Fastcom increases code signing efficiency while maintaining high levels of security

www.fastcom-technology.com

THE CHALLENGE: A BETTER SET-TOP BOX TO HELP FOXTEL MAINTAIN ITS COMPETITIVE EDGE

The pay TV marketplace is highly competitive, with consumers regularly demanding access to new content offerings. Even in Australia, where Foxtel leads the pay TV market, the introduction of new operators means Foxtel needs to stay even more focused on new innovations in order continue delivering a great subscriber experience.

Foxtel introduced the iQ3 set-top box (STB), which offers enhanced content streams, more recording space and other new features meant to increase subscriber satisfaction.

When designing the iQ3, Foxtel engaged with Fastcom, identifying three core requirements. Specifically, the STBs needed to:

- Support a multi-vendor security strategy, allowing Foxtel the flexibility to offer streams from multiple content providers as well as change providers as needed
- Prevent unauthorised access to subscription only content
- Provide Foxtel direct control over deployed devices to allow for efficient updates that respond to customer needs

THE SOLUTION: FASTCOM MCAS, ENABLED BY ENTRUST

Based on Foxtel's needs, Fastcom developed the initial specifications for its multiple conditional access system (MCAS) solution, quickly determining that it would require highly secure cryptography – starting with the manufacture of the STBs. In fact, the root key that provides a root of trust for all encryption and decryption on the device would need to be burned into the iQ3's core processors, establishing each device's identity and allowing for the creation of

Fastcom

keys to encrypt content from conditional access system (CAS)/ digital rights management (DRM) solutions.

To achieve the level of security demanded by the application, Fastcom determined that they needed to execute their key derivation algorithm within a FIPS-certified environment. Fastcom was familiar with hardware security modules (HSMs) and comfortable that they offered the required security and modularity.

After reviewing several vendor offerings, Fastcom selected Entrust nShield® HSMs because of its unmatched ability to deliver on all of the project's security requirements. Specifically, nShield CodeSafe features an unmatched capability that allows Fastcom to run its proprietary derivation algorithm and protect keys within a FIPS 140-2 Level 3 boundary.

During the implementation phase the Entrust team developed part of the encryption application code within the CodeSafe environment, which Fastcom then further modified. This provided Fastcom the head start it needed to build out the solution while allowing it to easily take over ownership of the core code.

Using the nShield HSM, Fastcom derives multiple subordinate keys from a single root key for Foxtel to incorporate into the iQ3 STBs. The keys are used by CAS vendors to encrypt content provided through CAS/DRM solutions, ensuring that content can only be rendered on a particular STB.

With Entrust nShield HSMs underpinning the MCAS solution, Foxtel is able to freely choose the applications, middleware and CAS/DRM solutions for its iQ3 STBs. This enables a multi-vendor approach, as well as efficient, low-cost updates to the STBs as needed, and the delivery of premium content to pay TV subscribers. Looking ahead, Fastcom envisions using the MCAS model to develop other customer premises equipment solutions that leverage its multi-vendor security approach..

KEY BENEFITS

- Easily change CAS vendors and middleware without costly updates to STBs
- Gain direct control over remotely deployed devices, improving the subscriber experience
- Protect revenue streams by securing premium content

ABOUT THE SOLUTION

Entrust nShield HSMs

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.

Fastcom

ENTRUST CODESAFE

The Entrust 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.

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 or handheld owners to maintain an 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.

ABOUT FASTCOM

Fastcom, an independent Swiss company, provides security solutions and technical consulting to the pay TV market.

Fastcom's MCAS solution is an integrated set of licensing authority services for customer premises equipment, such as pay TV set-top boxes (STBs). Leveraging a modular and scalable infrastructure, the MCAS simultaneously supports multiple conditional access systems (CAS) and digital rights management (DRM) solutions, while providing pay TV operators direct control of STBs in the field.

ABOUT FOXTEL

Foxtel is Australia's premier media company, offering pay TV and internet services to more than 2.8 million homes across the country.

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.

Fastcom

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 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 Entrust nShield HSMs, you buy only the capacity you need and can scale your solution easily as your requirements evolve

WHY ENTRUST?

- Entrust won the business based on the security and unique functionality of the nShield HSM, supported by Entrust's knowledgeable implementation expertise.

Entrust offered Fastcom:

- Industry-leading security. Fastcom knew it needed to deliver a solution that Foxtel could trust to protect premium content from unauthorized access once the iQ3 STBs were deployed into the field. With Entrust nShield HSMs at its core, the MCAS solution offers the highest levels of security and functionality
- A protected environment for executing its crypto algorithm. Fastcom had developed its own key derivation algorithm for which it wanted the highest level of protection available. Entrust CodeSafe is the only solution that enables applications to run within the FIPS-certified boundary of the HSM, where they are protected from attacks that are prevalent on standard server-based platforms
- Highly qualified security expertise. Experts from the Entrust professional services team collaborated with Fastcom to begin building the application that would derive the root-of-trust keys that protect the iQ3 STBs. Fastcom leveraged this jump start to expedite the development of the MCAS solution

mcas

Learn more at
entrust.com/HSM

Entrust is a trademark, registered trademark, and/or service mark of Entrust Corporation in the United States and/or other countries. ©2020 Entrust Corporation.

ENTRUST

Contact us:
HSMinfo@entrust.com