Fastcom aumenta a eficiência da assinatura de código, mantendo altos níveis de segurança

www.fastcom-technology.com

O DESAFIO: UMA CAIXA DE CONFIGURAÇÃO MELHOR PARA AJUDAR A FOXTEL A MANTER SUA VIA COMPETITIVA

O mercado de TV paga é altamente competitivo, com consumidores exigindo regularmente acesso a novas ofertas de conteúdo. Mesmo na Austrália, onde a Foxtel lidera o mercado de TV paga, a introdução de novas operadoras significa que a Foxtel precisa se manter ainda mais focada em inovações para continuar oferecendo uma ótima experiência ao assinante.

A Foxtel apresentou o set-top box iQ3 (STB), que oferece fluxos de conteúdo aprimorados, mais espaço de gravação e outros novos recursos destinados a aumentar a satisfação do assinante.

Ao projetar o iQ3, a Foxtel se associou à Fastcom, identificando três requisitos principais. Especificamente, os STBs precisavam:

- Apoiar uma estratégia de segurança de vários fornecedores, permitindo à Foxtel a flexibilidade para oferecer fluxos de vários fornecedores de conteúdo, bem como alterar fornecedores conforme necessário
- Impedir o acesso não autorizado a conteúdo somente para assinatura
- Fornecer controle direto à Foxtel sobre os dispositivos implantados para permitir atualizações eficientes que atendam às necessidades do cliente

A SOLUÇÃO: FASTCOM MCAS, HABILITADO POR ENTRUST

Com base nas necessidades da Foxtel, a Fastcom desenvolveu as especificações iniciais para sua solução de sistema de acesso condicional múltiplo (MCAS), determinando rapidamente que exigiria criptografia altamente segura - começando com a fabricação dos STBs. Na verdade, a chave raiz que fornece uma raiz de confiança para toda criptografia e descriptografia no dispositivo precisaria ser gravada nos processadores centrais do iQ3, estabelecendo a identidade de cada dispositivo e permitindo a criação de chaves para criptografar o conteúdo do sistema de acesso condicional (CAS)/soluções de gerenciamento de direitos digitais (DRM).

SAIBA MAIS EM ENTRUST.COM/HSM

Fastcom

Para atingir o nível de segurança exigido pelo aplicativo, a Fastcom determinou que precisava executar seu algoritmo de derivação de chave em um ambiente certificado por FIPS. A Fastcom estava familiarizada com os módulos de segurança de hardware (HSMs) e confortável porque eles ofereciam segurança e modularidade necessária.

Depois de analisar várias ofertas de fornecedores, a Fastcom selecionou os HSMs Entrust nShield® por causa de sua capacidade incomparável de atender a todos os requisitos de segurança do projeto. Especificamente, o nShield CodeSafe apresenta uma capacidade incomparável que permite à Fastcom executar seu algoritmo de derivação proprietário e proteger as chaves dentro de um limite FIPS 140-2 Nível 3.

Durante a fase de implementação, a equipe Entrust desenvolveu parte do código do aplicativo de criptografia dentro do ambiente CodeSafe, que a Fastcom posteriormente modificou. Isso forneceu à Fastcom a vantagem necessária para construir a solução, ao mesmo tempo que lhe permitiu assumir facilmente a propriedade do código principal.

Usando o HSM nShield, a Fastcom deriva várias chaves subordinadas de uma única chave raiz para a Foxtel incorporar aos STBs iQ3. As chaves são usadas por fornecedores de CAS para criptografar o conteúdo fornecido por meio de soluções CAS/DRM, garantindo que o conteúdo só possa ser processado em um STB específico.

Com so HSMs Entrust nShield sustentando a solução MCAS, a Foxtel pode escolher livremente os aplicativos, middleware e soluções CAS/DRM para seus STBs iQ3. Isso permite uma abordagem de vários fornecedores, bem como atualizações eficientes e de baixo custo para os STBs, conforme necessário, e a entrega de conteúdo premium para assinantes de TV paga. Olhando para o futuro, a Fastcom prevê o uso do modelo MCAS para desenvolver outras soluções de equipamentos nas instalações do cliente que alavancam sua abordagem de segurança de vários fornecedores.

PRINCIPAIS BENEFÍCIOS

- Alterar facilmente fornecedores CAS e middleware sem atualizações caras para STBs
- Ganhar controle direto sobre dispositivos implantados remotamente, melhorando a experiência do assinante
- Proteger os fluxos de receita garantindo conteúdo premium

SOBRE A SOLUÇÃO

Entrust nShield HSMs

Os HSMs Entrust nShield fornecem um ambiente reforçado e resistente a adulterações para a execução de processamento criptográfico seguro, proteção de chaves e gerenciamento de chaves. Com esses dispositivos, você pode implantar soluções de segurança de alta garantia que satisfaçam os padrões amplamente estabelecidos e emergentes de devido cuidado com os sistemas e práticas criptográficas ao mesmo tempo que mantém altos níveis de eficiência operacional.

Os HSMs Entrust nShield são certificados por autoridades independentes, estabelecendo benchmarks de segurança quantificáveis que dão a você confiança em sua capacidade de oferecer suporte a mandatos de conformidade e políticas internas. Os HSMs Entrust nShield estão disponíveis em vários formatos para oferecer suporte a todos os cenários de implantação comuns, desde dispositivos portáteis a dispositivos de data center de alto desempenho.

Fastcom

ENTRUST CODESAFE

O kit de ferramentas de desenvolvedor Entrust CodeSafe fornece a capacidade exclusiva de mover aplicativos confidenciais dentro do perímetro protegido de um HSM nShield com certificação FIPS 140-2 Nível 3. Usando essa abordagem, os aplicativos são protegidos contra manipulação e podem descriptografar, processar e criptografar dados dentro do ambiente seguro.

CODESAFE HABILITA AS ORGANIZAÇÕES A:

- **Evitar o roubo de propriedade intelectual** fornecendo controle remoto de aplicativos confidenciais, independentemente do ambiente, e oferecendo serviços criptográficos independentemente do sistema operacional ou da configuração usada pelo cliente, seja servidor ou mainframe. CodeSafe também permite que os proprietários de aplicativos ou dispositivos portáteis mantenham um ambiente de execução de aplicativos atualizado sem presença física
- **Proteger os aplicativos contra ataques** de hackers ou administradores desonestos, fornecendo a capacidade de assinar digitalmente aplicativos confiáveis para que sua integridade seja verificada antes do lançamento. CodeSafe também protege aplicativos contra roubo, mesmo em ambientes não controlados utilizando terceirização e contratação
- **Proteger os dados SSL confidenciais** fornecendo criptografia SSL de ponta a ponta, encerrando SSL e processando dados confidenciais dentro do HSM para protegê-lo de ataques.

SOBRE FASTCOM

A Fastcom, empresa suíça independente, fornece soluções de segurança e consultoria técnica para o mercado de TV paga.

A solução MCAS da Fastcom é um conjunto integrado de serviços de autoridade de licenciamento para equipamentos nas instalações do cliente, como set-top boxes de TV paga (STBs). Aproveitando uma infraestrutura modular e escalável, o MCAS suporta simultaneamente vários sistemas de acesso condicional (CAS) e soluções de gerenciamento de direitos digitais (DRM), enquanto fornece aos operadores de TV paga controle direto de STBs no campo.

SOBRE A FOXTEL

A Foxtel é a principal empresa de mídia da Austrália, oferecendo TV paga e serviços de Internet para mais de 2,8 milhões de residências em todo o país.

SOBRE A ENTRUST

A Entrust mantém o mundo movendo-se com segurança, permitindo identidades, pagamentos e proteção de dados confiáveis. Hoje, mais do que nunca, as pessoas exigem experiências seguras e contínuas, quer estejam cruzando fronteiras, fazendo uma compra, acessando serviços de governo eletrônico ou entrando em redes corporativas. A Entrust oferece uma gama incomparável de soluções de segurança digital e emissão de credenciais no centro de todas essas interações. Com mais de 2.500 colegas, uma rede de parceiros globais e clientes em mais de 150 países, não é de admirar que as organizações mais confiáveis do mundo confiem em nós.

Fastcom

COM ENTRUST NSHIELD HSMS VOCÊ PODE:

- Fornecer proteção certificada para chaves criptográficas e operações em hardware resistente a adulteração para aumentar significativamente a segurança para aplicativos críticos
- Obter aceleração criptográfica econômica e flexibilidade operacional incomparável em data centers tradicionais e ambientes em nuvem
- Superar as vulnerabilidades de segurança e os desafios de desempenho da criptografia somente de software
- Reduzir o custo de conformidade regulamentar e tarefas de gerenciamento de chaves do dia a dia, incluindo backup e gerenciamento remoto. Com os HSMs Entrust nShield, você adquire apenas a capacidade de que precisa e pode dimensionar sua solução facilmente conforme seus requisitos evoluem

POR QUE A ENTRUST?

- A Entrust venceu os negócios com base na segurança e na funcionalidade exclusiva do HSM nShield, com o suporte de sua experiência de implementação bem informada.

A Entrust ofereceu à Fastcom:

- Segurança líder do setor. A Fastcom sabia que precisava entregar uma solução em que a Foxtel pudesse confiar para proteger o conteúdo premium de acesso não autorizado assim que os STBs iQ3 fossem implantados em campo. Com os HSMs Entrust nShield em seu núcleo, a solução MCAS oferece os mais altos níveis de segurança e funcionalidade
- Um ambiente protegido para executar seu algoritmo de criptografia. A Fastcom desenvolveu seu próprio algoritmo de derivação de chave, para o qual desejava o mais alto nível de proteção disponível. O Entrust CodeSafe é a única solução que permite que os aplicativos sejam executados dentro dos limites certificados por FIPS do HSM, onde são protegidos de ataques que prevalecem em plataformas baseadas em servidor padrão
- Especialização em segurança altamente qualificada. Os especialistas da equipe de serviços profissionais da Entrust colaboraram com a Fastcom para começar a construir o aplicativo que derivaria as chaves de raiz de confiança que protegem os STBs iQ3. A Fastcom aproveitou este salto inicial para agilizar o desenvolvimento da solução MCAS

mcas

Saiba mais em
entrust.com/HSM

ENTRUST

Entre em contato conosco:
HSMinfo@entrust.com