Digital Rights Management and CKM®

Digital Rights Management (DRM) can be a difficult undertaking. The average lifespan of certain DRM technologies can be measured in days. Some DRM technologies are hacked even before they become standards. Others are hacked after wide deployment in the industry.

Along with the advent of Digital Rights Management and the electronic distribution of digitized media comes the need for strong and reliable digital security. In fact, one of the MPAA's (Motion Picture Association of America's) objectives for Digital Cinema (dCinema) is highly secure, end-to-end, conditional access content protection – including digital rights management and content watermarking protection.

TecSec has developed a role based access management technology called Constructive Key Management® (CKM®) that satisfies this objective as well as objectives for protecting other types of digitized media and intellectual property. CKM provides end-to-end security (regardless of the transport method) for the digital object using a unique and patented cryptographic methodology.

Furthermore, CKM provides Cryptographically Enforced Access Management™ – satisfying the objective of conditional access content protection. Access to any type of data is granted based upon roles and rules. These digital access rights are called Credentials and only those parties holding the proper Credentials may access the digital information. Credentials are stored on a Token, which is also used as an authentication method.

In CKM, data is encrypted using a working key based on Credentials describing how the data can be accessed. This working key is created at the time of encryption and then destroyed. The working key is re-constructed at the time of decryption, which is why the technology is called "Constructive" Key Management. CKM never uses the same key twice. This means that the compromise of one key does not compromise all of the media protected by CKM. Unlike other technologies, CKM provides 100% key recovery – solely to the system owner.

CKM allows DRM systems to solve a number of challenges:

- Enhanced risk management for many digital media business processes, particularly the virtual elimination of theft of intellectual property and associated fraudulent activities.
- Direct implementation of business models and contractual arrangements, including exhibition times and sunset dates, through the use of credentials.
- End-to-end encryption – the data is never in the clear and is protected whether in transit or on disk.
- Support for online and offline architectures, critically important to support playback or exhibition.
- Simplified, secure key management and distribution, because the keys are never distributed – they are created as needed to encrypt and decrypt media – they cannot be hacked.

- Direct support for decentralized key management models.
- Support for differential access to portions of the media. For example, different subtitles, chapters, endings or music tracks may be made visible to different classes of users.
- Support for different quality of service. For example, some users may have visibility to 16 or 32 audio tracks while others see only two.
- Inexpensive mechanism to implement security and inexpensive operating and maintenance costs.

Although DRM can be a difficult undertaking, it does not have to be - given the proper framework, architecture and security technology.

CKM, currently in its fifth generation, is relatively new to the marketplace. The technology is based on ANSI standards, including X9.69, Framework for Key Management Extensions, and is in the process of undergoing certification for the Federal Information Processing Standards (FIPS). It has been deployed in a number of government and commercial organizations and is currently being employed in the defense, corporate, banking and healthcare industries - precisely because the security offered by CKM is so robust, scalable, and conditional. The persistent protection (of both data at rest and in transit) provided by TecSec's technology solves many of the problems unresolved by Public Key Infrastructure (PKI) and peripheral security solutions.

TecSec is a privately held company located outside of Washington DC. Its focus is on Information Security and Secure Access Management of Information - enforced through Cryptography.