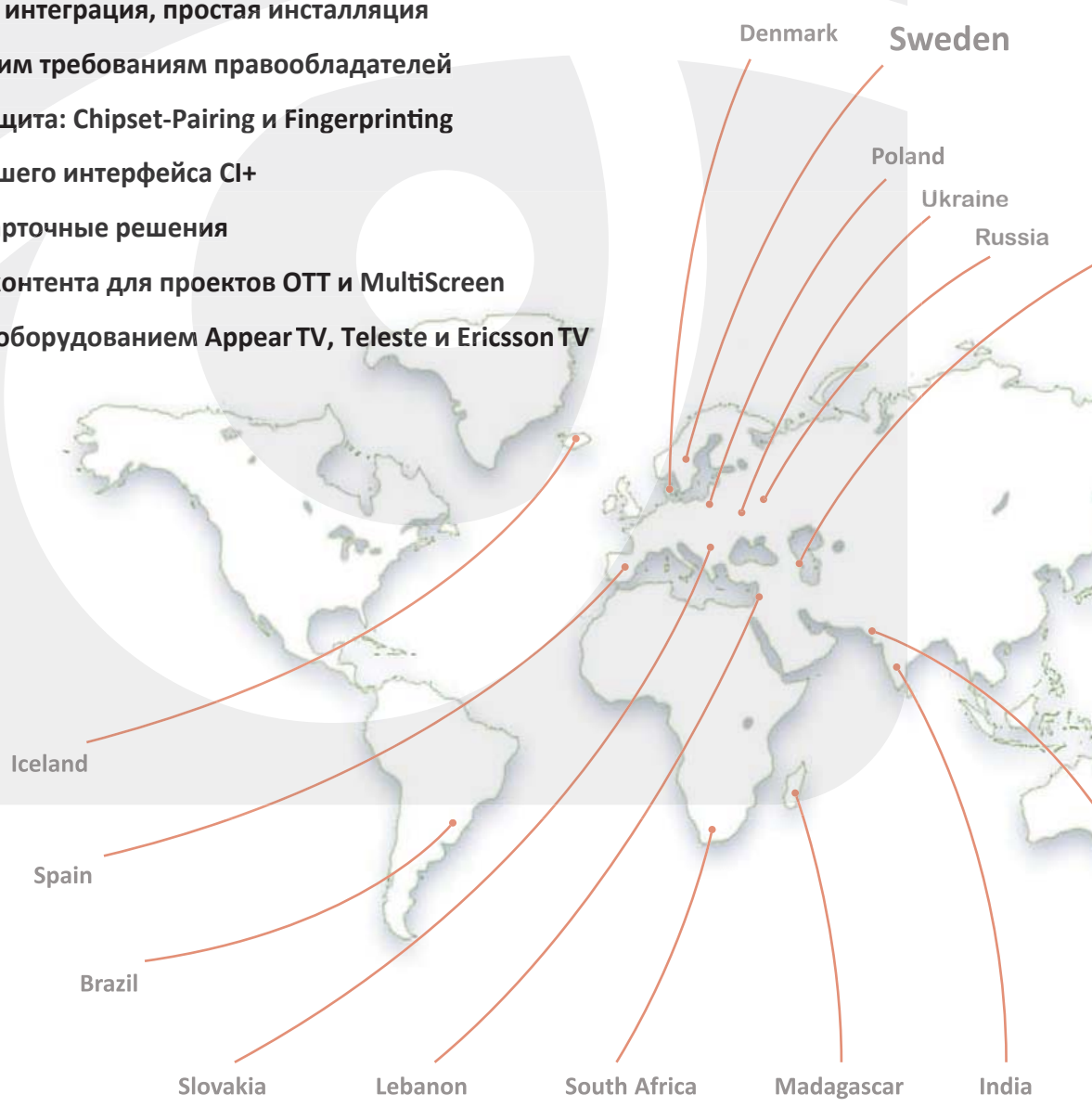
CryptoGuard – *Protect your content*

CryptoGuard Conditional Access System

Система CAS профессионального вещательного класса

SMS – CAS – DRM

- Сделано в Швеции
- Низкая стоимость входного билета
- Неограниченное число абонентов и ТВ каналов
- Неограниченное число комбинаций пакетов ТВ-контента
- Простая и быстрая интеграция, простая инсталляция
- Следование жестким требованиям правообладателей
- Анти-пиратская защита: Chipset-Pairing и Fingerprinting
- Поддержка новейшего интерфейса CI+
- Карточные и бескарточные решения
- Решения защиты контента для проектов OTT и MultiScreen
- Протестировано с оборудованием Appear TV, Teleste и Ericsson TV



КОНТУР
Digital broadband communications

CryptoGuard CAS

Шведская компания CryptoGuard основана в 2007 году.

Основной продукт, который компания представляет на рынке это одноименная система условного доступа CryptoGuard CAS для управления платным доступом абонентов к цифровому ТВ контенту, распространяемому через DVB и IPTV сети.

Имея множество гибких инструментов, CryptoGuard CAS позволяет оператору цифрового ТВ управлять платным абонентским доступом как к отдельным программам и пакетам программ, так и к отдельным ТВ событиям, например к премиальным спортивным и музыкальным передачам по схеме Pay Per View. Система позволяет управлять доступом к современным платным видео-сервисам такими как Video on Demand (VoD) и другими подобными возможностями.

Выходя на рынок, команда CryptoGuard поставила себе задачу по максимально конкурентно-способным ценам предлагать современную высококачественную систему условного доступа с удобным интерфейсом администрирования и множеством гибких возможностей для Оператора для реализации различных маркетинговых схем подписки и платного доступа, обеспечивая при этом наивысший уровень защиты видео-контента. Исключительно разумное ценообразование на систему CryptoGuard CAS делают её привлекательной и экономически-эффективной даже для небольших операторов цифрового ТВ.

В течение первых же нескольких лет работы компании система CryptoGuard CAS была выбрана более, чем 50-ю кабельными операторами Швеции. В 2010 году CryptoGuard приобрела шведскую софтверную компанию Prowill AB, имеющую заслуженный авторитет в индустрии систем платного цифрового телевидения. Команда специалистов Prowill привнесла в CryptoGuard свой многолетний и уникальный опыт по созданию эффективных и гибких систем управления абонентами (SMS). В считанные годы, систему CryptoGuard CAS выбрали множество операторов в скандинавских странах, Испании, Исландии, Пакистане, Индии, Польше, Азербайджане, Южной Африке, Бразилии, Мадагаскаре. Сегодня CryptoGuard CAS используется более чем в 100 сетях цифрового ТВ на трех континентах. В начале 2012 года число абонентов, получающих ТВ контент, защищённый CryptoGuard CAS превысило 1,3 миллиона подписчиков и постоянно продолжает расти.

Система поддерживает все технологии DVB вещания (DVB-C/C2, DVB-S/S2, DVB-T/T2), а также технологии IPTV и OTT (Over-The-Top).

Принцип работы CryptoGuard CAS

CryptoGuard CAS обеспечивает защиту цифрового ТВ контента путем скремблирования (шифрации) цифровых видео и аудио потоков на головной станции оператора и последующего де-скремблирования в абонентском приемнике. Используется алгоритм скремблирования, стандартизованный консорциумом DVB Project для систем условного доступа поддерживающих DVB SimulCrypt/Common Scrambling Algorithm, что принципиально обеспечивает совместимость CryptoGuard CAS со стандартным DVB SimulCrypt оборудованием головной станции многих производителей.

Ключевым компонентом системы является сервер CryptoGuard CAS, устанавливаемый на головной станции оператора или связанный с неё через IP-сеть. В состав сервера входит система управления абонентами (SMS), содержащая в своей базе данных постоянно обновляемые сведения о текущей платной подписке (разрешенном доступе) каждого абонента на ТВ/видео-сервисы, предоставляемые оператором. Сервер CryptoGuard CAS обеспечивает скремблирование ТВ контента и обновление статуса (подписки) абонентских смарт-карт. Сервер содержит генератор управляющих контрольных слов (CW), генератор ECM (Entitlement Control Message) сообщений и инжектор EMM (Entitlement Management Message) данных.

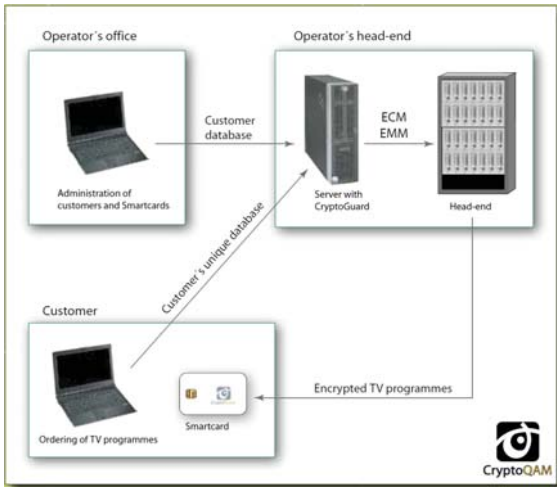
Контрольное слово является секретным кодом для шифрации видео и аудио данных. Контрольное слово представляет собой зашифрованный с высокой степенью защиты 48 битный ключ, изменяющийся 6 раз в течение одной минуты, что исключает неавторизованный доступ к ТВ контенту. В составе сообщений ECM контрольное слово регулярно передается в зашифрованном виде абонентскому приемнику, чтобы обеспечить дескремблирование ТВ контента.

ECM сообщения содержат также критерии доступа (Access Criteria, AC), присваиваемые программам для создания различных маркетинговых пакетов ТВ контента и продажи их абонентам на основе платной подписки в различных комбинациях, определяемых маркетинговой политикой оператора.

EMM сообщения (Entitlement Management Message) содержат постоянно обновляемую управляющую информацию, обеспечивающую изменение текущего статуса абонентских смарт-карт, подчиняясь системе управления абонентами (SMS).

EMM-инжектор загружает EMM-сообщения в мультиплексор головной станции для включения их в выходной DVB транспортный поток (DVB-TS), при этом EMM-инжектор управляет очередью отправки EMM-сообщений.

На приемном конце канала вещания - в абонентском приемнике STB с установленной смарт-картой происходит демодуляция, демультиплексирование DVB-TS, выделение ECM и EMM сообщений, анализ этих сообщений, определение прав владельца конкретной абонентской карточки на доступ к принимаемому ТВ контенту и дескремблирование контента.



Продукты CryptoGuard

Система условного доступа (CAS) и Система управления абонентами (SMS)

CryptoGuard CAS представляет собой законченное решение вещательного класса для DVB и IPTV, включающее Систему управления абонентами (SMS) и Систему условного доступа (CAS) с высочайшим уровнем защиты. Вы можете скремблировать множество сигналов раздельно или одновременно. Система управления абонентами позволяет Вам работать с абонентами, смарт-картами, заказами на просмотр контента, реализовать биллинг и т.п. Системы CAS и SMS могут быть использованы вместе и раздельно. Это означает, что Вы можете иметь одну систему CAS, подключенную к одной или к нескольким системам SMS, а также и наоборот. Вы также можете достаточно просто подключить программное обеспечение стороннего производителя к серверу CAS, например систему управления бизнесом типа ERP (Enterprise Resource Planning) или другую систему управления абонентами другого производителя, в большей степени отвечающую специфике Вашего бизнеса. Имеющийся документированный API (Application Interface) облегчает такую интеграцию.

IPTV и OTT

CryptoGuard работает по стандарту DVB-IPTV и может быть интегрирован с различными IPTV middleware софтверными платформами с сервисами VoD и OTT. Предоставляются программное обеспечение для IP или гибридных сетей, чтобы обеспечить абонентам эффективный и элегантный доступ к видео-сервисам в мультиэкранном режиме на различных абонентских устройствах. CryptoGuard также использовалась в системах, основанных на операционной среде Android как для линейного ТВ, так и для OTT.

CryptoLite

Решение предоплаченного доступа

CryptoLite представляет собой максимально упрощенное решение, в котором CAS сервер сразу встроен в головную станцию (используются только совместимые головные станции, в которые сервер CAS может быть встроен на заводе-производителе). Оператор продает одноразовые смарт-карты, дающие доступ к предоплаченному такой картой контенту. При этом не используются дополнительные серверы и управление абонентами в принципе отсутствует. Оператор просто определяет те каналы, которые входят в один платный пакет и эти каналы скремблируются головной станцией.

Hosted Solution

Распределенное решение на базе центрального и удаленных узлов

Система CryptoGuard CAS может быть физически разделена на Систему управления абонентами (SMS) и сервер CAS, содержащий главным образом ECM / EMM генератор и EMM инсертер. Вы можете через IP-сеть соединять несколько отдельных систем SMS с одним сервером CAS (не содержащем SMS), создавая распределенное решение (distributed hosted solution). Хостинг-партнеры могут создать распределенную систему CryptoGuard CAS для совместного бизнеса, где общий центральный CAS сервер обслуживает несколько систем SMS, каждая принадлежит своему провайдеру ТВ услуг или могут использоваться бизнес-схемы сдачи в аренду.

Генерация информации EPG и PSI/SI

CryptoGuard имеет программный модуль для создания электронной программы передач (EPG), позволяющий производить экстракцию EIT данных из входных DVB потоков (например, со спутника) и направлять эти данные в мультиплексор головной станции. Новейшая версия EPG-модуля позволяет также выполнять парсинг EIT-данных из базы EPG данных на основе стандартных XML-TV файлов. CryptoGuard имеет программный модуль для генерации PSI/SI данных, включая DVB таблицы NIT, SDT, SDT other, TOT и TDT. Программный модуль PSI/SI может быть поставлен вместе с системой условного доступа и установлен на один h/w сервер вместе с CAS, SMS и EPG. PSI/SI и EIT данные передаются на выход сервера как IP/UDP/MPEG-2 TS multicast потоки. Архитектура сервера PSI/SI данных построена на базе Linux PHP/MySQL, являющемся де-факто стандартом с общепризнанной надежностью для крупных WEB-решений.

Application Interface (API) для интеграции с ПО стороннего производителя.

Система управления абонентами CryptoGuard SMS выполнена на основе базы данных MySQL и операционной системы Linux. Открытая архитектура и документированный API позволяет выполнять интеграцию с системами стороннего производителя, различными бизнес-приложениями, внешним биллингом, системами анализа данных и CRM (Customer Relationships Management — управление взаимоотношениями с клиентами) и т.п.

Card-less Solution

Бескарточные решения

CryptoGuard имеет также бескарточные решения где защита контента основана на чипсетах, встроенных например в абонентские STB или CAM модули. Бескарточные системы могут быть использованы в различных устройствах при передаче DVB/IP потоков и в гибридных решениях.

Основные технические характеристики CryptoGuard CAS

Количество абонентов:	Неограниченно
Лицензирование по количеству абонентов:	Неограниченно, адаптируется под заказчика.
Количество ТВ каналов/пакетов контента/мультиплексов:	Неограниченно. По умолчанию – 512 заголовков (tag-ов), несколько каналов могут иметь одинаковый заголовок. Необходимость иметь более 512 заголовков - оговаривается при размещении заказа.
Возможность использовать одну систему CAS для обслуживания несколько сетей:	Да. Через IP-tunnel, с помощью Sub-серверов.
Управление смарт-картами (доступом к контенту) разными операторами или разными лицами:	Да. Например: оператор, владелец сети, поставщик программного контента.
Система управления абонентами (SMS) и встроенный биллинг:	Да
Документированный Application Interface для интеграции с внешним биллингом Оператора:	Да
Управление доступом смарт-карт к контенту:	Используются заголовки (tags) и номера программ. Определяется доступ к пакету, к каналу, дата истечения срока действия, контролируется положительный или отрицательный баланс карты и другие возможности.
Сервисы Pay Per View (оплата просмотра конкретной телепередачи), Video On Demand (видео по заказу):	Да
Продажа контента по подписке:	Через абонентскую службу, с помощью входа в систему с PIN-кодом, использование предоплаченных кодов активации, с помощью retailer login и др.
Использование свободно распространяемого ПО для работы с клиентской базой данных:	Да. MySQL, Linux.
Организация доступа клиента/оператора к серверу:	Через WEB интерфейс, без инсталляции специального клиентского ПО.
Настройка привилегий Администратора и пользователей:	Да. Права доступа определяются для Администратора и разных пользователей
Генерация PSI/SI-данных:	NIT, SDT, SDT actual/other, CAT, TDT, TOT, Private Sections.
Язык интерфейса:	По умолчанию – английский, адаптация к другим языкам.
Поддержка CAM–модулей и модулей CI+:	CAM интегрированный в сет-топ-бокс (STB), модули CI или CI+.
Paring (привязка) для защиты от пиратства:	Да. Двухсторонний pairing смарт-карты и STB, управляемый на канальном уровне. Pairing на уровне оборудования доступен для абонентских устройств (CAM, STB, карт) поддерживающих chipset pairing.
Защита от пиратского Интернет-шаринга управляющих слов CW (Dream Box и т.п.) :	Да, в обоих абонентских устройствах – в смарт-карте и в STB.
Антипиратская технология Finger Prints:	Да
Шифрование обмена данными между смарт-картой и абонентским декодером:	Да, уникальное шифрование для каждого STB. Высокий уровень защиты шифрованных данных обмена по технологии Cryptoguard Secure Path.
Возможность обновления ПО абонентских сет-топ-боксов через сеть по технологии Over The Air (OTA):	Да
Обновление системы CAS для повышения уровня защиты и новые релизы ПО:	Постоянное обновление ПО сервера CAS и смарт-карт.
Текстовые сообщения абонентам:	Да
Настраиваемое сообщение «У Вас нет прав просмотра этого канала. Позвоните в службу поддержки + 7 812 222 222»:	Да
Версия SimulCrypt:	ETSI TS 103 197 v1.2.1 / v1.3.1 (SimulCrypt 2 и 3).
Необходимый канал передачи данных между серверами:	Не менее 1Мб/с
Место, занимаемое сервером в стойке:	1U/ 19”
Страна производитель системы:	Швеция
Документации по созданию пакетов ТВ контента и по управлению абонентской подпиской:	Да
Служба технической поддержки:	Да

Минимальные требования к серверу для установки CryptoGuard CAS:
Сервер HP ProLiant DL320 G6 или аналогичный. OS Linux CentOS 5.8 64bit x86_64.
Процессор не ниже Intel Xeon 1.5Ghz Xeon 64 bit, RAM не менее 2 ГБ, HDD не менее 250 ГБ, 1 порт USB 2.0, 2 порта GigE.

КОНТУР
Digital broadband communications

Россия, г. Москва, ул. Искры, дом 9, корпус 2,
тел./факс: +7(495) 221-8188 (многоканальный),
E-mail: info@konturm.ru http://www.konturm.ru