When a digital film is sent and received in an encrypted fashion, there have to be methods of delivering and utilizing decryption keys to unlock the content.

A part of the key exchange is DRM (digital rights management), which establishes the rules for using the content. All of today's key management systems use some form of DRM to control access and use of the encrypted content. A DRM system allows the owners to distribute their films in a controlled way.

The owner specifies in which ways and under which conditions each cinematic asset may be accessed (digital rights, licensing), and the DRM system will try to ensure that each asset can only be accessed as specified by the owner.

The same DRM system can also be used to distribute films over the Internet. For example, a film studio may specify that each film may be shown in a licensed cinema for a given period starting at a given time.

"It's a difficult issue," said Walt Ordway, chief technology officer for the Digital Cinema Initiatives, a limited liability company that was established in March 2002 and whose members include Disney, 20th Century Fox, MGM, Paramount, Sony Pictures Entertainment, Universal and Warner Bros.

DCI just completed its final draft of standards in March of this year. This document establishes and documents specifications for an open architecture for digital cinema components that ensures a uniform and high level of technical performance, reliability and quality control, as well as addressing security concerns for this digital medium.

"This biggest issues now are over fingerprinting and watermarking, and we need to be careful. How do we set those standards without telling the bad guy how to do it?" Ordway added.

Fingerprints are used to enforce content copyright by enabling the copyright owner to trace back the source of a piracy act. An example would be that all users are given different copies of the content, such as now via a hard drive sent to the theater, where each copy contains a fingerprint—a user-specific watermark. If an unauthorized client redistributes the fingerprinted content, its uniqueness is used to trace back to the offending exhibitor.

Ordway declined to talk specifics about what is in the proposed standards but, according to other sources, the main topics around security that will be addressed are:

- Having security managers at the theaters
- Forensic features to help trace illegal use of content
- Requirements for distribution—link encryption
- Requirements for equipment implementation
• Encryption keys that work on a permission basis with time/date stamps and the management of all those encryption, decryption keys.

Right now, AES-128, the same encryption that banks use for online transfer of information, is what distributors use to secure the digital movie, according to Brian Claypool, senior product manager of cinema for Christi Digital Systems, maker of digital projectors used in about two-thirds of digital cinemas in the United States today.

Advanced Encryption Standard (AES), a Federal Information Processing Standard (FIPS), is an approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a block cipher that can encrypt and decrypt digital information. The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits.

What makes this encryption more impressive for films is that each frame is encrypted, according to Claypool. "Every frame is encrypted, so if somebody were to get lucky even once on the encryption, they'd only get one frame of the movie," Claypool said. "At the theaters, all they have is an encryption key that allows them to tell the hard drive it's OK to play the movie via the projector. It's just impossible to steal a movie."

Technicolor Digital Cinema, the company responsible for the distribution of Star Wars Episode III: Revenge of the Sith, is handling all content preparation for the movie, including the encryption.

The film is shipped to a theater on a hard drive, according to Technicolor Digital Cinema President Ahmad Ouri. Once it's been confirmed that the theater has received the encrypted film and loaded it onto a server, the encryption key is then delivered separately. "The film is useless without the key, and the key just tells the projector it's OK to show the film." In other words, it does not allow the movie to be copied in any way off the server."

The DCI addresses the issue of security and encryption but does not allow any details of standards in this area to be published.

"The less people know, the better," Claypool pointed out. "But the encryption used today for both transferring the digital film and showing it is pretty sophisticated." And, according to sources, will get much more so under the DCI standards that are proposed.

"The questions will be around, Who is going to certify a system?" Ordway said. "How can we be sure a vendor is supplying a DCI-compliant machine that meets all these requirements?"

"Studios are spending so much time and money to figure out these questions," said David Hancock, analyst for London-based Global Media Intelligence's Screen Digest.

Adding to the security dilemma is the low-tech dilemma of stopping those with camcorders from just sitting through a film and recording it. This week at the Cannes Film Festival, Thomson, parent company for Technicolor Digital Systems, will be demonstrating a new anti-piracy technology designed to scramble the quality of images illegally recorded with a camcorder during digital cinema screenings.
It will be completely unnoticeable to the theater viewer, according to Thomson, but will be strong enough to stop would-be hackers.

Security is the last of the big questions remaining for digital cinema, and finally the answers are starting to arrive.

Fuente: http://www.publish.com/article2/0,1759,1815768,00.asp