



**ENTRUST**

# Fastcom s'associe à Entrust pour assurer la protection des décodeurs de Foxtel



[www.fastcom-technology.com](http://www.fastcom-technology.com)



## LE DÉFI : UN MEILLEUR DÉCODEUR POUR AIDER À CONSERVER SON AVANTAGE COMPÉTITIF

Le marché de la télévision payante est très dynamique, les consommateurs demandant régulièrement à avoir accès à de nouvelles offres de contenu. Même en Australie, où Foxtel est le leader du marché de la télévision payante, l'arrivée de nouveaux opérateurs impose à Foxtel d'innover davantage afin de continuer à proposer un service excellent à ses abonnés.

Foxtel a lancé le décodeur iQ3, qui offre des contenus améliorés, plus d'espace d'enregistrement et d'autres nouvelles fonctionnalités destinées à accroître la satisfaction des abonnés.

Lors de la conception du iQ3, Foxtel s'est rapproché de Fastcom, et a identifié trois besoins essentiels. Concrètement, les décodeurs devraient :

- Prendre en charge une stratégie de sécurité multi-fournisseurs, permettant à Foxtel d'offrir des services provenant de plusieurs fournisseurs de contenu et de changer de fournisseurs si besoin
- Empêcher l'accès non autorisé au contenu réservé aux abonnés
- Fournir à Foxtel un contrôle direct sur les appareils déployés pour permettre des mises à jour performantes qui répondent aux besoins des clients

## LA SOLUTION : L'ASSOCIATION DES HSM DE ENTRUST AU MCAS DE FASTCOM

Sur la base des besoins de Foxtel, la société Fastcom a mis au point les premières modalités de sa solution de système d'accès conditionnel multiple (MCAS), et a rapidement constaté qu'elle allait avoir besoin de moyens de chiffrement hautement sécurisés, notamment pour la fabrication des décodeurs. Il faudrait effectivement que la clé racine qui constitue la racine de confiance pour tout le chiffrement et le déchiffrement sur le dispositif soit gravée sur les processeurs centraux de l'iQ3, ce qui permettrait de savoir l'identité de chaque dispositif et de créer des clés pour chiffrer le contenu à partir de solutions de contrôle d'accès (CAS) ou de gestion des droits numériques (DRM).

**DÉCOUVREZ-EN PLUS SUR [ENTRUST.COM/FR/HSM](http://ENTRUST.COM/FR/HSM)**

Pour atteindre le niveau de sécurité requis pour l'application, Fastcom a réalisé qu'il lui fallait pouvoir exécuter son algorithme de dérivation de clés au sein d'un environnement certifié FIPS. Fastcom connaissait les modules matériels de sécurité (HSM) et était convaincu que ces solutions permettraient de bénéficier des niveaux de sécurité et d'évolutivité requis.

Après avoir examiné plusieurs offres de fournisseurs, Fastcom a fait le choix des HSM nShield® de Entrust en raison de leur remarquable capacité à répondre à toutes les exigences de sécurité du projet. En particulier, la fonctionnalité CodeSafe unique de nShield permet à Fastcom d'exécuter son algorithme de dérivation propriétaire et de protéger les clés au sein d'un matériel certifié FIPS 140-2 niveau 3.

Pendant la phase de déploiement, l'équipe de Entrust a développé une partie du code de chiffrement de l'application au sein de l'environnement de CodeSafe, que Fastcom a ensuite modifié. Cela a permis à Fastcom d'avoir suffisamment d'avance pour élaborer la solution tout en s'appropriant facilement le code de base.

Grâce aux HSM nShield, Fastcom dérive plusieurs clés sous-jacentes à partir d'une seule clé racine afin que Foxtel les intègre dans ses décodeurs iQ3. Les clés sont utilisées par les fournisseurs de contrôle d'accès pour chiffrer le contenu fourni au moyen de solutions CAS/DRM, ce qui garantit que le contenu ne puisse être transmis que sur un décodeur donné.

Grâce aux HSM nShield de Entrust qui viennent renforcer sa solution MCAS, Foxtel est en mesure de choisir librement les applications, le progiciel et les solutions CAS/DRM pour ses décodeurs iQ3. Il est ainsi possible d'adopter une approche multi-fournisseurs, de procéder à des mises à jour efficaces et peu onéreuses des décodeurs

si nécessaire, et de fournir des contenus de qualité aux abonnés des services de télévision payante. À l'avenir, Fastcom envisage d'utiliser le modèle MCAS pour développer d'autres appareils pour les clients afin d'optimiser son approche de sécurité multi-fournisseurs.

## PRINCIPAUX AVANTAGES

- Possibilité de changer facilement de fournisseur de contrôle d'accès et de progiciel sans mises à jour onéreuses des décodeurs
- Contrôle direct des dispositifs déployés à distance, améliorant ainsi l'expérience de l'abonné
- Protection des flux de revenus par la sécurisation des programmes payants

## À PROPOS DE LA SOLUTION

### Les HSM nShield de Entrust

Les HSM nShield de Entrust procurent un environnement renforcé et inviolable qui permet de réaliser des opérations de chiffrement sécurisé, de protéger les clés et de les gérer. Ces appareils vous permettent de déployer des solutions hautement sécurisées qui respectent les normes en vigueur et émergentes relatives au respect des meilleures pratiques et à l'entretien des systèmes de chiffrement, tout en garantissant un degré élevé d'efficacité opérationnelle.

Les HSM nShield de Entrust sont certifiés par des autorités indépendantes, établissant des critères de sécurité quantifiables qui vous donnent confiance dans votre capacité à respecter les exigences de conformité et les politiques internes. Les HSM nShield de Entrust sont disponibles sous de multiples formes pour prendre en charge tous les scénarios de déploiement courants, allant des appareils portables aux appareils de centres de données ultra-performants.

## **CODESAFE DE ENTRUST**

La boîte à outils pour les développeurs CodeSafe de Entrust offre la possibilité unique de déplacer des applications sensibles dans le périmètre de protection d'un HSM nShield certifié FIPS 140-2 niveau 3. Avec cette approche, les applications sont protégées de toute manipulation et peuvent déchiffrer, traiter et chiffrer des données au sein de cet environnement sécurisé.

## **CODESAFE PERMET AUX ORGANISATIONS DE :**

- **Empêcher le vol de propriété intellectuelle** en permettant le contrôle à distance d'applications sensibles, quel que soit l'environnement, et en offrant des services de chiffrement quel que soit le système d'exploitation ou la configuration utilisés par le client, qu'il s'agisse d'un serveur ou d'un ordinateur central. CodeSafe permet également aux propriétaires d'applications de maintenir à jour l'environnement d'exécution des applications sans présence physique.
- **Protéger les applications contre les attaques** des pirates ou d'administrateurs malveillants en offrant la possibilité de signer numériquement les applications de confiance afin que leur intégrité soit vérifiée avant leur lancement. CodeSafe protège également les applications contre le vol, même au sein d'environnements non contrôlés ayant recours à l'externalisation et à la sous-traitance.
- **Protéger les données SSL sensibles** en fournissant un véritable chiffrement SSL de bout en bout, en terminant le SSL et en traitant les données sensibles à l'intérieur du HSM pour les protéger contre les attaques.

## **À PROPOS DE FASTCOM**

Fastcom est une société suisse qui fournit des solutions de sécurité et des services de consulting technique au marché de la télévision payante.

Le MCAS de Fastcom est une solution complète de Licensing Authority Services (LAS) pour les appareils installés chez les clients, tels que les décodeurs de télévision payante. Grâce à son infrastructure moderne et évolutive, le MCAS prend en charge simultanément plusieurs systèmes d'accès conditionnel (CAS) et solutions de gestion des droits numériques (DRM), tout en fournissant aux opérateurs de télévision payante un contrôle direct des décodeurs installés.

## **À PROPOS DE FOXTEL**

Foxtel est un géant de la télévision payante en Australie qui diffuse des contenus télévisés et Internet payants à plus de 2,8 millions de foyers dans tout le pays.

## **À PROPOS DE ENTRUST**

Entrust sécurise un monde en mouvement avec des solutions qui protègent les identités, les paiements et les données, dans tous les pays. Aujourd'hui, les gens souhaitent des parcours plus fluides et plus sûrs quand ils traversent les frontières, font des achats, utilisent des services administratifs en ligne ou des réseaux d'entreprises. Notre gamme unique de solutions pour la sécurité numérique et l'émission de titres sécurisés permet de répondre précisément à ces souhaits. Grâce à nos 2 500 collaborateurs, notre réseau international de partenaires et des clients dans plus de 150 pays, les organisations les plus fiables au monde nous font confiance.

## GRÂCE AUX HSM NSHIELD DE ENTRUST, VOUS SEREZ EN MESURE DE :

- Protéger de manière certifiée les clés et les opérations de chiffrement au sein d'un matériel inviolable afin de renforcer considérablement la sécurité de vos applications essentielles
- Bénéficier d'une accélération du chiffrement à moindre coût et d'une souplesse opérationnelle inégalée par rapport aux centres de données traditionnels et aux environnements cloud
- Remédier aux failles de sécurité et aux problèmes de performances inhérents au chiffrement logiciel
- Diminuer les coûts de la mise en conformité avec les réglementations en vigueur et des tâches quotidiennes de gestion des clés, notamment la sauvegarde et la gestion à distance. Avec les HSM nShield de Entrust, vous n'achetez que la capacité dont vous avez besoin et pouvez facilement faire évoluer votre solution en fonction de vos besoins

## POURQUOI AVOIR CHOISI ENTRUST ?

- Entrust a remporté le marché grâce aux fonctionnalités de sécurité unique de ses HSM nShield et l'expertise de ses équipes de déploiement

## Entrust a fourni à Fastcom :

- Ses solutions de sécurité de pointe. La société Fastcom savait qu'elle devait fournir une solution en laquelle Foxtel puisse avoir confiance pour protéger ses contenus payants des accès non autorisés une fois que les décodeurs iQ3 seraient opérationnels. Avec les HSM nShield de Entrust comme base, la solution MCAS fournit les plus hauts niveaux de sécurité et de fonctionnalité possibles
- Un environnement protégé pour l'exécution de son algorithme de chiffrement. Fastcom avait développé son propre algorithme de dérivation de clés et souhaitait pouvoir bénéficier du meilleur degré de protection possible. CodeSafe de Entrust est la seule solution qui permet aux applications de s'exécuter au sein de l'environnement de chiffrement d'un HSM certifié FIPS, où les clés sont protégées contre les attaques qui sont courantes sur les plateformes basées sur des serveurs standards.
- Une expertise hautement qualifiée en matière de sécurité. Les experts de l'équipe de services professionnels de Entrust ont collaboré avec Fastcom pour la création de l'application permettant de dériver les clés de confiance qui protègent les décodeurs iQ3. Fastcom a profité de ce lancement pour accélérer le développement de sa solution MCAS

