



ENTRUST



Prima Cinema develops new market for first-run movies using Entrust nShield HSMs

P R I M A[™]
C I N E M A

How a media company surmounted studio security concerns to deliver newly-released films straight to home cinemas.

THE CHALLENGE: DEVELOP A SECURE WAY TO DELIVER JUST-RELEASED FILMS DIRECTLY TO A HOME AUDIENCE

The founders of PRIMA Cinema wanted to exploit a new market opportunity to deliver just-released films to customers with home cinema systems at the same time the films were appearing in theatres. The number of high-end home theatres being built each year was growing quickly, as the number of people interested in watching films from home rather than at the cinema was steadily increasing. The PRIMA Cinema team felt they could make a significant play by delivering films with theatre-like quality to home cinemas, if they could just solve the biggest hurdle: security.

Film piracy is an enormous concern for studios and distributors who, by some accounts, lose billions of dollars each year when film and TV properties are illegally copied and distributed. When films are shown in theatres, theatre managers can monitor audiences to prevent “camming” – recording films in the theatre with a video camera – but for home theatres, a different kind of security would be needed. The PRIMA team knew that to get buy-in from studios and other content owners for their business model, they would need to devise a highly secure way to distribute and show films – while not diminishing the viewer experience.

LEARN MORE AT [ENTRUST.COM/HSM](https://www.entrust.com/hsm)



Prima Cinema

THE SOLUTION: MULTIPLE CRYPTOGRAPHIC LAYERS USING ENTRUST NSHIELD HSMs

To address the concerns of studios and distributors, PRIMA Cinema developed a system for encoding and distributing films to home theatres that involved multiple layers of encryption as well as strong authentication between their servers and home playback devices, using Entrust nShield® hardware security modules (HSMs) to generate and protect private encryption and digital signature keys.

Before distribution, PRIMA Cinema encrypts films using 256-bit AES with keys generated by an HSM. The playback device installed in home cinemas includes a trusted platform module (TPM) where private keys and certificates associated with the decryption and device authentication are secured and managed.

During manufacture, keys are never exposed outside the HSM and the consuming device – the application that controls all cryptographic processing and key handling is executed within the secure confines of the HSM using the unique nShield CodeSafe capability. The role-based access features of nShield Security World, common to all nShield HSMs, ensure that appropriate multi-person administrative controls are enforced to help prevent the possibility of an insider attack to the system. Films are transferred to playback devices via broadband and are protected with bi-directional certificate-based authentication. Additionally, a biometric fingerprint reader built into the playback device ensures that only the true registered owners can actually initiate a screening. Finally at the time of playback, a session-specific watermark is generated by the HSM and used to invisibly mark the video to deter camming of the film.

PRIMA Cinema's approach to security was subjected to independent review and found to satisfy the highly stringent requirements of content providers, and enabled the company to proceed to market as the first company in the history of cinema to be granted rights to license and distribute theatrically-released movies to private home theatres.

ABOUT THE SOLUTION

Entrust nShield 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.

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

With Entrust nShield 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 cloud environments
- Overcome the security vulnerabilities and performance challenges of software-only cryptography

LEARN MORE AT [ENTRUST.COM/HSM](https://www.entrust.com/hsm)



Prima Cinema

- Reduce the cost of regulatory compliance and day-to-day key management tasks including backup and remote management. With Entrust nShield HSMs, you buy only the capacity you need and can scale your solution easily as your requirements evolve

NSHIELD CODESAFE

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

nShield 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. nShield CodeSafe also allows application or handheld 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. nShield 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 ENTRUST?

Entrust won the business based on the security and functionality of its nShield HSMs which provided:

- **Greater security.** From the outset, the PRIMA Cinema team knew that to get approval from the studios it would need the higher assurance security of a FIPS-certified, hardened appliance approach instead of using inherently riskier standard application platforms. And PRIMA Cinema needed a proven solution with security certifications so that anyone reviewing the system would be easily satisfied as to its reliability and security pedigree. And they wanted a multi-layered approach to security, using industry standard algorithms and key lengths suitable for the strongest protection available. Entrust nShield HSMs delivered on all accounts
- **nShield CodeSafe.** Entrust nShield 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. PRIMA Cinema used CodeSafe to perform all key handling and encryption/decryption operations, providing the highest level of security possible



Prima Cinema

KEY BENEFITS

- Overcome vulnerabilities of performing security functions on standard application platforms by instead executing them inside a trusted environment
- Safeguard critical applications and secret encryption and signature keys 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 tasks

• **nShield Security World architecture.**

The nShield Security World architecture streamlined key management and enabled PRIMA to build and manage their overall system by making it easy to define all of the strict security and control the project required. The Security World architecture provides an unified administrator and user experience and guarantees interoperability whether one or hundreds of devices are deployed

- **Superior user experience.** Entrust nShield HSMs were able to transparently provide the strong security required by the studios without interfering with or compromising the quality of the user experience – an absolute must for PRIMA Cinema’s value proposition

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they’re crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it’s no wonder the world’s most entrusted organizations trust us.



Learn more at

entrust.com/HSM



ENTRUST