to support control, configuration, security, software updates, testing and status of the cinema systems. The network shall be 100Base-T Ethernet [ETH].
- **Central Storage**: contains all content available at a venue. Central storage may be combined with local storage. If only central storage is used, it is required provide the capacity to sustain the peak bit rate of all screens being fed simultaneously, along with ingest.
- **Media Network**: is a high bandwidth, switched interface that connects disc arrays with media blocks. It is required to support a sustained bitrate of 307 Mbps for each Media Block connected.

Media Block

The auditorium Media Block is a key component of both the security architecture and playback chain and is specified by DCI. The Media Block is responsible for:

- **Unpackaging**: the DCP is delivered to the Media Block upon playout. The Media Block unpackages the content into image, audio, timed text and caption streams.
- **Decryption**: content decryption is performed by a Media Decryptor inside the Media Block.
- **Decoding**: images transformed from JPEG2000 compressed form to uncompressed format.

- **Forensic watermarking**: DCI requires that both images and audio be watermarked upon playout. We address this issue later in this chapter.
- **Alpha channel overlay**: a module that overlays subpicture or timed text into the main image.
- **Content synchronisation**: the Media Block synchronises all content for playout.
- **Link encryption**: if the Media Block resides outside the Projector, the link between the two needs to be secure. In this case, a Link Encryption Block is present inside the Media Block. On the projector side, a Link Decryption Block is present inside the Projector Media Block.
- **Security functions**: the component responsible for the management of all security aspects inside an auditorium is the Security Manager, which also resides in the Media Block. These functions include device authentication, KDM verification, time validity check and content integrity, among others.

The Media Block needs to interface with other components within the auditorium cinema system. These interactions happen a 3 different levels:

- **Packaged content**: packaged content requires a data interface that can handle bitrates up to 307 Gbps. DCI specifies this interface to be Gigabit Ethernet.
- **Uncompressed essence**: uncompressed essence requires extremely high real-time bandwidths depending on its type. Uncompressed image requires up to 10 Gbps of bandwidth. If the Media Block resides inside the projector, this will be an internal interface. Otherwise, link encryption shall be used. For audio output to the cinema audio processor, the interface shall be AES3 [AE3].
- **Security messaging**: the Media Block needs to exchange security messages with the Screen Management System

and, if present, the Projector Media Block. This interface is standard Ethernet with Transport Layer Security [TLS] on top of TCP/IP [TCP]. We address security messaging later in this chapter.

Media Block Architecture and Configurations

With Media Block being a key component in the security architecture, DCI goes into a great detail defining its requirements and architecture, as well as those of the Security Manager. This section refers to DCI specifications. SMPTE, as already noted, does not define any standard for Media Blocks or its architecture.

Any component or element that participates in any security function is called a Security Entity. A Security Entity is a logical device that performs a specific security function. All Security Entities have an associated certificate that defines its role. DCI defines the following security entities:

- **Screen Management System**: is considered a Security Entity although it does not handle any security data. It is trusted to control the auditorium Security Manager and to authenticate the user operating it.
- **Security Manager**: is responsible for the management of content encryption keys and the collection of logging information.
- **Media Decryptor**: transforms encrypted image or audio content into its original plaintext form.
- **Link Encryptor**: encrypts content between Media Block and Projector Media Block physical link.
- **Link Decryptor**: decrypts content encrypted by a Link Encryptor.
- **Forensic Marker**: inserts information regarding the date and time of a playout and identification of the Media

Block in both image and audio essence, in realtime during playback.

- **Secure Processing Block**: a Security Entity whose function is to provide physical protection to other Security Entities contained within. The Media Block and the Projector Media Block are such entities.

Illustration 27 depicts the two possible configurations of auditorium Media Blocks. The first configuration corresponds to that of a Media Block and Projector which are physically separated. The second possible configuration is that of the Media Block integrated into the Projector. Note that the only difference is the presence of Link Encryption and Decryption entities.

All Security Entities except the SMS (which, according to DCI, is a non-secure Security Entity) must be contained within a Secure Processing Block. DCI defines two types of Secure Processing Blocks providing different levels of physical security:

- **SPB Type 1**: provides the highest level of physical protection. A Type 1 SPB is required to be tamper evident, tamper resistant and tamper responsive (in the case of tampering, all cryptographic keys shall be zeroed). We cover Type 1 SPBs later in this chapter when addressing FIPS 140-2 requirements and certification.
- **SPB Type 2**: provides a secure physical perimeter. A Type 2 SPB is required to be tamper evident and to signal "door open" events.

In Illustration 27, a thick solid black line represents a Type 1 SPB, while a thick dashed line represents a Type 2 SPB. As can be observed, the Media Block and Link Decryptor are Type 1, while the Projector Media Block is Type 2 SPB.

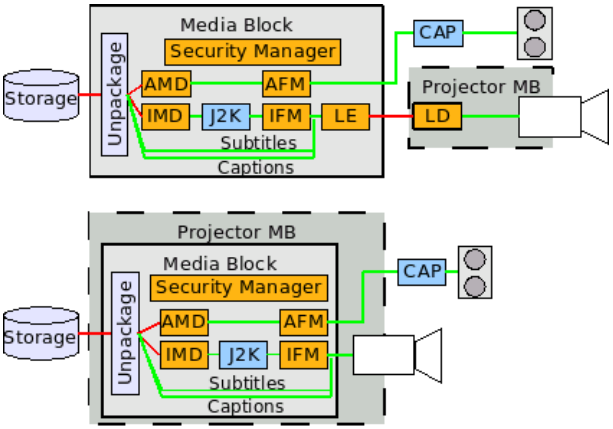


Illustration 27: Different configurations of Media Blocks and projectors. The diagram at the top depicts a Media Block separated from the projector, with a Link Encryptor and Link Decryptor blocks. The diagram at the bottom depicts a Media Block integrated into a Projector Media Block, attached to the projector. Red lines indicate encrypted content path while green lines indicate plaintext content paths.

Trust Management and Certification

Trust is a relationship of reliance defined between two entities regarding certain behaviour: "*A trusts B regarding X*". The relying party *A* believes that *B* will behave in certain predictable ways under certain circumstances (*X*).

To make a trust decision or define a trust relationship, the relying party requires some information or knowledge regarding the trusted party. This information may be found in the real world or obtained in the digital world, in the form of attributes, rights or capabilities.

A trust relationship may be explicit or implicit. An explicit trust relationship is one that explicitly transfers some authorisation from the relying party to the trusted party. In an implicit trust relationship, there is no actual transfer of

authorisation; rather, within the scope of an application or system, the relying party trusts the trusted party will behave as specified.

In the context of trust management, peer authentication is a requirement. Precisely, in order to define a trust relationship, the relying party must first authenticate the trusted party. Only then can trust be built. This is typically achieved through public key cryptography and certification.

Principals[26] must be able to obtain a key pair securely. There must be a way to look up other principals' keys and to publicise one's own public key. If a principal's private key is compromised, other principals must be made aware of this, so they will no longer trust that principal.

All this is typically achieved through certificates and public key infrastructures. A *public key certificate* (or *identity certificate*) is an electronic document incorporating a signature that binds together a public key and an identity. A *public key infrastructure* (PKI) is a set of protocols, services and standards supporting applications of public key cryptography. Typically, a PKI provides the following services:

- Key registration: issuing a new certificate for a public key.
- Key selection: looking up and obtaining another party's public key.
- Certificate revocation: cancelling a previously issued certificate.
- Trust evaluation: determining whether a certificate is valid and what operations it authorises.

In the scope of cigital cinema, DCI specifications and SMPTE standards cover, to some extent, certification and public key infrastructure.

[26] A principal is any entity (device, user, system, etc.) capable of "speaking", that is, issue signed statements.

SMPTE 430-2 “Digital Cinema Operations – Digital Cinema Certificate” defines the certificate structure, constrains its format for application of digital cinema, and defines the rules for validating a certificate.

DCI specifications, on the other hand, rely on SMPTE 430-2 and define many behaviour requirements covering, among others, management of trust and trusted devices, and revocation of trust. Note that these are requirements, and not normative behaviour.

Digital Cinema Certificates

Digital cinema certificates are associated with devices and are used to support the *confidentiality*, *integrity* and *authenticity* of communications, both extra-theatre and intra-theatre.

The certificate of a security device is a signed statement by the device manufacturer identifying the device's public key, providing attributes such as make, model and serial number, and the digital cinema roles it is capable of fulfilling.

According to SMPTE, the device manufacturer is the responsible for issuing and managing device certificates. The hierarchy of certification authorities controlled by a given manufacturer may have one or more level. That is, the root certification authority may issue certificates for all devices manufactured. However, for scalability and security reasons, the SMPTE standard 430-2 also supports a hierarchy of certification authorities controlled by the device manufacturer, as shown in Illustration 28.

The CA certificates (root and intermediate) are standard X.509 certificates for certification authorities (see [X.509] and [PKIX]). The root certificate is a self-signed certificate, in which the root CA signs its own public key. The root CA also issues certificates for other certification authorities, building a hierarchy of CAs. In these certificates, the root CA signs the public key of each surrogate CA.

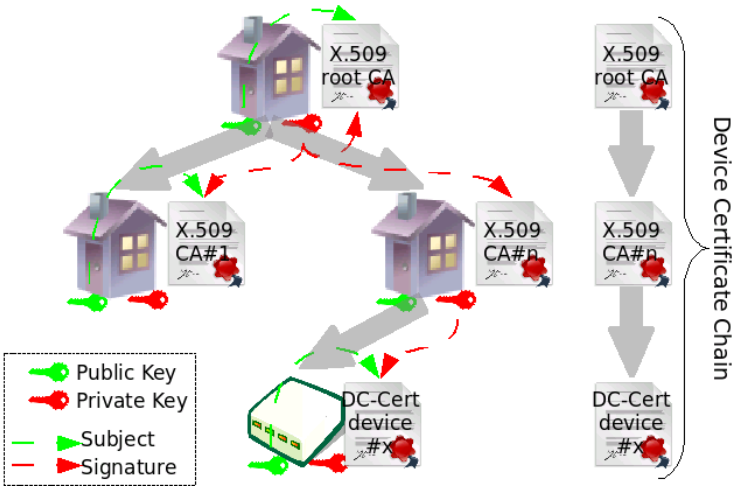


Illustration 28: Example of device manufacturer's certification infrastructure, with a root CA, one level of surrogate CA's and device certificates. The image also depicts the associated certificate chain of a device.

Device certificates, as standardised by SMPTE 430-2, are a constrained and overloaded version of X.509 certificates tailored for use in digital cinema applications. The constraints in certificate fields specify X.509 version 3 certificates, and the algorithms used for certificate signatures (SHA-256 with RSA encryption).

In order to support digital cinema device naming and device roles, DCI originally opted to do so by redefining and overloading the standard X.509 attributes, instead of through X.509 extensions. SMPTE later standardised the approach taken by DCI. These changes are summarised in Table 2.

DC Atr.	X.509 Atr.	Comments
Public Key Thumbprint	dnQualifier	Thumbprint of the public key of the issuer or subject of the certificate. *dnQualifier* is an attribute of the X.509 *Name* attribute.
n/a	Country Name	This attribute shall not be present in digital cinema certificates.
Root Name	Organization Name	Name of the organisation holding the root of the certificate chain. *OrganisationName* is an attribute of the X.509 *Name* attribute.
Organization Name	Organization Unit Name	Name of the organisation that issues or was issued the certificate. It is provided for human readability and is not processed upon validation. *OrganisationUnitName* is also an attribute of the X.509 *Name* attribute.
Entity Name and Roles	Common Name	List of roles the device implements, and a human readable name allowing the identification of the device. *CommonName* is also an attribute of the X.509 *Name* attribute.

Table 2: List of overloaded X.509 attributes for digital cinema certificates. The table also provides a short description of the new attribute semantics.

Digital cinema certificates are used for authenticating the origin of digital signatures. Digital signatures are used to ensure integrity and authenticity of data structures (such as CPLs, KDMs or Packing Lists) or communications (TLS-protected communication channels).

In order to validate a digital cinema certificate, one first needs to validate the certificate chain from the root certificate down to the device certificate. This validation is standard to X.509 certificates.

However, to validate the device certificate itself, a new set of validation rules is required, since the certificates are not standard X.509.

Trust Management

Trust management refers to the processes of key generation and registration, lookup of keys, evaluation of key and associated attributes, and the revocation of keys and/or key certificates. In the scope of digital cinema, these processes apply to device public key pairs and associated certificates.

Neither DCI Specifications nor SMPTE standards cover the processes of trust management extensively. DCI delegates all trust management to the Trusted Device List inside a Key Delivery Message. This list conveys the Digital Cinema certificates of those devices trusted by the entity generating the KDM. Only those devices in the TDL are authorised to use the content encryption keys.

SMPTE goes a little further and is in the process of standardising a Facility List Message. This message is an instance of an ETM and is used to list all the security equipment present at a facility.

The result of this approach is that trust management is effectively delegated to system implementers, without any standard or guidelines to comply to. We describe hereafter each of the processes in trust management and how they shall be applied to Digital Cinema.

Key generation is a key process in cryptography and security. Cryptography relies on the fact that keys (secret or private keys) are difficult to guess. Random numbers are used to create unguessable keys. Because of this, *random number generators* (RNG) are targeted by attackers. Precisely, knowledge of little state information of a random number generator may drastically reduce a brute force attack on a key (see [ARN] and [WRN]).

In public key cryptosystems, it is recommended that the owner of the key pair should also be the generator of such pair. In doing so, there is only one copy of a private key, and thus the compromise of the key is much more unlikely. Removing key

copies (for reference or backup) reduces the places where keys can be attacked ([RKM] provides best practices in key management, which also apply to trust management).

Another recommendation is to limit the usage of a key pair to either encryption or signature, not both. This reduces options to cryptanalyse the key pair. Note that this recommendation is not followed by DCI/SMPTE, since key pairs are used both to encrypt and sign.

Once the key pair is generated, the next step is **key registration**. Key registration results in the binding of keying material to attributes and other information associated with a particular entity or device. In digital cinema applications, this binding takes the form of a digital cinema certificate, issued by a manufacturer's CA, that identifies the device and lists its capabilities (role names, as seen in the previous section).

It should be stressed that this process is security-critical. Before issuing a certificate, the CA must verify, among others, that the entity (or device) requesting a certificate effectively possesses the private key; that this entity or device is genuine, and not a pirate clone; and that the certified capabilities of the device match the real ones.

Once a device has its key pair registered (and a certificate is issued), it is ready for installation and operation. However, in order for an application to address the device, it requires knowledge of the device's public key and certificate. This process is referred to as **key lookup**, and in digital cinema is a somewhat complex process.

The entity creating KDMs needs to know which devices are present at a given facility. This means that the cinema manager needs to communicate a list of devices. This is done by means of a Facility List Message[27]. A Facility List Message contains information on the facility itself (name, address,

[27] Standard in ballot process at the SMPTE: “SMPTE 430-7: Digital Cinema Operations – Facility List Message”

contact information, time zone, etc.) and a list of devices and their associated certificates.

When the entity creating KDMs receives this list, it needs to obtain a revalidation of each device certificate to avoid revoked keys or certificates, as the first step in **trust evaluation**.

The revalidation can come in two different flavours: Certificate Revocation Lists [CRL], and Online Certificate Status Protocol [OCSP]. A CRL is a signed list of certificate serial numbers that have been revoked. The OCSP protocol on the other hand, is a request/response protocol that provides status on individual certificates.

In order to obtain a revalidation, however, one needs to contact the CA that issued a given certificate. This may turn out to be a difficult task since the services supported by CAs may differ due to their nature (CRL vs. OCSP) and the implementation specificities hindering interoperability.

As an alternative, some people in the digital cinema community advocate for publicly available certificate databases. These would be publicly accessible services that are responsible for providing an updated list of valid certificates. It would then be the responsibility of this new entity to revalidate certificates.

The entity creating the KDMs is the sole entity responsible for **evaluating and defining trust**, following the model defined by DCI specifications. The decision to trust devices to handle digital content, apart from verifying the authenticity of device keys, may depend on other policies such as those of content owners. This definition of trust to play a piece of content is expressed as a Trusted Device List (TDL). A TDL is a list of devices within an auditorium that are trusted (thus authorised) by the content owner or KDM creator to participate in the playout of a particular content. This TDL is part of the KDM, and it is the responsibility of the Security Manager to enforce

it. It is important to distinguish here between a device being certified (by the manufacturer to meet DCI requirements), and a content owner trusting that same device (and thus, showing up in the TDL).

The last process in trust management is **key/trust revocation**. A public key, or a certificate over a public key, may need to be revoked for several reasons. For instance, if a CA has been compromised, then all certificates issued by that CA need to be revoked. In this case, one revokes a certificate and not the public key itself, because it is the CA, and not the device itself, that has been compromised. If it is the device, then one would need to revoke the key, and optionally the certificate as well.

Key Management

"*Key management includes all the provisions made in a cryptosystem design, in cryptographic protocols in that design, in user procedures and so on, which are related to the generation, exchange, storage, use, black-listing and replacement of cryptographic keys*". [WKM]

Secure methods of key management are extremely important. Once a cryptographic key is created (symmetric encrypting key or signing private key), it must remain secret to avoid mishaps. In practice, most attacks on public key systems will be aimed at the key management level, rather than at the cryptographic algorithm itself.

In the context of digital cinema, *key management* refers to the processes of creation, storage, distribution and use of content encryption keys. At a standards and specifications level, SMPTE covers the distribution of content encryption keys by defining the KDM in SMPTE 430-1 "Digital Cinema Operations – Key Delivery Message" [430-1]. DCI defines requirements and provides the rules governing the usage of content encryption keys for playout; that is, at exhibition level only. Note also that at SMPTE level, a recommended practice

entitled “Digital Cinema Operations – Key Delivery Bundle” still in ballot process, should define a message structure for delivering all KDMs targeted at a given facility.

In digital cinema, we can distinguish three different phases in key management. The first one is key creation, which covers the processes of creating an encryption key, using it to encrypt content, and storing it. The second phase covers the creation of the KDM and distribution to exhibitors. The last phase covers usage of keys to enable a show.

DCI and SMPTE define the encryption algorithm as AES 128 bits with CBC mode. According to DCI, the encryption of content and the creation of KDMs take place in a trusted environment. It assumes that system implementers and integrators will deliver systems that are secure, without going into the details as of what *secure* means. Special care needs to be taken for generating keys securely and distributing them between encryption and storage, since these are probably performed by different devices. Secure procedures and policies for backup of encryption keys also need to be in place.

To transport keys from the KDM generation facility to the exhibition site, a Key Delivery Message shall be used. The KDM is a security wrapper that delivers encryption keys for a feature, validity period and trust information (the Trusted Device List) targeted to a specific Security Manager at an exhibitor facility. The security wrapper guarantees that, independently of the transport mechanism used, keys remain secure. In order to do so, the KDM generator encrypts the encryption keys and the validity period with the Security Manager's public keys. This guarantees that only the targeted security manager can access the information. It also signs the KDM with its private key, providing integrity and authenticity of the message.

When a show is queued, the Screen Management System or Theatre Management System sends the KDM to the Security

Manager. The SM will verify the authenticity of the KDM and the validity date for using the keys, check that all devices in the auditorium suite appear in the TDL and, optionally, whether the content owner in the KDM matches that of the composition. The SM is also responsible for verifying and monitoring the integrity of all security devices in the auditorium suite. Precisely, DCI mandates that all security devices should be able to monitor their own integrity by detecting tampering attempts and maintenance activities. Upon request, these devices provide integrity status information to the SM.

After usage, the keys need to be zeroed, that is, instances of the key in clear text must be erased. It is up to the SM to decide when this takes place.

Logging and Audit Trails

Logging refers to the practice of recording sequential, often chronologically events. A computer program or device may automatically record events within a certain scope in order to provide an audit trail that can be used to diagnose problems.

In digital cinema, however, in order to allow exhibitors flexibility in their operations, stakeholders adopted a *control lightly – audit tightly* approach. Instead of a sophisticated DRM controlling how content is used, content owners specify the periods in which content can be played. Agreements are negotiated outside the security system. Exhibitors must then provide audit trails reporting the actual content usage. These audit trails or logs then need to be secured, guaranteeing **integrity** and **authenticity** properties.

The approach followed by both DCI and SMPTE is similar. Each secure device in an auditorium must generate secure logs and store them locally. The log format is XML, and is specified by an SMPTE document in ballot process to become standard SMPTE 430.4 “Digital Cinema Operations – Log

Record Format Specification". This log format relies on cryptographic primitives to provide **integrity** (of both content and sequence) and **authenticity** of origin. **Confidentiality** is not seen as a requirement, and the log format does not support it intrinsically. However, in order to allow filtering of audit trails, the format supports the removal of log record data (not the headers, which contain only "public" information). Filtering is needed since there is a single log, independently of the content and its owner.

This log format is a placeholder of log record data. It defines a log record as being composed of a log header containing an optional sequence number, a chaining hash with the previous log record, a hash of the log detail, and the detail itself. The chaining hash of a log record is computed by taking as input the log header, chaining hash and body hash of the previous record (see Illustration 29). This chaining hash guarantees that no log record has been removed from the sequence while allowing the removal of a log body. The signature of the log applies only to the last log record header and chaining and body hashes. This, along with the cryptographically secure log record chaining, provides proofs of integrity and authenticity or origin (secure device that generated the log).

Regarding the log record type and subtype, at the SMPTE level there is a recommended practice[28] in balloting process defining event types and subtypes. These cover events such as powering up/down, TLS establishment, playout actions, digital cinema certificates loading and removing, integrity check failures or presence of forensic marking, among others.

[28] "Digital Cinema Operations – Log Record Security Constraints" and is expected to become RP 430.5 once published.

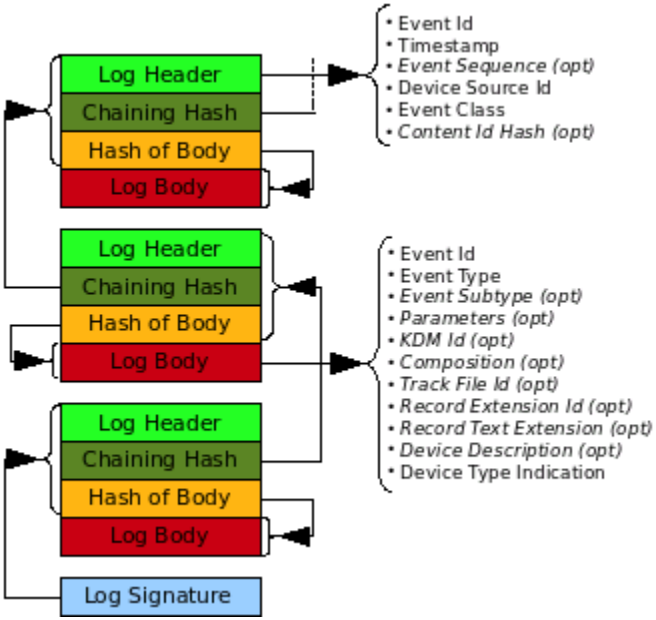


Illustration 29: Structure of log records and log signature. The illustration also depicts how log records are chained.

All secure devices in an auditorium shall be able to generate and store logging information. Practically this means that the Media Block and the Projector Media Block, if present, shall store and transmit secure logs. The log storage capacity of a Media Block is required to be, at least, one year, while for a Projector Media Block it is of two days.

The Media Block is responsible for collecting log information. This process is called *primary log distribution*, and shall happen as soon as possible after a show, and at least once a day. This primary distribution by means of auditorium security messages is created for this purpose, and, like any other security message, is protected by TLS (this will be discussed later in this chapter).

What happens to security logs after this point is only hinted by DCI and SMPTE. The collected log records need to be filtered depending on the agreements signed between distributor and exhibitor, and may differ on a per content basis. Where this filtering happens is not clearly defined. It could be the responsibility of the Screen Management System or Theatre Management System, or some other device.

There is also a *secondary log distribution* by which logging information, after being filtered, is transmitted to the appropriate party. This is typically the rights owner, distributor or system provider. Here again, DCI and SMPTE only mention that this needs to happen, without going into any details.

Forensic Marking

Forensic marking refers to the process of inserting messages hidden to the human eye (or ear) in digital cinema content at the moment of playout. Watermarking and fingerprinting are other names for forensic marking. The goal of this forensic marking is to identify when and where the content was camcorded, in the case of piracy. It is a measure aimed at discouraging organised professional camcording in cinemas.

Forensic marking is the fuzziest area in digital cinema security standards and specifications. DCI seems to require forensic marking for all image and sound content. However, this is not clearly stated and there are provisions for not requiring forensic marking.

No standard exists for forensic marking, in digital cinema or anywhere else. The high robustness and invisibility requirements, which strongly depend on the type of content, make forensic marking algorithms highly targeted at a specific application. There are numerous approaches, techniques and instantiations of forensic marking technologies.

DCI started the work for defining a forensic marking framework that would accommodate a variety of different algorithms based on the block substitution approach. These technologies are based on the substitution of certain blocks within an image by new ones that contain the hidden message. DCI later delegated this work to the SMPTE. At present, standardisation work in the forensic marking framework for digital cinema is in the early stages, and no document is in balloting process at the SMPTE.

The forensic marking framework defines 3 phases in the overall process: preparation, marking and detection. The preparation phase consists in identifying which image blocks or audio sections are suited to hide a message. When a block is identified, it is marked in the content metadata as such, thus lowering the complexity of the forensic marker. The marking phase happens at playout, where the forensic marking reads the content metadata and substitutes marked image blocks by a visually equivalent one hiding a message. The exact manner in which a message is hidden in the block depends on the algorithm or technology used. The same applies to the detection phase, since the detection algorithm depends on the marking one.

Content Security

Digital cinema content is delivered to cinemas as a Digital Cinema Package. In the production and distribution chain, DCI does not set any security requirements for digital content before the Digital Cinema Package is created. The security of a DCP shall provide the following properties:

- **Confidentiality**: this means ensuring that information is accessible only to those authorised to have access. This is typically achieved by encrypting content using cryptography, and then distributing the encryption key only to authorised users or devices (the auditorium Security Manager in this case).
- **Integrity**: this means that data cannot be created, changed or deleted without it being detectable. One must distinguish between *information integrity* – detecting accidental corruption of data – and *cryptographic integrity* – preventing undetectable and malicious corruption of data.
- **Authenticity**: this means that the creator of the data can be uniquely identified and authenticated. In other words, someone who has only access to the content itself may not claim ownership or creationship, apart from the legitimate owner.

Before showing how these properties are achieved, we need to understand the structure of the content itself. The content is a Digital Cinema Package. SMPTE has published several standards defining the structure and security of a Digital Cinema Package. These are the SMPTE 429 family of standards (see Illustration 6 on page 56 for a complete list). DCI specifications, on the other hand, set the general and security requirements of the Digital Cinema Package, which SMPTE considered when working on the standards.

Digital Cinema Package Structure

The *Digital Cinema Package* is the unit of delivery of content into the cinemas. A DCP wraps different types of content, along with a Packing List, in a single file. The Packing List specifies all the assets contained in the DCP as is, optionally, signed by the entity creating the DCP. Note that this entity shall have a valid Digital Cinema Certificate. The Packing

List, is standardised by SMPTE 429-8 “Digital Cinema Packaging – Packing List” [429-8].

A *Composition*, in the scope of digital cinema packaging, is a self-contained grouping of image, audio and possibly subtitles files that represent a complete feature (film, advertisement, trailer, etc.). There is a separate composition for each version or language audio track and subtitles track of a feature. For example, a DCP of a feature film for the European market with French, Italian, German and Spanish audio tracks would contain four separate compositions.

A DCP may deliver one or more full compositions, or parts of compositions, along with other assets. Since the contents of a given composition may be delivered through different packages, the Packing List allows the creation of associations between packages.

A *Composition Playlist* (CPL) is a document, and DCP asset, which represents a composition as an ordered sequence of *reels*. CPLs are standardised by SMPTE 429-7 “Digital Cinema Packaging – Composition Playlist” [429-7]

The concept of *reel* is inherited from the 35mm world. A reel is a conceptual period of time having a specific duration. A reel is composed of one or more *track files* (maximum one of each type) containing exactly all the essence for that specific period.

A *track file* is the container for content of a specific type (image, audio or subtitles) for a feature presentation (film, trailer, advertisement or other). All track files follow the same basic structure, and have three logical parts: the File Header which contains the header metadata, the File Body which is the essence container, and the File Footer.

Each track file essence is further broken down into 1 frame -equivalent time units. These essence units are then encoded

using KLV-triplets[29]. In other words, each image frame is encoded separately in a KLV triplet. All audio information corresponding to an image frame is encoded in a different KLV triplet, and the same applies to subtitles or timed-text.

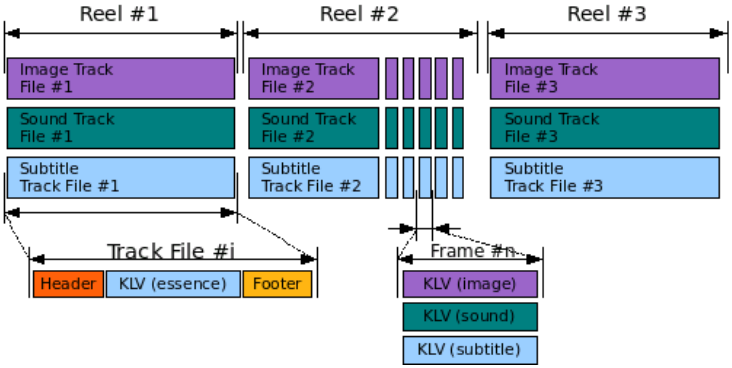


Illustration 30: Structure of digital cinema essence, from reels at the composition level down to individual frames. A reel is composed of an image and audio track files, possibly a subtitles track file. All types of track files share the same structure. The content of each track file is split per frame and individually encoded.

We will now discuss how a Digital Cinema Package and its content are secured for storage and transmission. We should note that security applies at two levels here: the delivery level of the Digital Cinema Package, and the content level of each composition.

Digital Cinema Package Security

The Packing List optionally contains a signature of the entity that created the package. This signature allows the creator of the package as well as the package itself to be authenticated.

Per each asset in the package, the Packing List also contains its SHA-1 hash value (see [CHF] and [SHA]). Although

[29] See SMPTE 336M "Data Encoding Protocol using Key-Length-Value" and [KLV].

SMPTE 429-8 defines the signature of a Packing List as optional, DCI mandates it. If the Packing List is signed, all asset hashes provide the guarantee that the DCP has not been tampered with. If no signature is present, this hash value allows the verification that DCP has not been accidentally corrupted due to transmission or storage errors.

Composition Security

DCI requirements state that content security in a DCP shall provide *confidentiality*, *integrity* and *authenticity* properties. We now see how the different data structures and elements in a DCP guarantee these properties.

A Composition Playlist (CPL) is the document which specifies the manner in which the track files forming a composition are rendered. A CPL represents a composition as an ordered sequence of Reels. Each Reel contains one or more Assets, which identify Track File segments to be reproduced in parallel.

The CPL is created by the entity responsible for content mastering. This entity must possess a Digital Cinema Certificate which identifies it. The CPL itself is signed[30] with the RSA public key of the entity, which provides *integrity* and *authenticity* of the CPL.

Among other information, the CPL contains an ordered list of reels. Each reel element contains the list of track files (assets) that composes it. Each track file element further contains a key identifier, which uniquely identifies the key used for essence data encryption and integrity check, and a SHA1 hash of the track file itself. This hash value allows the *integrity* of each individual track file to be verified. Furthermore, given that the CPL is signed, this hash validation also guarantees the *authenticity* of the composition.

[30] SMPTE 429-7 specifies the signature field to be optional. DCI specifications require CPLs to be signed.

Track files in a composition may be in plaintext or encrypted forms[31], depending on the type of essence and type of composition. For instance, an advertisement may be delivered in plaintext form.

If a track file is marked as encrypted, the same cryptographic context is used for all frames. The cryptographic context field is added to the header of the file. This field identifies the AES key to encrypt/decrypt the content, and specifies the encryption (AES-CBC[32] 128 bits) and integrity (HMAC-SHA1 128 bits) algorithms used.

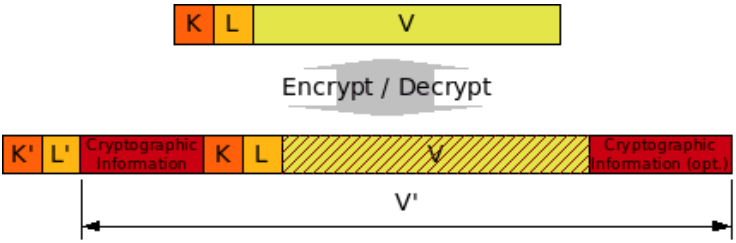


Illustration 31: Plain text KLV-triplet and the corresponding Encrypted KLV-triplet. The image depicts how a KLV-triplet is transformed due to an encryption or decryption operation. Encrypted data are indicated with diagonal red lines.

Each individual frame – encrypted or not – in a track file is encoded in a KLV-triplet. There are, however, some differences between a KLV-triplet carrying plaintext essence data and one carrying encrypted essence data, as shown in Illustration 31.

This KLV-triplet for encrypted essence contains the following information:

- Key K' indicating that the triplet carries encrypted essence.

[31] DCI specifications seem to imply that only image and audio track files can be encrypted.

[32] Cipher-Block Chaining Mode. See [BCM] for information on block cipher modes of operation.

- Length L' of V', as depicted in Illustration 31.
- Cryptographic information of the encrypted essence, which contains a link cryptographic context in the track file header.
- The original K and L values that will be used for reconstructing the original triplet on decryption.
- The encrypted essence data as depicted in Illustration 32.
- Optional[33] cryptographic information of the encrypted essence. This field identifies the track file and sequence number of the frame, and contains a message authentication code of all data from the encrypted essence (starting at the IV) until the sequence number.

The HMAC-SHA1 computation requires a cryptographic key, which is obtained via a key derivation function, which takes the encryption key as input.

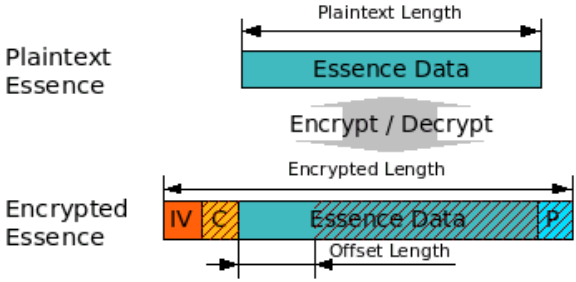


Illustration 32: Plaintext Essence and the corresponding Encrypted Essence. Encrypted data are indicated with diagonal red lines.

It is important to highlight how this HMAC value guarantees the *integrity* and *authenticity* of both the encrypted essence and, indirectly, the plaintext one. Firstly, a successful HMAC test proves that 1) the correct AES key is being used, 2) the essence data are authentic, since only the entity that encrypted

[33] Although SMPTE 429-6 declares this field to be optional, DCI requires its presence.

the essence could create the HMAC, and 3) the encrypted essence data have not been tampered with. Secondly, the track file identifier and sequence number are used to compute the HMAC value, which ensures that frames in the track file have not been mixed up.

The last step now is the encryption of the essence data in a frame (the V value in Illustration 31). As already explained, the encryption algorithm is AES-CBC with a 128 bit key. The encrypted essence data structure, as shown in Illustration 32, contains the following elements:

- 16 bytes of *initialisation vector* or *IV* (see [CIV]) which is needed to initialise the block cipher.
- 16 bytes of *check value* C, encrypted with the same AES key. The value C is computed from the plaintext essence data. This value provides a first level of integrity on the decrypted data, and assurance that the correct AES key is being used for decryption.
- 0 or more bytes of plaintext essence. Precisely, the cryptographic scheme standardised in SMPTE 429-6 allows some heading bytes of essence to remain in plaintext form. The goal is to allow applications to access this metadata without the need to decrypt it.
- the essence data, padded to a multiple of 16 bytes (which is the size of the block cipher) and encrypted.

Security Communications

A goal of both DCI and SMTPE is to provide interoperability at device level. This is a requirement in order to have an open architecture and marketplace where different vendors can compete. To achieve this interoperability, we need standardised messages and protocols. These are defined at two levels:

- **Extra-Theatre Messages**: these are self-contained one-way messages that originate or end at the exhibition site. These messages carry security information such as encryption keys or logs. An example of such messages is the Key Delivery Message.
- **Intra-Theatre Protocols**: these are request-response protocols between the Security Manager and the Screen Management System or the Projector Media Block.

Extra-Theatre Messages

For extra-theatre messaging, DCI relies on SMPTE standards in this area, namely SMPTE standard "Digital Cinema Operations – Generic Extra-Theater Message Format" [430-3], and "Digital Cinema Operations – Key Delivery Message" [430-1]. We cover KDMs in the "Key Management" section later in this chapter.

Extra-Theatre Messages (ETMs) are an XML generic security container that provides the properties of *uniqueness*, *confidentiality*, *integrity* and *authentication*. The main advantage of this generic container approach is that the container itself guarantees these security properties. Any other message defined on top of it automatically has the same properties. This minimises the risk of new message types undermining the integrity of the security system.

Each ETM has three main elements:

- **Authenticated Public**: information in this element is readable by anyone with access to the message, but is not modifiable. This element identifies the message itself, the signer of the message, specifies the issue date, and has placeholders for both standard and proprietary extensions (which are not critical for interoperability).
- **Authenticated Private**: this contains one data element that is encrypted using an AES key. For each recipient of the message, there is an element that contains the

abovementioned AES key, encrypted with the RSA private key [RSA] of a recipient.

- **Signature**: this element allows the validation of both message integrity and authentication. The signature verification is a 2-step process. First, the hash of each of the message parts is computed and compared against values in the signature. Then, these 2 hash values are canonicalised and compared with the result of decrypting the signature value with the signer's RSA public key.

The fact that it is a generic container allows it to be used between any security devices or entities in the digital cinema chain[34].

Intra-Theatre Communications

Within an auditorium, the entire equipment suite needs to communicate in order to set up and carry out a presentation. To achieve device-level interoperability within an auditorium, a set of digital cinema specific protocols needs to be standardised, as well as a network stack.

Security communications take place between the Screen Management System, the Security Manager and, if present, the Link Decryptor Block inside the projector. The protocols defined for interoperability should cover key management, time synchronisation, log and status reporting, as well as security operations reporting[35].

Both DCI and SMPTE[36] specify that security devices within a cinema shall communicate using Transport Layer Security

[34] Note that this message format may be used in applications other than digital cinema.

[35] The Screen Management System requesting the Security Manager to perform a validation check of a KDM, for instance.

[36] This work is covered by a document in ballot process. When published, it should appear as SMPTE standard 430.6 “Digital Cinema Operations – Auditorium Security Messages for Intra-Theater Communications”.

[TLS]. TLS is a security protocol over TCP/IP, which is the intra-theatre network infrastructure. SMPTE standardised security messages over TLS shall use port 1173. TLS provides peer authentication and communications confidentiality, integrity, freshness and authenticity. In order to authenticate each of the peers, DCI mandates all security devices to posses an RSA key pair and an associated digital cinema certificate (see the "Certificates" section later in this chapter).

Intra-theatre security protocols shall follow a request-response message paradigm. The protocols shall be synchronous, meaning that a request must be responded to before a new request is issued. Security devices must be designed to avoid hang-ups. If they are unable to respond, they shall respond with an error rather than waiting.

In its specifications, DCI present a proposal for intra-theatre request and respond messages for communications between the Screen Management System and the Security Manager, and the Security Manager and the Link Decryptor Block. However, their description is only semantic, avoiding a detailed syntactic specification. Thus, they are of little practical use for device interoperability.

SMPTE goes a bit further, and defines the structure of intra-theatre messages and specifies request and response messages between Security Manager and Link Decryptor Block for time synchronisation, log collection, status reporting and key management.

Request and response messages shall be encoded as Key Length Value triplets [KLV]. KLV is a binary encoding SMPTE standard (SMPTE 336M "Data Encoding Protocol Using Key-Length-Value"). Information is encoded into KLV triplets, where the key identifies the data, the length provides its length, and the value is the information itself.

SMPTE standardises the following request-response pairs, which are a subset of the meta-messages defined by DCI:

- **Get Time**: for time synchronisation.
- **Get Event List / Get Event Id**: for the Security Manager to collect log information.
- **Query SPB**: which queries for the status of an SPB and the security entities inside it.
- **LE Key Load**: through which the Security Manager instructs the Link Decryptor Block to load a link encryption key.
- **LE Key Query Id / LE Key Query All**: which query the keys active in the Link Decryptor Block.
- **LE Key Purge Id**: through which the Security Manager instructs the Link Decryptor Block to purge a key from memory.

These messages do provide for interoperability between a Screen Management System and the Link Decryptor Block within an auditorium. But this is only a small part of interoperability for security messaging inside an auditorium. We address this issue later in this chapter, in the section "(Un)Completeness of DCI/SMPTE and Other Issues".

FIPS Device Certification

There are two approaches to mitigate this class of attacks. One can isolate the security system so that it becomes impossible for an attacker to gain physical access to it. This implies creating a physical security perimeter around the system with appropriate access controls and constant monitoring of the system (security cameras).

Another approach consists in protecting only the critical security parameters and cryptographic operations physically. That is, only the hardware and software that implement cryptography are protected. This approach places the security perimeter inside the security system, and prevents physical

attacks (or makes them very difficult) even if the attacker gains physical access to the system.

It is important to note, however, that there are attacking techniques that exploit information gained from the physical implementation of a cryptosystem. They are called *side-channel* attacks (see [SCA]) and are typically based on timing information (amount of time used to perform an operation), power consumption, electromagnetic radiation leaked or even sound. In all cases, the underlying principle is that physical effects caused by the operation of a cryptosystem can provide useful extra information about secrets in the system such as cryptographic keys, internal state information or full or partial plaintexts.

SMPTE, as a standardisation body, is agnostic of implementation details and thus, it is not its job to standardise physical security. DCI, on the other hand, sees this as a critical aspect of the system, and defines requirements for the physical implementation of security devices.

DCI defines two levels of physical security: one aimed at protecting image essence entering the projector, and another aimed at protecting the Media Block.

All projectors shall have a Type 2 Secure Processing Block (in DCI terminology). A Type 2 SPB consists of a physical enclosure whose purpose is to protect essence as far as practical. The enclosure must detect the opening of the access door. Inside this enclosure, there is either a Media Block or a Link Decryption Block, depending on the auditorium configuration.

For the Media Block and the Link Decryption Block (if present), DCI mandates to comply with the physical requirements defined for FIPS 140-2 level 3 cryptographic modules.

FIPS 140-2 is a standard that specifies the security requirements and standards for cryptographic modules which

include both hardware and software components. The goal is for US federal agencies and departments to validate that a cryptographic module is covered by a FIPS 140-2 certificate which specifies the exact module name, hardware, software, firmware and/or applet version numbers.

The standard specifies four different security levels to provide a wide spectrum of data sensitivity. For each level, the standard defines the security requirements in 11 different areas. These levels are:

- **Level 1**: lowest level which imposes very limited requirements. Loosely, all components must be "production-grade" and various kinds of insecurity must be absent.
- **Level 2**: adds requirements for physical tamper-evidence and role-based authentication.
- **Level 3**: adds requirements for physical tamper-resistance, identity-based authentication and physical or logical separation between the interfaces through which critical security parameters enter and leave the module and its other interfaces.
- **Level 4**: makes the physical security requirements more stringent, and requires robustness against environmental attacks.

DCI adopts FIPS 140-2 level 3 as a baseline for Type 1 SPB. It makes exceptions, however, in 7 out of the 11 areas of security requirements. In two areas, the security requirements are downgraded to level 2 (design assurance and electromagnetic emissions), while in five, the security requirements are adapted to digital cinema.

FIPS 140-2 established the Cryptographic Module Validation Programme (CMVP). All of the tests under the CMVP are handled by third-party, accredited laboratories. Cryptographic modules are tested against the requirements covering 11 areas

related to the design and implementation of a cryptographic module. Within most areas, a cryptographic module receives a security level rating (1 to 4) depending on what requirements are met. For other areas that do not provide for different levels of security, a cryptographic module receives a pass/fail rating.

An overall rating is issued for the cryptographic module, which indicates:

1. the minimum of the independent ratings received in the areas with levels, and
2. the fulfilment of all the requirements in other areas.

On a vendor's validation certificate, individual ratings are listed, as well as the overall rating.

Trust Model with DCI/SMPTE

In the previous chapter we created a trust model for the whole cinema chain, from post-production down to exhibition. Then we incorporated a new player in the model, the *system-to-be*, and shifted goals, resources and security constraints to it.

In this section we will examine the trust model defined by DCI specifications and SMPTE standards. We argue that a system should model and fully support the policies and procedures of the organisation in which it is used. A flaw in the trust model may be exploited to attack the system. On the other hand, if the system prevents or hinders a user from performing a task, the user will try to circumvent the security system to do so.

It is important to note that, in the same way that a good trust model does not result in a secure system (although it is a first step in the right direction), a system with a flawed trust model is not necessarily insecure.

Illustration 33 depicts the refined delegation model derived from DCI specifications. If we compare this model with the

one from the previous chapter (see Illustration 22 on page 103) we may make some important observations.

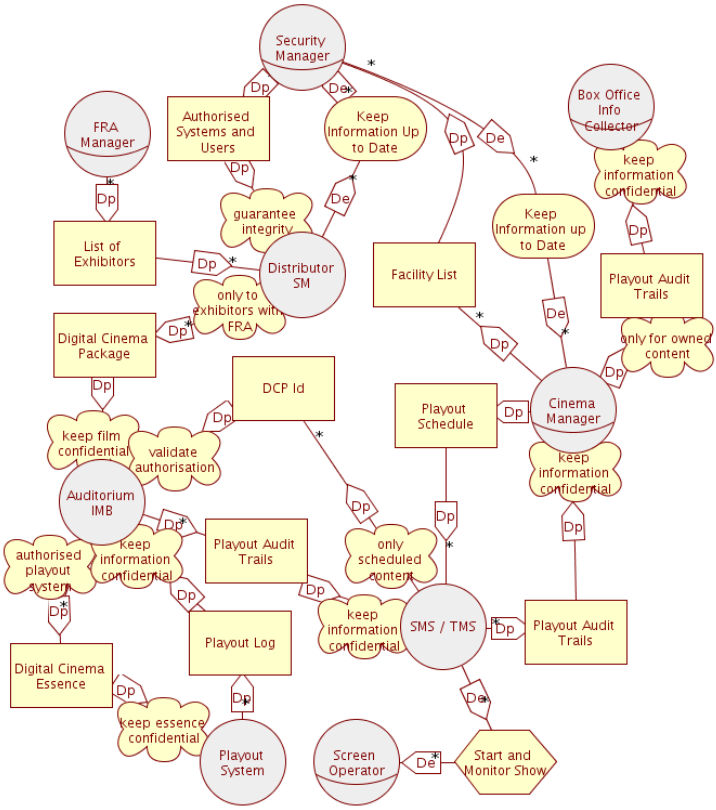


Illustration 33: Refined delegation model between Distributor *and* Exhibitor *derived from the digital cinema system defined by DCI and SMPTE.*

The first observation is that the security constraints at the exhibitor level are spread among different agents – human or system. This means that the security measures are also making it more difficult to implement and manage. In Illustration 22 on page 103, we may observe that the exhibitor security

system is responsible for implementing all the security constraints at the exhibitor level. It only depends on the playout system keeping the film confidential, and on the exhibitor security manager[37] keeping information on authorised users and systems up to date.

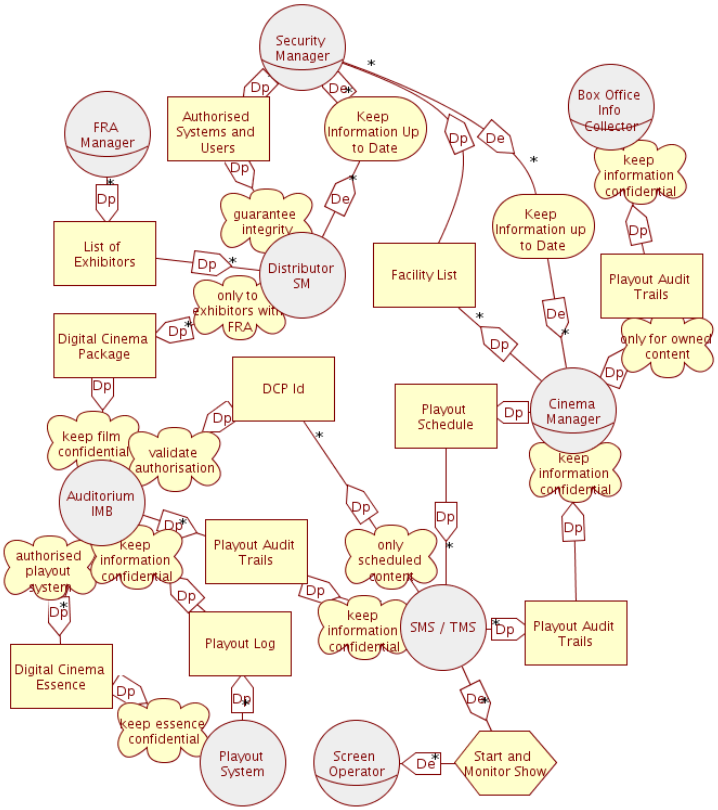


Illustration 34: Refined delegation model between distributor *and* exhibitor *derived from the digital cinema system defined by DCI and SMPTE.*

[37] Note that here we refer to the human agent, and not to the S*ecurity Manager* inside the *Media Block* defined by DCI.

We may also observe how DCI specifications break the balance which exists between distributor and exhibitor. Precisely, since the distributor authorises individual auditoriums instead of facilities, exhibitors are no longer free to schedule a film in any auditorium. Furthermore, exhibitors are also constrained by the validity period of KDMs, which, again, is defined by the exhibitor. One may argue that distributors may create KDMs for all auditoriums in a facility and specify long validity periods, which is a perfectly valid point. However, we are looking at the trust model, and not at the precise use made of the system. From a trust model point of view, DCI clearly breaks the balance between distributor and exhibitor, in favour of the distributor. If we look at the 35mm world, an exhibitor, once in possession of a copy, is free to play the film in any auditorium for the duration of the film rental agreement.

But perhaps what stands out most with DCI's security system is the disappearance of the exhibitor from the system model. In our model from the previous chapter, the Exhibitor Security System represents the exhibitor from a system point of view. Content is sent to an exhibitor, and audit trails are also collected from an exhibitor. With DCI, on the other hand, content is sent to auditoriums, and audit trails are collected from the cinema manager. At the system level, the exhibitor has vanished. Again, we do not claim that, because of this, DCI is more or less secure. Our point is that a system must adapt to the organisation[38] within which it is used. If, at the organisation level, there is an agent – an exhibitor in this case – after incorporating the security system, the agent should either still be there or be represented by the system.

[38] Remember that we consider the whole cinema chain as a single organisation, as explained in chapter 4.

(Un)Completeness of DCI/SMPTE and Other Issues

Both DCI and SMPTE have done a tremendous amount of work to achieve an open, interoperable and secure digital cinema system. While SMPTE's area of focus is on standards defining protocols, formats, messages and other data structures, DCI defines a system architecture and requirements, while relying on SMPTE and other standards.

The current specification of the Digital Cinema Initiatives LLC in its recent version 1.1 was approved on April, 12th 2007[39] and is available online [DCI]. With the goal to establish interoperability between technology providers and compatibility of devices within the digital cinema marketplace, the specification follows a bottom-up approach tackling many important and fundamental issues in several areas, such as Digital Cinema Distribution Master, Image Compression, Packaging, Transport, Theatre Systems, Projection and Security.

Due to this approach, there are some gaps to be filled in order to achieve an overall picture of the evolving system. The motivation behind this is supposedly the fact that there are several business models established and diverse practices in place that make it difficult to get a kind of top-down completeness for an overall global picture of digital cinema. However to achieve real security, compatibility and interoperability these gaps need to be filled. The following paragraphs give further details on potential issues with the specification and its use in terms of achieving the defined goal.

[39] A new errata for "DCI Digital Cinema System Specification" version 1.1 was published on August 27th, 2007 [DCE]

The Bottom-Up Approach

Focused on the exhibition environment, the DCI specifies a full set of requirements concerning key access management, event logging and necessary infrastructure components in order to implement a secure exhibition environment. Most of the technology is based on international standards from SMPTE, IEEE, NIST and IETF. The logical walk through a cinema is specified on a level, providing consistency on a certain level of abstraction. However the syntax of intra-cinema messages, for example, is not specified, although they can be regarded as the message-based communication language within a theatre management system. This is one missing detail for having interoperable equipment from different vendors.

Another aspect concerns the handling of log reports. They are built from log events recorded inside a theatre management system and provide substantial information about the security status of the equipment used inside a cinema. They must be made available to the rights owners. But further details on the cases of equipment failure and the interaction with the device vendors are not given. This and other issues originate from a lack of top-down completeness.

If DCI and/or SMPTE are to continue standardisation and specification work covering the whole distribution chain, a top-down look at digital cinema security is a must.

Theatre Architecture

A consequence of the bottom-up approach to security from DCI, and consequently SMPTE, is the lack of an entity within the cinema security system representing the exhibitor itself. In security, a principal is an entity (device, system or user) that is able to "*speak*"; that is, it is able to issue signed statements.

As we have already explained, this is a problem at the trust model level. The lack of the exhibitor principal, although not

critical for the security of the system, has some collateral consequences in the distributor-exhibitor communications. SMPTE and DCI define, for instance, the Facility List Message. This message may be signed, but by whom? It is not the function of the Security Manager, or of the Screen Management System.

At present, this may not be such a critical issue. However, as more cinemas convert to digital and the system becomes more automated, secure communications between distributor and exhibitor (not Security Managers) will be required. Secondary log distribution and KDM delivery requests are examples of this.

Intra-Theatre Protocols

SMPTE is in the process of approving a document specifying the Auditorium Security Messages. However, the document contains only protocols for communication between the Media Block and the Projector Media Block for Link Encryption keying and log reporting. However, if we are to have a truly open and interoperable auditorium environment, we will need standards for more protocols, in terms of both security and system management.

If we look at the auditorium architecture components defined by DCI and depicted in Illustration 35, we can identify those points where interoperable protocols will be required. These protocols shall cover security management, but also equipment suit and content management.

One may argue that these protocols are not required; after all, already thousands of screens have been converted to digital both in the US and Europe without these standards.

However, we are only at the beginning of digital cinema, with closed systems delivered as a whole by system providers. As the market matures and we pass from an "*initial rollout phase*" to a "*full rollout phase*", the lack of these standards will

prevent a truly open market for digital cinema device manufacturers.

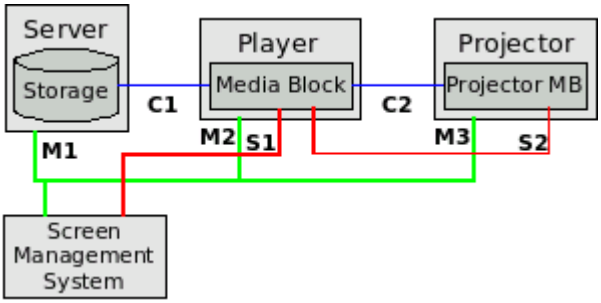


Illustration 35: Auditorium security architecture with annotated protocols between elements. A blue line indicates content path, a green line indicates control and management protocols, and a red line indicates security management protocols

Certificate Infrastructure

One fundamental technology based on the X509v3 is adopted in the DCI specification – Digital Cinema Certificates as specified by SMPTE. Because this specification makes use of certain extensions, implementations of this specification imply that the technology providers also have to provide a fully functional root certification authority for their devices. A reason for this is the fact that most, if not all, of the well-known certificate service providers do not comply with the specification of SMPTE with the root certificates they provide. Therefore, they cannot participate in certificate chains conforming with SMPTE. It would not weaken the DCI security system to allow “usual” root certificates, and it could facilitate fair competition in the digital cinema marketplace and reduce the complexity of relations between stakeholders of the DC chain.

Another advantage of allowing commercial certification authorities in the digital cinema market would be that device manufacturers would no longer be required to create, support

and manage their own certification authority. Certification is a critical point in the security system, and should be handled by professionals in this area.

Chapter 6
Threat Analysis of European Digital Cinema

Introduction

A secure system is difficult to achieve mainly because it has to be “secure by design”; meaning that the philosophy of the development of such a system should be clear since the beginning. Security is not something one can “plug” into an unsecured system in order to get a secure version of it. In most cases, this approach would not work or would be very expensive.

In the case of a digital cinema system, this task is hard to achieve for several reasons: the assets and threats are not well defined and are difficult to evaluate, the probable evolution of the industry is not very clear and it takes a long time to design the system.

In this chapter, we conduct a complete analysis of the digital cinema system as defined by DCI and SMPTE according to the current state of development, using a Threat Analysis Methodology based on Attack Trees (TAMAT) designed by Thomson. First, we give a short introduction to the methodology. The analysis which follows consists of two parts: the definitions of the context of the analysis and the definitions of the threats. Attack trees are used to depict attacks implementing relevant threats. Results are presented in a graphical format, on a valuation grid.

Introduction to TAM^{AT}

The Threat Analysis Method based on Attack Trees (TAM^{AT}) is a method developed by the Thomson Security Laboratories as

a lightweight alternative to existing methods (common criteria, EBIOS, or ISO17799). Its goal is to identify threats and determine the probability of their occurrences together with the severity of their impact.

In a deployed system, the analysis results highlight the actual security level of the target system and help to choose effective security solutions. In a system still in a design phase, it helps point out the problems that may occur. Therefore, the results of the analysis provide guidelines to express recommendations on the design. Here, the work is done with the latter case in mind.

A standard TAM^{AT} is an iterative process involving several steps presented in the illustration below. The first step is aimed at defining the target of the analysis through formal definitions of several elements (perimeter, assets and scales). The second step identifies the threat and defines the risk aversion table. A first evaluation of the threats is conducted, based on detailed analysis, and the target of the final evaluation is decided. Typically, this is done in order to restrain the scope of the focused analysis if it is conducted under certain constraints (time, money, etc.). The focused analysis defines attacker categories and realises complete valuated attack trees for each threat. After that, the positions of the threats are updated on the risk aversion table according to each attack tree root valuation. The updated risk aversion table is the main output of the analysis.

The analysis methodology we have used is based entirely on TAM^{AT}. Here, as the system is not yet deployed and implementations have not yet been considered and proposed, the third step is not completely covered. In this book, we provide the target of evaluation and the corresponding attack trees, under common implementation assumptions; however, the valuation of these attack trees and the update of the position of each threat on the valuation grid could not be

considered. Indeed, these final steps of the analysis depend greatly on actual systems and should therefore be carried out for each specific implementation. We will now describe each step of the analysis in detail in order to provide the reader with a background of the methodology and of this chapter.

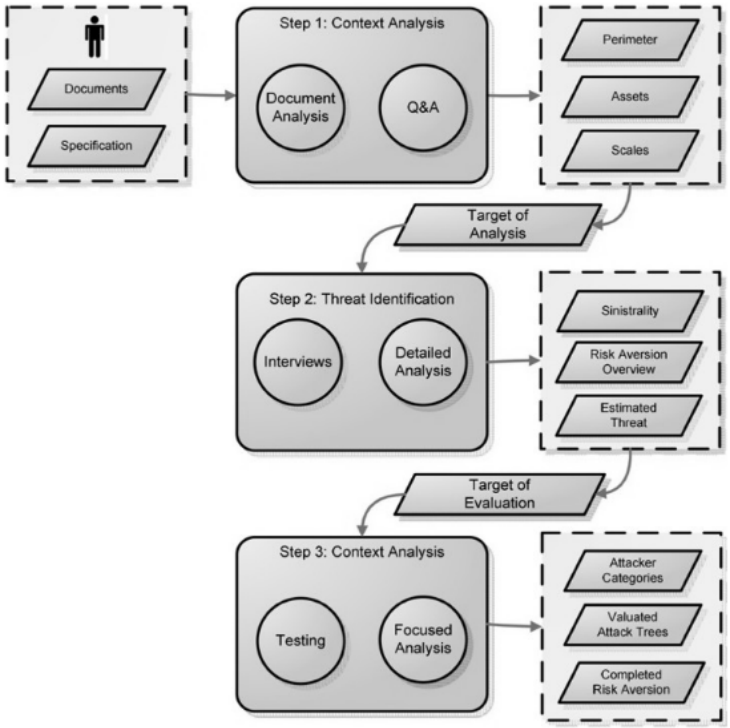


Illustration 36: Standard TAMAT description.

In the first section of this chapter, the scope of the analysis is defined. Through a set of different **perimeter** definitions, we provide details of what is taken into account and what is left outside the scope of the analysis. Several aspects of the system are addressed by these perimeters, which include:

- *workflow perimeter,* a sequence of operations required to produce, distribute and exhibit any content;
- *components perimeter,* all devices taken into consideration;
- *human perimeter,* all people involved in the cinema business, from rights owners to audience;
- *processes perimeter,* separated actions needed for the DC business.
- *infrastructure perimeter,* a set of infrastructures of each of the DC players;
- *physical perimeter,* list of controlled/uncontrolled environments.

Assets are also defined in this first step. They are physical or virtual objects which are valuable from a business point of view. The security of the whole system is supposed to guarantee usage of these assets following a set of rules, and no attacker is able to transgress these rules to his or her substantial advantage. Several **scales** are needed to sort the threats according to several aspects. These scales are usually defined according to 3 to 5 categories. The three principal scales we will use are:

- *impact*, which directly reflects the severity of the impact that an attack would have if it occurred. It can be valuated regarding an amount of money or regarding other subjective values;
- *potentiality*, which reflects how frequently an attack may occur.
- *risk acceptability/risk aversion*, which reflects the risk acceptance as a function of the impact and potentiality.

The three scales are then combined to create a **valuation grid**.

In the second section, we discuss the potential threats. We start by discussing the **sinistrality** of the system, i.e. the history of

security-related incidents leading to system problems (mainly financial loss). As this analysis addresses an undeployed system, there is no real sinistrality. However, we discuss which security aspects will not be altered by the introduction of digital cinema, posing the same threat as in the current 35mm chain. We present the four **attacker categories** that should be considered for the last step of the analysis. After that, we list what we consider to be the main **potential threats** specific to digital cinema, and propose valuated attack trees for those we believe to be relevant. This valuation finally allows the positioning of each threat on the valuation grid.

TAM^{AT} terms and definitions

The definitions of the analysis terms are listed here. As the definitions are not always straightforward, the reader should refer to this section if there are doubts about the exact meaning of certain terms.

Asset: any element of a system that has value and thus may be subject to attacks. An asset can take on many forms: physical equipment, data, software or brand image, among others.

Attacker: person (or organisation) who may obtain substantive benefit from using a system in a wrong way. The attacker can be outside or inside the system. The benefits an attacker may seek are very diverse and not well specified: they range from large amounts of money (Mafia) to 5 minutes of so-called “fame” on certain websites (garage hacker).

Attack Trees (AT): multi-levelled diagrams consisting of one root, leaves and children. From the bottom up, child nodes are conditions which must be satisfied to make the direct parent leaf true; when the root is satisfied, the attack is complete. Each leaf may be satisfied only by its direct child nodes. Each leaf may require one or more of many child nodes to be satisfied. In this case, OR conditions and AND conditions may apply: if only one of the child leaves has to be satisfied, we

say that they are OR-related (the parent leaf is in *italics*); if every child leaf has to be satisfied, they are AND-related (the parent leaf is in **bold**).

Impact: consequences of security incidents caused by a threat. Impact is generally financial but is not limited to this aspect. It may also be the loss of brand image, competitive advantage, technical reputation, etc.

Potentiality: indicates how frequently the attack may occur (e.g. once a week). In some cases the range of potentiality may by different from one asset to another (e.g. infrastructure or transient data).

Probability: indicates the level of difficulty of the attack and thus the probability of being attacked. It is not to be confused with the potentiality.

Risk: probability of occurrence of a threat, weighted by the severity of its impact. This probability depends on many factors, including the value of the asset, the cost of the attack, the danger for the attacker, etc.

Sinistrality: gathering of historical incidents of a system.

Threat: a potential to cause security incidents which may result in damages to a system and its assets. Threats may be either accidental or deliberate. In the latter case, they are called attacks and are conducted by malicious people (the attackers).

Vulnerability: weakness of an asset that may be exploited by a threat. The vulnerability of an asset related to a threat is measured by its *weakness*, i.e. how easily the vulnerability might be exploited by the threat. It is expressed in terms of skill and resources necessary to exploit it.

Context Analysis

This section begins with the definition of the analysis context as a set of perimeters and assets, presenting what is inside the scope of the analysis and what is left outside. Then, the valuation grid is introduced with all scale definitions. Because DCI specifications provide the only currently available guidelines for the implementation of the system, we will refer to specific primitives using the DCI terminology. The overall "DCI implementation philosophy" is the framework of this analysis, therefore, the context is described within this framework.

Perimeter Definition

Here we will define the boundaries of the system under consideration. The analysis will be carried out on the sub-system.

Workflow Perimeter

The global workflow of digital cinema has already been described earlier in this book (see Chapter 4). Here we discuss the workflow considered in the framework of this analysis.

Many pirate copies of films are made available on the internet before their cinema release; some of them are unfinished versions probably from some post-production stage, but some completed versions are also leaked. These versions are perfect copies of the final film, ready to be printed. However, this threat is not specific to digital cinema distribution and will still exist in the digital cinema era. Therefore, we will exclude the area of content creation from the perimeter of analysis. Thus, in terms of workflow, we should cover all the elements starting from the point where the film enters the digital cinema area until the projection on screen. The workflow we consider for this analysis starts once the first stage of production is

complete: artistic creation and content production are therefore not taken into account.

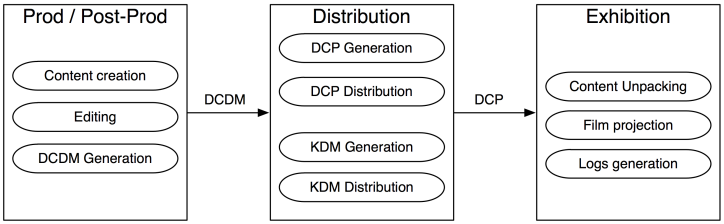


Illustration 37: Workflow perimeter

The workflow (see Illustration 37) starts with the post-production phases such as content creation (film shooting, audio and music recording, etc.), editing and the generation of a final packaging – called Digital Cinema Distribution Master (DCDM) – containing everything needed for the distribution to generate the DCPs (Digital Cinema Package).

During the distribution phase, several DCPs are generated, by encoding and encrypting the relevant DCDM parts (video, audio depending on language needed, subtitles, etc.) together with the generation of the corresponding KDMs. Then the DCPs and KDMs are distributed to the exhibitors. This distribution can be organised hierarchically, form nationwide distributor to local distributors.

Exhibition phases cover content unpacking, from the DCP/KDM pair, the film projection and the establishment of the audit trail.

Component perimeter

The component perimeter depends greatly on the implementation to consider. However, in order to give a complete description of the context of this analysis, we shall present a list of the components inside the scope of this study:

- Projector
- Media Block
- Player
- Theatre Management System / Screen Management System
- Content Storage
- KDM generator
- Media Encryptor
- Certificate database
- Theatre Network
- Distribution Network
- Log report network
- ...

This list is provided as an example rather than as an exhaustive record of the components to take into account for a final system.

Human Perimeter

The different human roles involved in the system are the following:

- The ***content creator*** do the creation work to generate the content. They may work or have a contract with film studios. Once their creative work has been issued, they have no further control of what happens. The final work is generally done in post-production houses by ***post-production operators*** until validated by the ***content creator***.
- The ***packaging operators*** receive the clear content from the post-production houses and package it to the appropriate format. This includes the encoding, encryption, packaging and licence generation.
- The ***distribution operators*** receive protected content and the associated licence from the packaging houses. Their

role is to duplicate the protected content to other hard disks, and to generate new licences through the use of dedicated tools. These duplicated content and generated licences can then be shipped to the exhibitors. They may also use dedicated tools to achieve this duplication, encryption and shipping by means other than physical disks (satellite distribution, network distribution, etc.).

- The ***exhibition operators*** receive protected content and the associated KDM from the distributor they are affiliated to. They may arrange their own show playlists for their cinema by deciding which film will play in each room at a given time. They may add some automation events. They will use a cinema management system to manage the shows. They will also be responsible for putting the right files in the right places (protected content and licences). They may also provide their distributors with the – possibly filtered – log reports generated by the devices they use, and therefore give the real number of projections that have taken place.
- The ***cinema-goers*** (or audience) go to the cinema to enjoy the entertainment. They are generally not concerned about security aspects and copyright issues. Their only requirements are to watch a good film, with good sound and picture quality (and perhaps a good ice cream and no screaming children running around!).
- The ***transporters*** are generally subcontractors whose role is mainly to carry wallets between successive operators in the chain.
- The ***engineering staff*** of the manufacturers develop the material and software that are used in the digital cinema chain. They have to respect some specifications and implementation requirements in order to reach the given level of security. They have thorough knowledge of the products.

- The ***DC certification operators*** use dedicated tools to generate the certificates to be built in the devices.

Apart from the ***content creator***, all other roles should be considered for the analysis.

Processes Perimeter

We will consider three main processes of the digital cinema chain: content process, equipment process and trust management process.

The ***content process*** and ***equipment process*** are presented in Illustration 38. The first one consists of all stages in the use of a specific content, from creation and preparation to playback and audit trail generation. The latter defines the consecutive stages of a piece of equipment in the DC chain, from development to on-site installation.

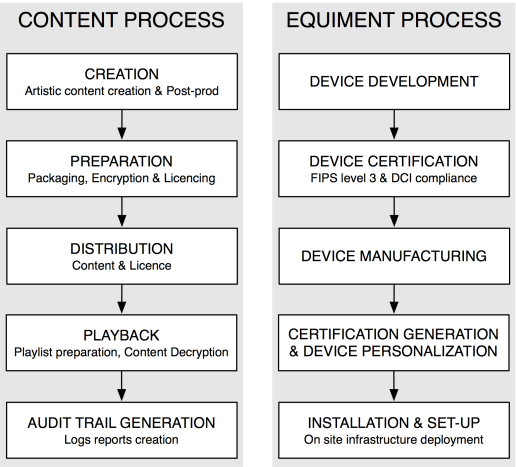


Illustration 38: Content and equipment processes

The third process is called the ***trust management process***. It is more transversal and is related to the first two processes. Illustration 39 shows the different phases in this process. Once a device needs to be trusted, it must be registered to a database through the use of a certificate. This database must be managed by adding information related to new devices in use and deleting references to devices which have been removed from the trusted environment (such as broken or obsolete devices as well as stolen devices). Trusted device lists are also established in order to simplify the treatment and generation of licences by allowing the trusted devices list of a facility to be considered rather than each specific device separately.

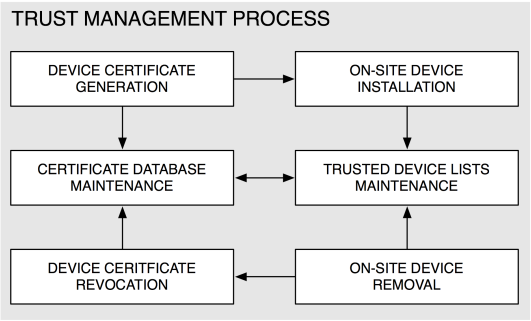


Illustration 39: Trust Management Process

The digital cinema chain also consists of several other processes which we will not consider here. For example, these include business processes or artistic creation and validation processes. Though such processes are inherent parts of the DC chain, they are not relevant from a security point of view in the framework of this analysis.

Implementation Specific Perimeters

Here, we list other types of perimeter which could be included in an extensive description of the context of an actual implementation of the digital cinema chain and its detailed

analysis. As our purpose in this chapter is to remain as generic as possible while taking into account the current tendencies of system implementation, we feel it is mandatory to mention these perimeters here, though we are not able to define them properly due to the small number of system deployments as of yet.

The ***infrastructure perimeter*** definition is entirely related to implementation. Here, we will consider that state-of-the-art wired network security is used for implementation in each facility (firewall, DMZ, etc.). The ***physical perimeter*** defines the physical boundaries of what is taken into account for the analysis. Every physical perimeter should be carefully analysed in the case of a deep analysis of an actual system in order to ensure basic physical security (locked door, physical access control, etc.). Here, we will consider both supervised and unsupervised environments: post-production facilities are an example of supervised environments and exhibition audience rooms are an example of unsupervised environments. The ***geographical perimeter*** definition could limit the analysis to countries under the same regulations in terms of digital cinema activities.

To summarise, it is worth noting that the definition of these perimeters, as defined in TAMAT, is significant for the analysis of an implemented system, while an abstract-level analysis such as the one presented in this chapter, does not have to embrace all these particular aspects.

Other Perimeter Restrictions

Several aspects of digital cinema which we did not consider relevant to our security discussions, such as business-related activities and processes, are not covered in our analysis. The “artistic content creation” activities and processes are also not considered, mainly because as long as these processes are not finished, the intermediate results of these activities are not considered as valuable assets (although the resulting scenarios,

music scores, dailies, etc. are valuable for the ongoing process of making the film).

Another aspect we have left out of the scope of this analysis is the traitor tracing activities linked to watermarking and watermark detection. Although this is obviously part of digital cinema security, we believe the current state of these technologies does not allow us to study them in an efficient way. However, it is promising and could lead to strong incentives to enforce some security policies at exhibition sites as well as in post-production facilities.

Assets identification

The Film

This is **THE** main asset of the digital cinema chain. The complete cinema chain and the whole film industry is built around this main asset, and huge amounts of money are invested in the domain. This high-value asset is the product which is basically "sold" to the final end-user who agrees to pay to watch it.

The main threat concerning the film is that a copy becomes available on file-sharing networks before or during its availability in cinemas. Therefore, the value is not only dependent on the projection itself but is dependent on the exclusivity of the content. In this respect, showing live events (sport events, concerts, conferences, etc.) provides high-value content because of the scarcity [BOM] of the content: the customer will not be able to see it anywhere else.

When a film is stolen, there are various potential uses of a pirate copy (summarised on Table 3), involving different communities:

- Generate a low-resolution copy (DivX-like) and distribute it illegally on file-sharing networks; or

- Generate a high-quality copy (HD-DVD-like) and distribute/sell it on the black market to criminal organisations that will use them to generate counterfeited illegal copies of HD-DVD or DVDs; and then
- Sell them to traditional markets (counterfeiting); or
- Sell them to underground markets;
- Generate a digital cinema quality copy (e.g. unencrypted DCP) and use it in dishonest projection cinemas (controlled by criminal organisations or in underground cinemas) without paying anything to the studios and without signing contracts with the distributors.

We can distinguish several types of clear copies, depending on:

- The presence or not of the invisible watermark. With the watermark, it is possible to know where and when the theft of content occurred. Therefore it is possible to find out who is responsible and take the appropriate actions (public announcement, legal actions, ending of commercial relations, etc.). Without the watermark, there is no way to find out where the copy took place.
- The level of quality: perfect original quality, re-encoded DVD-like or better, camcorded, etc. This level depends on the point in the chain where the copy was made (before encryption, after encryption, etc.), the category of attacker and the planned use of the pirate copy. An amateur will probably make a poor-quality re-encoding for internet distribution while an organised crime attacker would try to get a high-quality copy to be able to produce HD-DVDs and maybe unauthorised projections in underground cinemas. We can also differentiate pure digital copies from the copies which require an analogue stage, such as camcording.

Name	Original	HD	SD	<< SD
Formats	DCDM, 2k/4k	HD-DVD	DVD, DTV	Analogue DivX
Use for projection in cinemas	Yes	No	No	No
Use for HD-DVD duplication	Yes	Yes	No	No
Use for DVD duplication	Yes	Yes	Yes	No
Use for Internet distribution	Yes	Yes	Yes	Yes

Table 3: Potential pirate uses for each film format

The presence of "secondary" assets (different audio languages or subtitles) would also increase the severity of the incident because this could allow more "clients" to be addressed by making different versions.

We can rank the severity of impact of the different clear copy incidents according to a four-level scale (Table 4).

Watermark presence	Copy Quality	Level
Yes	<< SD quality	**Low**
	SD quality	**Medium**
	HD quality	**Medium**
	Original quality	**Medium**
No	<< SD quality	**High**
	SD quality	**High**
	HD quality	**Critical**
	Original quality	**Critical**

Table 4: Severity of impact of different clear copies

However, the film itself is an abstract element and is therefore not a direct asset. The film can be instantiated in different forms, at different stages in the digital cinema chain. These instantiated versions take the form of data files that may be stolen or copied: these are the real assets.

DSM

The Digital Source Master (DSM) is created in post-production. It is composed of the raw material that has to be converted and packaged specifically for digital cinema or for other purposes. There is no specification on the format and structure of the DSM. A theft at this level would therefore be difficult to exploit. However it would be very valuable, as it contains all elements of the film, and therefore would allow multiple versions to be generated for multiple markets.

DCDM

The Digital Cinema Distribution Master (DCDM) is the format that has been specified for exchanging the data essence to the encoding and playback systems. The DCDM is the last stored version of the film that is not encrypted.

However, the DCDM is based on uncompressed content. Therefore, the size of data is quite important. For example a 4K (4096 x 2160 pixels) video at 24 frames per second, with 12-bit colour components requires nearly 1GByte per second, easily leading to a file of several TBytes for a complete film.

The theft of a DCDM would require significant storage capabilities, time to transfer the copy, as well as packaging and encoding knowledge, and it would provide a very high-quality copy without any forensics.

DCP

The Digital Cinema Package (DCP) is the format used to distribute the content towards the exhibitors. The content is first compressed, then encrypted, and finally packaged. The typical size of a DCP is around 200GB, and can therefore be easily copied onto inexpensive and small external hard disks (can be hidden easily) in a reasonable amount of time.

Encryption makes use of AES cipher in CBC mode with a 128-bit key, considered as state-of-the-art cryptography.

According to the cryptography research community, a brute force attack (trying each key until getting the right one) is not realistic for at least the next 25 years [KEY]. Therefore, the DCP alone is not a valuable asset.

However, at some point in the process, the content is encoded before being encrypted. At this point, it is very vulnerable and valuable as it is the relatively small and perfect representation of the final content without any forensic marking.

DCP + Content Key

When the attacker succeeds in getting a content key that allows the film to be decrypted, he will also need a copy of the DCP. In this case, the association of the DCP and the corresponding content key is a critical asset.

Moreover, with these data, it would be possible to decrypt the DCP on a standard computer using an off-the-shelf AES algorithm implementation and obtain a perfect clear content without any watermark.

Content Key

The content key is the key that is used to encrypt and decrypt the content (symmetric-key cryptography). Alone, it seems of no use unless it is associated with the corresponding DCP. In this case, knowledge of this asset is equivalent to having a clear copy without any watermark, because it can be used to decrypt the DCP by using standard AES implementations.

Moreover, the very small size of the key allows an easy distribution over the internet. We could even imagine that dedicated websites, hosted in computer crime-friendly countries, could provide databases of content keys just as they propose software-cracking keys today and drive a market whose total value of pirated software has been estimated [PFS] at half the value of paid software.

KDM

The KDM can be understood as the licence related to a given content for a given recipient. It contains the content key in an encrypted manner so that only the intended recipient can decrypt it using its secret key.

- **KDM during construction:** At some point, the KDM needs to be generated. This is generally done in a KDM generator. As input, it requires the content key to be obtained in order to include it in the KDM itself. At this stage, the content key is vulnerable to theft. The KDM also needs to be properly generated, i.e. with no possibility for a pirated device to recover the content key included in the KDM by allowing this device to decrypt the KDM.
- **KDM during distribution:** In a given implementation, the system may use two categories of KDM for distribution or exhibition. The transformation from the former to the latter breaks the rules of end-to-end protection to the extent that at some moments, the content of the KDM is no longer under the protection of any encryption. Indeed, it needs to be decrypted first to be re-encrypted for the exhibition target.

Trust

Trust can be defined at several levels in the digital cinema chain. We will focus on the extreme levels:

- High-level trust between the players in the chain: this trust is the foundation of any commercial relation. In this domain, trust has already been established between studios, distributors and exhibitors. However, if one of them fails to implement the security models defined together, then the others' trust towards this player will be hindered and may even lead to legal action.
  Although this trust is a valuable asset from the business point of view, it is not the role of the security system to

enforce it. As pointed out in chapter 4, the security system is based on the assumption that each player in the system values this trust and considers it part of his or her basic business requirements. Financial interests are indeed so important that this trust is mandatory.

- Low-level trust in the devices as specified in the DCI: the trust model is based on public-key cryptography, and uses certificates for the different security elements in the devices. These certificates mainly ensure the confidentiality of critical assets (e.g. KDM between distributor and server or projector) during transfer from one element to another. However they are also used for other purposes (signature to verify integrity). A certificate consists in a pair of keys that are mathematically related, with the private key being kept secret while the public key can be told to everyone. The certificates are generally set by the manufacturer before the installation. If the private key leaks, then the identity of this device can easily be usurped and lead to critical asset disclosure.

Elements of trust:

- **KDM issuer private key:** This private key is used to sign the KDM. It allows a compliant device at exhibition level to verify the authenticity of the KDM.
- **Distributor and exhibitor private keys:** These private keys are necessary to decrypt the KDM in order to access the content key. To be exploited, it is necessary to get a DCP and the associated KDM for that given content and for that given target distributor or exhibitor.

To summarise, we consider that trust between the different players in the digital cinema chain is mandatory from a business point of view. As regards security, the whole system relies on a Public Key Infrastructure (PKI) and is therefore susceptible to all related issues such as leaking of all content keys previously issued to a device in the case of its private key

being revealed through any process. Again, we shall make the assumption that this PKI is well set up and reliable, in order to perform our high-level analysis. Further analysis of the implemented and deployed system should ensure that this assumption actually holds.

Log Reports

The log reports reflect all the events that occurred during the exhibition process. This allows the content owner and/or distributor to check whether the exhibitor is respecting the rules or not. The log reports are protected in integrity and continuity to prevent the modification or removal of a suspicious log event by the exhibitor.

From another point of view, the log reports also constitute an asset as the enclosed information is valuable regarding exhibitors' activities, such as trailers and advertisements played. Such information could be valuable for distributors' competition monitoring and spying, and should be kept confidential, with each distributor getting the right feedback from the exhibitors, i.e. the information related to the distributed features. No more, no less.

Scales

As mentioned above, the TAMAT method is based on qualitative scales. In this section, we will define the scales as a sorted sequence of categories.

Impact

The impact levels (***I0***..***I4***) defined in Table 5 are a direct reflection of the severity of the impact that an attack would have if it occurred. They can be evaluated in terms of an amount of money or subjective values.

Level	Impact	Description
I0	None	No Impact
I1	Low	Little economical cost
I2	Medium	Loss in revenue
I3	High	Important cost and/or revenue loss
I4	Critical	Business closes

Table 5: Impact scale definition

"Little economical cost" is considered here as an impact with small consequences on a functional level (some KDM gets lost and must be sent again, for example), implying some minimal additional cost. These costs may be seen as normal and included in the global cost of the system, even if they may be the result of some low impact attacks. "Loss of revenue" impact is the consequence of attackers aiming at accessing content "for free"; bypassing the return on investment. This is the case with low-quality copies leaked onto the internet. "Significant cost and/or loss of revenue" is the same on a bigger scale; massive DVD replication, for example. "Business closes" is the biggest impact on our scales. This is the consequence of a major breakthrough leading, for example, to the collapse of the entire public key infrastructure. In this case, the whole system has to been reconsidered, redesigned and rebuilt.

Potentiality

The potentiality levels (***P0***..***P4***) defined in Table 6 reflect how an attack may potentially occur, i.e. the chance an attacker has to succeed in this task.

Level	Potentiality	Frequency
P0	Negligible	Not possible
P1	Low	Unlikely
P2	Medium	Possible but difficult
P3	High	Feasible
P4	Critical	Repeatable

Table 6: Potentiality scale definition

Here, we distinguish between “Feasible” and “Repeatable”. Both tasks are as easy, but in the latter case, the attacker is also able to perform this task as many times as he wants. In the former case, an action can be carried out easily once but may lead to immediate countermeasures or new policy definitions so that it may be hard to succeed again.

Risk Acceptability

The asset identification process is therefore to valuate the corresponding risk acceptance according impact severity and potentiality ranking. The definition of this scale is presented in Table 7.

Level	Acceptability	Effects
RA0	Negligible Risk	No countermeasure is needed
RA1	Identified Risk	Risk is tolerated: countermeasures may be applied or not depending on cost issues
RA2	Serious Risk	Risk may endanger the business at long term: corrective actions should be planned
RA3	Critical Risk	Risk may endanger the business at short term: corrective actions must be planned and implemented in the best time frame
RA4	Insupportable Risk	Business is already endangered: Immediate corrective actions to be taken to continue business. “*Panic on board!!!*”

Table 7: Risk acceptability scale definition

Valuation Grid

The three scales presented in the previous section may be combined to build a three-dimensional valuation grid, as presented in Illustration 40.

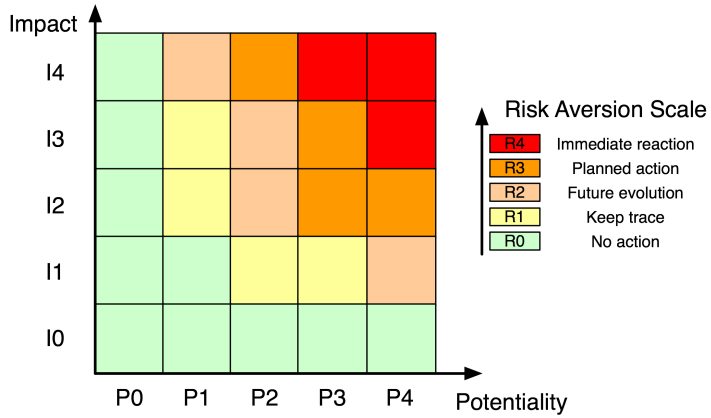


Illustration 40: Risk aversion table.

Threat Identification and Attack Trees

In this section, we begin by identifying the different attacker categories we believe are relevant for our analysis. We then focus on potential threats and discuss the actual goals of attackers in terms of each threat. If we feel that such goals do exist, we take the threat into account and present a corresponding attack tree; if not, we conclude that there is not enough incentive to mount such an attack. The attack trees for the threats under consideration are presented as a conclusion to our analysis.

Attacker Categories

We have classified the different potential attackers for a digital cinema system into 4 different categories, as detailed in this section.

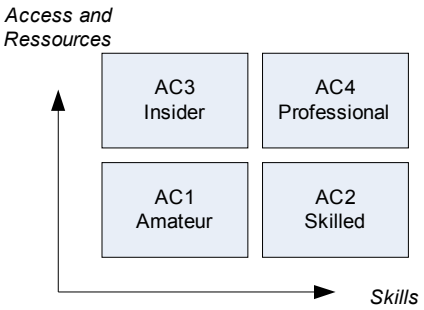


Illustration 41: Attacker categories

AC1: Amateur Attacker

Amateur attackers have no specific knowledge of components involved in the digital cinema workflow and only have access to public areas, which limits the potential attacks. However, they may gather information from the internet and pay special attention to news or forums related to hacking, vulnerabilities or technical incidents. They may thereafter corroborate all vulnerabilities to forge their attack or even reproduce a successful attack detailed on the internet. Furthermore, they may spend a long time preparing and performing an attack. They do not, however, take many risks to achieve it.

On the other hand, some amateur attackers will perform an attack only because of an opportunity that they think will not occur again (e.g. trainee dispatching post who steals a letter). Their motivation is fun, but not money. They may want to demonstrate their competence to the hacker community but are not necessarily recognised as being part of it.

Typical known attacks in this category are camcording attacks.

AC2: Skilled Attacker

Skilled attackers have good knowledge of the digital cinema system and the related technologies. They master and have access to high-end workstations, networks and hacker tools.

They are even able to develop specific tools to perform an attack. They only have physical access to public areas but their hacking skills may allow them to penetrate computer networks. However, they do not want to take too many risks.

The motivation is either money or respect from their peers. They may be members of an organised team of hackers who share knowledge and technical resources, and compete against each other.

Such an attacker will, for example, try to remove the watermark from a camcorded copy.

AC3: Insider Attacker

Insider attackers are employees of companies involved in a certain step in the digital cinema chain. They have access to high-value content and physical restricted areas. Some insiders have to perform some security critical operations such as content encryption or KDM generation. Their motivation is to steal content for themselves or for further small profit. Insiders may also collude with amateur or skilled attackers by offering them to benefit from their privileged access. As mentioned earlier, a vast majority of leakage in film production and distribution is due to insiders.

For example, an employee of an exhibitor could provide an attacker with access to the projection area, allowing him to camcord a film in a relatively controlled environment.

AC4: Organised Crime

Organised crime (Mafia) is the most powerful attacker. They operate on a large scale, and can afford multiple professional attackers, with advanced skills as well as high-level equipment. Processing time, authority and even morality are of no concern to them.

They can manage multiple complicities with cinema owners, employees, distributors and insiders at any level, and make use

of many techniques (e.g. bribing). Their motivation is money and they need to operate on a large scale to maximise their "return on investment". The main goal nowadays could be the mass release of pirate copies to compete with official DVDs. However, such organisations are very fast to adapt to new markets, and they may come up with other innovative "business models" (underground cinemas or illegal super-distribution over a large geographical area).

In the case of the distribution of live events, we could also imagine other attackers in the same category but with different motivations, i.e. terrorists. Their goal would not be to make some money but to spread terror. This could be done, for example, by replacing a planned live projection of a sports event by another content, such as a terror message.

Sinistrality

In a usual TAMAT, sinistrality should list all known attacks on the system that occurred prior to the analysis. However, there is no sinistrality known in digital cinema systems. This is mainly due to the non-existence of fully compliant and deployed systems, and also to confidentiality issues.

However, there are still parts of the sinistrality of current (analogue) cinema systems that are applicable to digital cinema. They include the following main threats:

Unauthorised copies by insiders before the print release: this threat is still applicable today. The film is not protected before its encryption. It would require the studios and post production houses to adopt content protection technologies for the whole creation process. Some solutions exist (e.g. Thomson Nexguard) but are not yet widely deployed in this domain.

Camcording by audience or insider: unlike analogue cinema, digital cinema will benefit from forensic marking to identify the leakage origin of camcorded copies. This will

increase the involvement of exhibitors in the piracy war. However, we are still at an early stage of the widespread introduction of marking modules into digital cinema devices. Previous devices therefore do not include this function.

Even if camcording is a possible attack on the cinema industry, insider attacks appear to be more of a threat. A recent study (2004) [BYE] showed that, of 285 pirated films available on the internet, 77% resulted from insider piracy activity while only 16% had been camcorded. Moreover, 78% of them came from someone in possession of a DVD-quality format of the content available, on average, 2 months before the official DVD release date. Leakage from inside production and post-production facilities is therefore not a myth but a concrete issue.

Potential Threats and Attack Trees

The potential threats we identified are sorted into 4 categories, depending on which player of the industry they are aimed at. For each threat, we discuss what an attacker's goal would be and the benefit he could expect from mounting an attack to implement this threat, if it indeed exists. Based on this discussion, we decide whether or not to consider this an actual potential threat, and present a valuated attack tree accordingly.

A Note on Valuated Attack Trees

A valuated attack tree presents the potentiality of realisation of each node of each attack tree, for each category of attacker. Here, we will consider these potentialities according to the scale defined earlier (in the “Scales” section) depicted as a number from 0 to 4 (corresponding to P0 to P4). We will use the concise notation (P_{AC1},P_{AC2},P_{AC3},P_{AC4}), to denote the potentiality valuation of a node, for each corresponding category of attacker.

To do so, one proceeds by starting from the valuation of each leaf node (there are supposed to be atomic actions an attacker should perform to gain an advantage over the system). Then, the internal nodes valuation is computed by using simple rules described as follows:

ATTACK TREE – internal nodes valuation

For each internal node:

1. if its child nodes are linked by an ***OR*** operator, the valuation of the internal node is the minimal valuation among the child node valuations. This corresponds to the assumption that the attacker will rely on the simplest way to succeed in the action described by the considered internal node, i.e. through the easiest child action.
2. if its child nodes are linked by an ***AND*** operator, the valuation of the internal node is the maximal valuation of all the child node valuations. As all child actions must be accomplished in order to get to the action described by the internal node we consider here, it is straightforward that the hardest actions determine the difficulty of the parent action.

These rules are then applied for leaf nodes to the root throughout every node of the tree. The final valuation of the whole attack is the valuation of the root node.

Eventually, a valuated attack tree allows the positioning of the corresponding threat on the valuation grid and provides information about which aspects of the attack represent the actual weakness of the system, and may suggest focusing further work on these points in order to improve the security of the whole system. These grids will be presented at the end of this chapter.

Threats on Certification Party

Certify a pirated device: As a certification authority (CA) is the foundation of a device's trust establishment, it is mandatory that only lawful devices are certified. If a pirate device – with a private key known to the attacker, for example – is certified, an attacker could use it to extract the content key from the corresponding KDM, in order to steal the content. The whole security of the system is based on the assumption that every certified device is tamper resistant and no sensitive information was or will be leaked from this device. Moreover, in an attack against the certification party database, the device may not actually need to exist, and could simply fake this existence (phantom device). *We will consider this threat.*

Estimated impact: **I2 –** Loss of revenue

Description of the AT (see Illustration 42)

The attack could be implemented in two ways. Firstly, one could try to get a pirated device certified by a lawful authority, meaning that one manages to get a recognised CA to generate a certificate for a device for which the attacker has been able to provide consistent device data (such as serial numbers of included components, for example). Secondly, an attacker could also try to get his own CA trusted. To do so, he could simply use an open implementation of a CA and acquire distributors' trust.

According to the recent SMPTE work and DCI specifications, device manufacturers will also have to play the role of certification authorities. As this is not an easy task to perform and no specific expertise in this field exists in the manufacturing industry, there is a serious risk that this operation will not be done properly, and will provide insiders with multiple weak points and flaws to exploit. Our valuation of this attack tree takes this aspect into account.

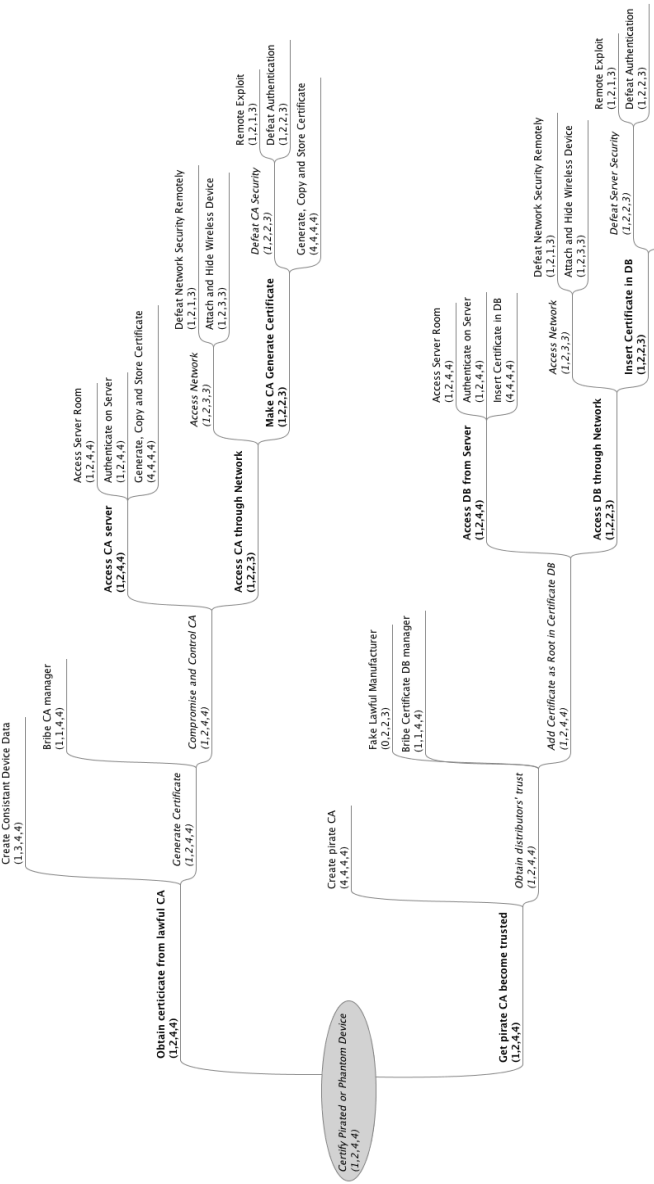


Illustration 42: Attack tree: Certify Pirated or Phantom Device

Duplicate a device: The physical duplication of a device allows double usage of this device. For example, if an exhibitor is able to duplicate all devices (server, projector, etc.) needed for a projection room, he would then be able to project a film in parallel in two rooms, with no constraints on the time or place of the second room. Moreover, duplicate log reports produced by such activity can easily be removed, leaving this activity unnoticed for the rest of the industry. However, as we said before, we believe such an attack would not benefit the exhibitor as it would jeopardise his own business. *Therefore, we will not consider this threat.*

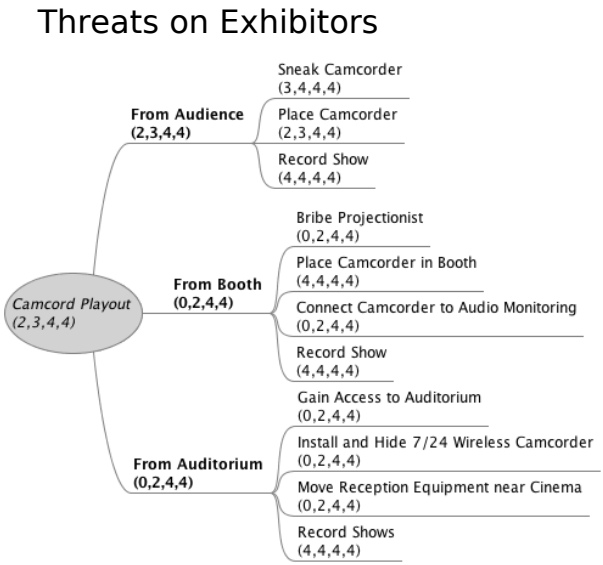


Illustration 43: Attack Tree: Camcord playout

Steal low-quality content by camcording: Already possible in the analogue cinema industry, this is a threat on the system because it makes the content available (in a low-quality format) to someone other than the stakeholders. A lot of

attackers could benefit from the implementation of such a threat. *We will therefore take it into account.*

Estimated impact: **I2 –** Loss of revenue

Description of the AT (see Illustration 43)

There are basically three different ways to camcord a film, depending on the location of the camera. Amateur and skilled attackers prefer to camcord from the audience while an insider (or organised crime) has access to a restricted area – such as the projection booth – and prefers to camcord from there. Additionally, access to the audio monitoring system leads to a better pirate copy than the one made in the audience. Parallax effects will also be less significant.

Installing some dedicated device inside the infrastructure of the cinema facility, in order to access content wirelessly, seems very difficult.

Steal high-quality content: This threat is also not DC specific as one could also steal a 35mm reel. However, the DCP format of the content, made available on a hard drive disk, greatly increases the risk linked to this threat. This format allows easier processing of the content than a 35mm reel. Moreover, data on such storage devices are available through the use of standard computers and processes such as compression, and DVD master preparation can be done on widely available – and reasonably priced – machines. The benefit of such an attack is clear: high-quality content is definitely a major asset for the piracy industry. *We will also take this threat into consideration.*

Estimated impact: **I3** – Significant cost and/or loss of revenue

Description of the AT (see Illustration 44)

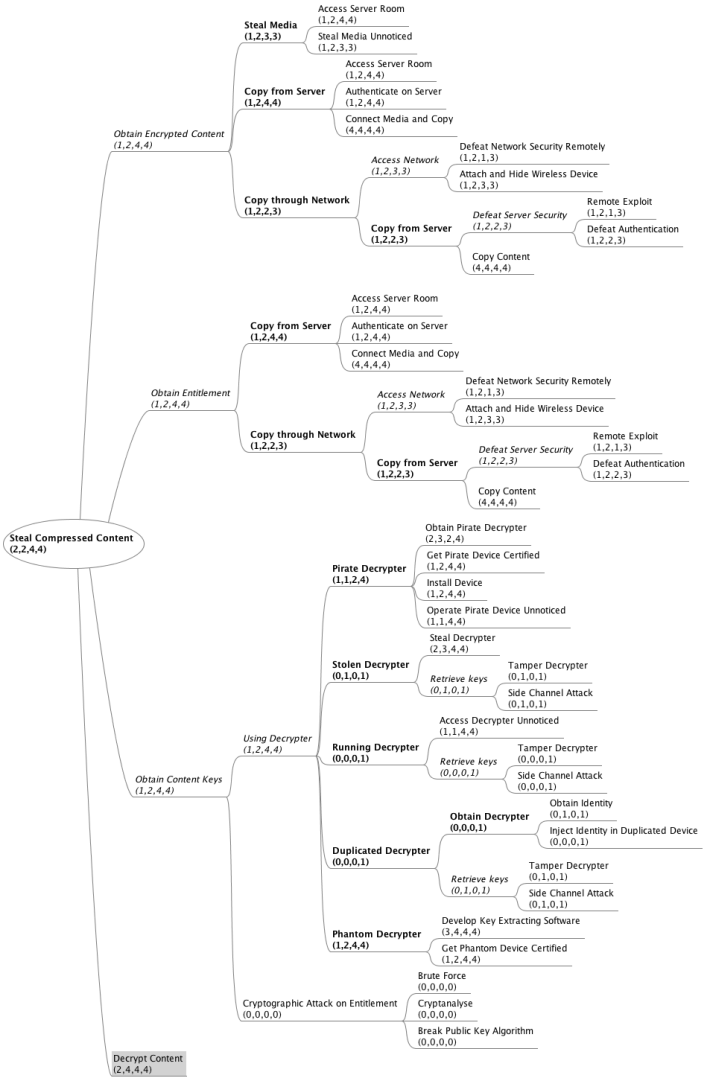


Illustration 44: Attack tree: Steal Compressed Content

Our valuation seems to reveal a paradox: obtaining the content key is as easy as obtaining protected content or entitlement. So why should one protect the content? This is due to an important human factor in the protection of the content key: the action "Get Phantom Device Certified" is the flaw in that branch. As mentioned above, we strongly believe that letting each manufacturer play the role of certification authority is a very risky approach. Dealing with these fundamental aspects of security (certificate generation and management) is not their core business and necessitates advanced knowledge of how this kind of work should be done. The probability that something will go wrong here is high.

Unreported play-out: Play-outs at the wrong facility or outside the time-window, without being reported, are a threat to the industry. We consider that standard cinema facilities could not succeed in such an attack for two main reasons. Firstly, it seems difficult to organise an unnoticed play-out with usual customers; electronic ticketing systems and published schedules of the shows will not allow a practical implementation of such events. Secondly, attempting to abuse the trust of their industry partners (producers and distributors) could seriously jeopardise their own business. It is therefore safe to assume that common sense will prevent such attacks on a large scale, in regular exhibition facilities.

Only the set-up of a widespread and illegal underground network of cinema facilities with unreported play-outs could benefit a "Mafia-like" attacker. Nevertheless, such an attack is equivalent to the full breaking of the digital cinema chain, with the use of unreported, cracked or pirated devices (servers and projectors). It would then be easier to access a clear version of the content in order to distribute and exploit it easily in this underground network. *We will therefore not consider this threat because other threat are prerequisite to this one.*

Disrupt play-out: Play-out disruptions such as show modification and play-out cancelling are, respectively, threats to the integrity of the content and to the industry. However, it seems that no one can take advantage of these attacks on a large scale. *We will not consider this threat.*

Steal/modify logs: The logs are definitely an asset for some of the players in the industry. They are signed gatherings of information that can be used for a wide range of operations, from contract enforcement to competitor spying. However, we consider that this information (even if not signed) is available by other means, which are usually cheaper and well developed, such as the press, websites and on-site monitoring of the audience in cinema facilities. Therefore, no attacker could obtain a substantial benefit from trying to mount such an attack. *We will not consider this threat.*

Threats on Distributors

Steal high-quality content: As this is currently the case in European distribution, distributors will probably be designated to provide the duplication of the DCP. Therefore, unencrypted high-quality content will be available at distribution level and will be very vulnerable as it will be handled outside a controlled environment. It is worth noting that the European situation differs from the one addressed in the DCI specifications, as the 7 major US studios have their own distribution companies; they consider distribution as part of their business and only address the exhibition level of the digital cinema chain. *We will therefore consider this threat.*

Estimated impact: **I3** – Significant cost and/or loss of revenue

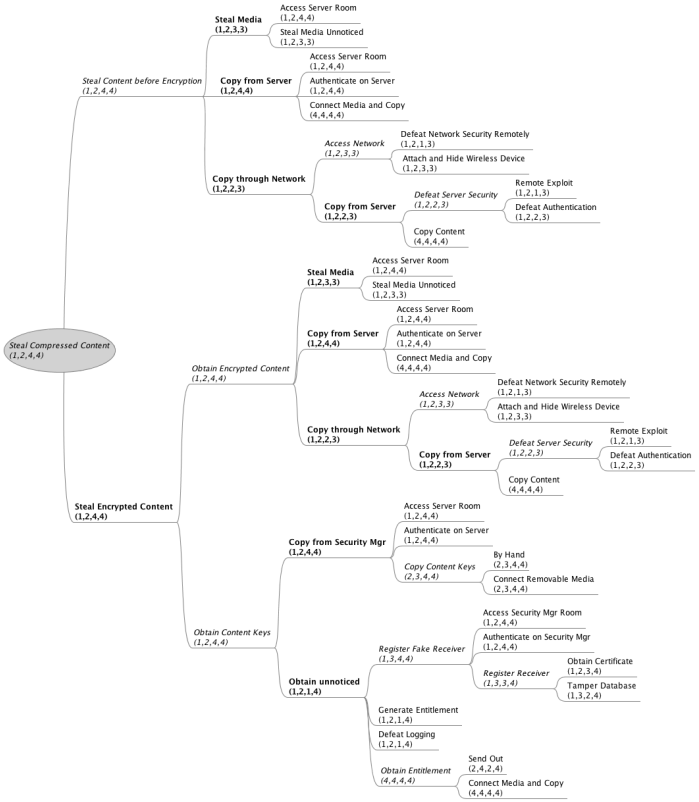


Illustration 45: Attack tree: Steal Compressed Content

Description of the AT (see Illustration 45)

Distribution may handle different types of activity, one of which is the encryption of compressed content. Therefore, we can assume the coexistence of both unencrypted and encrypted contents in distribution facilities. An attack may thus be aimed at obtaining content from one of the two. Our valuation shows that, again, insider attacks lead to equity of both approaches, as shown by the sinistrality study.

Register pirate exhibitor: By succeeding in introducing a pirate exhibitor in the distributor database (so that this distributor generates a KDM which the pirate exhibitor can decrypt and recover the content key from), the attacker can gain access to the content. This attack seems difficult to implement because it relies on the assumption that there will be little or no control when KDMs are generated at distribution level, so that one could obtain a KDM encrypted for a device for which one knows the private key. As we do believe proper care will be taken, ensuring that only certified public keys will be used for KDM encryption, *we will not take this threat into account.*

Unauthorised content editing: What would be the possible advantages an attacker could obtain from carrying out unauthorised content editing? This is hard to say. However, unauthorised editing is not specific to digital cinema; modifying a master copy is – at first sight – independent of the technology. As the master content is not encrypted, we believe that heightened access control will be implemented to secure the content from theft. The only remaining potential attacker is the distributor: some employee at the distribution site will definitely have access to clear content and could possibly be able to modify it. But, as we believe a distributor has no incentive to modify the features he distributes, *we will not consider this threat.*

Steal business information: Distributors will probably be intermediaries forwarding the logs from exhibition back to the producers. During this process, business-related information could be disclosed: logs contain confidential information about exhibitors' activities and relationships between exhibitors and distributors. An attack on the confidentiality of the logs may therefore be profitable for business analysts. However, as these logs only contain information that can also be obtained by other means (as we see in what is already happening today in this field), we consider that it would be rather complex and

hazardous to prefer mounting an attack on the logs rather than getting the information by these other means. *Therefore, we will not consider this threat.*

Prevent/disturb distribution: One might fear that the distribution of digital content may be more vulnerable than the distribution of actual physical film copies. As a matter of fact, this is not the case. The generation of a secure DCP/KDM pair is much faster than the physical duplication of a celluloid film copy; meaning that if, for any reason, a copy does not make it to the exhibitor, an alternative solution may be found in a very short time. Network (wired or wireless) distribution may eventually ensure that no such concern will stand for long, providing acknowledgement on data transfers. Therefore, we claim no widespread disturbance of distribution will occur – once the proper implementation of the distribution process is in place. *We will not consider this threat.*

Threats on Producers

Steal high-quality content: This is already possible nowadays, as this part of the industry migrated from analogue to digital processes several years ago. However, it is clear that this is a serious threat to the film industry as the high-quality content allows any pirate use: projection, (HD)-DVD duplicates, internet peer-to-peer sharing and streaming. All attackers could have an incentive in mounting an attack to achieve this goal. Moreover, the content is still "in the process of being created", meaning some operations are performed on the content (such as post-rating edition) so that the clear content is accessible, allowing very efficient insider attacks. A solution could be implemented to enforce no-leakage policies, but they would most certainly become obstacles to the smooth running of the work. *We will consider this threat.*

Estimated impact: **I3 –** Significant cost and/or loss of revenue

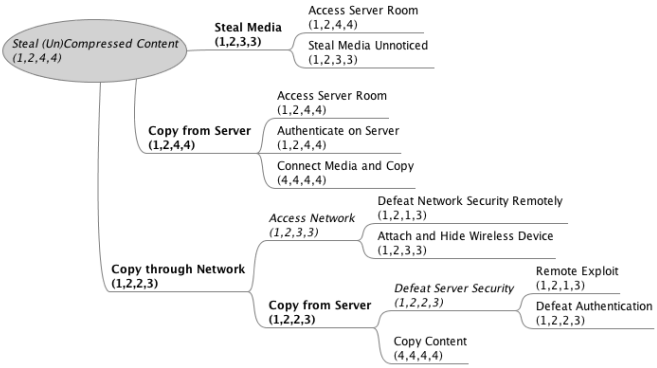


Illustration 46: Attack tree: Steal (Un)Compressed Content

Description of the AT (see Illustration 46)

Because content is still in some edition phase at production level, we assume that the content is not encrypted for the efficiency of production and post-production processes. Two approaches could lead to content theft, depending on content storage: one involves stealing media on which the content is stored, another involves making a copy of the content through a connection to the server storing the content. The latter can be done remotely if access to the server network may be obtained. Again, the valuation points out that insiders are the biggest threat to the system.

Destroy content: Digital storage may be seen as less reliable than the storage of physical copies: a few operations, executed properly, can ruin an entire digital archiving system, whereas it is difficult to annihilate an entire storage facility. However, as digital storage designers are aware of this weakness, multiple storage measures are often implemented, together with the development of several tools (such as server mirroring, Byzantine agreement protocols, etc.) in order to

ensure up-to-date backup availability in the case of a storage failure. Although this technology is now mature and very reliable, it seems contradictory to the basic principles of security, i.e. sensitive data should not be duplicated, otherwise every copy will have to be secured. This is especially true in the case of production facilities, where it is highly likely that no security at all will be applied to content, since quick and easy access to any resources is primary. As this threat is highly dependent on the implementation and architecture of the digital storage system, *we will consider this threat, and we present an attack tree assuming a basic implementation of such a system.*

Estimated impact: **I3 –** Important cost and/or revenue loss

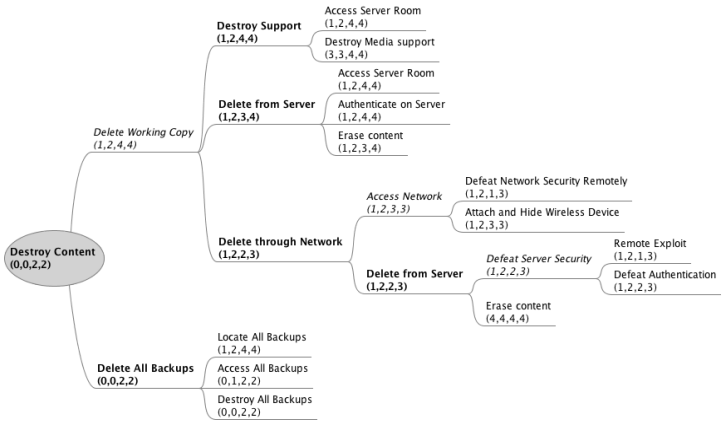


Illustration 47: Attack tree: Destroy Content

Description of the AT (see Illustration 47)

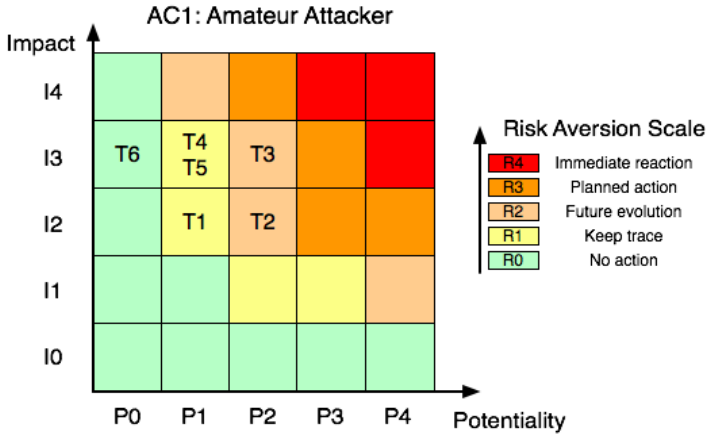
In order to delete content at the production site, an attacker has to delete the working copy of the content as well as every backup that exists. As backup may be physically stored anywhere or hosted in multiple server systems with write-only

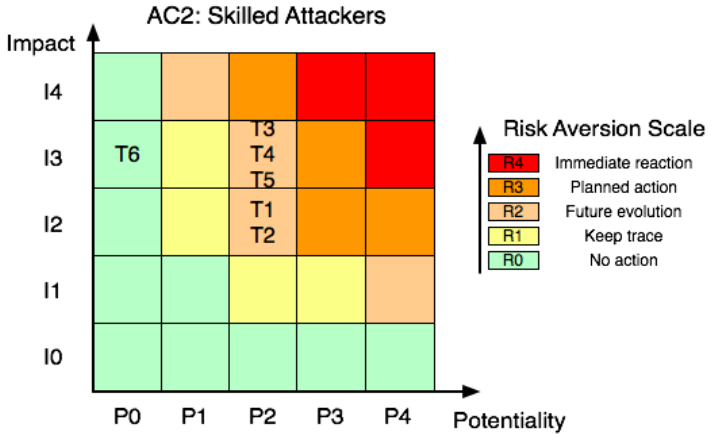
capabilities, the potentiality of success in such an enterprise would be very low for all categories of attacker, if the system is designed properly (and this is not a difficult task).

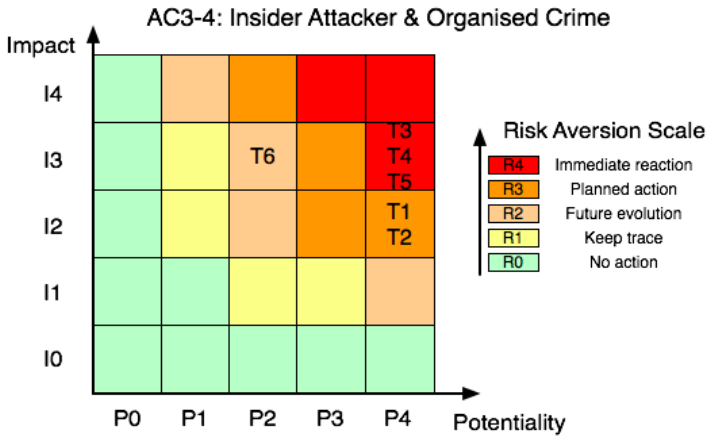
Conclusion

In this chapter, using the canvas of TAMAT, we have provided a framework and template for the analysis of digital cinema system implementation. A definition of the scope of the analysis has been given on a high level of abstraction so that our analysis template is as generic as possible. We have proposed scales of evaluation and the corresponding valuation grid. Attacker categories have been presented and an extensive list of threats has been discussed. A valuated attack tree has also been proposed for each relevant threat, providing a risk evaluation of these threats to the system. We will now end this analysis with the 4 valuation grids in a visual evaluation of the relevant threats at each defined scale.

Threat Description		**Impact**	**P_{AC1}**	**P_{AC2}**	**P_{AC3}**	**P_{AC4}**
Threat on Certification Parties						
T1	Certify pirated device	I2	P1	P2	P4	P4
Threats on Exhibitors						
T2	Steal Low Quality Content	I2	P2	P3	P4	P4
T3	Steal High Quality Content	I3	P2	P2	P4	P4
Threats on Distributors						
T4	Steal Compressed Content	I3	P1	P2	P4	P4
Threats on Producers						
T5	Steal High Quality Content	I3	P1	P2	P4	P4
T6	Destroy Content	I3	P0	P0	P2	P2


AC1: Amateur Attacker
Impact
I4
I3
I2
I1
I0
T6
T4
T5
T3
T1
T2
P0
P1
P2
P3
P4
Potentiality
Risk Aversion Scale
R4
Immediate reaction
R3
Planned action
R2
Future evolution
R1
Keep trace
R0
No action


AC2: Skilled Attackers
Impact
I4
I3
I2
I1
I0
T6
T3
T4
T5
T1
T2
P0
P1
P2
P3
P4
Potentiality
Risk Aversion Scale
R4
Immediate reaction
R3
Planned action
R2
Future evolution
R1
Keep trace
R0
No action



These valuation grids point out that insiders are the main threat to the digital cinema industry. Indeed, they have access to content and sometimes also have to perform security operations for which they have no expertise.

Organised crime will therefore try to exploit this weakness, probably by bribing insiders, in order to achieve any of the goals presented above.

Chapter 7
Beyond DCI & SMPTE: Fulfilling European Needs

Both DCI and SMPTE have played and will continue to play a key role in making digital cinema a reality. The advances in digital cinema technologies and standards, as well as economic models, have been largely driven by Hollywood. With the biggest budgets in the industry for production, promotion and distribution, Hollywood has the most to gain economically with the transition to digital.

However, as we have already seen in Chapter 2, the European cinema market is very different from the Hollywood market. So now the question is raised as to whether these standards, requirements and specifications, as well as the business and financial models, fit European needs.

In this chapter, we will try to answer these questions. We identify the specific European needs with regard to digital cinema. For those needs not fulfilled by existing standards or models, we suggest approaches to a "solution". The first section addresses the financial aspects of the transition to digital, while the other sections focus on security and technological aspects.

Financing and VPFs in European Context

Digital cinema development has two main components, namely a technological one and a business/financial one. In terms of technology, SMPTE aims at interoperability, developing international standards for digital cinema devices. The focus until now has been centred on the exhibition environment. DCI specifications, on the other hand, aim at

defining requirements for digital cinema systems. Being a Hollywood-backed initiative, these requirements fulfil their needs, mostly in terms of content security and management. We have covered both DCI specifications and SMPTE standards extensively in Chapter 5.

From a financial and business point of view, Hollywood studios support a Virtual Print Fee (VPF) model [GOD]. The basic principle of this model is to revert the savings at distributor level to financing the investment in equipment incurred by exhibitors. This financial model is inspired by Hollywood content distribution. The release of Hollywood content targets a whole geographical area simultaneously. This requires a large number of film prints, which, once used by a cinema, are destroyed or reused for *2nd-run* venues and other markets. With this distribution model, there is a direct link between a 35mm print and a venue playing a film. Since prints are rarely shared among exhibitors, under the VPF model, the savings the distributor makes for one print are reverted to one exhibitor. In Europe, Hollywood content is released in the same manner.

The VPF model is very simple and fits the reality of Hollywood distribution, which are important merits. Furthermore, it has unlocked equipment financing, thus strongly contributing to digital cinema rollout.

European Reality

But in Europe, there is also a significant amount of content released following a “use and pass” distribution model. With much smaller budgets and the linguistic fragmentation of Europe, distributors make a reduced number of 35mm prints, which are shared by exhibitors.

According to [MED], Europe produces around 1000 films per year, which enjoy a market share of between 15 and 55%, depending on the country. In contrast, US films (Hollywood

and alternative), while smaller in number, achieve market shares of between 65 and 85%.

The distribution of European and other non-US films is strongly fragmented in Europe. Linguistic, national and cultural differences make the number of distributors in Europe reach over 800. Along with this fragmentation, we have localised 35mm prints which are thus unusable in other markets, and typically low promotion budgets resulting in higher investment risk in duplication. All these factors make film releases staged, with a small number of prints being shared by many exhibitors.

Dangers of "*US-style*" Financing

Regrettably, transition to digital cinema in Europe is also driven by Hollywood content and, to a lesser extent, big-budget European films. The major digital cinema system providers and financing organisations (AccessIT/Christie, Ars Media Allience and Thomson) have plans to propose financing based on the VPF model, or already do so. XDC is a unique case, proposing financing of digital cinema equipment targeted and adapted to each country's specificities.

The reason we say "*regrettably*" is because these proponents of digital cinema financing serve the needs of Hollywood and other big-budget content, and mostly ignore European and alternative films. Under the VPF model, it is effectively the distributors who finance digital cinema equipment, through an investment organisation. These organisations happen to be system integrators and film distributors. Furthermore, they legally own and thus control the equipment.

This implies that under the VPF model, all parties have financial interests in showing content from distributors who have signed a VPF deal. And only distributors of big-budget films have the financial means to so.

All these facts represent a serious danger for both cinemas programming European and alternative productions, and for the content owners themselves.

Danger for European Cinemas

Cinemas with a significant focus on European and international productions have very few choices available for financing digital cinema equipment. Investing parties through VPF are also system integrators and content distributors. They have a lot of power over exhibitors thanks to their vertical integration (content, system ownership and management, and investment). In addition, in order to maximise VPF income, their interest is to push content from signed distributors onto screens. They are in a position of locking out content from digital screens.

Other than the VPF model and XDC operational renting and leasing, the only European initiatives come from the UK Film Council and European Union's MEDIA Programme. Both promote European cinema by asking cinemas to programme a significant percentage of European films in exchange for financing. The UKFC finances 100% of equipment and operation costs, while the EU's MEDIA Programme offers a grant of up to €7500 per screen. However, both offers are limited to a reduced number of screens.

Danger for European Distributors

European distributors, on the other hand, may not have the resources for signing VPF deals. The cost for a distributor of releasing a film in 35mm and digital under VPF is roughly the same. But with digital distribution, the distributor must pay the VPF per cinema, while with 35mm, this cost is paid only once. The differences are significant.

This fact, along with the power that vertical integrators have in choosing the content played on the screens they equip, may lead to a situation in which European content is effectively

locked out from digital screens. Clearly, European producers, distributors and alternative content cinemas need a different financing model that matches the European content distribution reality.

Towards "*European-style*" Financing

The principle of converting the savings in distribution costs into investment for digital cinema equipment is valid for the US, Europe and worldwide. Everybody in the industry agrees that those who benefit the most from the transition to digital should pay for this transition.

But a financing model for Europe needs to take two important aspects into account:

- Freedom of choice: European cinemas offer a mix of European, US and international content. Variety and freedom of choice are key to the European reality.
- Universal access to digital screens: This freedom of choice means that access to equipment must be universal and under the control of the cinema owner, and not the investor.

Europe is in urgent need of finding a successful financing model. Failure to have one will undoubtedly lead to a 2-speed digital cinema transition: the speed of Hollywood, and that of the rest of the world.

This is a huge risk for the European cinema industry. While Europe transitions to digital, digital and 35mm projectors will share screens only during the transition process. Unless digital screens are open to alternative content, the market share of European content will drop, since less screens will be available. At exhibition level, if cinemas are forced to take the VPF route, in order to maximise income, prime content will be proposed by the investor.

Extra-Key Fee

Daniel Goudineau proposes in his report “Farewell to Film? What is at Stake in Digital Projection?” [GOD] a financing model for European cinema, the extra-key-fee (EKF). The principle of EKF is the same as the VPF, i.e. to turn savings into investment. The difference is that while the VPF is founded on the print notion (soon part of the past), the EKF proposes a fee linked to the issuing of KDMs.

Goudineau's point of view is that third parties in digital cinema that finance and manage digital cinema equipment and VPF collection accumulate too much power. They are in a position to decide who plays what and when, since they control the generation of KDM.

His proposal is therefore to remove that power by having another neutral party manage the generation of KDMs and the collection and redistribution of EKFs. In addition, for European independent cinemas to keep their independence, he also proposes to create a pool of investors helping to make the switch to digital technology.

Goudineau makes his proposal as “food for thought”, without working out the details. In general, however, critics of this model claim that introducing a new party involved in the distribution of digital content unnecessarily adds complexity and carries an extra step and a potential point of failure in the generation and distribution of KDMs.

Digital Projection Fee

Although we agree with the philosophy behind the EKF model, we believe there are better ways to realise it.

We agree that vertical integration of investment, ownership, and system management, as well as the power it carries is a threat to European cinema diversity. In order to re-balance power, we believe that the investment arm must be independent of distribution, system provision and cinema

network management. The investment organisation would operate under direct or indirect control of national governments or the European Union.

Once a screen switches to digital, the investor would collect a fee from the distributor each time a film is played called a digital projection fee (DPF). Auditorium audit trails are a secure source of information supporting the collection of these fees.

With this model, independent cinemas may choose whether to buy equipment from a system provider such as AccessIT or Thomson, or go shopping for their own equipment.

The generation and management of KDMs remains in the hands of distributors, and will continue to be subject to the agreements they reach with exhibitors.

The entry barrier for an independent distributor is also minimal, since it only needs to package content which conforms to SMPTE standards and is able to generate KDMs. Once a distributor possesses the tools to do so, business continues as usual, but for digital content.

Europe Beyond DCI & SMPTE

DCI and SMPTE are to credit for the existing manufacturer and industry confidence in digital cinema technology. They have done tremendous work in allowing today's rollout of digital cinema installations. It is a good beginning, but there is still a long way to go to achieve the industry's goals of interoperable, open and secure digital cinema systems.

In this section, we present the short-, mid- and long-term technological needs. Although we adopt a European view of the needs of digital cinema, they should also apply to other non-European markets.

In the **short term**, efforts should focus on exhibitor interoperability, both in terms of system components and

standard communications with distributors. In the **mid term**, the security level found in cinemas should be extended throughout the chain, from content production to light on screen. In the **long term**, once there is a wide rollout of digital cinema installations, the effort should be focused on integrating business practices as part of the security system.

Short-Term Needs

The major providers of digital cinema equipment have so much power that they endanger the availability of installed systems to alternative and small budget productions. As we have seen, there is a financial aspect with the VPF model, as well as a technological one.

Currently available standards and specifications do not provide for full device interoperability or system openness in delivering keys to cinemas and retrieving audit trails from them.

The lack of interoperability leads to a concentration of offers by manufacturers and system providers. Manufacturers bundle different products together, such as SMS, server and SM, reducing competition on the market. Furthermore, even if there were standards providing full device interoperability, there are no compliance tests for SMPTE. Only DCI has recently defined compliance tests, partially covering SMPTE.

The lack of interoperability in key delivery and audit trail retrieval makes proprietary system providers develop solutions. Again, the result is that they retain the control over key delivery. In practice, the systems deployed are closed to any content other than that distributed by the system provider.

In order to have technically open and interoperable digital cinema systems, some developments need to be made. In our opinion, this is the first priority for European and alternative content and cinemas.

Intra-Theatre Protocols

Interoperability efforts by DCI and SMPTE have been focused on the SM downstream, that is, on the specification of protocols for Link Encryption key management and log reporting from a projector MB. However, no effort has been put into defining how KDMs are delivered to SMs, or how audit trails are retrieved from them.

KDMs are delivered to cinemas, but not directly to SMs; rather, they are probably delivered to the SMS or TMS, and sent to the SM upon content presentation. In the same manner, audit trails are to be retrieved from the SMs, probably by the SMS or TMS.

We believe SMPTE should be the organisation to develop these standards.

Extra-Theatre Messaging

According to SMPTE and DCI, extra-theatre messaging covers all exchange of information between a cinema and a distributor. Extra-Theatre Messages shall be used to deliver keys to cinemas and retrieve audit trails.

In this area, the only existing standard for ETM is the KDM. However, the KDM is an XML data structure containing content encryption keys and trust information. There are no protocols (or messages) defined for cinemas to request the delivery of KDMs, or for distributors to request the delivery of audit trails.

Standards at this level would open the system to any distributor. Furthermore, these standards are required in order to support interoperable automation. Today, KDMs are delivered to cinemas manually, via USB keys or CDs. This system does not scale well. With the number of digital cinema screens increasing exponentially, the automated delivery of KDMs will soon become a necessity.

Again, SMPTE seems to be the appropriate standards organisation to define these Extra-Theatre Messages.

Interoperability Testing

Standards are definitely the road to interoperability. However, getting a standard fully defined is a very difficult task. It is not until people start implementing and testing interoperability with other implementers that issues appear. This allows the identification of areas of the standard which were ambiguous or which need further work.

In order to have guarantees that devices and systems are 100% compliant to standards and thus interoperable with those of other manufacturers, a set of "interoperability tests" need to be defined. Device manufacturers and system integrators could then claim interoperability with SMPTE standards. This is seen as a major priority also by US exhibitors [VIC].

Mid Term Needs

After both security and interoperability have been addressed for the cinema environment, the next priority should be the extension of this security to the whole digital cinema chain.

It is important to remember that security is an end-to-end process. With 35mm content, the origin of piracy comes mainly from post-production and distribution environments, as pointed out by [BYE]. With digital content all along the chain, the risk of piracy only increases.

Camcording continues to be a piracy threat. Digital projection, however, allows the use of technologies to prevent camcording, or at least to identify where and when it happened.

We address both end-to-end security and watermarking and anti-camcording technologies in separate sections later in this chapter.

However, we want to stress the fact that the use of these technologies should be optional, and left to each content owner and distributor. Precisely, as we have argued in Chapter 1, in security, one size does not fit all. Owners of high-value content require a high level of security. However, imposing such levels of security and mandating the use of watermarking technologies, for instance, may be a problem rather than a benefit for alternative content distributors, whose priority is to get their content on the maximum number of screens.

Long Term Needs

Cinema is a 100-year old industry that accepts and assimilates changes very, very slow. The industry needs confidence and assurance before fully accepting changes. Changes need to be progressive, occurring one step at a time.

With regard to digital cinema, we are in the process of taking the first step: deploying digital projection systems and distributing content in digital form. It will take years to complete, and for industry to gain confidence in the new shape the business takes.

During the transition to digital, we expect the cinema distribution business to remain unchanged. Negotiations and deals will continue to be reached on the human level, and overseen with the help of audit trails.

Once this step is complete, the industry will be able to move towards incorporating the management and enforcement of agreements by computer systems. Today this is referred to as Digital Rights Management. However the term might be misleading, since DRM is usually associated with the consume space. We cover DRM later in this chapter.

End-to-End Digital Cinema Security

As already introduced by the security analysis of the DCI specification in previous chapters, security must be seen as an end-to-end process from production via distribution to consumption. With the specification of content encryption, key management and logging mechanisms, the security perimeter should cover the whole digital film chain from production facilities to the cinema screen. The incorporated security system is based on the "control lightly, audit tightly" approach and builds on standardised technologies such as PKI infrastructure based on X.509v3 certificates, cryptographic algorithms (RSA), forensic marking and XML Digital Signatures for security messages. It is essentially a key access and event logging management system focused on the exhibition environment.

The distribution and post-production areas are not specified much; the DCI specification therefore leaves some questions open in this area. The possible models for trust establishment and trust management are not specified, especially concerning PKI infrastructure. According to studies in France [CNC] [GOD] and Germany [FFA] there are different business models that influence the infrastructure model accordingly.

In both countries, a nationwide common database of certificates managed by a trusted independent organisation and accessible to all entities requiring access to certificates – exhibitors, distributors, installers and KDM service providers – is seen as a useful model. Certificates are supplied by installer companies or exhibitors, but the trust management – especially in the case of revocation – is not trivial.

In France, a rather centralised approach of a single service provider generating exhibitor KDMs is foreseen, whereas in Germany, several KDM service providers commissioned by

distributors would be more adapted to the current market situation. Other European countries might have a different approach somewhere in between the French, German or US model, which tends to be a rather direct relationship. The collection and aggregation of log records might also be handled differently – French exhibitors see this responsibility at their own level, while in Germany it is seen at the KDM service providers' level – acting as a kind of proxy for distributors, content providers and/or other rights owners. There is ongoing discussion in industry forums such as the *Inter-Society Digital Cinema Forum* (ISDCF) [ISD] to derive recommendations and best practices in order to satisfy the different needs of local markets.

However, to complete the trust management model, the possible feedback from log report analysis has to be taken into account in the certificate management system, no matter whether a centralised or diverse approach is taken.

From Post-Production to Exhibition

The DCI specification defines an open system that provides the necessary extensibility to cover additional enhancements in order to meet the globally different market needs. A possible new role in the distribution chain might be that of the aforementioned ‘KDM Service Provider’. It would basically be a service offering for classical distributors providing the technical complement of their legal and more business-oriented tasks. Additionally the collection and aggregation of log records from exhibitors could be another task for such a service provider to reduce the complexity for small exhibition facilities or light weight theatre management systems.

The means to realize such a model are already in place with the Key Delivery Message format as standardized by SMPTE 430-1. Further additions to the DC defined roles are not

necessary, since the system can take the roles of a Secure Processing Block providing physical protection (SPB) and an accompanying Security Manager (SM).

Insiders also Attack

The biggest threat to any system, and the most difficult to protect against, are those carried out by "*insiders*". An insider is a person with legitimate access to a system. An "*insider attack*" is an attack to a computer system executed by an insider.

This class of attacks is the most difficult to protect against, precisely because the attacker already has access to the system, thus making any perimeter protection measures such as firewalls or physical access useless.

Insider attacks are a growing concern among security professionals everywhere, to the extent that in 2004, the US Secret Services' National Threat Assessment Center did a study specifically targeting the insider threat [USS]. According to Deloitte, the human factor is the number one security issue in 2007 [DHF]. Even computer systems used by banks and financial institutions, designed to prevent this kind of attack, are vulnerable. In Chapter 4, we already presented the case of John Rusnak, a currency trader at a bank who, exploiting a flaw in the organisational model implemented by the system, caused a loss to the bank of nearly $700 million.

The cinema industry is no exception. According to [BYE], over 75% of films illegally shared on peer-to-peer networks are copies leaked from post-production and distribution. These leaks are probably more accidental than intentional: a copy is made "to show to the family", then some family member makes a copy to show to friends, who make a copy which ends up being uploaded to a peer-to-peer network.

DCI has done a big job defining security measures to prevent insider attacks, at exhibition level. Content is stored in

encrypted form, and no user has access to the decryption keys. Cinema operators must authenticate to the SMS before any show can be played. Secure audits are generated tracing all access to content. However, it has treated both production and distribution environments as "*trusted environments*" when clearly, they are not.

In order to defeat casual leakages in production and distribution environments, it would suffice to apply some basic security technologies, while respecting the security principles described in Chapter 1:

- Keep content encrypted in storage, from digital dailies to DCDM.
- Perform user authentication and manage authorisation via Role-Based Access Control or similar technologies.
- Keep accurate logs in order to detect suspicious activities.

These technologies can be integrated in systems and applications in use today without a big effort. It is a small price to pay to potentially eradicate digital content piracy before cinema release.

As for the security system controlling all access to content and the distribution of keys, we have presented a high-level trust and delegation model in Chapter 4. These models can serve as inspiration or as a basis for the development of such systems. The adherence to the security principles discussed in Chapter 1 should result in reasonably secure systems preventing casual piracy by insiders.

Log Aggregation and Redistribution

The tight auditing approach of the DCI specification is based on very specific requirements concerning the logging of events relevant to the overall security of the system. Such log records are ascertained by Security Managers and can be aggregated to

log reports – both are XML-based formats that provide a system-independent definition of structured data. There are no transport specific requirements concerning the redistribution of log records and reports. In practice, a cinema network (PSTN, ISDN, DSL, etc.) can be used as well as a redistribution via physical media, such as a USB stick. The following paragraph briefly describes the workflow of log aggregation in a multi-stage scenario.

We can assume that an infrastructure consisting of producers A, B and C has a trusted business relationship with a distributor that utilises a KDM distribution service provider and log aggregation service provider (K&L SP). The exhibition facilities X, Y and Z have a trusted business relationship with the K&L SP which provides them with the DCPs, KDMs and certificates necessary to show the digital cinema packages from A, B or C. Based on the contracts between producers and distributor, the digital cinema content is made available to the exhibitors, and the KDMs for the trusted equipment of the exhibition facility that is known to the distributor are produced and delivered. The exhibition facilities in turn send their log reports back to the distributor, who is in charge of aggregating and filtering the log reports for each specific producer or rights owner.

The distributor in this scenario acts as a kind of proxy between producers and exhibitors and is able to audit the log reports for possible misbehaviour or manipulation on behalf of an exhibitor. In the case of equipment failure, the device vendors could be informed in order to initiate a certificate revocation. This multi-stage model extended to include more than one distributor can be mapped to the present situation of the film distribution market in Germany, for example, and possibly other European countries. It stands as an example for the currently existing business relations that can be addressed by the DCI specification.

Watermarking and Fingerprinting

Digital watermarking is a technology which invisibly transports some data in the essence of a document. This section is a reminder of the key characteristics. Generic watermarking principles rely on embedding and detection.

Two-Step Process

Video watermarking is a two-step process, involving embedding in the first step and detection in the second. The watermarking system embeds a virtual barcode in the essence of each frame of the video at ingest, on servers or on live content. This invisible label can then be read regardless of video editing and format changes (analogue, digital, lossless or lossy compression).

Video watermarking technology makes it possible to mark and trace content. The data are embedded in each frame during the stamping phase. At any time, the watermark data can be read back, allowing the content to be identified and the link with the metadata or other information to be restored. This detection and reading can be carried out on sequences as short as a few minutes. The user can precisely distinguish each of the sequences detected thanks to the association of identifiers (cinema server) and date and time stamps (hour of projection) combined during the content stamping process.

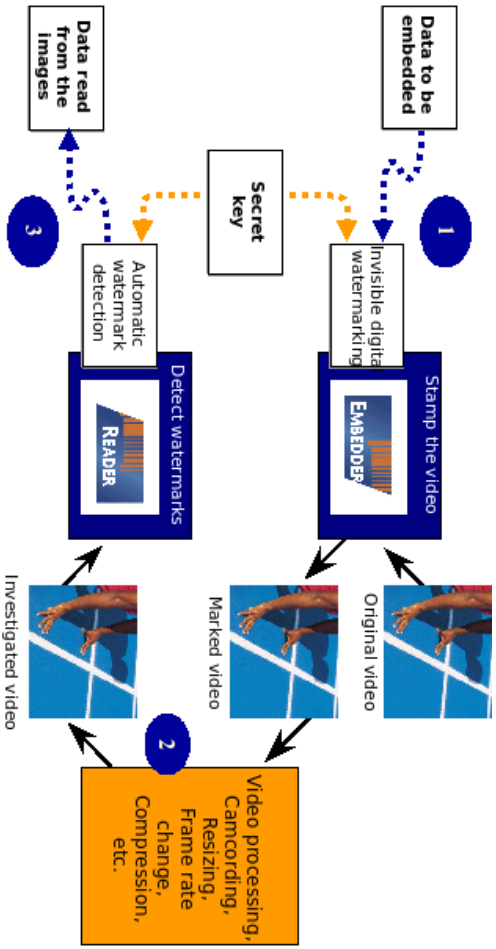


Illustration 48: Shows the processes of watermark embedding, image processing and watermark detection.

Watermark in the Image Essence

The key feature of this technology is that it is independent of the video format. The stamped data survive any number of transitions, whether digital, compressed (DCT-based such as MPEG, or Wavelet-based, for example) or analogue. The

stamping is independent of the video format because the data are embedded in the visible part of the images. The second intrinsic feature is that despite this, the picture is not affected. The stamping is invisible to the human eye, and the marking does not impact any video processing.

This is counterbalanced by the volume of information which can be carried. The capacity can be easily adapted to the use of identifiers, and time and date stamping. These types of stamping are used to establish a link with databases which include all information corresponding to video content (content description, metadata, projection server, etc.).

Watermarking is not only independent of the video format, but the information is indelible and resilient in the case of format conversion, image resolution change, cropping, compression etc.

Depending on the application, the detection process is adapted to deliver the result in the most effective way, such as oblivious detection for forensic tracking of camcorded pirate copies.

System Security: Watermark Encoding Key/Seed

In the watermarking system, the *Embedder* feature in the projector and the *Reader* devices used as an investigation station share a secret key which is used as a seed to define how the watermark is encoded in the images. An investigation station may manage a list of several watermark keys.

The management of this secret key used for watermark coding ensures independent and secure operations. Key management can be organised on a per-cinema-operator basis or on a per-studio basis, for example.

Note that the system should be designed so that the keys can be handled efficiently and securely. At rollout for a new customer, a specific series of keys should be generated.

For security reasons, the system should also allow regular updates with change of the keys in all digital cinema servers (renewability). Note that for the *Reader* devices, current and former keys should be easily made operational.

The second critical parameter is the set-up of the current date and time for the timestamp information part of the watermark data. Ideally the regular current time updates should be driven by a central server.

Watermarking as a Security Tool for Digital Cinema

In the digital cinema scope, watermarking will be used as a deterrence tool, which extends the security once the content is decrypted. It will not prevent the pirate from camcording a film; instead, it will incite cinema managers and staff to do their best to stop tentative pirates. The watermark will carry the cinema/room ID and date/time of projection. Therefore, when an illegal copy is found (for instance on a peer-to-peer network) and is suspected to come from an in-cinema capture, detection of the watermark will give the cinema name, the projection room ID, and the date and time at which the film was camcorded. If some cinema/room is often found among pirated films, or if the date/time of projection often matches a given projectionist, we can suspect either active piracy from insiders (for instance the projectionist records the film from the projection room, using a tripod, thus enabling very good quality capture), or passive negligence (cinema staff let customers come in with a camcorder). If such piracy happens too often in a given cinema, content owners (i.e. studios), backed by the watermark evidence, may deny or restrain a cinema's access to valuable content, for instance by delaying

the release of major films in the cinema. This will therefore incite cinema managers to enforce security control.

To achieve a good level of security, it is necessary to be careful about the insertion point of the watermark. To reduce the possibility of attacks, it should be applied in a secure perimeter, i.e. inside the digital cinema server. Of course it would be ideal to insert it directly on the encrypted stream to minimise potential flaws, however, no watermarking in the encrypted domain technology currently exists. Watermarking can therefore be applied on the decrypted compressed stream or on the uncompressed video. The first solution slightly reduces the possibility of attack; however, it is much less flexible, as new watermarking solutions will have to be developed if the compression standard changes or evolves. This is why we recommend applying watermarking on the uncompressed video.

Requirements

The watermarking system in digital cinema will have to meet the following requirements:

- **Invisibility**: watermarking is required to be visually transparent to the critical viewer ("golden eye"). Transparency may be controlled by using butterfly tests.
- **Forensic mark detection/recovery: r**ecovery can take up to a 30-minute content sample for positive identification.
- **Robustness**: watermarking is required to survive the following attacks:
    - Video processing attacks, such as digital-to-analogue/ analogue-to-digital conversions (including multiple D-A/A-D conversions), re-sampling and re-quantisation (including dithering and re-compression) and common signal enhancements to image contrast and colour.

  - Resizing, letter boxing, aperture control, low-pass filtering and anti-aliasing, brick wall filtering, digital video noise reduction filtering, frame-swapping, compression, scaling, cropping, overwriting, the addition of noise and other transformations.
  - Collusion - the combining of multiple videos in an attempt to make a different fingerprint or to remove it.
  - Format conversion, the changing of frequencies and spatial resolution, for example among NTSC, PAL and SECAM, into another and vice versa.
  - Horizontal and vertical shifting.
  - Arbitrary scaling (aspect ratio is not necessarily constant).
  - Camcorder capture and low bit rate compression (e.g. 500 Kbps H264, DivX, WM9, 1.1 Mbps MPEG-1).
- **Payload size** : the payload is divided into ID / timestamp. The ID is unique for each DC server so its length will be between 15 to 20 bits (32,768 to 1,048,576 unique identifiers). We choose the timestamp to change every 15 minutes and to have a periodicity of one year. Thus 16 bits are sufficient to encode date and time.
- **Interoperability:** watermarking does not require interoperability between detection systems, as the detection operation is usually performed “off line” as part of a security investigation. Multiple watermarking solutions may be qualified and will allow Media Block solutions providers to select the solution of their choice.

Anti-Camcording

According to the Motion Picture Association of America, Hollywood loses billions of dollars a year on unauthorised copies of film. While it is difficult to evaluate precisely the

real loss, any pirate copy arriving on the black market during or prior to the release window of a film in cinemas can have direct consequences on studio revenues. Furthermore, unauthorised copies can affect DVD sales and rentals, which can represent more than 60% of motion picture revenues.

Among all forms of piracy, illegal camcording in a cinema represents one major attack. Pirate DVDs, using camcorded bootlegs, can be found on the black market very soon after the opening of a film. The “pirate industry” is very quick; a film shot in a US cinema is sent to Asia for DVD replication and can be back in the US for sale within 3 or 4 days.

The quality of a camcorder copy can vary greatly. At one extreme, when the pirate has the cooperation of a cinema employee, the quality can be so good that a buyer or viewer of this content may not be aware that it is an unauthorised copy. At the other extreme, the copy can be blurry, warped, and cropped and can sometimes even contain the heads of other audience members. The audio can similarly contain auditorium and audience noise. However, if the price is low enough, the "customer" often will accept a relatively high degree of degradation.

There are three main ways to prevent illegal camcording in cinemas. The first is to detect a recording camcorder in the cinema. There are some low-tech solutions such as screening at the entry of the cinema and the use of night vision goggles. Several companies have already proposed more high-tech approaches. Researchers try to detect the electronic signature of a camcorder or identify the optic elements. This track is very challenging. To remain discreet, the pirates are creative in the art of stealth. For example, it is optically very difficult to distinguish between the lens of a camcorder and an eye glass, and it is electronically very difficult to distinguish between a running camcorder and a mobile phone. False positive detections remain a significant problem for all of these

technologies. A well-known social engineering technique is to voluntarily trigger a large amount of false positive events. After a while, the guardians will give up. Nevertheless, the potential of such approaches remains high as they have the great advantage of being independent of the projection technology and thus independent of the evolution from analogue to digital.

The second approach is to flood the camcorder sensors by emitting infra-red beam lights towards the audience. A simple countermeasure is to add the right infra-red filter on the lens, however, this approach can thwart most novice pirates.

The third technical approach to prevent unauthorised copying by camcorder is to introduce techniques that degrade the quality of the captured film. This is also a very challenging problem and we refer to this class of technical approach as "anti-camcorder" technology. Currently, a wide range of quality is traded among file sharers. Early “cams” often have very bad quality. After a while, better quality began to appear, for instance when films were recorded from the projection booth.

Anti-camcorder technology must fulfil several requirements:

- It must be transparent to legitimate spectators in the cinema; a group that includes *golden eyes* and colour blind viewers. The technology cannot introduce any perceptible artefacts into the content.
- The visible effect on a camcorder copy must be disturbing enough to discourage the pirate. For high-quality captures it may be sufficient to introduce an “illegal copy” message that is difficult to remove, but for low-quality captures the degradation must be more severe.
- It must work on all camcorders.

Once these primary requirements have technically achieved invisibility and the discouraging jamming effect, a set of

secondary goals are mandatory to transform the technology into a success story:

- Robustness to removal attempts
- Upgradeability of the system to stay ahead in the race against pirates
- Low additional cost of technology

Robustness means that the pirate must not be able to use processing tools to remove the jamming effect. If it is ever possible, then at least it must take many days. The anti-camcorder technology will be considered successful if a delay of 2 weeks is obtained.

The cost of introducing the technology can be significant. Current efforts are focused on digital projection environments, where the required signal processing technology is readily available**.** This is an advantage since most cinemas will migrate towards digital cinema in the coming years, but it is mandatory not to miss this window.

Technical solutions that modify the displayed content impact the architecture of both server and projector. They can require significant changes in the optical engine of the projector, the addressing scheme of the DMD or the data path of the server. All of these aspects require a strong collaboration with manufacturers, including Texas Instruments for DLP projectors. The manufacturers must be convinced that, in the end, the additional cost will bring final benefit for all cinema stakeholders.

We describe hereafter two distinct approaches. The first one is called the *temporal modulation* approach. It exploits one difference between the camcorder and the human eye. The camcorder is a sampling device, whereas the human eye is not. The Shannon Theorem suggests that sampling any signal at a rate less than twice the highest frequency will introduce an aliasing effect. A 60Hz camcorder can capture signals up to

30Hz without aliasing. The idea is then to introduce a signal higher than 30Hz into the film content. This is technically possible thanks to the flexibility of the addressing scheme of DLP projectors which, today, are able to display images at rates of up to 144Hz.

The first requirement for anti-camcorder technology is to remain transparent to the spectators. The frequency modulation must be chosen in a range which the eye does not perceive. The human eye is sensitive to flicker at rates below 50Hz. This leaves a range of frequencies, between 50Hz and 60Hz, in which temporal modulation can introduce aliasing on camcorder copies without being visible to the eye.

Unfortunately, the current understanding of flicker sensitivity is only correct in static conditions. When we move our eyes (by chewing popcorn for example), the continuous integration of the eye is modified and we are able to distinguish higher frequencies than the predicted 50Hz threshold. Another limitation of this approach comes from our assumptions about camcorder sampling. Some advanced camcorders have adjustable electronic shutters with variable integration periods (e.g. up to 1/15s). This will result in the introduction of a blurring effect but will also limit the amount of aliasing introduced.

In a second approach, called the *metamerism* approach, the differences between how a camcorder and the human eye process colour are exploited. The metamerism effect is the capability of the eye to perceive the same colour even if the visual spectrum that generates this perception is different. In other words, we can create the same yellow perception for the eye with a 3-primary projector (RGB) or with a 4-primary projector (RGB + Cyan primary for instance). On the other hand, camcorders have only three sensors (RGB) with fixed sensitivity curves. In general, they do not exactly “perceive” the same colour as the human eye.

The basic approach is to display part of the image with a 3-primary system and the rest with a different 4-primary system such that the eye will perceive the desired colour and the camcorder will get a disturbed image.

Again, the primary challenge is transparency. As this method relies on colour perception, the wide variation of colour perception in the population must be considered. Colour blindness introduces an interesting sub-population. Within the constraints of transparency, a successful technology will introduce significant colour distortion in the camcorder capture.

Among the secondary challenges, implementation cost can be significant. Current projection systems are based on 3 primaries and the introduction of a forth will require a modification of the optical engine of the projector. An intermediate solution could be to use a second projector, but a final solution should integrate everything in one.

In conclusion, anti-camcording technology will be an important component of the total effort to prevent piracy in the cinema business. Several approaches are possible with their corresponding technical challenges. Nothing is easy, but solutions are possible. This is a promising battlefield.

DRM and Interoperability

In the current situation of standardised DRM systems, one can observe commonalities in the underlying concepts, even if the models differ in detail. Two DRM system specifications are taken here as examples, i.e. MPEG-21 and Open Mobile Alliance (OMA) DRM. The latter is adopted by the mobile device manufacturing industry and tends to spread into other industry areas as well, while MPEG-21 DRM is still in the standardisation process of ISO/IEC.

Both DRM systems are more complicated than the security system specified by DCI, since they include a rights expression language and an ontology-like extensible model of the terms used within the rights expressions. The advantage of applying a rights expression language is that an entity A can express more precisely which rights and conditions are granted for a work to an entity B, which wants to process, consume or derive something from that work. The necessary infrastructure for trust establishment and trust management remains, and also exists in the DCI system (see [DRL]).

The impact of dealing with DRM systems that do apply rights expression languages is rather huge, since each device processing content assets needs to implement the necessary interpreters for rights expression, and must implement the rights enforcement properly. This is a complexity issue and probably a reason for having a rather pragmatic key access management solution adopted in the DCI specification in order to enable a smooth transition of the film industry into the digital age.

A possible evolution of the current DCI security system could start by facilitating more detailed rights expressions. Currently, key management allows access to be granted to a DCP within a certain period of time for a specified list of authorised devices. This is certainly sufficient in the context of DCP playback in cinemas. However, if the scope is broadened to cover the processes between production and post-production or in the archival sector, several uses can be identified, where more detailed rights expression could come into the scene. For example, the derivation from digital film works to provide other subtitles, foreign language synchronisations or versions for other digital media such as DVD, requires a specific content access and produces a contractually agreed result. The access to and usage of archived material could also benefit from a more sophisticated expression of rights.

In order to refine the expressions of granted rights, there must be a commonly agreed language for expressible rights, which could be subject to standardisation. The two abovementioned standardisation activities provide extensible specifications of such next-generation DRM systems, and in the near future we will see the extent to which they become adopted by the digital cinema industry. Interoperability between such DRM systems boils down to interoperable semantics of terms and rights expressions, and is realisable to the extent that rights expressions can be unambiguously mapped from one DRM system to another.

Archives

Archival is another important area in which film material is preserved for longer periods of time. Nowadays, the format for long-term preservation of film material is still analogue. Digital access for browsing archives, search and retrieval, etc., is based on metadata that are stored in various digital formats. The DCI specification does not address this sector at all.

Within the EDCINE project, archival follows a different preservation approach. The EDcine Digital Film Archive System is going one step further, by storing the full asset (metadata and film content resources) digitally. As an ingest format a Digital Cinema Distribution Master (DCDM) can be used among other digital resource formats. The advantage of this approach lies in the possibility to derive dissemination packages from the stored assets in various formats automatically for d-cinema, TV-mastering, online access, DVD authoring or re-processing/restoration. Another beneficial aspect is the ability to enhance the search and retrieval possibilities based on additional metadata that can be automatically derived from the content.

With respect to the protection of the intellectual property of content owners, online access and web-based browsing utilises

open standards for content protection and DRM, such as ISMAcryp and OMA v2.0. TV dissemination packages apply conditional access based on MPEG-2.

Chapter 8
Conclusions and Recommendations

The transition to digital cinema has just started. As with any other new technology market, digital cinema adoption is following a technology adoption cycle. However, as [TTD] clearly describes, today we are still in the *early adopters* phase (see Illustration 49), with a handful of cinema chains deploying digital cinema systems. This is the situation in the United States, the market for which standards, specifications and business models have been defined. Europe is lagging behind the US with regard to *crossing the chasm*, jumping from early adopters to a majority of cinemas starting the transition. There are still many issues to address, from financial and business models down to standards and specifications; many more than for the US.

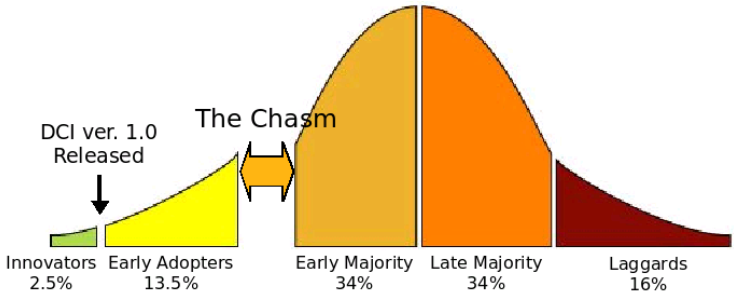


Illustration 49: Technology adoption lifecycle of digital cinema, with "the chasm" as defined by Geoffrey A. Moore [CTC].

In this chapter, we first define the priorities in Europe which will allow the chasm to be crossed, going from a phase of early adopters to that of an early majority. Then we provide a list of 10 recommendations which, in our opinion, if followed,

will help achieve a wide rollout of digital cinema systems, while allowing the projection of both blockbusters and independent films.

Top Security Priorities for European Digital Cinema

At this stage, it is unnecessary to highlight the European specificities compared with those of the US, with regard to digital cinema. The main problem Europe faces is the fact that all standards, specifications and financial and business models are inspired by Hollywood first-run films. The VPF (virtual print fee) financial model does suit the needs of European producers and distributors. The concentration of power in the hands of system providers and investors endangers the plurality and freedom of choice of the European cinema industry. The lack of a complete set of standards providing full interoperability leads to closed proprietary systems.

In order to overcome these limitations and drawbacks while preventing a 2-speed digital cinema deployment, with the first speed being that of Hollywood content, Europe must take action. In our opinion, Europe's top priorities should be:

- open, free and universal access to digital cinema installations for any type of content, from Hollywood blockbusters to small-budget European productions;
- lower entry barrier for the European and independent cinema industry to the digital cinema world, in financial (cost of equipment) and technological (availability of systems matching requirements) terms;
- to guaranteeing an acceptable level of security for the entire content production, distribution and exhibition chain.

The route to achieving these goals goes through legislation, business and financial aspects, technology and standards. The

recommendations listed below aim at fulfilling the abovementioned priorities.

Recommendations

As we have explained several times throughout this book, security cuts across many different layers, with strong inter-layer dependencies. In the area of security, more than in any other, one requires a good understanding of the *overall picture* in order to make the right decisions at a specific level.

We have grouped the recommendations below into four areas: legal and financial, organisational (trust) model, security system, and standards and specifications.

Legal and Financial

In Chapter 7 we argued that the virtual print fee model for financing digital cinema equipment is not appropriate for most content produced and distributed in Europe. In fact, it is only appropriate for big releases, while favouring distributors.

Recommendation #1

Define a European financial model which suits independent and European film distribution and exhibition. Base model on usage (extra-key fee, digital projection fee or other), rather than one inspired by 35mm distribution.

Precisely, if the lifespan of a 35mm reel is 50 projections[40], and a cinema makes 100, it only receives the VPF corresponding to one 35mm reel, not two. On the other hand, if a cinema shows a film only 25 times, the cost for the distributor is the same as for 35mm. It is a *win-win* situation for distributors, while for exhibitors it is a *win-win-but-less* situation.

[40] Assuming 3 projections on weekdays and 5 at weekends, this corresponds to 2 weeks on screen.

The relationship between financing and security exists, although indirectly. Under the VPF model, and the *de facto* concentration of investment, film distribution and system provision by organisations means that both system providers and cinemas have economical interests in showing films from distributors who have signed the VPF deal. This situation means that there is little interest in having system interoperability (openness to any content) and a lot of interest in keeping the system proprietary (under control of the system providers).

Recommendation #2

Convince the European Commission and national governments of the need to ensure open, universal and free access to digital cinema equipment in cinemas. Any type of content from any distributor or origin must be playable in any auditorium without restrictions. Push for legal and/or, financial and/or technical measures to achieve this goal.

There are numerous ways to achieve this goal, i.e. legal, financial and technical, or a combination thereof. A legal measure could, for instance, mandate that investors financing digital cinema systems must be independent of system providers and film distributors.

From a financial perspective, one can imagine to subsidising the distribution of European and independent films in digital form. In Europe, content production and distribution is heavily subsidised. It is not unreasonable to imagine extending these subsidies to digital distribution and exhibition. With a high enough subsidy, investors/distributors would have no financial interest in favouring content from their own distributors versus independent ones.

Trust Model

Any system or application should be designed to fit naturally within an organisation. Failing to do so may, and probably will, lead to users circumventing it or finding workarounds. This is critical with security systems.

In the 35mm cinema industry, all stakeholders were more or less happy with the *status quo* of the business. Distributors and exhibitors had found an equilibrium in their relationship, whereby everybody was happy. Exhibitors had (have) the freedom to move shows around, or extend *de facto* the length of their film rental agreements, as they were in possession of the film print.

This equilibrium has potentially been broken in the digital world. Now agreements are enforced by technical means. Distributors have the power to dictate on which screen and for how long a film must be played. Exhibitors are left without the freedom to reschedule shows or extend the number of weeks they play. This is bad for business (exhibitors are the most concerned by maximising audiences), and terrible for security.

Precisely, the most damaging attacks on any system are those carried out by insiders. From the perspective of a digital cinema security system, exhibitors are insiders. Under normal circumstances, an exhibitor will have no interest whatsoever in attacking the system. However, if the security systems prevent them from conducting business as usual, they become a threat. They would then be motivated to circumvent the security system in order to achieve their business goals.

Recommendation #3

Re-balance distributor/exhibitor relationship by defining agreements valid for a long period of time (months); always issue KDMs for all auditoriums in a cinema.

When one looks at the work of DCI and SMPTE, someone external to the industry might assume that exhibitors are the enemy in the fight against piracy. Exhibition is considered an untrusted environment with malicious users, while production, post-production and distribution are considered trusted environments with lawful users.

However, reality is very different [BYE]. On the one hand, exhibitors have little interest in promoting piracy, since it hurts their own business. On the other hand, over 75% of content available on illegal peer-to-peer networks appears before cinema release.

Recommendation #4

Production, post-production and distribution environments are not trustworthy. Implement security measures preventing "casual" content theft immediately: encrypt digital content, control access by user and device/application, implement extensive logging policies. Combine these with physical measures for people and media (locks, access codes) and organisational measures (chain of custody).

Digital Cinema Security Systems

One of the pseudo-definitions of a "secure system" reads: a system is secure if the cost of breaking the system is higher than the profit made by breaking it. One may argue that this definition is more or less correct and precise, or that it ignores other non-economic aspects of security. These arguments are true, yet the idea is valid.

When we look at cinema production, we see that the cost of producing a film ranges from €10,000 up to €100,000,000.

As a consequence, the impact of piracy is thus very different, and in some cases it even turns out to be a positive thing (as seen in [NTB]).

Furthermore, if we look at the programming of European cinemas, we can loosely classify cinemas into 3 categories: those playing Hollywood blockbusters and other big European or independent productions almost exclusively; those programming big (first- or second-run) and independent productions, and those focused almost exclusively on European and alternative content.

DCI specifications impose very high security requirements on digital cinema systems. Some producers claim DCI specifications provide military-grade security. This is perfectly fine, because Hollywood studios (those behind DCI specifications) invest heavily in film production and want to protect their investment; *high content value = high security cost*.

However, imposing the same security level on all digital cinema systems for all types of content is forcing some stakeholders to pay for security they do not need.

Recommendation #5

Consider security profiles other than DCI specifications. More precisely, evaluate possible alternative implementations specifically targeted at content with lesser security requirements.

Cost is definitely an entry barrier for independent producers and cinemas. We are not proposing to allow Hollywood content to be played by sub-DCI systems. Rather, we are calling for the European production industry to consider whether a lower security level (for instance, no FIPS 140-2 certification) fits their needs, and if so, to write DCI-type specifications, drafting requirements for security system implementation.

With cost being a barrier to the transition to digital for some players, open-source and free developments can remove that barrier and facilitate entry for organisations with very limited resources.

Recommendation #6

Promote, encourage and support open-source developments providing the necessary tools for small-budget distributors to participate in the digital cinema chain. These tools should provide content encryption and packaging, KDM generation and delivery, and log aggregation and retrieval.

Open-source projects for JPEG-2000[41] compression and MXF[42] packaging compliant with DCI already exist. A project along the same lines dealing with digital cinema security would undoubtedly be of help to the European cinema industry.

The lack of security specifications or implementation guidelines for production, post-production and distribution environments poses a serious risk to the cinema industry. Providers of such systems need to think about security from the outset. Security cannot just be added later: it must be built in from the beginning.

Recommendation #7

Specify, design and implement production, post-production and distribution digital cinema security systems with security implemented from the beginning. Start development process ideally by modelling an organisation through trust modelling. Respect the basic security principles at all levels, from network security to software development.

41 Open Jpeg – http://www.openjpeg.org/
42 Free MXF – http://www.freemxf.org/

Numerous tools and documentation are freely available on the internet, along with many books, providing guidance in securing networks or in developing secure systems. A very good resource is the "*Open Web Application Security Project*"[43].

Standards and Specifications

As we have seen in the threat analysis in Chapter 6, one of the biggest threats to the security of digital cinema comes from the fact that device certification authorities are to be implemented and managed by device manufacturers themselves.

Furthermore, the fact that Digital Cinema Certificates are a constrained and overloaded version of the X.509 version 3 standard makes them unmanageable by available solutions, thus requiring specific developments.

Recommendation #8

Re-evaluate the DCI certification model. Study possibility of delegating certificate and PKI management to professional certification authorities.

Security in general is difficult, and the business of certification authority even more so. There is a lot at stake with digital cinema security, and certificates are the basis upon which security is built. The management of certificates should be left to professional organisations using proven solutions.

As we have already explained, the digital cinema systems deployed today are effectively locked and under the control of the system provider. There is a financial component to this locking, but also a technological one. Precisely, the fact that there is a lack of standards providing interoperable KDM request and delivery, and audit trail request and retrieval,

[43] OWASP – http://www.owasp.org/

along with a lack of a fully specified audit trail standard, leads to proprietary solutions in these areas.

Recommendation #9

Create the necessary standards and/or specifications guaranteeing open and universal access to cinema systems. Specifically, define protocols for KDM request and delivery; interoperable log record contents.

But there is still more work to be done on standardisation. Today we are in a situation in which DCI specifications and SMPTE standards have built enough industry confidence in technology and prospects of interoperability to initiate digital cinema deployments.

Recommendation #10

Achieve a competitive digital cinema equipment market by continuing work at SMPTE level to create the missing standards providing full device interoperability. Encourage the creation of digital cinema standards compliance tests guaranteeing full device interoperability.

Interoperability is key to competitive markets in which manufacturers compete over functionality sets and costs. Without interoperability, the cost of digital cinema systems remains artificially high, and can represent yet another barrier to the entry of European players with very limited financial resources.

References

[428-1] “SMPTE 428-1 Digital Cinema Distribution Master – Image Characteristics.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2006

http://store.smpte.org/product-p/smpte%200428-1-2006.htm

[428-2] “SMPTE 428-2 Digital Cinema Distribution Master – Audio Characteristics.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2006

http://store.smpte.org/product-p/smpte%200428-2-2006.htm

[428-3] “SMPTE 428-3 Digital Cinema Distribution Master – Audio Channel Mapping and Channel Labelling.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2006

http://store.smpte.org/product-p/smpte%200428-3-2006.htm

[428-7] “SMPTE 428-7 Digital Cinema Distribution Master – Subtitle.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2007

http://store.smpte.org/product-p/smpte%200428-7-2007.htm

[429-3] “SMPTE 429-3 Digital Cinema Packaging – Sound and Picture Track File.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2007

http://store.smpte.org/product-p/smpte%200429-3-2007.htm

[429-4] “SMPTE 429-4 Digital Cinema Packaging – MXF JPEG 2000 Application.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2006

http://store.smpte.org/product-p/smpte%200429-4-2006.htm

[429-6] “SMPTE 429-6 Digital Cinema Packaging – MXF Track File Essence Encryption.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2006

http://store.smpte.org/product-p/smpte%200429-6-2006.htm

[429-7] “SMPTE 429-7 Digital Cinema Packaging – Composition Playlist.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2006

http://store.smpte.org/product-p/smpte%200429-7-2006.htm

[429-8] “SMPTE 429-8 Digital Cinema Packaging – Packing List.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2007

http://store.smpte.org/product-p/smpte%200429-8-2007.htm

[429-9] “SMPTE 429-9 Digital Cinema Packaging – Asset Mapping and File Segmentation.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2007

http://store.smpte.org/product-p/smpte%200429-9-2007.htm

[430-1] “SMPTE 430-1 Digital Cinema Operations – Key Delivery Message.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2006

http://store.smpte.org/product-p/smpte%200430-1-2006.htm

[430-2] “SMPTE 430-2 Digital Cinema Operations – Digital Certificate.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2006

http://store.smpte.org/product-p/smpte%200430-2-2006.htm

[430-3] “SMPTE 430-3 Digital Cinema Operations – Generic Extra-Theater Message Format.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2006

http://store.smpte.org/product-p/smpte%200430-3-2006.htm

[431-1] “SMPTE 431-1 Digital Cinema Quality – Screen Luminance Level, Chromaticity and Uniformity.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2006

http://store.smpte.org/product-p/smpte%200431-1-2006.htm

[431-2] “RP 431-2 Digital Cinema Quality – Reference Projector and Environment.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2007

http://store.smpte.org/product-p/rp%200431-2-2007.htm

[432-1] “EG 432-1 Digital Source Processing – Color Processing for D-Cinema.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2007

http://store.smpte.org/product-p/eg%200432-1-2007.htm

[432-2] “EG 432-6 Digital Source Processing – D-Cinema Low Frequency Effects (LFE) Channel Audio Characteristics.” *SMPTE Technology Committee DC28 Digital Cinema*. The Society of Motion Picture and Television Engineers. 2007

http://store.smpte.org/product-p/eg%200432-2-2006.htm

[AE3] "AES/EBU." *Wikipedia, The Free Encyclopedia*. 27 Oct 2007, 11:34 UTC. Wikimedia Foundation, Inc. 30 Oct 2007

http://en.wikipedia.org/wiki/AES3

[AES] "Advanced Encryption Standard." *Wikipedia, The Free Encyclopedia*. 18 Oct 2007, 07:55 UTC. Wikimedia Foundation, Inc. 27 Oct 2007

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[ARN] J. Kelsey et al. Cryptanalyctic Attacks on Pseudorandom Number Generators. In *Fast Software Encryption, Fifth International Workshop Proceedings (March 1998)*, Springer-Verlag, 1998, pp. 168-188.

http://www.schneier.com/paper-prngs.pdf

[BCM] "Block cipher modes of operation." *Wikipedia, The Free Encyclopedia*. 13 Oct 2007, 15:09 UTC. Wikimedia Foundation, Inc. 7 Nov 2007

http://en.wikipedia.org/wiki/
Block_cipher_modes_of_operation

[BOM] O. Bomsel, G. Le Blanc. *Dernier tango argentine, le cinéma face à la numérisation*, Les Presses de l'École des Mines de Paris, 2002

[BOS] “Once Again, Online Availability Doesn't Dampen Box Office for Simpsons Movie.” *Techdirt, The Insight Company for the Information Age*, 31 Jul 2007. Techdirt Inc.

http://www.techdirt.com/articles/20070731/095311.shtml

[BRE] P. Bresciani, A. Perini. Tropos: An Agent-Oriented Software Development Methodology. In *Journal of Autonomous Agents and Multiagent Systems*, vol. 8, pp. 203-236, 2004

http://citeseer.ist.psu.edu/bresciani02tropos.html

[BSE] “First $4bn summer for US cinema”, *BBC News International*, 27 Aug 2007, BBC – British Broadcasting Corporation

http://news.bbc.co.uk/2/hi/entertainment/6965203.stm

[BYE] S. Byers et al. Analysis of Security Vulnerabilities in the Movie Production and Distribution Process. In *Telecommunications Policy*. Vol. 28, Issues 7-8, Aug.-Sept. 2004, pp 619-644

http://lorrie.cranor.org/pubs/drm03-tr.pdf

[CNC] *Digital projection in cinema* (Provisional document), Centre National de la Cinématographie (CNC), June 2007

http://www.cnc.fr/CNC_GALLERY_CONTENT/DOCUMENTS/UK/publications/digital_projection.pdf

[CCP] “The Common Criteria Project”

http://www.commoncriteriaportal.org/

[CCW] "Common Criteria." *Wikipedia, The Free Encyclopedia*. 12 Aug 2007, 16:29 UTC. Wikimedia Foundation, Inc. 18 Sep 2007

http://en.wikipedia.org/wiki/Common_Criteria

[CHF] "Cryptographic hash function." *Wikipedia, The Free Encyclopedia*. 1 Nov 2007, 15:39 UTC. Wikimedia Foundation, Inc. 6 Nov 2007

http://en.wikipedia.org/wiki/Cryptographic_hash_function

[CIV] "Initialization vector." *Wikipedia, The Free Encyclopedia*. 21 Aug 2007, 09:36 UTC. Wikimedia Foundation, Inc. 7 Nov 2007

http://en.wikipedia.org/wiki/Initialization_vector

[CSE] "Computer security." *Wikipedia, The Free Encyclopedia*. 20 Nov 2007, 22:52 UTC. Wikimedia Foundation, Inc. 25 Nov 2007

http://en.wikipedia.org/wiki/Computer_security

[CRD] “Camcording or Recording Devices in Movie Theaters.” *National Conference of State Legislatures*, 2007, The National Conference of State Legislatures Foundation.

http://www.ncsl.org/programs/lis/CIP/tape-in-theaters0304.htm

[CRL] “RFC3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.” *IETF Networking Group*, Internet Engineering Task Force, Apr 2002

http://tools.ietf.org/html/rfc3280

[CRY] "Cryptography." *Wikipedia, The Free Encyclopedia*. 18 Oct 2007, 01:14 UTC. Wikimedia Foundation, Inc. 19 Oct 2007

http://en.wikipedia.org/wiki/Cryptography

[CTC] G. Moore. *Crossing the Chasm*, ISBM 0-88730-717-5, Harper Business, 1991

[CTP] “Digital Cinema System Specification Compliance Test Plan ver. 1.0” *Digital Cinema Initiatives*, 17 Oct 2007, Digital Cinema Initiatives, LLC.

http://www.dcimovies.com/DCI_CTP_v1_0.pdf

[DCC] Digital Cinema Initiatives, LLC

http://www.dcimovies.com/

[DCE] “Errata to DCI Digital Cinema System Specifications ver. 1.1” *Digital Cinema Initiatives*, 27 Aug 2007, Digital Cinema Initiatives, LLC.

http://dcimovies.com/errata/v1_1/DCI_Errata_1-55_20070827.pdf

[DCI] “DCI Digital Cinema System Specification ver. 1.1”, *Digital Cinema Initiatives*, 12 Apr 2007, Digital Cinema Initiatives, LLC.

http://dcimovies.com/DCI_DCinema_System_Spec_v1_1.pdf

[DCO] “DCI Digital Cinema System Specification ver. 1.0”, *Digital Cinema Initiatives*, 20 Jul 2005, Digital Cinema Initiatives, LLC.

http://dcimovies.com/v1errata/
DCI_Digital_Cinema_System_Spec_v1.pdf

[DHF] “Deloitte: Human factor is No. 1 IT security issue.”, *SC Magazine for IT Security Professionals*, Haymarket Media Inc. 20 Sept 2007

http://www.scmagazineus.com/Deloitte-Human-factor-is-No-1-IT-security-issue/article/35758/

[DRL] X. Orri et al. Digital rights language support for evolving digital cinema requirements, In *SPIE: Security and Watermarking of Multimedia Contents V*, 2003, pp.563-573

[DSI] "Digital signature." *Wikipedia, The Free Encyclopedia*. 18 Oct 2007, 01:16 UTC. Wikimedia Foundation, Inc. 19 Oct 2007

http://en.wikipedia.org/wiki/Digital_signature

[DWW] "Digital watermarking." *Wikipedia, The Free Encyclopedia*. 17 Sep 2007, 15:50 UTC. Wikimedia Foundation, Inc. 18 Sep 2007

http://en.wikipedia.org/wiki/Digital_watermarking

[EDC] *European Digital Cinema Forum*

http://www.edcf.net/

[EOF] “The Grand Unified Theory of the Economics of Free”, *Techdirt, The Insight Company for the Information Age*, 3 May 2007. Techdirt Inc.

http://www.techdirt.com/articles/20070503/012939.shtml

[ETH] "Ethernet." *Wikipedia, The Free Encyclopedia*. 27 Oct 2007, 01:17 UTC. Wikimedia Foundation, Inc. 29 Oct 2007

http://en.wikipedia.org/wiki/Ethernet

[EYU] E. Yu, *Modelling Strategic Relationships for Process Reengineering*, PhD Thesis, Dept. of Computer Science, University of Toronto, 1995

[FFA] S. Fößel et al. *System Specification for Digital Cinema in Germany*, Fraunhofer Institute, commissioned by German Federal Film Board, 30 March 2007 *[In German]*

http://www.ffa.de/start/download.php?file=/digitaleskino/FFA_Systemspezifikationen_V1.01.pdf

[FIP] Federal Information Processing Standards, Computer Security Division, National Institute of Standards and Technology.

http://csrc.nist.gov/publications/fips/

[FIR] D.H. Deans. Film Industry Revenue: Past, Present and Future. In *Digital Lifescapes Blog*. Sept 14, 2006

http://dhdeans.blogspot.com/2006/09/film-industry-revenue-past-present.html

[FIW] "FIPS 140." *Wikipedia, The Free Encyclopedia*. 28 May 2007, 14:01 UTC. Wikimedia Foundation, Inc. 18 Sep 2007

http://en.wikipedia.org/wiki/FIPS_140

[FJA] A. Fuchs. Digital Alternative. In *Film Journal International*, December 19, 2006

http://www.filmjournal.com/filmjournal/search/article_display.jsp?vnu_content_id=1003523541

[FJB] B. Mead. Europe Eyes Digital. In *Film Journal International*, June 25, 2007

http://www.filmjournal.com/filmjournal/search/article_display.jsp?vnu_content_id=1003603161

[FJC] A. Fuchs. Digital Delight. In *Film Journal International*, February 13, 2007

http://www.filmjournal.com/filmjournal/search/article_display.jsp?vnu_content_id=1003545063

[FJD] B. Mead. ShoWest 2007 The Big Picture. In *Film Journal International*, March 13, 2007

http://www.filmjournal.com/filmjournal/search/article_display.jsp?vnu_content_id=1003557377

[FJE] A. Fuchs. Digital Diplomat. In *Film Journal International*, November 27, 2006

http://www.filmjournal.com/filmjournal/search/article_display.jsp?vnu_content_id=1003438757

[FJF] D. Toumarkine. Next Year's Model. In *Film Journal International*, August 21, 2007

http://www.filmjournal.com/filmjournal/search/article_display.jsp?vnu_content_id=1003628487

[FJG] D. Toumarkine. Book'em! Independent Film Buyers Help Sustain Cinema Biz. In *Film Journal International*, March 12, 2007

http://www.filmjournal.com/filmjournal/search/article_display.jsp?vnu_content_id=1003556930

[FVA] “Film, video and audio-visual distribution 2004/2005.” S*tatistics Canada – The Daily*, Canada's Statistical Agency, Aug 28, 2006

http://www.statcan.ca/Daily/English/060828/d060828a.htm

[GBE] "Gigabit Ethernet." *Wikipedia, The Free Encyclopedia*. 27 Oct 2007, 20:55 UTC. Wikimedia Foundation, Inc. 29 Oct 2007

http://en.wikipedia.org/wiki/Gigabit_ethernet

[GIA] P. Giorgini et al. Security and Trust Requirements Engineering. In Foundations of Security Analysis and Design III – Tutorial Lectures, LNCS 3655, pp. 237-272, Springer-Verlag GmbH, 2005

http://citeseer.ist.psu.edu/763869.html

[GIB] P. Giorgini et al. Modelling Security and Trust with Secure Tropos. In *Integrating Security and Software Engineering: Advances and Future Vision*. pp. 160-189, IDEA Group, 2006

http://dit.unitn.it/~zannone/publication/gior-mour-zann-06-IDEA.pdf

[GOD] D. Goudineau *FAREWELL TO FILM? What Is at Stake in Digital Projection?*, commissioned by CNC, Centre National de la Cinématographie, August 2006.

http://www.cnc.fr/Site/Template/T1.aspx?SELECTID=1921&ID=1226&t=1 *[In French]*

http://www.cnc.fr/Site/Template/T1.aspx?SELECTID=2324&ID=1540&t=1 *[In English, short version]*

[HSD] A. Thomas. Half of Screens to be Digital by 2013. In *Variety*, November 12, 2007

http://www.variety.com/article/VR1117975781.html

[IDC] M. Karagosian. Introduction to Digital Cinema. *MKPE Consulting LLC Whitepaper*, Dec 2003

http://mkpe.com/publications/digital_cinema/insasia/introduction_to_dc.php

[ISD] *Inter-Society Digital Cinema Forum*, 19 Sep 2007, Inter-Society for the Enhancement of Cinema Presentation, Inc.

http://www.isdcf.com/

[ISE] "Information security." *Wikipedia, The Free Encyclopedia*. 24 Nov 2007, 15:55 UTC. Wikimedia Foundation, Inc. 25 Nov 2007

http://en.wikipedia.org/wiki/Information_security

[JAM] E. Hansen. "Jamming Camcorders in Movie Theaters." In *C|Net News.com*, 10 Oct 2002. CNET Networks Inc.

http://www.news.com/2100-1023-961484.html

[JP2] JPEG 2000 committee

http://www.jpeg.org/jpeg2000/

[JLJ] "Jon Lech Johansen." *Wikipedia, The Free Encyclopedia*. 15 Sep 2007, 03:54 UTC. Wikimedia Foundation, Inc. 18 Sep 2007

http://en.wikipedia.org/wiki/Jon_Lech_Johansen

[JPW] "JPEG 2000." *Wikipedia, The Free Encyclopedia*. 25 Sep 2007, 23:40 UTC. Wikimedia Foundation, Inc. 3 Oct 2007

http://en.wikipedia.org/wiki/Jpeg2000

[JRU] S. Burke. Currency Exchange Trading and Rogue Trader John Rusnak. In *Concept*, Villanova University, 2004

http://www.publications.villanova.edu/Concept/2004/John_Rusnak.pdf

[KEY] D. Giry, J.-J. Quisquater, *Cryptographic Key Length Recommendation Website*, version 17.10, 19 Nov 2007

http://www.keylength.com/

[KLV] "KLV." *Wikipedia, The Free Encyclopedia*. 16 Oct 2007, 05:08 UTC. Wikimedia Foundation, Inc. 24 Oct 2007

http://en.wikipedia.org/wiki/Klv

[MAS] F. Massacci and N. Zannone. Detecting Conflicts between Functional and Security Requirements with Secure Tropos: John Rusnak and the Allied Irish Bank. In *Social Modelling for Requirements Engineering.* MIT Press, 2006

http://citeseer.ist.psu.edu/massacci06detecting.html

[MED] "European Cinema Yearbook 2007 Advanced Edition", *Cinema D'Europa Media Salles*, 18 Oct 2007, MEDIA Salles project – EU MEDIA Programme.

http://www.mediasalles.it/ybk07adv/

[MKF] "Digital Cinema Frequently Asked Questions" *MKPE Consulting*, 1 Sep 2007, MKPE Consulting, LLC.

http://www.mkpe.com/digital_cinema/faqs.php

[MMO] "MPAA Moves on to Making Up Stats About Camcording in the UK Market." *Techdirt, The Insight Company for the Information Age*, 5 Sep 2007. Techdirt Inc.

http://www.techdirt.com/articles/20070905/233533.shtml

[MMU] "Does the MPAA Simply Make Up Piracy Numbers Out of Thin Air?." *Techdirt, The Insight Company for the Information Age*, 2 May 2007. Techdirt Inc.

http://www.techdirt.com/articles/20070502/173805.shtml

[MOF] M. Karagosian. Motivating Factors. *MKPE Consulting LLC Whitepaper*. Feb 2004

http://mkpe.com/publications/digital_cinema/insasia/motivating_factors.php

[MOU] H. Mouratidis, P. Giorgini. Enhancing Secure Tropos to Effectively Deal with Security Requirements in the Development of Multiagent Systems. In *Proceedings of the 1st International Workshop on Safety and Security in Multiagent Systems*, *AAMAS 2004*, New York, 2004

http://homepages.uel.ac.uk/H.Mouratidis/Mouratidis_SASEMAS_CR.PDF

[MXW] "Material Exchange Format." *Wikipedia, The Free Encyclopedia*. 4 Sep 2007, 05:14 UTC. Wikimedia Foundation, Inc. 3 Oct 2007

http://en.wikipedia.org/wiki/MXF

[NTB] "Piracy isn't THAT bad and they know it", *Release Weblog*, 14 Nov 2007

http://www.rlslog.net/piracy-isnt-that-bad-and-they-know-it/

[NYP] "Radiohead Tells Fans to Name Their Own Price for Latest Album Downloads; Gives Them a Reason to Pay", *Techdirt, The Insight Company for the Information Age*, 1 Oct 2007. Techdirt Inc.

http://www.techdirt.com/articles/20070930/214524.shtml

[OCSP] "RFC2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP." *IETF Networking Group*, Internet Engineering Task Force, Jun 1999

http://tools.ietf.org/html/rfc2560

[OPG] *OWASP Guide 2.1 draft*, Open Web Application Security Project, Feb 2006. OWASP Foundation

http://www.owasp.org/index.php/OWASP_Guide_Project#OWASP_Guide_3.0_.28Current.29

[PFS] "*2005 US Piracy Fact Sheet*", Motion Picture Association of America, 2006

http://www.mpaa.org/USPiracyFactSheet.pdf

[PKC] "Public-key cryptography." *Wikipedia, The Free Encyclopedia*. 16 Oct 2007, 12:44 UTC. Wikimedia Foundation, Inc. 19 Oct 2007

http://en.wikipedia.org/wiki/Public-key_cryptography

[PKIX] "PKIX – Public Key Infrastructure (X.509) Group." *IETF Working Groups*, Internet Engineering Task Force, 26 Sep 2007

http://www.ietf.org/html.charters/pkix-charter.html

[POC] G. MacDonald. Pirates of the Canadians. In *Saturday's Globe and Mail*, 13 Jan 2007

http://www.theglobeandmail.com/servlet/story/RTGAM.20070112.wpirates13/BNStory/Entertainment/home

[RKM] "NIST 800-57 Recommendation for Key Management – Part 1: General." *NIST Special Publication*, National Institute of Standards and Technology, May 2006

http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf

[RSA] "RSA." *Wikipedia, The Free Encyclopedia*. 28 Oct 2007, 16:13 UTC. Wikimedia Foundation, Inc. 4 Nov 2007

http://en.wikipedia.org/wiki/Rsa

[SCA] "Side channel attack." *Wikipedia, The Free Encyclopedia*. 24 Oct 2007, 03:12 UTC. Wikimedia Foundation, Inc. 19 Nov 2007

http://en.wikipedia.org/wiki/Side_channel_attack

[SEC] "Security." *Wikipedia, The Free Encyclopedia*. 23 Nov 2007, 19:33 UTC. Wikimedia Foundation, Inc. 25 Nov 2007

http://en.wikipedia.org/wiki/Security

[SEN] "Security engineering." *Wikipedia, The Free Encyclopedia*. 9 Nov 2007, 21:16 UTC. Wikimedia Foundation, Inc. 25 Nov 2007

http://en.wikipedia.org/wiki/Security_engineering

[SHA] "SHA hash functions." *Wikipedia, The Free Encyclopedia*. 1 Nov 2007, 20:37 UTC. Wikimedia Foundation, Inc. 6 Nov 2007

http://en.wikipedia.org/wiki/SHA_hash_functions

[SIC] "Amazingly, Downloadability of Michael Moore's Film Didn't Appear to Hurt Box Office", *Techdirt, The Insight Company for the Information Age*, 3 Jul 2007. Techdirt Inc.

http://www.techdirt.com/articles/20070703/124746.shtml

[SIM] “Once Again, Online Availability Doesn't Dampen Box Office for Simpsons Movie”, *Techdirt, The Insight Company for the Information Age*, 31 Jul 2007. Techdirt Inc.

http://www.techdirt.com/articles/20070731/095311.shtml

[SKA] "Symmetric-key algorithm." *Wikipedia, The Free Encyclopedia*. 14 Oct 2007, 23:06 UTC. Wikimedia Foundation, Inc. 19 Oct 2007

http://en.wikipedia.org/wiki/Symmetric_key_algorithm

[SMP] Society of Motion Picture Experts

http://www.smpte.org/

[SWD] “Star Wars Downloads: Free Publicity You Have.” *Techdirt, The Insight Company for the Information Age*, 20 May 2005. Techdirt Inc.

http://www.techdirt.com/articles/20050520/1225209_F.shtml

[SYB] *Statistical Yearbook 2006/2007*, Research and Statistics Unit, UK Film Council, 2007

http://www.ukfilmcouncil.org.uk/information/statistics/yearbook

[TAN] M. Karagosian. Then and Now. *MKPE Consulting LLC Whitepaper*, Apr 2005

http://mkpe.com/publications/digital_cinema/insasia/then_and_now.php

[TCP] "Transmission Control Protocol." *Wikipedia, The Free Encyclopedia*. 29 Oct 2007, 18:38 UTC. Wikimedia Foundation, Inc. 30 Oct 2007

http://en.wikipedia.org/wiki/Transmission_Control_Protocol

[TCS] "Trusted Computer System Evaluation Criteria." *Wikipedia, The Free Encyclopedia*. 3 Aug 2007, 15:45 UTC. Wikimedia Foundation, Inc. 18 Sep 2007

http://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria

[TFS] “Producer Thanks Pirates for Stealing His Film”, *TorrentFreak Weblog*, 13 Nov 2007

http://torrentfreak.com/
producer-thanks-pirates-for-stealing-his-film-071113/

[TLS] "Transport Layer Security." *Wikipedia, The Free Encyclopedia*. 28 Oct 2007, 19:20 UTC. Wikimedia Foundation, Inc. 30 Oct 2007

http://en.wikipedia.org/wiki/Transport_Layer_Security

[TTD] M. Karagosian. Report on the Transition to Digital Cinema in 2007. *MKPE Consulting LLC Whitepaper*, Jun 2007

http://www.mkpe.com/publications/digital_cinema/reports/
May2007_report.php

[USS] “National Threat Assessment Center - Insider Threat Study”, *United States Secret Service*

http://www.ustreas.gov/usss/ntac_its.shtml

[VIC] M. Karagosian. The Value of Interoperability and Certification to Exhibition. *MKPE Consulting LLC Whitepaper*, Oct 2006

http://www.mkpe.com/publications/digital_cinema/
certification/certification_exhibitors.php

[WKM] "Key management." *Wikipedia, The Free Encyclopedia*. 20 Apr 2007, 06:26 UTC. Wikimedia Foundation, Inc. 7 Nov 2007

http://en.wikipedia.org/wiki/Key_management

[WRN] L. Dorrendorf et al. Cryptanalysis of the Random Number Generator of the Windows Operating Systems. In *Cryptology ePrint Archive: Report 2007/419*, International Association of Cryptologic Research, 4 Nov 2007

http://eprint.iacr.org/2007/419.pdf

[WSC] M. Howard, D. LeBlanc, *Writing Secure Code, 2nd Edition*, ISBN 0-7356-1722-8, Microsoft Press, 2003

[X.509] "X.509: Information technology – Open Systems Interconnection – The Directory: Public key and attribute certificate frameworks." *Telecommunication Standardization Sector of ITU - ITU-T*, International Telecommunication Union, Aug 2005

http://www.itu.int/rec/T-REC-X.509-200508-I

[YIJ] "A Year In Jail for Filming 20 Seconds of a Movie?." *Techdirt, The Insight Company for the Information Age*, 2 Aug 2007. Techdirt Inc.

http://www.techdirt.com/articles/20070802/172828.shtml