ENTRUST

Foxtel and Fastcom rely on Entrust HSMs and Entrust Cloud Signing Services

As one of Australia's leading media companies, the Foxtel Group provides pay TV and Internet services to more than 1.6 million homes and commercial premises across the country through its Foxtel subscription TV service. The Foxtel Group has more than 4.4 million subscribers to its services. Its portfolio includes cable television, direct broadcast satellite television, and IPTV streaming services, as well as leading brands including BINGE, Kayo Sports and Fox Sports Australia.

With the pay TV marketplace being highly competitive and consumers getting more and more demanding, Foxtel needs to stay strongly focused on new innovations in order to continue delivering a great subscriber experience. As a key element of Foxtel's offering, their iQ set-top box (STB) is being continuously developed further and enhanced with new features.

In 2017, Foxtel engaged with Entrust partner Fastcom Technology SA. A leading company in securing physical and data flows, Fastcom has been selected to optimize the security and management for Foxtel's iQ set-top boxes – from the formerly iQ3 to the most up-to-date iQ5. The iQ5 has been launched in 2021 and offers customers access to the full Foxtel experience via IP. Foxtel's newest STB also allows the aggregation of multiple services from different vendors, positioning itself as versatile platform for a better customer experience.

KEY FACTS

Customer
Foxtel

Industry
Pay TV, Content & Media

Challenge
- Support a multi-vendor security strategy, allowing Foxtel the flexibility to offer streams from multiple content providers and change providers as needed
- Prevent unauthorised access to subscription only content
- Provide Foxtel direct control over deployed devices
- Secure signing of STB software updates

Solutions
Entrust nShield and Entrust nShield as a Service

Technology Partner
Fastcom

FOXTEL   **fastcom** TECHNOLOGY

Foxtel

« **Our partnership with Entrust brings together extensive knowledge in the two domains of data security and pay TV industry. This enables our MCAS solution to implement efficient security processes that are aligned with modern business requirements and customer demands.** »

Fabrice Moscheni, Managing Director at Fastcom Technology

To realize optimized security and management for the iQ5, by ensuring maximum flexibility and a highly convenient consumer experience at the same time, Foxtel defined some core requirements:

- Specifically, the STBs need to support a multi-vendor security strategy, allowing Foxtel the flexibility to offer streams from multiple content providers and change providers as needed.

- Besides, Foxtel needs direct control over deployed devices to allow for efficient updates that respond to customer needs.

- And, as a matter of course, unauthorised access to subscription-only content has to be prevented.

Since Fastcom's MCAS solution can meet all these requirements and has already proven its qualities with Foxtel's previous STBs, the choice was quickly made. Using the MCAS services also for the iQ5 is a continuation of Foxtel's strategy to retain full control over its set-top boxes, allowing for faster market response and for more efficient resource planning.

Let's have a look at the solution in detail:

The MCAS solution and its benefits for Foxtel

Allowing secure keys and credentials management, Fastcom's MultipleCAS solution (i.e. MCAS) is an integrated set of licensing authority services for customer premises equipment, such as pay TV set-top boxes. MCAS enables pay TV operators to independently choose the applications, middleware, and security solution running on their STBs. Leveraging a modular and scalable infrastructure, the MCAS solution simultaneously supports multiple conditional access systems (CAS) and digital rights management (DRM) solutions. It provides pay TV operators with the security services to deploy and manage their STB devices in the field as it ensures the secure generation, derivation, storage and provisioning of the needed keys.

These security services are structured in a modular manner and, based on the pay TV operator 's choice, are performed by Fastcom on its behalf.

To deliver the MCAS services, there is a dedicated MCAS infrastructure in place – including the necessary hardware,

maintenance and security processes. And this is where Entrust comes into play: The MCAS solution uses Entrust nShield hardware security modules (HSMs) to securely generate and manage the cryptographic keys embedded within the television receiver's chipset. Entrust nShield HSMs provide a FIPS 140-2 Level 3 certified environment with strict dual supervision and control that establishes the foundation of trust for the licensing authority services, also known as keys and credentials management.

Besides, Fastcom and Foxtel are now working with Entrust's Cloud-based nShield as a Service to securely and efficiently sign and encrypt software packages.

MCAS and Entrust nShield HSMs

Fastcom developed the initial specifications for its MCAS solution 10 years ago, quickly determining that it would require highly secure cryptography – already 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 needs to be burned into the iQ5's core processors, establishing each device's identity and allowing for the creation of keys to encrypt content from a conditional access system or digital rights management solution.

To achieve the level of security demanded by the application, Fastcom had to execute the generation of these keys within a FIPS-certified environment. Knowing about the high security and modularity of hardware security modules (HSMs), Fastcom started to review several vendor offerings. At the end of the elevation process, Entrust nShield has been chosen because of its unmatched ability to deliver on all of the project's security requirements. Entrust nShield HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection,

and key management. Specifically, Entrust nShield allows Fastcom to run their proprietary derivation algorithm and protect keys within a FIPS 140-2 Level 3 boundary.

Using the nShield HSM, Fastcom derives multiple subordinate keys from a single root key for Foxtel to incorporate into the iQ5 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 underlying the MCAS solution, Foxtel is now able to freely choose the applications, middleware and CAS solutions for their iQ5 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.

If needed, Foxtel could easily change specific CAS vendors and middleware without the need to run costly updates on the STBs. The pay TV operator gains direct control over remotely deployed devices, improving the experience for subscribers and protecting revenue streams by securing premium content.

Foxtel

> « **Fastcom's MCAS solution provides us with total control on our iQ5 applications, middleware and CAS security systems. We are also enjoying great flexibility in terms of updates and changes, which are possible at any time for a minimum of cost. So we can not only ensure highest security levels, but also a great user experience for our customers.** »
>
> Thomas Russo, Head of Middleware Development & Security at Foxtel

HSMs and Digital Signing in the Cloud

In order to provide a highly comfortable and seamless experience, Fastcom recently developed a cloud version of their MCAS solution, at the basis of Entrust's nShield as a Service offering. The integration of the MCAS solution with Entrust cloud-based HSMs now allows a frictionless and highly secure digital signing process: The access to the cloud offerings is secured with smart cards. After the log-in, the Foxtel admins can upload the software package to be signed and encrypted by the cloud-based MCAS solution. Once signed and encrypted, the software package is sent back to them. This allows a 24/7 digital signing and encryption service, accessible from everywhere at any time. As an essential part of the cloud-based MCAS solution, Entrust assures the quality and business continuity of their HSM functionality along with its nShield as a Service offering. As a result, Foxtel can now securely and efficiently sign and encrypt software packages in the cloud, while benefiting from optimal quality of service and business continuity.

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted experiences for identities, payments, and digital infrastructure. We offer an unmatched breadth of solutions that are critical to enabling trust for multi-cloud deployments, mobile identities, hybrid work, machine identity, electronic signatures, encryption, and more. With more than 2,800 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

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com   entrust.com/contact