Fastcom은 높은 수준의 보안을 유지하면서 코드 서명 효율성을 높입니다

www.fastcom-technology.com

당면 과제: FOXTEL이 경쟁 우위를 유지하는 데 도움이 되는 향상된 셋톱 박스

유료 TV 시장은 경쟁이 치열하며 소비자는 늘 새로운 콘텐츠를 필요로 합니다. Foxtel이 유료 TV 시장을 주도하는 호주에서도, 새로운 사업자의 시장 진출은 Foxtel이 계속해서 훌륭한 가입자 경험을 제공할 수 있도록 혁신에 더욱 집중해야 함을 의미합니다.

Foxtel은 향상된 콘텐츠 스트림, 더 많은 녹화 공간 등 가입자 만족도를 높이는 새로운 기능이 탑재된 iQ3 셋톱 박스(STB)를 출시했습니다.

iQ3를 설계할 때, Foxtel은 Fastcom과 협력하여 세 가지 핵심 요구 사항을 확인했습니다. 특히 STB는 다음과 같은 기능이 필요했습니다.

- 멀티 벤더 보안 전략을 지원하여 Foxtel이 필요에 따라 여러 콘텐츠 공급업체의 스트림을 제공하고 제공 업체를 변경할 수 있는 유연성을 제공
- 구독 전용 콘텐츠에 대한 무단 액세스 방지
- 배포된 장치를 Foxtel이 직접 제어하여 고객 요구에 대응하는 효율적인 업데이트 가능

솔루션: ENTRUST가 지원하는 FASTCOM MCAS

Foxtel의 요구 사항을 기반으로 Fastcom은 매우 안전한 암호화가 필요하다는 것을 신속하게 결정하면서 STB 제조부터 시작하여 MCAS(다중 조건부 액세스 시스템) 솔루션에 대한 초기 사양을 개발했습니다. 실제로 장치의 모든 암호화 및 해독에 대한 신뢰 루트를 제공하는 루트 키가 iQ3의 코어 프로세서에 빌트인되어 있고, 이것이 각 장치의 ID를 설정하고 조건부 액세스 시스템(CAS)/디지털 권한 관리(DRM) 솔루션으로부터 세부 정보를 암호화하는 키 생성 여부를 판단합니다.

Fastcom

애플리케이션에 필요한 보안 수준을 달성하기 위해 Fastcom은 FIPS 인증 환경 내에서 키 파생 알고리즘을 실행해야 한다고 결정했습니다. Fastcom은 HSM(하드웨어 보안 모듈)에 익숙했으며 이것이 그들에게 필요한 보안 및 모듈성을 제공한다는 것도 잘 알고 있었습니다.

여러 벤더의 제품을 검토한 후, Fastcom은 프로젝트의 모든 보안 요구 사항을 충족하는 탁월한 능력 때문에 Entrust nShield® HSM을 선택했습니다. 특히, nShield CodeSafe는 Fastcom이 자체 파생 알고리즘을 실행하고 FIPS 140-2 Level 3 경계 내에서 키를 보호할 수 있는 탁월한 기능을 제공합니다.

구현 단계에서 Entrust 팀은 CodeSafe 환경 내에서 암호화 애플리케이션 코드의 일부를 개발했으며 Fastcom은 이를 추가 수정했습니다. 이로써 Fastcom은 솔루션을 구축하는 데 필요한 위치 선점이 가능해졌고, 핵심 코드의 소유권도 손쉽게 장악할 수 있게 되었습니다.

Fastcom은 nShield HSM을 사용하여 Foxtel이 iQ3 STB에 통합할 수 있도록 단일 루트 키에서 여러 하위 키를 추출합니다. 이 키를 CAS 벤더가 CAS/DRM 솔루션을 통해 제공되는 세부 정보를 암호화하는 데 사용합니다. 따라서 해당 정보가 특정 STB에서만 제출될 수 있게 됩니다.

Entrust nShield HSM으로 MCAS 솔루션을 강화함으로써, Foxtel은 iQ3 STB에 맞는 애플리케이션, 미들웨어 및 CAS/DRM 솔루션을 자유롭게 선택할 수 있습니다. 이를 통해 멀티 벤더 접근 방식은 물론, 필요에 따라 STB에 대한 효율적이고 저렴한 업데이트가 가능하며 유료 TV 가입자에게 프리미엄 콘텐츠를 제공할 수 있습니다. Fastcom은 MCAS 모델을 사용하여 멀티 벤더 보안 접근 방식을 활용하는 다른 고객 구내 장비 솔루션을 개발할 계획입니다.

주요 장점

- 값비싼 STB 업데이트 없이 CAS 벤더 및 미들웨어를 쉽게 변경
- 원격으로 배포된 장치를 직접 제어하여 가입자 경험 향상
- 프리미엄 콘텐츠를 보호하여 수익원 보호

솔루션 소개

Entrust nShield HSM

Entrust nShield HSM은 암호화 처리, 키 보안 및 관리를 안전하게 이행할 수 있도록 강화된 조작 방지 환경을 제공합니다. 이 제품으로는 원칙적인 암호 시스템과 모범 사례 관련, 널리 인정받는 표준과 새로운 표준 모두를 충족하고, 고도로 정밀한 보안 솔루션을 배포할 수 있을 뿐만 아니라 고도로 효율적인 운영 수준을 유지할 수 있습니다.

Entrust nShield HSM은 독립 기관의 인증을 받았으며, 정량화가 가능한 보안 벤치 마크를 설정하여 규정 준수 의무 및 내부 정책을 지원할 수 있다는 확신을 고객에게 제공합니다. Entrust nShield HSM은 휴대용 장치에서 고성능 데이터 센터 어플라이언스에 이르는 모든 일반적인 배포 시나리오를 지원하기 위해 다양한 폼 팩터로 제공됩니다.

Fastcom

ENTRUST CODESAFE

Entrust CodeSafe 개발자 툴킷은 민감한 애플리케이션을 FIPS 140-2 Level 3 인증 nShield HSM의 보호되는 경계 내에서 이동할 수 있는 고유한 기능을 제공합니다. 이 접근 방식을 사용하면 애플리케이션을 조작으로부터 보호하고 보안 환경 내에서 데이터를 해독, 처리 및 암호화할 수 있습니다.

CODESAFE는 다음과 같은 장점을 제공합니다.

- 환경에 관계없이 민감한 애플리케이션에 대한 원격 제어를 제공하고, 고객이 사용하는 운영체제 또는 구성에 관계없이 서버나 메인프레임을 가리지 않고 암호화 서비스를 제공하여 지적 재산 도난을 방지합니다. 또한 CodeSafe를 사용하면 애플리케이션 또는 장치 소유자가 물리적으로 다른 위치에서도 최신 애플리케이션 실행 환경을 유지할 수 있습니다.
- 출시 전에 무결성을 확인할 수 있도록 신뢰할 수 있는 애플리케이션에 디지털 서명 기능을 제공하여 해커나 불량 관리자의 공격으로부터 애플리케이션을 보호합니다. 또한 CodeSafe는 아웃소싱 및 계약을 활용하는 통제되지 않은 환경에서도 애플리케이션을 도난으로부터 보호합니다.
- 진정한 종단간 SSL 암호화를 제공하고, SSL을 종료하며, HSM 내에서 민감한 데이터를 처리하여 공격으로부터 보호함으로써 민감한 SSL 데이터를 보호합니다.

FASTCOM 소개

스위스 독립 기업인 Fastcom은 유료 TV 시장에 보안 솔루션과 기술 컨설팅을 제공합니다.

Fastcom의 MCAS 솔루션은 유료 TV 셋톱 박스(STB)와 같은 고객 구내 장비에 대한 통합 라이선싱 인가 서비스 세트입니다. 확장 가능한 모듈식 인프라를 활용하는 MCAS는 여러 CAS(조건부 액세스 시스템) 및 DRM(디지털 권한 관리) 솔루션을 동시에 지원하는 동시에 유료 TV 운영자가 현장에서 STB를 직접 제어할 수 있게 해줍니다.

FOXTEL 소개

Foxtel은 호주 최고의 미디어 회사로 전국 280만 이상의 가정에 유료 TV 및 인터넷 서비스를 제공합니다.

ENTRUST 소개

Entrust는 믿을 수 있는 신원, 결제 및 데이터 보호를 가능케 함으로써 안전한 세상을 유지합니다. 사람들은 국경을 넘고, 구매를 하고, 전자 정부 서비스에 접속하고 기업 네트워크에 로그인하는 것이 원활하고 안전한 경험이기를 오늘날, 그 어느 때보다도 더 요구합니다. Entrust는 이와 같은 모든 상호작용의 핵심에 있는 디지털 보안 및 자격 증명 발급 솔루션에 있어 견줄 데 없는 다양성을 자랑합니다. 2,500명이 넘는 동료 및 글로벌 파트너로 구성된 네트워크, 그리고 150개국 이상의 고객을 보유한 당사는 세계에서 가장 신뢰 받는 기관들의 신뢰를 받고 있습니다.

Fastcom

ENTRUST NSHIELD HSM을 사용하면 다음과 같은 장점을 누릴 수 있습니다.

- 변조 방지 하드웨어 내에서 암호키 및 암호화 작업에 공인된 보안을 제공하여 중요한 애플리케이션에 대해 한층 강화된 안전성 제공
- 비용 효율적인 암호화를 가속화하고, 기존 데이터센터나 클라우드 환경과는 비교할 수 없는 운영 유연성 확보
- 소프트웨어 한정 암호화의 보안 취약성과 성능 문제 극복
- 규제 준수 관련 비용 절감, 백업 및 원격 관리 등을 비롯한 일상적인 키 관리 업무 감소 Entrust nShield HSM을 사용하면 필요한 용량만 구매하고 요구 사항 변화에 맞추어 손쉽게 솔루션을 확장할 수 있습니다

왜 ENTRUST일까요?

- Entrust는 자사가 갖춘 풍부한 지식과 구현 전문성과 함께 nShield HSM의 보안 및 고유 기능을 근거로 사업을 수주했습니다.

Entrust는 Fastcom에게 다음과 같은 장점을 제공했습니다.

- 업계를 선도하는 보안. Fastcom은 iQ3 STB가 현장에 배포되면 무단 액세스로부터 프리미엄 콘텐츠를 보호할 수 있다고 Foxtel이 신뢰할 수 있는 솔루션을 제공해야 한다는 점을 인식했습니다. Entrust nShield HSM을 핵심으로 하는 MCAS 솔루션은 최고 수준의 보안 및 기능을 제공합니다.
- 암호화 알고리즘을 실행하기 위한 보호 받는 환경입니다. Fastcom은 최고 수준의 보호를 구현하기 위해 자체 키 파생 알고리즘을 개발했습니다. Entrust CodeSafe는 HSM의 FIPS 인증 경계 내에서 애플리케이션을 실행할 수 있는 유일한 솔루션으로, 이러한 경계 내의 애플리케이션은 표준 서버 기반 플랫폼에 확산된 공격으로부터 보호 받습니다.
- 높은 수준의 보안 전문성. Entrust 전문 서비스 팀의 전문가들은 Fastcom과 협력하여 iQ3 STB를 보호하는 신뢰 루트 키를 생성하는 애플리케이션을 구축하기 시작했습니다. Fastcom은 이 새로운 도약을 활용하여 MCAS 솔루션 개발에 박차를 가했습니다.

mcas

에서 자세히 보기
entrust.com/HSM

ENTRUST

연락처:
HSMinfo@entrust.com