CryptoGuard CAS



Виробник: CryptoGuard

Опис

CryptoGuard CAS - це система умовного доступу для цифрового ТБ. Вона дозволяє оператору кабельного ТБ повністю контролювати доступ абонентів до телеканалів і окремих програм. Сигнали цифрового ТБ передаються в мережу в зашифрованому вигляді, що дозволяє обмежувати до них доступ і надавати його тільки по платній підписці.

Багато виробників і власники контента також вимагають, щоб їх телепрограми поширювалися тільки в закритому вигляді. Для перегляду зашифрованих телеканалів Ваші абоненти повинні мати спеціальну смарткарту, вставлену в абонентський приймач (STB) або ж в в модуль умовного доступу (CAM). CryptoGuard CAS працює зі всіма технологіями: супутникове ТБ, кабельне ТБ, наземне цифрове ТБ і IPTV. Також підтримуються будь-які формати - чи то SD, чи HD.

Гарантований захист

Картки CryptoGuard захищені від всіх відомих методів зламу систем скремблювання, даючи Вам і Вашим клієнтам максимальний захист від піратів, і Вам, як оператору, гарантовані максимальні продажі.
Піратські картки не можуть бути використані, щоб розблокувати коди Cryptoguard. Компанія CryptoGuard настільки впевнена в цьому, що гарантує заміну ключів і коду існуючих смарткарт. Однією з умов є те, що Ви використовуєте CryptoGuard смарткарти із затвердженими абонентськими приймачами або модулями умовного доступу.

Pairing

Система шифрування CryptoGuard включає в себе ефективний захист від шарінга без будь-яких додаткових витрат. Абонентська смарткарта в парі з приставкою або CA модулем складають єдине ціле. Карта працює тільки для одного абонента. Це називається «pairing» і означає, що секретний ключ не може поширюватися через Інтернет. Багато правовласники контента тепер вимагають, щоб здвоєння обов'язково використовувалося для розповсюдження програм в HD якості.

Архітектура сервера Cryptoguard CAS

Сервер CryptoGuard включає в себе:

- Систему управління абонентами (SMS)
- Генератор ECM і EMM
- Генератор сервісних таблиць PSI/SI
- Сервер для мовлення OTA оновлень для приймачів
- Генератор і редактор EIT

Усередині ECM в зашифрованому з допомогою operating keys вигляді передаються CW від аудіо- і відеопотоків програми. CW передаються парами (парне і непарне, фактично поточне і наступне), що дозволяє приймачу почати дескремблювання відразу після налаштування на програму. Також в ECM передається додаткова інформація, яка визначає, чи дозволений кожному конкретному абоненту перегляд поточної програми або передачі. Ще в ECM передається поточна дата і час, які порівнюються з періодом дії підписки абонента на дану програму або пакет програм.

У EMM передаються індивідуальні та групові дані про підписки абонентів, у тому числі і про скасування підписок. З допомогою EMM також можуть оновлюватися діючі ключі. Для шифрування даних і формування контрольної суми в EMM використовуються management keys або майстер-ключі (master keys). Управляючі ключі зазвичай прошиваються в смарт-карту при її випускові та більше ніколи не змінюються.

Характеристики

Максимальна кількість абонентів	До 1.000.000
Мови інтерфейсу системи управління	Англійська, Шведська, Польська, Іспанська, Німецька, Французька. Може бути адаптований для будь-якої мови.
Вбудований біллінг і система управління абонентами	Є, web-based
Можливість інтеграції з зовнішнім біллінгом	Є. З допомогою документованого API
БД для зберігання даних	MySQL
Ліцензування	Без обмеження по кількості абонентів
Pay-TV, PPV	Підтримується
Розмежування ролей	Є. Вбудована система управління правами доступу до інтерфейсу
Кількість телеканалів	Не обмежена. Кількість AC - 512
Кількість пакетів телеканалів	Не обмежена
Кількість мультиплексорів, що підключається	Не обмежена
Відправлення текстових повідомлень абонентам	Є

Налаштовуване повідомлення при відсутності прав на відкриття каналу	Є. Наприклад «У Вас відсутні права на відкриття цього каналу. Зв'яжіться зі службою підтримки 08-xxxxxx»
Стандарт шифрування	Simulcrypt ETSI TS 103 197 v 1.2.1 і v 1.3.1
Зашифрований канал для обміну інформацією між смарткартою і абонентським	Є, унікальний для кожного типу приймача
Прив'язка смарткарти до приймача (Pairing)	Є, двостороння прив'язка, контрольована на канальному рівні
Захист від «інтернет шарінга» типу «Dreambox»	Є, і в смарткарт, і в абонентському приймачеві
Активація смарткарт	На пакет, на канал, на вказаний період часу, з контролем позитивного і негативного балансу на рахунку
Підтримувані типи	Тільки виробники, що пройшли сертифікацію на максимальний рівень захисту
Оновлення ключів	«Over-the-air»
Країна-розробник	Швеція
Оновлення версій	Регулярне оновлення версій серверного ПЗ протягом усього терміну техпідтримки
Швидкість каналу для обміну даними між серверами	Мінімум 384kbit/s (3G)
Можливість редагування PSI/SI таблиць	Є, вбудований редактор і генератор NIT, SDT actual/other, CAT, TDT, TOT і користувальницьких дескрипторів
Можливість редагування і мовлення EIT таблиць	Є, вбудований редактор і генератор EIT з можливістю імпорту EPG з файлів у форматі XMLTV

Системні вимоги до сервера:

- HP ProLiant DL320 G6 або аналогічний
- процесор не нижче Intel Xeon 1.5Ghz Xeon 64-bit
- RAM НЕ менше 2 GB
- HDD не менше 250GB
- 1 USB 2.0 порт
- 2 гігабітних мережевих адаптери
- OS Linux CentOS 5.8 64bit x86_64