Fastcom aumenta l'efficienza della firma del codice mantenendo alti i livelli di sicurezza

www.fastcom-technology.com

LA SFIDA: UN SET-TOP BOX MIGLIORE PER MANTENERE IL VANTAGGIO COMPETITIVO

L'aspettativa di ricevere regolarmente nuovi contenuti rende quello della pay TV un mondo altamente competitivo. Persino in Australia, dove Foxtel è leader di mercato, l'introduzione di nuovi operatori l'ha obbligata a concentrarsi ancora di più sull'innovazione per poter continuare a offrire esperienze eccezionali agli abbonati.

Foxtel ha introdotto il set-top box (STB) iQ3, che offre uno streaming migliore dei contenuti, un maggiore spazio di registrazione e altre nuove funzionalità destinate ad aumentare la soddisfazione degli abbonati.

Foxtel ha coinvolto Fastcom per la progettazione di iQ3, identificando tre requisiti fondamentali. Nello specifico i STB dovevano:

- Supportare una strategia di sicurezza concertata tra i diversi distributori che permettesse a Foxtel di offrire contenuti da più fornitori e di cambiare questi ultimise necessario
- Impedire l'accesso non autorizzato ai contenuti esclusivi
- Garantire che Foxtel avesse un controllo diretto sui dispositivi distribuiti per permettere aggiornamenti efficaci secondo le esigenze dei clienti

LA SOLUZIONE: MCAS FASTCOM, ABILITATA DA ENTRUST

Basandosi sulle esigenze di Foxtel, Fastcom ha sviluppato le specifiche iniziali per la soluzione MCAS (Multiple Conditional Access System), determinando ben presto la necessità di una crittografia con un alto livello di sicurezza a partire dalla produzione dei STB stessi. Infatti, la chiave di root che fornisce la root of trust per la crittografia e decriptazione sul dispositivo doveva essere masterizzata nei core processor dell'iQ3, determinando l'identità di ciascun apparecchio e permettendo la creazione di chiavi per crittografare contenuti da soluzioni CAS (Conditional Access System) o DRM (Digital Rights Management).

Fastcom

Per raggiungere il livello di sicurezza richiesto dall'applicazione, Fastcom ha determinato la necessità di eseguire l'algoritmo di derivazione della chiave all'interno di un ambiente certificato FIPS. Fastcom aveva esperienza con gli HSM (Hardware Security Module) e sapeva che avrebbero fornito la sicurezza e modularità necessarie.

Dunque, dopo aver preso in considerazione una serie di offerte, ha selezionato gli HSM nShield® di Entrust a causa della loro ineguagliabile capacità di soddisfare tutti i requisiti di sicurezza del progetto. Nello specifico, nShield CodeSafe presenta una funzionalità ineguagliabile che permette a Fastcom di eseguire l'algoritmo proprietario di derivazione e di proteggere le chiavi all'interno di un perimetro di sicurezza conforme allo standard FIPS 140-2 di livello 3.

Durante la fase di implementazione, il team di Entrust ha sviluppato una parte del codice crittografico all'interno dell'applicazione in ambiente CodeSafe, modificato in seguito da Fastcom. In questo modo è stato possibile creare la soluzione detenendo al contempo la titolarità del codice principale.

Grazie agli HSM nShield, Fastcom deriva più chiavi subordinate da una singola chiave di root che Foxtel può incorporare nei STB iQ3. Le chiavi vengono usate dai fornitori CAS per crittografare contenuti forniti tramite soluzioni CAS/DRM, garantendo l'accesso ai contenuti esclusivamente su un STB specifico.

Grazie agli HSM nShield di Entrust alla base della soluzione MCAS, Foxtel è in grado di scegliere liberamente le applicazioni, il middleware e le soluzioni CAS/DRM per i propri STB iQ3, permettendo un approccio concertato tra i diversi distributori e aggiornamenti efficaci e a basso costo dei STB quando necessario, nonché la fornitura di contenuti premium senza soluzione di continuità. In futuro, Fastcom prevede di utilizzare il modello MCAS per sviluppare altre soluzioni on-premise presso il cliente per sfruttare il suo approccio alla sicurezza concertato tra i vari distributori.

VANTAGGI PRINCIPALI

- Facilità nel cambiare fornitori CAS e middleware senza dover ricorrere ad aggiornamenti costosi dei STB
- Un controllo diretto sui dispositivi distribuiti da remoto che avrebbe migliorato l'esperienza del cliente
- Protezione dei flussi di reddito tramite la messa in sicurezza dei contenuti premium

DETTAGLI DELLA SOLUZIONE

HSM nShield di Entrust

Gli HSM nShield di Entrust forniscono un ambiente affidabile a prova di manomissione per offrire attività sicure di elaborazione crittografica, protezione e gestione delle chiavi. Consentono di implementare soluzioni a elevata sicurezza che soddisfano standard di diligenza consolidati ed emergenti per i sistemi crittografici e le migliori pratiche, mantenendo comunque alti i livelli di efficienza operativa.

Gli HSM Entrust nShield sono certificati da autorità indipendenti, che stabiliscono benchmark di sicurezza quantificabili per assicurare ai clienti il rispetto degli obblighi di conformità e delle norme aziendali. Gli HSM Entrust nShield sono disponibili in vari fattori di forma adatti agli scenari di implementazione più comuni, dai dispositivi portatili alle appliance ad alte prestazioni nei data center.

Fastcom

CODESAFE DI ENTRUST

Il kit di strumenti per sviluppatori CodeSafe di Entrust offre l'esclusiva funzionalità di spostare applicazioni sensibili all'interno del perimetro protetto nShield HSM con certificazione FIPS 140-2 di livello 3. Attraverso l'uso di questo approccio, le applicazioni sono protette da manipolazioni e possono decodificare, processare e codificare i dati all'interno di un ambiente sicuro.

CODESAFE CONSENTE ALLE ORGANIZZAZIONI DI:

- **Prevenire i furti di proprietà intellettuale** fornendo il controllo remoto delle applicazioni sensibili indipendentemente dall'ambiente e offrendo servizi di crittografia indipendentemente dal sistema operativo o dalla configurazione utilizzata dal cliente, sia server che mainframe. CodeSafe consente, inoltre, ai proprietari di applicazioni o dispositivi portatili di mantenere aggiornato l'ambiente di esecuzione delle applicazioni senza presenza fisica
- **Proteggere le applicazioni dagli attacchi** di hacker o amministratori disonesti, fornendo la possibilità di firmare digitalmente le applicazioni affidabili in modo che la loro integrità sia verificata prima del lancio. In aggiunta, CodeSafe protegge le applicazioni dai furti, anche in ambienti non controllati che utilizzano l'outsourcing e la stipula di contratti
- **Proteggere i dati SSL sensibili** fornendo una vera e propria crittografia SSL end-to-end, terminando le sessioni SSL ed elaborando i dati sensibili all'interno dell'HSM per proteggerli dagli attacchi

INFORMAZIONI SU FASTCOM

Fastcom, un'azienda svizzera indipendente, fornisce soluzioni di sicurezza e consulenza tecnica al settore della pay TV.

La soluzione MCAS di Fastcom è una gamma integrata di servizi di licenza per le soluzioni on-premise presso il cliente, come i STB (set-top box) per la pay TV. Sfruttando un'infrastruttura modulare e scalabile, MCAS supporta allo stesso tempo soluzioni CAS (Multiple Conditional Access System) e DRM (Digital Rights Management), garantendo agli operatori della pay TV un controllo diretto sui STB sul campo.

INFORMAZIONI SU FOXTEL

Foxtel è la principale azienda mediatica australiana che offre servizi di pay TV e internet a oltre 2,8 milioni di case in tutto il Paese.

INFORMAZIONI SU ENTRUST

Entrust permette al mondo di continuare ad avanzare in sicurezza attraverso sistemi di identificazione, pagamento e protezione dei dati ad alta affidabilità. Oggi più che mai, le persone si aspettano esperienze sicure e ottimizzate, che si tratti di attraversare le frontiere tra Stati, effettuare un acquisto, accedere ai servizi elettronici della pubblica amministrazione o collegarsi a una rete aziendale. Entrust offre un'ineguagliabile gamma di soluzioni di sicurezza digitale ed emissione di credenziali, il vero fondamento di tutte queste interazioni. Con oltre 2.500 colleghi, una rete di partner globali e clienti in più di 150 Paesi, non sorprende che le organizzazioni più fidate al mondo scelgano noi.

Fastcom

CON GLI HSM NSHIELD DI ENTRUST È POSSIBILE:

- Ottimizzare la sicurezza delle applicazioni critiche fornendo una protezione certificata per le chiavi e le operazioni crittografiche all'interno di hardware a prova di manomissione
- Ottenere un'accelerazione crittografica a costi contenuti e una flessibilità operativa ineguagliata tanto nei data center tradizionali quanto negli ambienti cloud
- Superare i rischi di sicurezza e le difficoltà prestazionali della crittografia basata unicamente su software
- Ridurre i costi relativi alla conformità normativa e alle attività quotidiane di gestione delle chiavi, tra cui il back-up e la gestione remota. Gli HSM nShield di Entrust consentono alle aziende di acquistare solo la capacità di cui hanno bisogno, ma offrono la scalabilità necessaria a ridimensionare la soluzione in risposta all'evoluzione delle esigenze

PERCHÉ ENTRUST?

- Entrust si è aggiudicata l'incarico grazie alla sicurezza e alla funzionalità dei suoi HSM nShield, supportati dalle competenze di Entrust sulla loro implementazione.

Entrust ha offerto a Fastcom:

- Una sicurezza leader del settore. Fastcom doveva creare una soluzione che Foxtel potesse utilizzare per proteggere contenuti premium da accessi non autorizzati a partire dalla distribuzione dei STB iQ3 nel mercato. Grazie agli HSM nShield di Entrust, la soluzione MCAS offre i più alti livelli di sicurezza e funzionalità.
- Un ambiente protetto per l'esecuzione dell'algoritmo crittografico. Fastcom aveva sviluppato un proprio algoritmo di derivazione della chiave per cui voleva garantire il più alto livello di sicurezza disponibile sul mercato. CodeSafe di Entrust è l'unica soluzione che consente alle applicazioni di funzionare all'interno del limite crittografico dell'HSM certificato FIPS, dove vantano una protezione dagli attacchi che sono diffusi sulle piattaforme standard basate su server.
- Competenza garantita nel mondo della sicurezza. Gli esperti del team di servizi professionali di Entrust hanno collaborato con Fastcom per creare l'applicazione che avrebbe derivato le chiavi di root per proteggere i STB iQ3. Fastcom ha sfruttato questo vantaggio per accelerare lo sviluppo della soluzione MCAS

mcas

Scopri di più su
entrust.com/HSM

ENTRUST

Per contattarci:
HSMinfo@entrust.com