THALES

www.thales-esecurity.com

QUBE CINEMA REVOLUTIONIZES DIGITAL CINEMA DISTRIBUTION WITH HELP FROM THALES HARDWARE SECURITY MODULES

How a manufacturer of digital cinema technology cornered the market on online key management for digital cinema distribution by providing the highest levels of trusted content protection.

The Challenge: Find a secure way to manage digital cinema keys online.

As a manufacturer of servers, projectors, mastering and distribution technology for digital cinema, Qube Cinema saw a unique opportunity to introduce a highly disruptive technology to the market as the film industry was completing a decade-long transition from physical to digital distribution. Digital offered tremendous benefits – it was much less expensive to produce and send hard drives than multiple reels of film prints. Digital films could be distributed much more quickly, enabling distributors to better meet demand. Digital films wouldn't degrade over time, and they could be projected by less-skilled labor.

The biggest hurdle, and the reason the film industry lagged behind other industries in converting from analog to digital, was security. Content owners – the companies producing films – were incredibly concerned about piracy and wanted incredibly high security measures.
Theater owners and distributors, on the other hand, didn't want to have to deal with complicated or costly security measures that would harm profitability and introduce operational burden. The Qube team knew that if it could find an efficient way to manage digital cinema keys online with the highest grade of security that was also remarkably easy to operate, it could revolutionize the industry.

The Solution: KeySmith: An online key management system powered by Thales HSMs.

To address the need for efficient security in distributing digital cinema, Qube used Thales Hardware Security Modules (HSMs) to develop an easy-to-use distribution system with the strongest level of security available in the industry. In Digital Cinema, movies are encoded and encrypted into a Digital Cinema Package (DCP) and distributed via hard drive or satellite feed, then can be decrypted at the theater with information

KeySmith QUBE

www.qubecinema.com

Key Benefits

- Overcome security vulnerabilities of host-side applications by executing them inside a trusted environment
- Safeguard critical applications from manipulation, malware and Trojans
- Make HSM cryptographic services available to support a wide variety of connecting devices
- Deliver certified protection with FIPS 140-2 Level 3 approved tamper-resistant hardware
- Reduce the cost of key management task

contained in a unique Key Delivery Message (KDM) that unlocks the film for a specific theater, timeframe and number of showings.

KeySmith satisfies the requirements of content owners and distributors alike. Content owners no longer need to worry about the software-based, in-house encryption measures typically used by distributors, or about the worst case scenario – losing the encryption keys and getting locked out of their own content. Thales HSMs provide the highest grade of protection for content encryption keys in the industry, while simultaneously ensuring that keys are never lost. For distributors and theater owners, the Qube system also provides a level of operational ease that removes any barriers to implementing high security, or temptation to sacrifice security for the sake of convenience.

Here's how the system works: a studio or independent filmmaker submits a movie for distribution. It gets converted to a DCP, which is an industry standard format for the media files and metadata that make up a movie. Within the DCP, a set of AES keys are used to encrypt individual files. A Distribution KDM (DKDM) that securely carries these keys is then made available to the distributor's KeySmith account. This DKDM enables KeySmith to generate KDMs for individual theaters. Thales HSMs create a unique RSA public/private key pair and associated digital certificate for each company within KeySmith. These HSMs encrypt the AES keys with the recipient theater's public key using an application that runs inside the certified security boundary of the HSM. Only the intended recipient can decrypt the package with the associated private key which is unique and securely installed at manufacture. Within KeySmith, the AES keys are handled solely within the security boundary of the HSM. KeySmith can also deliver the KDMs directly to the theaters. This is typically done after the theaters receive the movie via hard drive or satellite download. It's a highly efficient system that provides ease of use for distributors while at the same time ensuring high assurance protection of the movie content – two critical elements of the Qube business value proposition.

About the Solution

Thales HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With these devices you can deploy high assurance security solutions that satisfy widely established and emerging standards of due care for cryptographic systems and practices – while also maintaining high levels of operational efficiency.

Thales HSMs are certified by independent authorities, establishing quantifiable security benchmarks that give you confidence in your ability to support compliance mandates and internal policies. Thales HSMs are available in multiple form factors to support all common deployment scenarios ranging from portable devices to high-performance data center appliances.

With Thales HSMs you can:

- Deliver certified protection for cryptographic keys and operations within tamper-resistant hardware to significantly enhance security for critical applications.
- Achieve cost-effective cryptographic acceleration and unmatched operational flexibility in traditional data center and cloud environments.
- Overcome the security vulnerabilities and performance challenges of software-only cryptography.
- Reduce the cost of regulatory compliance and day-to-day key management tasks including backup and remote management. With HSMs from Thales, you buy only the capacity you need and can scale your solution easily as your requirements evolve.

Thales CodeSafe:

The Thales CodeSafe developer toolkit provides the unique capability to move sensitive applications within the protected perimeter of a certified nShield HSM. Securely loaded and executed on FIPS 140-2 Level 3 HSMs, applications are protected from manipulation and can decrypt, process, and encrypt data inside the secure environment.

CodeSafe enables organizations to:

- **Prevent intellectual property theft** by delivering remote control of sensitive applications no matter the environment, and offering cryptographic services regardless of the operating system or configuration used by the customer, whether server or mainframe. CodeSafe also allows application owners to maintain up-to-date application execution environment without physical presence.
- **Protect applications** from attack by hackers or rogue administrators by providing the ability to digitally sign trusted applications so that their integrity is verified prior to launch. CodeSafe also protects applications from theft, even in uncontrolled environments utilizing outsourcing and contracting.
- **Protect sensitive SSL data** by providing true end-to-end SSL encryption, terminating SSL and processing sensitive data inside the HSM to protect it from attacks.

Why Thales

Qube's decision to use Thales was influenced by several major factors:

- **CodeSafe.** Thales HSMs provide a security feature that no other solution offers: CodeSafe enables applications to run within a secure environment – inside the HSM -- where they are protected from attacks that are prevalent on standard server-based platforms. Qube used CodeSafe to perform all key handling and encryption/decryption operations, providing the highest level of security possible.
- **Reliability and Reputation.** Qube knew that to gain the trust of studios and the film industry, it would need to choose the most reliable and credible security solutions that would withstand the highest levels of scrutiny. With proven performance, tamper-resistant hardware and FIPS 140-2 Level 3 certified protection for cryptographic keys, Thales HMSs fit the bill perfectly.
- **Resiliency and availability.** Thales HSMs enable Qube to ensure the availability of keys to distributors – a critical aspect of building trust in this service industry. With Thales HSMs running in multiple geographic locations to ensure resiliency, Qube can easily back up keys and keep multiple HSMs in synch to serve up keys for global users.
- **Scalability.** Thales HSMs enable Qube to issue and manage an unlimited number of keys – critical to the potential growth of the online service Qube offers digital cinema providers.
- **Responsiveness.** Qube was impressed with the level of pre- and post-sales service and support they received from Thales.

Follow us on:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Unit 4101, 41/F, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com