Обзор

625-net.ru

ТЕМАТИЧЕСКИЙ ОБЗОР ПРОДУКТОВ И РЕШЕНИЙ

В ЭТОМ РАЗДЕЛЕ

Что такое система условного доступа?

Система условного доступа (Conditional Access System, CAS) — программно-аппаратное решение для ограничения доступа к программам цифрового ТВ. Кодирование позволяет эффективно осуществлять оплату просмотра телевизионных программ.

Автор: Дэвид Мордисон

Дэвид Мордисон (David Mordison),
Родился в 1968 году в Москве. В 1990 г. с отличием окончил Московский авиационный технологический институт (МАТИ).
В индустрии телекоммуникаций с 1997 года в должности эксперта-аналитика по защите информации и технического консультанта.
Хобби: игровые виды спорта, боулинг, горные лыжи.

Прежде чем погрузиться в технические детали, давайте сначала попробуем разобраться, что же такое "система условного доступа" (СУД), зачем и кому она нужна и какие функции выполняет.

С термином "система" все ясно — это набор взаимосвязанных компонентов, условно объединяемых в некий "черный ящик" и выполняющих в комплексе набор функций. Термин "доступ" тоже не вызывает вопросов. С одним "но": доступ это не простой, а условный, то есть он предоставляется в зависимости от выполнения определенных условий. Пожалуй, самым простым объяснением будет аналогия: вы идете в кино, покупаете билет и предъявляете его на входе в кинозал билетеру. Наличие билета является обязательным условием для допуска вас в зал и, соответственно, дает вам право просмотра кинокартины.

По большому счету, везде, где есть доступ и условия его получения, есть или должна быть система, проверяющая выполнение данного условия и предоставляющая доступ. Мы пользуемся системой условного доступа каждый день, открывая (и закрывая) дверь ключом, в общественном транспорте, в кино, театре, музее, везде, где проверяют билеты на входе и т.д. Если обобщенно выразить условие предоставления доступа как оплату, то так же обобщенно можно сказать, что задача системы условного доступа — предоставлять его только тем, кто

оплатил, и только к тому, за что заплачено. В этом смысле СУД — это страж бизнеса, инструмент, позволяющий предпринимателю (оператору телевизионной платформы) взимать с абонентов плату за предоставляемые услуги. СУД может также применяться для предоставления контента и без оплаты, и тем не менее доступ к контенту предоставляется только абонентам оператора. Эта практика может быть применима и в России. Например, по усмотрению оператора, некий пакет телеканалов (например, "Социальный") предоставляется бесплатно, но только при условии использования авторизованного оператором фирменного абонентского устройства. В данном случае оператор гарантирует защиту контента правообладателям, контролирует доставку контента и популяцию абонентских устройств, а также имеет возможность продвигать свой бренд и дополнительные платные пакеты каналов услуги. С другой стороны, в данной схеме оператор может субсидировать абонентские устройства, при этом СУД должна гарантировать защиту данной субсидии, т.е. невозможность "перепрошивки" абонентского устройства с дальнейшей его перепродажей на другие рынки.

Система условного доступа в телевидении

В контексте телевидения данное выше определение "страж бизнеса" вполне соответствует задачам, возлагаемым на систему, — с одной лишь оговоркой: обычно СУД не оперирует коммерческими (денежными) понятиями, это входит скорее в обязанности биллинга. СУД имеет дело с правами доступа: как в аналогии выше, кинофильм — это контент, вы — пользователь, билет — право доступа, билетная касса — это система биллинга, билетер — система условного доступа, которой в принципе все равно, за сколько вы купили билет, — главное, чтобы он у вас был. Телевизионный сигнал, передаваемый по вещательной сети (эфир, по кабелю, через спутник и т.д.) распространяется посредством электромагнитных волн. Волны подчиняются законам физики, поэтому как-то обусловить доступ к ним невозможно: прием телевизионного сигнала доступен каждому, в чьем распоряжении есть соответствующее приемное оборудование. Обычное радио также принимается на любой радиоприемник. Поэтому, чтобы защитить телевизионный сигнал от неавторизированного доступа, его "портят" перед передачей в эфир, а затем "исправляют" в приемном оборудовании, но только если выполняются условия доступа. Этот процесс называется скремблированием (от англ. scrambling) и, соответственно, дескремблированием (descrambling).

Типовая схема ГС платформы платного телевидения
Расшифровка на приемном оборудовании работает в обратном порядке:
1. Демультиплексор выделяет из транспортного потока контент и ассоциированные с ним ECM, подает зашифрованный контент на дескремблер, а ECM — в клиентское приложение СУД, установленную в приемном оборудовании.
2. Клиентское приложение СУД выделяет из ECM критерии доступа к контенту и проверяет соответствие прав просмотра данным критериям. Если они удовлетворяют критериям, СУД восстанавливает контрольное слово и предоставляет его на дескремблер. В противном случае СУД сообщает о недостаточности прав для просмотра, и доступ к контенту не предоставляется.
3. Дескремблер, используя полученное от СУД контрольное слово, расшифровывает контент

СХЕМА ШИФРОВАНИЯ В DVB РАБОТАЕТ СЛЕДУЮЩИМ ОБРАЗОМ:

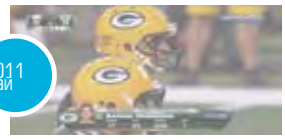
- Контент (например, телевизионный канал) подается на мультиплексор.
- Мультиплексор (а точнее, его компонент, называемый SCS — SimulCrypt Synchronizer) случайным образом генерирует контрольное слово.
- Через стандартный интерфейс (OpenCAS) SCS передает контрольное слово и определенный идентификатор контента в СУД.
- СУД генерирует сообщение контроля прав просмотра, ECM (Entitlement Control Message). Данное сообщение включает в себя: а) описание критериев доступа к указанному контенту (по переданному ей идентификатору), то есть "у кого есть доступ" к контенту; и б) указания, как получить данное контрольное слово на приемном оборудовании, то есть "как открыть" контент.
- СУД возвращает сгенерированный ECM на SCS.
- Мультиплексор зашифровывает контент, используя сгенерированное контрольное слово, а полученное от СУД ECM микширует в поток данных (транспортный поток) вместе с зашифрованным контентом (каналом).

ТЕМАТИКА ОБЗОРОВ 2011


2011 февраль
Высокоскоростные камеры


2011 март
Аксессуары для телевизионных объективов


2011 апрель
Системы автоматизации телевизионного производства и вещания


2011 май
Средства оформления эфира и титрования


2011 июнь
Вещательные серверы


2011 август
Системы условного доступа и защиты авторских прав (CAS/DRM)


2011 сентябрь
Оборудование для работы с сигналом 3 Гбит/с


2011 октябрь
Оборудование и технологии для IP-вещания


2011 ноябрь
Системы замедленного воспроизведения и повтора


2011 декабрь
Камерные радиосистемы

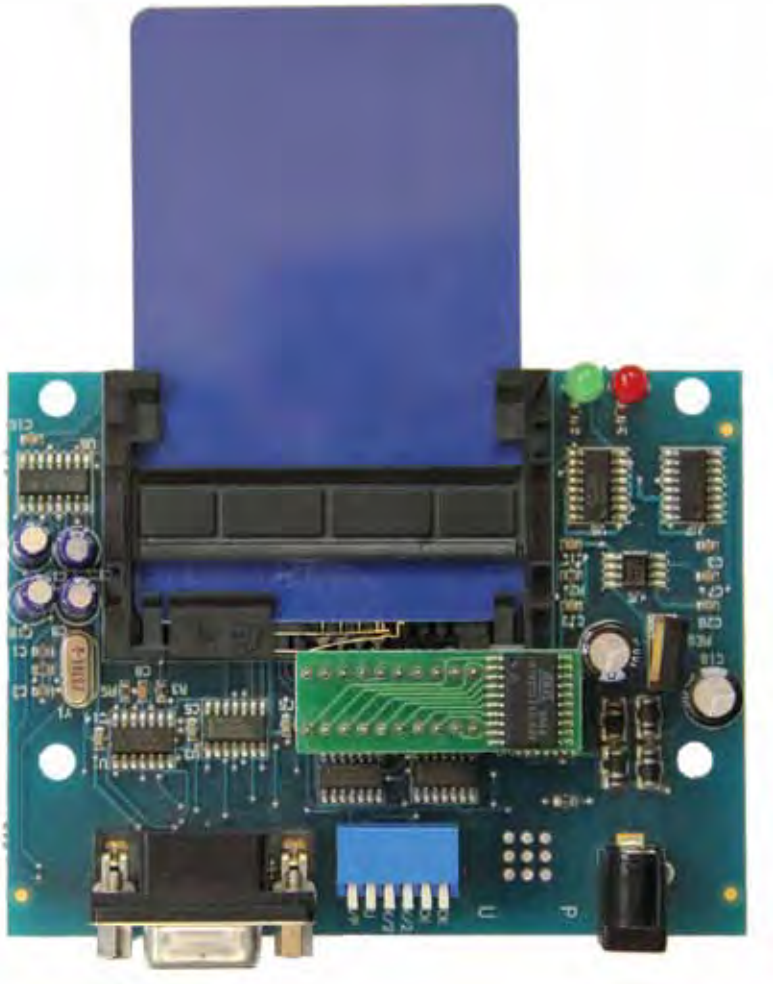
В аналоговом телевидении изображение кодируется при помощи электрического сигнала, надежно скремблировать и дескремблировать который достаточно сложно. Существовали различные методы скремблирования сигнала (например, Cut-n-Rotate), но не будем заострять на этом внимание, поскольку аналоговое телевидение доживает свой век, а его скремблирование и вовсе уже далеко в прошлом.

В цифровом телевидении изображение кодируется в пакеты цифровых данных (MPEG), а для защиты контента данные зашифровываются при вещании и расшифровываются при приеме.

Цифровое телевидение (и, соответственно, шифрование) стандартизировано: в Европе (и в России в частности) применяется стандарт DVB, который оговаривает применение алгоритма шифрования DVB CSA (Common Scrambling Algorithm) для скремблирования контента. Этот алгоритм напоминает по реализации DES (схожесть в использовании так называемых S-блоков) и является симметричным шифром, то есть для расшифровки данных требуется знать тот же ключ, что использовался при шифровании. Используя терминологию DVB, данный ключ называется "контрольным словом" (англ. Control Word). Поэтому в цифровом телевидении в обязанности СУД входит обеспечить пользователей ключами для расшифровки контента в соответствии с предоставляемыми им правами просмотра. Для выполнения данной задачи СУД имеет разнесенную архитектуру: часть ее компонентов устанавливается на вещательной станции; они поддерживают шифрование и передачу данных относительно прав доступа. Кроме того, компоненты СУД присутствуют в приемном оборудовании, обеспечивая контроль прав доступа и управление расшифровкой контента.

Возникают два вопроса: откуда клиентское приложение СУД знает о правах просмотра и каким образом клиентское приложение СУД восстанавливает контрольное слово? Права доступа поступают на приемное оборудование в сообщениях управления правами просмотра, EMM (от англ. Entitlement Management Message). Когда пользователь оплачивает определенные права просмотра, биллинг сообщает об этом СУД. Последняя генерирует EMM, которое адресуется указанному абоненту и в котором клиентскому приложению СУД сообщается, какие права просмотра были оплачены.

Ответ на второй вопрос сложнее. DVB не оговаривает архитектуру СУД, поэтому реализация систем различных поставщиков проприетарна. В целом можно выделить два типа архитектуры СУД: одна (так называемая "СУД на алгоритме") применяет специальные секретные алгоритмы, которые "умеют" воссоздать контрольное слово на основе информации в ECM; вторая (так называемая "СУД на ключах") шифрует контрольное слово с помощью ключей (так называемые ключи доступа), которые, в свою очередь, передает абонентам через персональные EMM в соответствии с правами просмотра; в ECM присутствует зашифрованное контрольное слово. Опустим дискуссию о преимуществах и недостатках каждой схемы, все они нашли свое применение на рынке.



На иллюстрации показано пиратское устройство, известное как Glitcher (существовало несколько вариаций с различными названиями), которое использовалось для взлома и перепрограммирования смарт-карт. Устройство подключалось через COM-порт к персональному компьютеру, на котором пользователь мог управлять процессом и задавать параметры, программы распространялись через сеть. Стоимость данного устройства колебалась от 2500 долларов США в начале их появления до 50 долларов, когда выбор стал шире.

Атаки, пиратство, история

История взлома защиты на платформах платного телевидения начинается, согласно легенде, от "Звездного пути". Английская платформа SKY (в те времена еще аналоговая) получила эксклюзивные права на вещания данного сериала. А поскольку официальную подписку на SKY можно было получить только в Великобритании, поклонники сериала на материковой Европе были крайне разочарованы, имея возможность принимать сигнал SKY со спутника и не имея возможности его дескремблировать.

Среди них нашлись умельцы, взломавшие систему защиты контента SKY, как уверялось, исключительно для просмотра "Звездного пути". Очевидно, от анархистов-филантропов взлом платформ быстро взял курс в коммерческом направлении и стал пиратством: за вознаграждение, которое существенно меньше стоимости легальной подписки,

предоставляется неавторизованный оператором доступ к закрытому вещаемому контенту.
Пиратство начинается с анализа защиты системы. Нахождение "дырок", то есть возможности получать доступ к контенту без наличия на то соответствующих прав, еще не является достаточным условием для пирата начать свой бизнес. Ему надо найти способ, как на этом делать деньги, то есть как это продать. Причем продать нужно так, чтобы другие пираты не смогли быстренько смекнуть, в чем дело, и начать свой маленький, но быстро растущий пиратский бизнес (пиратство на пиратстве?). Самым простым способом до сегодняшнего момента была продажа пиратских устройств, с помощью которых можно было получить доступ к контенту, или продажа пиратских смарт-карт.

Атаки на смарт-карты

При кажущейся сложности анализ чипов смарт-карт является достаточно рутинным инженерным делом, хотя и требующим специальных знаний, навыков и специального дорогостоящего оборудования. Специальные знания можно получить, изучая электронику, в частности технологии VLSI в ВУЗе, навык приходит с опытом, а специальное оборудование может быть найдено в лаборатории в том же ВУЗе либо взято в аренду. Если анализ и взлом первых смарт-карт еще мог с успехом проходить в гараже или дома на кухне, то с развитием технологии уже требовались оптический микроскоп высокого разрешения, лазерный резец, микрозонды на микроманипуляторах и т.д. Сегодня технология производства чипов для смарт-карт продвинулась уже настолько, что для анализа потребуются как минимум электронный микроскоп и СИП-машина (FIB).
До недавнего времени атаки на смарт-карты были основным направлением деятельности пиратов ввиду своей эффективности, достаточной простоты и легкости реализации (продажи). Пираты продавали либо сами смарт-карты, либо устройства, с помощью которых пользователь может самостоятельно перепрограммировать свою легальную или запрограммировать "чистую" смарт-карту. Здесь можно условно выделить три основных подвида:

"Белые карты" — это стандартные не фирменные смарт-карты (их пластиковый корпус обычно белого цвета, отсюда и название), которые программируются для выполнения тех же функций расшифровки контрольного слова, которые выполняет легальная смарт-карта СУД оператора, но без проверки прав просмотра. Такая карта может быть либо эмулятором, в который надо прописывать ключи, либо точной копией ("клоном") легальной и оплачиваемой карты. Данный "подвид" еще до недавнего времени был весьма популярен (например, Gamma card).

"Зеленые карты" — некий гибрид между пиратским устройством и смарт-картой; является, по сути, печатной платой (отсюда название), на конце которой имеются контакты, идентичные с расположением контактов смарт-карты. Данной "смарт-

"ЭФФЕКТ ДОМИНО"

Термин "эффект домино"не является методом взлома, он применяется для описания ситуации, когда различные платформы, использующие СУД одного производителя, оказываются под угрозой, если взламывается защита на одной из платформ (повалили одну фишку домино, и за ней повалились все остальные — отсюда и название). Это происходит потому, что хакеры, изучив систему, переносят полученные знания на другую платформу с той же СУД. Таким образом, фаза анализа и поиска "дыр" сокращается до минимума, обычно используются те же пиратские устройства или карты (как на примере упомянутого случая с Gamma card). При возникновении данного эффекта поставщик СУД модернизирует или меняет систему на всех платформах, зачастую с полной заменой смарт-карт, что неоднократно имело место в истории.

картной" стороной устройство вставляется в абонентское устройство. На плату монтируются различные компоненты, выполняющие либо эмуляцию функций смарт-карты, подобно "белой карте", либо служащие для подключения к ПК или иному устройству, а порой и как интерфейс для легальной смарт-карты.

MOSC — очень эффективный вид пиратства, предполагающий использование оригинальной карты, в которую вносятся определенные изменения (отсюда и название — Modified Original Smart Card). Пользователь может либо самостоятельно "модифицировать" свою смарт-карту с помощью пиратского устройства или купить у пиратов уже модифицированную смарт-карту. Известен случай, когда пираты наладили целый производственный процесс по модификации оригинальных смарт-карт оператора в лабораторных условиях, используя лазерный резец, микроскоп и микроманипулятор.

Метод перехвата (Cardsharing)

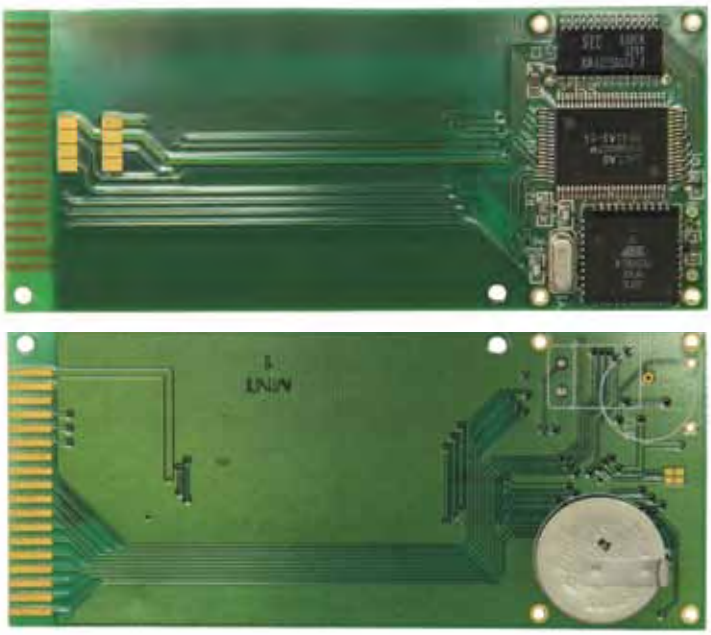
Такой способ получил широкое распространение в последнее время, "вытеснив" остальные, более трудоемкие в плане анализа методы взлома и пиратства. Схему еще в первой половине 90-х годов предсказал Джон МакКормэк (John McCormac) в своей "Черной книге". Схема проста: при передаче контрольного слова от легальной смарт-карты на абонентское устройство (или внутри устройства) контрольное слово "перехватывается" и распространяется через сеть на другие устройства, на которых нет ни легальной подписки, ни даже смарт-карт. Полученное по сети контрольное слово подается напрямую в дескремблер. Сегодня, с развитием высокоскоростных сетей широкополосного доступа, данная схема заработала в полную силу. Этим занимаются уже не любители-энтузиасты, а профессионалы-бизнесмены, открывающие настоящий "супермаркет контрольных слов" в сети для тысяч каналов, вещаемых различными операторами.

Средства предупреждения и борьбы с пиратством

Поскольку криптография систем не подвергается атакам, нет особого смысла усиливать криптозащиту. Иными словами, криптостойкость используемых в СУД алгоритмов не влияет на уровень защищенности системы. Защита от пиратства заключается, в первую очередь, в защите смарт-карты и абонентского оборудования от анализа и манипуляций.

Проприетарный дизайн смарт-карт — показал себя весьма эффективной мерой для усложнения анализа. Данный подход используют лишь крупные производители СУД, остальные используют стандартные смарт-карты "с полки" (от англ. off-the-shelf), архитектура и образцы которых доступны и хакерам.

Наличие проприетарных компонентов в микросхеме смарт-карты — наиболее эффективная мера для предотвращения клонирования смарт-карт. Проприетарные компоненты (ASIC) реализуются по дизайну производителя СУД в виде специальных аппаратных блоков в чипе смарт-карты на той же силиконовой подложке, что делает невозможным их отделение от чипа смарт-карты, а также весьма затрудняет их анализ. Данная мера, как и предыдущая, реализуется на данный момент лишь крупными производителями СУД.



На иллюстрации показана "зеленая карта", которая эмулировала работу легальной смарт-карты. Известное как Battery Card, данное устройство примечательно в качестве курьеза именно наличием батареи. В ней программа эмуляции хранилась на чипе памяти ОЗУ (RAM), который запитывался от элемента питания. Данный (странный с инженерной точки зрения) дизайн обусловлен стремлением пирата защитить свою "интеллектуальную собственность" от посягательства других пиратов. Если отключить батарею, программа автоматически стиралась из памяти, а без нее устройство не представляло ценности. Затем пираты упростили дизайн, используя специальные чипы памяти ППЗУ (NVRAM), доступ к данным в которых защищался паролем.

Кастомизация решений защиты — предназначена предотвратить "эффект домино". У крупных производителей СУД имеются средства обеспечить необходимый уровень кастомизации решений, предоставляемых различным заказчикам, что в значительной мере снижает вероятность возникновения "эффекта домино".

Электронные контрмеры — применяются для борьбы с фактами пиратства путем обновления данных или программного обеспечения на смарт-картах. Сюда же можно отнести и замену ключей доступа, хотя на практике это малоэффективная мера, поскольку замена ключей доступа на смарт-картах требует значительной полосы в вещательном потоке и занимает довольно много времени, при этом пираты достаточно быстро вычисляют и раздают "своим" пользователям новые ключи. Обновление ПО смарт-карт (или "пэтчи") — это гораздо более эффективная мера. "Белые" и "зеленые" карты их "не переваривают", а следовательно, данные пиратские устройства легко отсеять. Для MOSC это обычно миниатюрные программы-чистильщики, которые подгружаются на смарт-карту, находят и уничтожают модификации кода.

Привязка смарт-карты к чипу абонентской приставки — весьма эффективная мера для борьбы с cardsharing. Современные абонентские устройства построены на видеопроцессорах, сочетающих в себе все основные компоненты приема и декодирования контента (так называемые SoC — System on Chip). На силиконовой подложке данных процессоров, предназначенных для приема платного телевидения, обычно присутствуют и блоки для привязки смарт-карты (pairing). К этим

блокам относятся: защищенная одноразово программируемая память (OTP — One-time Programmable) и схема последовательной расшифровки "лесенка ключей" (от англ. Key Ladder). На заводе-изготовителе чипа в память OTP прописывается некий секретный ключ, который является самым верхним ярусом в "лесенке ключей". Данный ключ известен лишь производителю СУД. В дальнейшем по серийному номеру чипа СУД "знает", какой секретный ключ зашит в чипе данного абонентского устройства. Она пересылает соответствующую информацию на смарт-карту, вставленную в данное устройство. С этого момента смарт-карта зашифровывает передаваемые на приставку контрольные слова, используя ключ привязки (Pairing Key). Расшифровка контрольного слова происходит с помощью "лесенки ключей" внутри чипа, непосредственно перед подачей контрольного слова в блок дескремблера в чипе. Вне чипа видеопроцессора контрольное слово не появляется.

Операционная безопасность — некоторые (обычно крупные) производители СУД используют комплексный подход к защите платформ, для чего подкрепляют технологию мерами операционной безопасности, создавая группы для отслеживания активности хакеров и пиратов. Таким образом можно пресечь пиратство еще до того, как оно "набрало обороты" и нанесло ущерб бизнесу оператора.

Современные СУД

В числе наиболее распространенных систем условного доступа сегодня можно назвать (в алфавитном порядке): Conax, DRE Crypt, Irdeto, Nagravision, NDS, Viaccess. В системах IPTV к данному списку можно добавить и следующих игроков: Microsoft, SecureMedia (куплена Motorola), Verimatrix и Widewine (куплена Google).

В России также представлены практически все, за исключением, пожалуй, Nagravision. В IPTV преобладает Verimatrix. В принципе, с усилением тенденции консолидации операторов платного телевидения в крупные платформы, предоставляющие разнообразные услуги помимо традиционного линейного телевидения, формируется спрос не только на "голую" систему условного доступа, а скорее, на комплексное законченное решение. В подобных решениях крупные производители систем условного доступа имеют явное преимущество, поставляя интегрированные наработанные решения "под ключ" самостоятельно или посредством системного интегратора. При кажущейся более высокой начальной стоимости данного решения оно оказывается надежнее, проще и дешевле в плане поддержки и эксплуатации. Менее крупные производители предлагают так называемые "экосистемы", сочетающие в себе решения от нескольких производителей.

ТЕНДЕНЦИИ СУД

Развитие технологии и тенденции конвергенции сетей и платформ доставки контента ставят перед СУД ряд новых задач, которые выходят за рамки традиционного понимания ее функционала. С одной стороны, производители контента ищут новые пути его монетизации. Операторы стремятся привлечь большую аудиторию и снизить отток абонентов. Для последних открываются новые пути получения контента, зачастую бесплатного (или условно бесплатного), при этом абоненту нужна свобода в выборе не только контента, но также времени и места его просмотра. Все эти движущие силы должна учитывать СУД, от которой сегодня ожидается нечто большее, чем традиционная защита контента и услуг на пути доставки на абонентское устройство. Современная СУД, в числе прочего, должна осуществлять поддержку смежных и переплетающихся бизнес-моделей на нескольких платформах, работать с различными абонентскими устройствами, защищать контент и обеспечивать установленные оператором или правообладателем права доступа для записанного контента, в том числе при его передаче между устройствами и внутри домашней сети.

VideoGuard Express – NDS

Производитель: NDS Ltd. **Год первой инсталляции в России:** 1998. **Пользователи:** "Акадо" (Москва), П.А.К.Т. (Санкт-Петербург).
Контакты: Ираклий Накашидзе, региональный директор по продажам, глава российского представительства, тел: (495) 225-8549, (903) 599-4469, e-mail: inakashidze@nds.com, www.nds.com

VideoGuard Express представляет собой интегрированное комплексное законченное решение, специально разработанное компанией NDS для быстрого развертывания на платформе заказчика и обеспечения базового набора функций при минимальных затратах, с возможностью дальнейшего наращивания и расширения. Данное решение построено на проверенных и зарекомендовавших себя технологических разработках компании и включает в себя:

- систему условного доступа, оснащенную уникальной технологией защиты VideoGuard, прочно лидирующую во всем мире как наиболее надежная среди всех прочих систем;
- систему контроля и планирования телевещания, обеспечивающую для оператора возможность реализовать различные модели бизнеса;
- систему генерации таблиц сервисной информации DVB SI с целью передачи данных для "электронной программы передач" (EPG) в транспортном потоке DVB;
- связующее программное обеспечение для абонентских приставок (middleware) NDS MediaHighway, позволяющее осуществлять разработку и запуск на приставке различных программных приложений: EPG, pay-per-view ("домашний кинозал"), "видео-по-запросу", DVR, игры и т.д. Оптимизировано для максимально эффективного использования ресурсов бюджетных абонентских приставок;
- NDS Guide — встроенное программное приложение на абонентских приставках для отображения EPG. Кроме детальной семидневной программы передач с кратким содержанием (синопсисом) для каждой, данное приложение имеет адаптируемый дизайн и предоставляет возможность выбора телепрограмм.

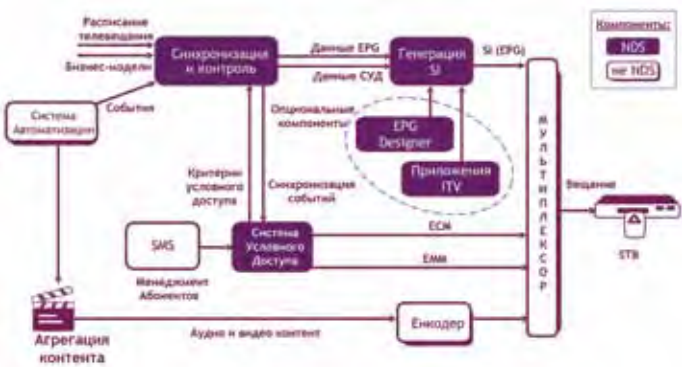
На схеме представлены компоненты VideoGuard Express и взаимодействие между ними
Система VideoGuard Express призвана обеспечить решение не только сегодняшних задач по реализации платформы платного телевидения; благодаря своей модулярной структуре она открывает перспективы на будущее расширение платформы. Чтобы снизить требуемые капиталовложения при строительстве платформы, обычно вначале абонентам предлагается лишь базовый пакет цифровых услуг цифрового ТВ. По мере развития платформы оператор может расширить пакет предоставляемых услуг, получая дополнительный доход и привлекая большую зрительскую аудиторию. К числу таких услуг, например, относятся:

- просмотр программы с моментальной оплатой (IPPV);
- "видео-по-запросу" (VOD), включая режимы Push-VOD и Pull-VOD;
- персональный видеорекордер (PVR) со встроенным или внешним накопителем;
- интерактивное телевидение (игры, целевая реклама, тотализатор и т.д.);
- система оценки рейтинга телепередач и сбора статистики о просмотре (AMS).

Данные приложения работают в абонентской приставке на базе связующего ПО, включенного в пакет решений NDS VideoGuard Express.

Ключевые характеристики

- Полное резервирование системы в стандартной конфигурации;
- Поддержка до 32 удаленных мультиплексоров через широкополосную сеть по каналу VPN;
- Поддержка авторизации до одного миллиона абонентов;
- Расширяемость путем добавления типовых компьютерных компонентов;
- Генерация сервисной информации (DVB SI) и таблиц EIT;
- Поддержка шифрования до 200 телеканалов и 100 радиоканалов;
- Объединение каналов в пакеты с гибким ценообразованием;
- Возможность подписки на каждый канал отдельно (a-la-carte);
- Реализация услуг PPV с предварительным заказом и предоплатой (OPPV);
- Максимальная гибкость в бизнесе: покупка просмотра до резолюции отдельной передачи;
- Гибкая адресация абонентов по группам, формируемым на основе профиля, конфигурируемого оператором, включая, например, географический критерий;
- Быстрый и изящный графический интерфейс пользователя для абонентской приставки, включающий EPG на 7 дней, сортировку и поиск телепередач по жанрам, заказ программ с напоминанием о начале показа, списки любимых и блокируемых каналов, экранную помощь, многоязычное меню и другое;
- Возможность реализации одинакового интерфейса пользователя на различных моделях абонентских приставок — сокращает операционные расходы на техническую поддержку;
- Адресуемые сообщения (OSD);
- Рассылка электронных сообщений (B-mail), адресуемых индивидуально или группе абонентов, обеспечивает прямую связь с абонентами, например для пересылки состояния счета непосредственно на абонентскую приставку, без затрат на рассылку бумажных документов.

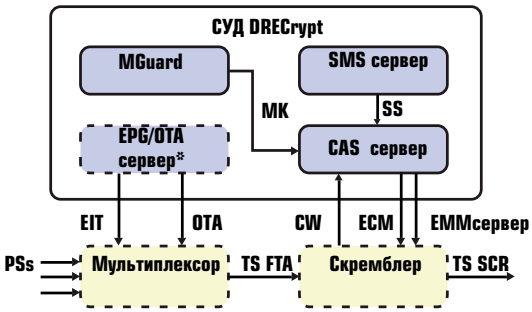


NB

VIDEOGUARD EXPRESS — бюджетное решение для базовой платформы цифрового ТВ, которое обеспечит надежную защиту и гибкость платформы. Она отвечает потребностям бизнеса оператора сегодня и в то же время с помощью модульного построения предлагает перспективы на будущее. Технология защиты VideoGuard не имеет аналогов, поскольку она основана на применении специальных секретных алгоритмов, разработанных по заказу учеными-криптографами с мировым именем. Алгоритмы реализованы в аппаратном обеспечении системы, в частности в смарт-карте. В системе VideoGuard нет "сервисных ключей", с помощью которых в других системах регламентируется доступ к контенту. Соответственно, не требуется рассылка данных ключей абонентам, что значительно повышает надежность защиты и экономит полосу вещания, отводимую под СУД.

DRECrypt – DRECrypt

Производитель: ООО "Цифра". **Год первой инсталляции в России:** 2005. **Пользователи:** "ТриколорТВ", "Платформа HD" и ряд кабельных операторов. **Партнеры:** Spm Group, Satellite, "Сетевые решения" и другие.



Система условного доступа DRECrypt представляет собой программно-аппаратный комплекс, состоящий из набора промышленных серверов исполнением 1 RU, специализированных устройств защиты, программного обеспечения и вспомогательных устройств, установленных на головной станции оператора.
Компоненты, входящие в СУД DRECrypt:
- CAS-сервер — ядро системы, которое осуществляет шифрование CW, генерирует пакеты EMM и ECM;
- SMS-сервер — содержит базу подписчиков и позволяет осуществлять оперативное управление;
- MGuard — устройство, осуществляющее генерацию случайных чисел и обеспечивающее защиту от несанкционированного доступа.

Дополнительные возможности СУД DRECrypt

1. Мультипровайдерность — возможность смарт-карты работать с двумя и более провайдерами, вещающими с применением стандартов DVB-S, DVB-C, DVB-T.
2. "Инфокас" — функция предназначена для демонстрации абонентам информационных оповещений, отображаемых принудительно на экранах ТВ.
"Инфокас" предоставляет возможность:
- информирования абонентов о предстоящем обновлении ПО, о задолжности, об истечении предоплаченного периода и др.;
- объявления о социально значимых событиях в городе;
- экстренного оповещения населения в ЧС.

3. Геокод — сервис, позволяющий регламентировать просмотр каналов по географическому признаку:
- возможность запуска регионального контента;
- возможность присвоения нескольких геокодов пользователю;
- возможность шифрования служебной; информации с помощью геокода (EMM, ECM).

Дополнительно поставляемое оборудование

1. EPG-сервер — трансляция электронной программы передач на несколько дней. Позволяет организовать просмотр ТВ-программы за отдельную плату.
2. OTA-сервер — обновление программного обеспечения абонентских терминалов через эфир.

Дополнительные мультимедийные сервисы СУД DRECrypt

1. Рекламный баннер — новый тип телевизионной рекламы, не прерывающей ТВ-программу и не отвлекающей от ее просмотра. Существует несколько способов реализации данного сервиса:
- межпрограммный рекламный баннер/ролик;
- баннер/ролик с привязкой к инфопанели;
- рекламный баннер/ролик, демонстрирующийся в момент включения/выключения ресивера.

2. ТВ-чат — интерактивный сервис, который позволяет абонентам обмениваться в телевизионном чате сообщениями, которые транслируются в потоке и отображаются на экранах телевизоров пользователей в реальном времени в рамках служебных сообщений.
3. ТВ-почта — этот сервис предоставляет абонентам возможность обмениваться email-сообщениями и просматривать входящие письма на экране телевизора без использования сети Интернет. Это позволяет пользователю получать индивидуальные и групповые почтовые сообщения, содержащие как текстовую, так и графическую информацию, с их воспроизведением на экране телевизора.
4. Funbox — данный сервис обеспечивает многоадресное вещание предварительно сформированного медийного контента по расписанию в несколько потоков со смещением во времени.
5. Экстренное оповещение населения:
- возможность наглядного обучения населения действиям в ЧС по средствам размещения информационных видеороликов на базе оператора связи;
- возможность массового или адресного обращения к аудитории при отказе прочих систем оповещения;
- эффективная защита передаваемой информации.

Организация дистанционного кодирования с помощью CAS Remote DRECrypt

В центре обработки данных СУД DRECrypt (ЦОД СУД DRECrypt) установлены глобальные SMS и CAS серверы, центральный маршутизатор. Головные станции операторов цифрового кабельного телевещания включают в себя локальные маршутизаторы, а также мультиплексоры-скремблеры и другое приемопередающее оборудование. На головные станции операторов устанавливаются локальные скремблеры и глобальные SMS и CAS серверы, содержащие в себе соответствующие виртуальные серверы. Каждый виртуальный SMS и CAS сервер закреплен за отдельным оператором. Связь между ЦОД СУД DRECrypt и головной станцией оператора организуется при помощи защищенных туннелей в сети Интернет, формируемых маршрутизаторами. Выход в Интернет центрального маршрутизатора осуществляется при помощи постоянного фиксированного канала связи.

NB

ВЫГОДЫ ОТ ИСПОЛЬЗОВАНИЯ СХЕМЫ CAS REMOTE DRECRYPT

Во-первых, отсутствуют расходы на приобретение, установку и содержание аппаратной части СУД DRECrypt, т.к. оно находится в ЦОД СУД DRECrypt.

Во-вторых, затраты связаны только с лицензионными отчислениями за пользование ПО DRECrypt и аренду канала Интернет;

В-третьих, функциональность и все преимущества СУД DRECrypt остаются прежними.

NetUP CAS/DRM – NetUP

Производитель: NetUP. **Год первой инсталляции в России:** 2006. **Пользователи:** "Югрател", "Теле-сервис Тула", Latnet TV.

NB

Трехуровневое шифрование контента. Бескарточная система авторизации абонентов и дешифровки контента на абонентских устройствах. Поддержка видеопотоков формата H.264. Простота, низкая стоимость и удобство интеграции в IPTV-комплекс.

Система сокрытия производства компании NetUP позволяет осуществлять шифрование мультимедийных потоков и затем передавать их по незащищенным каналам связи. Только авторизованные абоненты, подписанные на данную услугу, смогут воспроизводить такие потоки. Благодаря системе сокрытия оператор IPTV может контролировать доступ к контенту и строить финансовые взаимоотношения с абонентами.

Система условного доступа компании NetUP является оптимальной для применения в составе комплекса IPTV. NetUP CAS/DRM поставляется в качестве отдельного сервера и не требует дополнительного оборудования для шифрования, а также клиентских смарт-карт доступа для дешифровки контента. Аутентификация и идентификация пользователей осуществляются при помощи сервера NetUP IPTV Middleware.

Особенности и преимущества системы NetUP CAS/DRM

NetUP CAS/DRM предназначена для использования в качестве компонента NetUP IPTV Complex. Система обладает очень высокой защищенностью от взлома и подбора ключей шифрования контента. При этом она отличается простотой и низкой стоимостью по сравнению с конкурентами.

Система использует алгоритм CSA (Common Scrambling Algorithm). Это позволяет задействовать аппаратные средства декодирования зашифрованных потоков на IP-STB, что особенно актуально для воспроизведения видео в формате High Definition. Есть также поддержка алгоритма AES-128 в режиме EBC и CBC.

NetUP CAS/DRM обеспечивает поддержку вещания контента в форматах SD и HD, вплоть до H.264 (MPEG-4 AVC).

Программное обеспечение NetUP CAS/DRM способно работать на различных платформах, в том числе x86, PowerPC, ARM, SuperHitachi.

NetUP CAS/DRM может взаимодействовать с абонентской базой до 1 000 000 пользователей. Однако есть ограничения по потоку данных, проходящему через сервер CAS. Один сервер не может пропускать через себя более 400 Мб/с. Для увеличения пропускной способности системы условного доступа используется несколько серверов NetUP CAS/DRM.

Принципы работы NetUP CAS/DRM

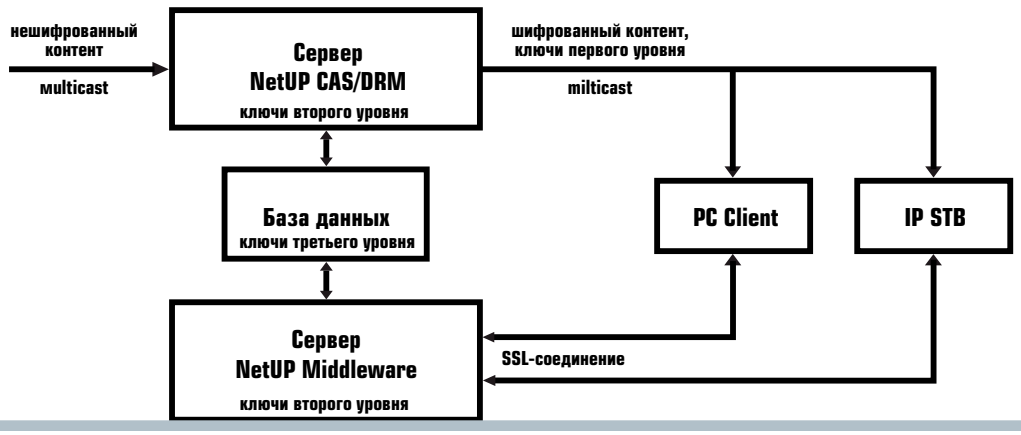
Сервер CAS принимает контент из IP-сети на один из сетевых интерфейсов, шифрует контент и отправляет его через другой сетевой интерфейс в IP-сеть, к которой подключены абоненты IPTV. Зашифрованный контент принимается STB-клиентом или PC-клиентом. На приставке должно быть установлено программное обеспечение NetUP, которое принимает и дешифрует контент, а также реализует графический интерфейс Middleware.

В IPTV-комплексе производства NetUP сервер CAS тесно взаимодействует с сервером Middleware, с помощью которого осуществляется аутентификация абонентов. Серверы CAS и Middleware, входящие в состав одной системы, связаны между собой общей базой данных.

Принципы шифрования

С каждой единицей медиаконтента ассоциируется ключ шифрования. В системе NetUP CAS/DRM используется трехуровневое шифрование:

- ключи третьего уровня являются постоянными и выделяются один раз для каждой единицы контента при первом шифровании. Эти ключи хранятся в общей для CAS и Middleware базе данных;
- ключи второго уровня динамически генерируются на основе ключей третьего уровня и текущего времени. Срок жизни ключа второго уровня — 1 час. Так как на серверах CAS и Middleware время синхронизировано, каждый из них может генерировать идентичные ключи второго уровня независимо друг от друга. По запросу ключ второго уровня может передаваться на IP STB, но только для доступных абоненту единиц контента;
- ключи первого уровня используются непосредственно для шифрования передаваемых пакетов данных и передаются в зашифрованном виде параллельным потоком вместе с контентом. Ключ первого уровня генерируется динамически на основании соответствующего ключа второго уровня, IP-адреса и текущего времени. Время жизни ключа первого уровня — несколько секунд.



Verimatrix Content Authority System (VCAS) – Verimatrix

Производитель: Verimatrix. **Год первой инсталляции в России:** 2006.
Пользователи: ОАО "Башинформсвязь", ОАО "Таттелеком", ЗАО "ИСКРАТЕЛЕКОМ", ООО "Нэт Бай Нэт Холдинг", ОАО "Центральный телеграф".

Автор: Алексей Бугай

NB

Verimatrix — бескарточная система (абоненту не нужна карта доступа).
Работает для всех основных видов абонентских устройств: STB, компьютеры, мобильные терминалы, телевизоры с подключением к Сети.
Работает для всех основных технологий: IPTV, OTT, DVB-x
Вывод: позволяет строить на одной системе криптования универсальные системы подачи контента.

Алексей Бугай, заместитель генерального директора по развитию бизнеса CTI

Современное платное интерактивное телевидение появилось совсем недавно — в начале 2000-х годов. Однако с самого начала оно претерпевало значительные изменения. От классического IPTV — к интернет-ТВ, затем к концепции "трех экранов", чтобы сейчас прийти к гибридным вариантам в комбинациях с DVB-x/IPTV/OTT и "ТВ на всех экранах".

Характер устройств, способных донести до нас все прелести интерактивного ТВ, также активно менялся. Начав с обычной абонентской приставки, телевидение "захватило" персональные компьютеры, мобильные телефоны, медиацентры, планшетные компьютеры и даже телевизоры с подключением к сети Интернет. Правда, поддерживать такое бурное развитие телевидения довелось не только производителям систем управления ТВ, middleware.

Самую активную роль в предоставлении контента на любых терминалах сыграли системы его защиты. В ряде случаев отрасль ждала развития именно систем закрытия контента на определенных устройствах, чтобы перейти в активное наступление с их использованием.

Компания CTI, один из пионеров IPTV в стране, с первых же своих разработок стала использовать систему цифрового управления правами доступа к контенту. В ходе непродолжительного начального периода в явные лидеры, по итогам наших тестов, вышла разработка компании Verimatrix, и ее продукты прочно вошли в экосистему интерактивного ТВ CTI. За последние годы наша компания убедилась в том, что выбор сделан совершенно верно. В ходе нелегкого противостояния различных систем защиты контента компания Verimatrix доказала, что в состоянии разработать и поставить качественные продукты в соответствии с любыми требованиями рынка.

На текущий момент продукты компании Verimatrix не просто покрывают все потребности операторов. На протяжении последних пяти лет произошли серьезные изменения у традиционных операторов ТВ: кабельных и спутниковых. Они также решили расширить границы своей деятельности, используя преимущества альтернативной доставки контента — через сеть Интернет. Одной из основных задач стал поиск такой системы закрытия контента, которая позволила бы в одной абонентской приставке комбинировать преимущества совершенно различных технологий. И эта задача блестяще была решена компанией Verimatrix.

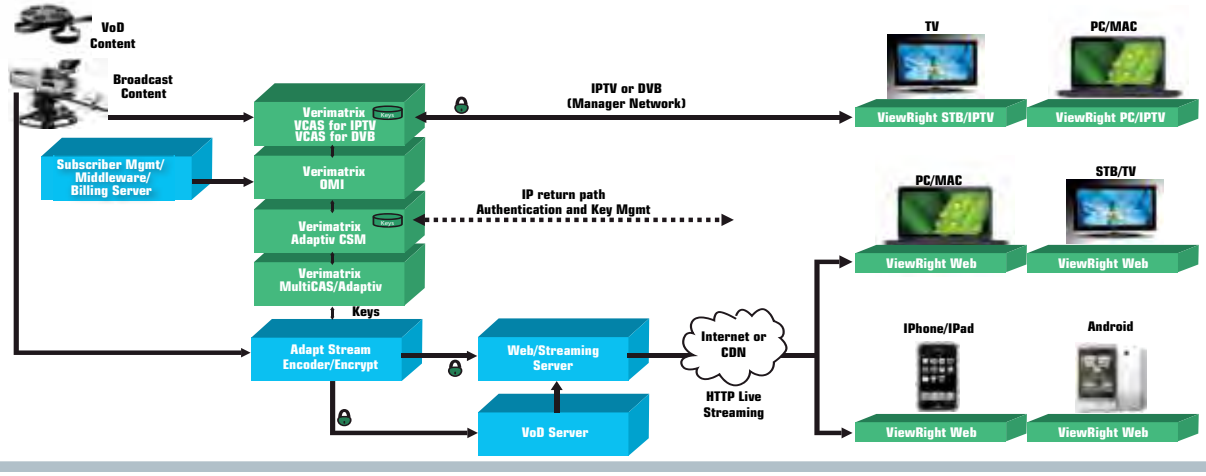
Компания CTI на собственном опыте убедилась, что вне зависимости от сложности проекта и типа используемых устройств, существует система закрытия, которую можно применять со 100%-й гарантией успеха, даже в случае когда оператор хочет представить рынку интерактивное решение, способное развиваться и распространяться на платформы, которые сейчас кажутся совершенно неприспособленными к этому.

Выбор нашей компании — решения компании Verimatrix, которая не останавливается на достигнутом и всегда нацелена на перспективу. Ее решения доказали свою состоятельность на всех современных платформах.

VERIMATRIX CONTENT AUTHORITY SYSTEM

Новейшим решением Verimatrix для защиты контента является система Verimatrix Content Authority System (VCAS). Она обеспечивает управление доступом к контенту в сетях любого типа: IPTV, интернет-ТВ, DVB, мобильное ТВ, IP over Cable. Разработанная с использованием индустриальных стандартов безопасности и защиты информации (PKI, AES, SSL и др.), VCAS обеспечивает надежную защиту контента. Модульный дизайн, гибкость и высокая масштабируемость позволяют использовать VCAS как операторам с небольшим количеством абонентов, так и крупным операторам связи.

VCAS обеспечивает защиту контента от несанкционированного доступа и исключает его копирование и последующее распространение. Принцип защиты построен на единой системе хранения, генерирования и управления ключами доступа, а также выделенного канала доступа к указанной системе. Verimatrix — очень гибкая и удобная в работе — не связана с ограничениями на архитектуру остальных компонентов системы, не требует аппаратной модификации абонентской приставки. На сегодняшний день она интегрирована более чем со 150 моделями абонентских приставок ведущих мировых производителей.



Conax Contego – Conax

Производитель: Conax AS. **Год первой инсталляции в России:** 2003. **Пользователи:** Операторы эфирного и спутникового вещания.
Дилеры: "Контур-М", "АМТ Групп", TelCo Group, "В-Люкс".

Компания Conax имеет 25-летний опыт в разработке систем защиты контента, реализованных в едином комплексном решении.
Поднимая безопасность распространения цифрового ТВ-контента на новый уровень, Conax Contego представляет собой новое поколение систем защиты контента и позволяет максимально обезопасить премиум-контент от несанкционированного доступа. Эта новейшая система построена в соответствии с современными требованиями.

Conax Contego позволила отойти от концепции "черного ящика", которая используется в большинстве систем защиты контента, и создана с учетом удобства работы, что делает ее эксплуатацию ясной и простой в управлении. К ее основным преимуществам относятся:
- более высокий уровень безопасности, гибкости и масштабируемости по сравнению с другими системами, доступными на рынке;
- лучший инструмент для обеспечения безопасного распределения контента через любые платформы и любой тип сети;
- динамическая архитектура отвечает любым требованиям резервирования;
- интуитивно понятная система управления.

Открытые и общедоступные системы защиты контента Conax представляют собой передовую технологию для всех типов сетей, бизнес-моделей и гибридных комбинаций. Conax Contego является очень гибким решением, разработанным специально для сервисов платного ТВ следующего поколения. Conax Contego является полностью масштабируемой системой и поддерживает все современные бизнес-модели, востребованные на рынке. Основные характеристики включают: усовершенствованный в борьбе с пиратством механизм, смарт-карты и бескарточные опции безопасности, расширенная языковая поддержка, поддержка стандартов DVB, ISDB-T и OpenCable, DRM-контроль (Digital Right Management), защита гибридных ТВ-приставок (STB), поддержка CI Plus и CableCARD, поддержка многоадресного вещания, система "умный дом" и домашние сети, совместимость с абонентскими приставками более чем двухсот производителей.

Универсальность

Conax Contego масштабируется горизонтально, то есть емкость и производительность могут быть легко увеличены путем добавления дополнительных аппаратных средств. Это позволяет операторам начать с базовой установки и расширять ее по мере производственной необходимости, чтобы соответствовать меняющимся требованиям и новым бизнес-моделям. Conax поддерживает бесшовную интеграцию с технологиями третьих сторон. Это делает возможным свободный выбор лучших в своем классе комбинированных решений для индивидуальных платформ.

Простой доступ к новой функциональности

Conax Contego поддерживает все бизнес-модели, доступные на рынке, такие как подписка, "оплата-за-просмотр", "видео-по-запросу", DRM и другие. Возможность инсталляции "все-в-одном" включает в себя все опции Conax Contego, что позволяет операторам платить только за функциональные возможности, которые они выбрали в соответствии с индивидуальным решением. Система лицензирования упрощает установку, поддержку и модернизацию.

Безопасность и простота пользования

Conax Contego имеет удобное управление системой и навигацию. Система управления включает в себя много важных функций, таких как пошаговый мастер, диагностика, составление отчетности и ведение журнала. Conax Contego также включает в себя комплексную систему мониторинга, которая следит за состоянием установки и аппаратной платформы.

Одна система — любая операция

Conax Contego поддерживает любую технологию распределения контента и разработана для защиты контента, передаваемого на широкий спектр абонентских устройств, например STB, IDTV, ПК и мобильные телефоны. Conax Contego может поддерживать вещательный и широкополосный тип доставки контента потребителю при помощи смарт-карт или без них.

NB

Опции Conax Contego

- Subscription является функциональным ядром системы, дающим возможность продавать контент с использованием различных бизнес-моделей подписки, таких как подписка на ограниченное время или подписка с открытой датой, а также поддерживает другие функции, необходимые для базовых операций платного ТВ. Эта опция поддерживает как управление доступом конкретного подписчика к контенту, так и продление подписки на следующие месяцы при условии соблюдения условий доступа. Авторизация происходит помесячно.
- Contego Pairing — это опциональное дополнение безопасности, обеспечивающее криптографический обмен данными между смарт-картами и STBs, работающими вместе. Основной задачей использования опции Pairing является предотвращение раздачи контрольного слова.
- Pay Per View — это опциональное дополнение, которое дает возможность использования бизнес-моделей Near Video On Demand и Event Pay Per View, когда оператор может назначать цену за отдельные события или фильмы.
- On-demand обеспечивает поддержку классической модели Video On Demand.

Cloaked CA – Irdeto

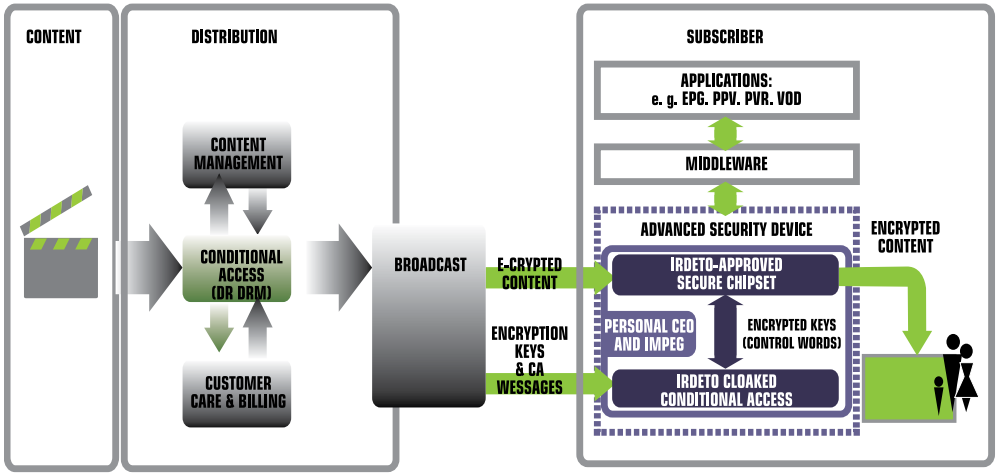
Производитель: Irdeto. **Первая инсталляция:** 2004. **Пользователи:** "Космос-ТВ", "Радуга ТВ", "ГеоТелекоммуникации", "Орион Экспресс", "Гелиос, ЗАО" "Телекомпания «СТРИМ»", ТБТ, "Комстар — Регионы Ростовский филиал".

Миссия компании Irdeto заключается в обеспечении инновационного, безопасного, надежного решения по управлению цифровым контентом и создании систем защиты для предоставления своим клиентам новых возможностей в бизнесе. На протяжении более 40 лет Irdeto создает надежные решения по безопасности для индустрии платного ТВ.

Следуя духу инноваций, компанией Irdeto была разработана новая технология, которая впервые в индустрии вещательного ТВ позволила операторам значительно уменьшить затраты на системы условного доступа (СУД). Irdeto Cloaked CA — бескарточное решение, полностью совместимое со стандартом DVB, оно исключает все расходы на логистику, необходимость поддержания запасов смарт-карт (нет "замороженных" средств), а также позволяет избежать трудностей, связанных с распространением и заменой смарт-карт. Irdeto Cloaked CA-клиент не может быть потерян или поврежден абонентом. Уникальная привязка к приставке позволяет персонализировать каждый Cloaked CA-клиент, что исключает возможность клонирования. Технология Cloakware защищает Cloaked CA-клиент от взлома и модификаций.

Irdeto Cloaked CA (Software CAS) обеспечивает уникальные преимущества для операторов:
- Cloaked CA-клиент активируется, когда активируется абонент. Оплата за него может производиться после начала потребления услуги абонентом, а это — значительное уменьшение замороженных активов;
- время на изготовление и доставку, по сравнению с решением, базирующимся на смарт-картах, сведено практически до нуля, то есть менее жесткие требования к планированию;
- отсутствие логистики. Irdeto Cloaked CA исключает все проблемы, связанные с распространением смарт-карт и логистикой, что влечет уменьшение затрат времени и денег для оператора;
- нет необходимости в привлечении компании-перевозчика и дистрибьютора — отсутствие связанных с перевозчиком рисков;
- нет необходимости в товарных запасах на складах — экономия на складских расходах (средства, сотрудники, пространство);
- отсутствие логистики и почтовых расходов при замене карт — отсутствие рисков (задержка, потеря);
- отсутствие возможности кражи во время дистрибуции. Снимаются многие вопросы, связанные с доверием к персоналу и дистрибуторам. Как следствие, уменьшение расходов и увеличение продаж за счет возможности привлечения гораздо большего количества дистрибуторов;
- отсутствие возможности физического повреждения и утери карточки абонентом. Простота пользования и надежность увеличивают доверие абонентов и, как следствие, прибыль оператора;
- простота интеграции — Irdeto Cloaked CA-клиент полностью совместим со стандартами DVB.

Преимущества с точки зрения безопасности:
- уникальные технологии обеспечивают защиту Irdeto Cloaked CA-клиента. Он является полностью обновляемым дистанционно, непосредственно у абонента. СУД Irdeto с универсальным клиентом может обеспечить такой же уровень защиты, как и решения на основе смарт-карты;
- в решении Irdeto Cloaked CA используются запатентованные технологии безопасности Cloakware для защиты программного кода и данных. На сегодняшний день эти технологии обеспечивают защиту данных в более чем двух миллиардах устройств в мире;
- Irdeto Cloaked CA-клиент может быть привязан к приемнику (или другому устройству) несколькими способами, в процессе привязки клиент персонализируется под это устройство. Это делается для предотвращения клонирования клиента — самой большой проблемы безопасности систем на основе ПО-клиента без обратного канала.



NB

CLOAKED CA — БЕСКАРТОЧНОЕ РЕШЕНИЕ IRDETO

Irdeto Cloaked CA — бескарточное решение, полностью совместимое с DVB-стандартом, исключает все расходы на логистику, необходимость поддержания запасов смарт-карт, а также трудности, связанные с распространением и заменой смарт-карт. Irdeto Cloaked CA-клиент не может быть потерян или поврежден абонентом. Уникальная привязка Irdeto Cloaked CA-клиента к приставке позволяет персонализировать каждый Cloaked CA-клиент и исключает возможность клонирования. Технология Cloakware защищает Cloaked CA-клиента от взлома и модификаций. Irdeto Cloaked CA-клиент полностью обновляем дистанционно, непосредственно у абонента. СУД Irdeto с Универсальным Клиентом обеспечивает такой же уровень защиты, как и решения на основе смарт-карты. В решении Irdeto Cloaked CA используются запатентованные технологии безопасности Cloakware для защиты программного кода и данных. Защищенный загрузчик приставки обеспечивает высокую степень защиты от пиратских модификаций программного обеспечения приставки.