Fastcom erhöht Effizienz des Code Signing bei Wahrung eines hohen Maßes an Sicherheit

www.fastcom-technology.com

DIE HERAUSFORDERUNG: VERBESSERTE SET-TOP-BOX ZUR WAHRUNG DES WETTBEWERBSVORTEILS VON FOXTEL

Der Pay-TV-Markt ist stark umworben und die Kunden fordern regelmäßig Zugang zu neuen Inhalten. Sogar in Australien, wo Foxtel Marktführer für Pay-TV ist, muss das Unternehmen aufgrund aufkommender neuer Anbieter zunehmend Innovationen hervorbringen, um seinen Abonnenten weiterhin eine großartige Erfahrung bieten können.

Foxtel führte die iQ3-Set-Top-Box (STB) ein, die erweiterte Streaming-Inhalte, mehr Speicherplatz und andere neue Funktionen bietet, die die Zufriedenheit der Abonnenten steigern sollten.

Bei der Entwicklung von iQ3 identifizierte Foxtel in Zusammenarbeit mit Fastcom drei wichtige Anforderungen. Die STB musste Folgendes bieten:

- Unterstützung einer Multivendor-Sicherheitsstrategie, wodurch Foxtel die Flexibilität erlangt, Streams von unterschiedlichen Anbietern zu ermöglichen sowie die Anbieter gegebenenfalls zu ändern
- Verhinderung unautorisierten Zugriffs auf abonnementpflichtige Inhalte
- Direkte Kontrolle für Foxtel über bereitgestellte Geräte für effiziente Updates, die auf die Bedürfnisse der Kunden eingehen

DIE LÖSUNG: FASTCOM MCAS, ERMÖGLICHT DURCH ENTRUST

Auf Grundlage der Bedürfnisse von Foxtel entwickelte Fastcom die anfänglichen Eigenschaften für sein Multiple Conditional Access System (MCAS) und stellte schnell fest, dass eine sichere Verschlüsselung vonnöten war – bereits bei der Herstellung der STBs. Der Root-Key, Vertrauensanker für alle Ver- und Entschlüsselungsprozesse im Gerät, musste in den Kernprozessor des iQ3 integriert werden, um die Identität jedes Geräts festzustellen. Dadurch könnte die Erstellung von Schlüsseln zur Verschlüsselung von Inhalten aus Conditional Access Systems (CAS)/Systemen für digitale Rechteverwaltung (DRM) erfolgen.

Fastcom

Um das erforderliche Maß an Sicherheit zu erreichen, beschloss Fastcom, dass der Schlüsselableitungsalgorithmus innerhalb einer FIPS-zertifizierten Umgebung ausgeführt werden musste. Fastcom kannte Hardware-Sicherheitsmodule (HSMs) und wusste, dass diese die erforderliche Sicherheit und Modularität ermöglichen würden.

Nach Berücksichtigung verschiedener Angebote, wählte Fastcom Entrust nShield® HSMs aus, da nur sie die Möglichkeit boten, alle nötigen Sicherheitsanforderungen des Projekts zu erfüllen. Ganz konkret bietet nShield CodeSafe die einzigartige Möglichkeit für Fastcom, seinen eigenen Ableitungsalgorithmus zu verwenden und Schlüssel innerhalb der FIPS 140-2 Level 3-Grenzen zu schützen.

Während der Implementierungsphase entwickelte das Team von Entrust einen Teil des Codes für die Verschlüsselungsanwendung innerhalb der CodeSafe-Umgebung, den Fastcom anschließend weiterentwickelte. So erhielt Fastcom den Vorsprung, der nötig war, um die Lösung auszubauen und gleichzeitig die Inhaberschaft am Kerncode zu übernehmen.

Mithilfe des nShield HSM leitet Fastcom verschiedene untergeordnete Schlüssel aus einem einzelnen Root-Key ab, die Foxtel in die iQ3-STBs integrieren kann. Die Schlüssel werden von CAS-Anbietern verwendet, um Inhalte, die über CAS-/DRM-Lösungen bereitgestellt werden, zu verschlüsseln und so sicherzustellen, dass die Inhalte nur über bestimmte STBs abgerufen werden können.

Mit Entrust nShield HSMs als Grundlage der MCAS-Lösung kann Foxtel die Anwendungen, Middleware und CAS-/DRM-Lösungen für seine iQ3-STBs frei wählen. So ist nicht nur ein Multivendor-Ansatz möglich, sondern auch effiziente, kostengünstige Updates der STBs sowie die Bereitstellung von Premiuminhalten für Pay-TV-Abonnenten. In Zukunft möchte Fastcom mithilfe des MCAS-Modells weitere Lösungen für Kundengeräte entwickeln, die seinen Multivendor-Sicherheitsansatz nutzen.

WICHTIGSTE VORTEILE

- Einfache Änderung der CAS-Anbieter und Middleware ohne teure Updates der STBs
- Direkte Kontrolle über ferninstallierte Geräte für ein verbessertes Nutzererlebnis
- Schutz der Einnahmequellen durch Sicherung von Premiuminhalten

ÜBER DIE LÖSUNG

Entrust nShield HSMs

Entrust nShield HSMs bieten eine gefestigte, manipulationssichere Umgebung für sichere kryptographische Verarbeitung, Schlüsselschutz und Schlüsselverwaltung. Mit diesen Geräten können hochsichere Lösungen eingesetzt werden, die etablierte sowie neue Sorgfaltsstandards für kryptographische Systeme und Praktiken erfüllen, während gleichzeitig ein hohes Maß an betrieblicher Effizienz beibehalten wird.

Entrust nShield HSMs sind von unabhängigen Behörden zertifiziert und legen quantifizierbare Sicherheits-Benchmarks fest, sodass Kunden sich darauf verlassen können, dass Compliance-Vorgaben und interne Richtlinien eingehalten werden. Entrust nShield HSMs sind in verschiedenen Formfaktoren erhältlich, um alle gängigen Einsatzszenarien von tragbaren Geräten bis hin zu Hochleistungs-Rechenzentrumsgeräten zu unterstützen.

Fastcom

ENTRUST CODESAFE

Das Entrust CodeSafe Entwickler-Toolkit bietet die einzigartige Möglichkeit, sensible Anwendungen innerhalb des geschützten Umkreises eines FIPS 140-2 Level 3-zertifizierten nShield HSM zu verschieben. Durch diesen Ansatz sind Anwendungen vor Manipulationen geschützt und können Daten innerhalb dieser sicheren Umgebung entschlüsseln, verarbeiten und verschlüsseln.

VORTEILE VON CODESAFE FÜR UNTERNEHMEN:

- **Der Diebstahl geistigen Eigentums wird verhindert**, indem die Fernsteuerung sensibler Anwendungen unabhängig von der Umgebung ermöglicht und kryptographische Dienste unabhängig vom Betriebssystem oder der Konfiguration des Kunden, ob Server oder Mainframe, angeboten werden können. CodeSafe ermöglicht es Anwendungs- oder Geräteeigentümern außerdem, die Anwendungsausführungsumgebung ohne physische Anwesenheit auf dem neuesten Stand zu halten.
- **Anwendungen werden vor Angriffen durch Hacker oder betrügerische Administratoren geschützt**, da vertrauenswürdige Anwendungen digital signiert werden können, sodass ihre Integrität vor dem Start überprüft wird. CodeSafe schützt Anwendungen auch vor Diebstahl, selbst in nicht kontrollierten Umgebungen, wo mit Outsourcing und Auftragsvergabe gearbeitet wird.
- **Sensible SSL-Daten** werden durch eine echte End-to-End-SSL-Verschlüsselung, die Beendigung von SSL und die Verarbeitung sensibler Daten innerhalb des HSM vor Angriffen geschützt.

ÜBER FASTCOM

Fastcom ist ein unabhängiges Schweizer Unternehmen, das Sicherheitslösungen und technische Beratung am Pay-TV-Markt anbietet.

Die MCAS-Lösung von Fastcom ist ein integriertes Set mit Diensten für Lizenzierungsstellen für Kundengeräte wie Pay-TV-Set-Top-Boxen (STBs). Durch die Nutzung einer modularen und skalierbaren Infrastruktur unterstützt MCAS gleichzeitig mehrere Conditional Access Systems (CAS) und Lösungen für digitale Rechteverwaltung (DRM), während Pay-TV-Anbieter direkte Kontrolle über die STBs im Feld haben.

ÜBER FOXTEL

Foxtel ist das größte Medienunternehmen in Australien und bietet über 2,8 Millionen Haushalten im ganzen Land Pay-TV sowie Internetdienste an.

ÜBER ENTRUST

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

Fastcom

MIT ENTRUST NSHIELD HSMS KÖNNEN SIE:

- zertifizierten Schutz für kryptographische Schlüssel und Operationen innerhalb manipulationssicherer Hardware bereitstellen, der die Sicherheit kritischer Anwendungen deutlich erhöht,
- in herkömmlichen Rechenzentren und Cloud-Umgebungen kryptographische Operationen kostengünstig beschleunigen und beispiellose operative Flexibilität erreichen,
- die Sicherheitslücken und das mangelnde Leistungsvermögen einer Kryptographielösung, die rein Software-basiert ist, überwinden,
- die Kosten für die Einhaltung gesetzlicher Vorschriften und die täglichen wichtigen Verwaltungsaufgaben einschließlich Back-up und Fernverwaltung senken. Sie kaufen nur die Entrust nShield HSMs, die Sie aktuell benötigen. Sollten Ihre Anforderungen zunehmen, können sie die Kapazität Ihrer Lösung jederzeit anpassen

WARUM ENTRUST?

- Entrust erhielt den Auftrag aufgrund der gebotenen Sicherheit und der einzigartigen Funktionalität des nShield HSM, gestützt durch die fundierte Implementierungserfahrung von Entrust.

Entrust bot Fastcom:

- Branchenführende Sicherheit. Fastcom wusste, dass es eine Lösung brauchte, mit der Foxtel die Premiuminhalte zuverlässig vor unautorisiertem Zugriff schützen kann, sobald die iQ3-STBs bei den Kunden sind. Aufbauend auf Entrust nShield HSMs bietet die MCAS-Lösung ein Höchstmaß an Sicherheit und Funktionalität.
- Eine geschützte Umgebung zur Ausführung seiner Verschlüsselungsalgorithmen. Fastcom hatte seinen eigenen Schlüsselableitungsalgorithmus entwickelt und wollte diesen bestmöglich schützen. Entrust CodeSafe ist die einzige Lösung, die es Anwendungen möglich macht, sich innerhalb der FIPS-zertifizierten Grenzen des HSM zu bewegen, wo sie vor Angriffen sicher sind, wie sie etwa auf Server-basierten Plattformen vorkommen.
- Umfassendes Sicherheitsfachwissen. Die Experten des Teams von Entrust arbeiteten mit Fastcom zusammen, um die Entwicklung der Anwendung zu starten, die die Root-of-Trust-Schlüssel zum Schutz der iQ3-STBs ableiten würde. Fastcom konnte diesen Vorsprung nutzen, um die Entwicklung der MCAS-Lösung voranzutreiben.

mcas

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com