CryptoGuard – *Protect your content*

CryptoGuard DRM and OTT Solutions

КОНТУР

Digital broadband communications

Технология OTT хорошо отвечает запросам современных молодых людей, которые желают смотреть любимый ТВ/видео-контент на их мобильных гаджетах, когда и где они пожелают – дома в кровати, в путешествии, в гостях, по дороге на учебу или работу. Операторы, предоставляющие платные ТВ/видео сервисы, рано или поздно понимают необходимость внедрения OTT, чтобы быть не хуже своих конкурентов.

Современные телезрители привыкают к возможности высококачественного просмотра видео повсюду. Оператор, предоставляющий платное ТВ, желающий запустить OTT сервисы должен инвестировать в головное оборудование и также оплачивать услуги сетей доставки контента (Content Delivery Networks), таких как Akamai, LimeLight, TaTa и им подобных. Для многих операторов такая ситуация вызывает головную боль, поскольку возникает необходимость затрат и инвестиций, а потребители желающие получить новые сервисы не готовы много платить за них.

CryptoGuard является сегодня первым CAS/DRM вендором, который разработал решение, делающим доступным высококачественное OTT решение как в отношении OTT технологии, так и сети доставки контента (CDN).

Далее мы поясним - почему наше решение радикально снижает стоимость и позволяет оператору бесплатно использовать общепризнанные программные продукты от производителей мирового класса.

Краткая справка

Digital rights management (DRM) – это технология контроля доступа к контенту, используемая производителями и право-обладателями для ограничения использования цифровых устройств и ограничения использования защищенной правами аудио-визуальной информации. DRM предотвращает неавторизованное распространение и использование контента. DRM обеспечивает, например, оплату контента пользователями через своего провайдера. Для чего DRM организует взаимодействие, например, межу пользователем, контент-провайдером (или интернет-сервис провайдером), DRM-центром и платежным шлюзом. Производится ряд операций, необходимых для проверки авторизации и оплаты контента, в том числе - запрос на контент, аутентификация пользователя, шифрование или авторизация контента, запрос на оплату, одобрение и подтверждение оплаты.

Подход CryptoGuard к DRM

Новые фильмы в высоком разрешении, доступные к просмотру на устройствах от Apple защищены **Fair Play** - технологией DRM, разработанной Apple. Когда мы смотрим контент от Netflix – американского поставщика фильмов и сериалов на основе потокового мультимедиа, или от американского контент-провайдера HBO, то на устройствах Microsoft контент защищен DRM **Microsoft PlayReady**. В свою очередь, на устройствах с ОС Android мы можем смотреть фильмы, защищенные DRM **Google Widevine**. Таким образом мы видим, что контент-провайдеры одобряют так называемые “нативные” DRM системы. Красота таких систем в том, что они бесплатны для использования контент-провайдерами, операторами платного ТВ и технологическими вендорами.

Поскольку Apple Fair Play, Google Widevine и Microsoft PlayReady бесплатны для использования и одобрены студиями, подход CryptoGuard к DRM заключается в том, чтобы поддерживать эти DRM системы из единой головной станции.

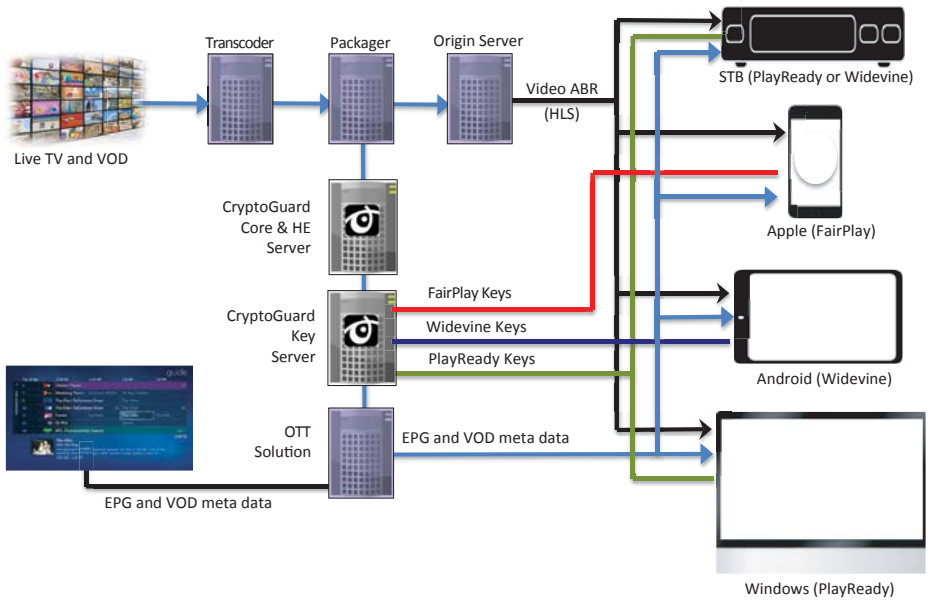
Это означает, что оператор может управлять правами на контент по отношению к пользователям и устройствам из головной станции CryptoGuard.

Возможно, что какой-то ТВ канал не разрешит оператору предоставлять для его канала сервис **Start-Over TV** (воспроизводит текущее телешоу с самого начала), но вероятно другой ТВ канал может разрешить Start-Over, но не даст разрешения на **Catch-Up TV** (просмотр ТВ передач через некоторое время после их выхода в эфир). Следующий поставщик контента может разрешить оператору оба этих сервиса, но, возможно ограничит их условием использовать не более, чем на 3-х пользовательских устройствах одновременно. Все такие “установки” контент-провайдеров, вместе с условиями для вещаемых “в живую” ТВ каналов легко управляются в головной станции CryptoGuard.Подход CryptoGuard к DRM обеспечивает также ряд других экономических преимуществ. Разработчики, создающие свои приложения для смартфонов и планшетов предпочитают иметь дело с широко распространёнными нативными DRM (например Google Widevine или Microsoft PlayReady), а не с проприетарными DRM, поскольку работать с нативными DRM существенно проще и такие решения в своей основе уже созданы и “обкатаны” на большом парке устройств.

Следующее преимущество состоит в том, что все нативные DRM работают с общепринятым HTTP стримингом видео, таким как стандартный HLS стриминг, что означает на практике очень значительное снижение расходов, связанных с транскодерами, “пэкиджерами” (packager) и оборудованием сети доставки контента (Content Delivery Network).

Выбор CryptoGuard означает отсутствие платы за DRM на пользовательских устройствах, упрощение разработки OTT решения в целом и снижение затрат на головное оборудование и сеть доставки контента.

CryptoGuard DRM Solution



На картинке выше показана условная блок-схема CryptoGuard DRM & OTT Solution.

Мультипрофильный транскодер на входе создает множество копий входных потоков с различными разрешениями и битовыми скоростями. Например, “живой” входной видео-поток с битовой скоростью 4 Мб/с транскодируется в несколько выходных потоков со скоростями от 0,5 до 4 Мб/с и различными разрешениями. Это необходимо поскольку каждое пользовательское устройство может перенастраиваться по входу с одного видео-потока на другой на “лету” в условиях нестабильной скорости передачи данных в сети. При улучшении или ухудшения текущего состояния канала передачи данных пользовательское устройство каждый раз будет настроено на прием видео-потока с максимальным качеством, доступным в данный момент.

Происходит адаптивная настройка битовой скорости, т.е. используется технология Adaptive Bit Rate (ABR). Качество сети меняется, но просмотр видео не прерывается. ABR применима к сетям различной физической природы, например WiFi или LTE.

“Пекиджер” (также используется термин “сегментер”) нарезает каждый видео-поток на небольшие фрагменты – chunk (ломоть), длительностью обычно порядка 10 секунд. Эти фрагменты описываются в файле плей-листа (m3u).

Пекиджер обеспечивает также криптование видео-контента с использованием AES ключей, приходящих от системы CryptoGuard .

“Оригинирующий сервер” (Origin Server) принимает все небольшие видео-файлы от сегментера и делает их доступными для клиентских устройств на своем Web-сервере.

Поскольку все DRM системы, используют HTTP видео-стримминг, такой как HLS, один и тот же ключ используется для криптования контента для всех DRM систем.

В конечном итоге сервер OTT решения предназначен для обеспечения всех клиентских устройств текстом, картинками, видео-трейлерами и метаданными всего контента так, чтобы пользователь мог выполнять браузинг между “живыми” ТВ каналами и сервисами типа Catch Up и VoD.

Когда пользователь выбрал “живой” ТВ канал или записанный видео-контент для просмотра, его пользовательское устройство затребует ключ (key) для этого контента от имени пользователя, вошедшего (log in) в систему.

Key Server производит верификацию запроса на контент и посылает назначенный ключ (appropriate key) пользовательскому устройству для де-криптования контента.

Все пользовательские устройства должны иметь коннект с OTT сервером, CryptoGuard Key сервером и Origin сервером.

Key сервер обрабатывает огромное количество запросов от пользовательских устройств и мы рекомендуем использовать пару таких серверов, один из них - резервный.

Обычно OTT серверы могут обеспечивать взаимодействие с 50 тыс. пользовательских устройств, и мы также рекомендуем здесь использовать пару серверов с резервированием.

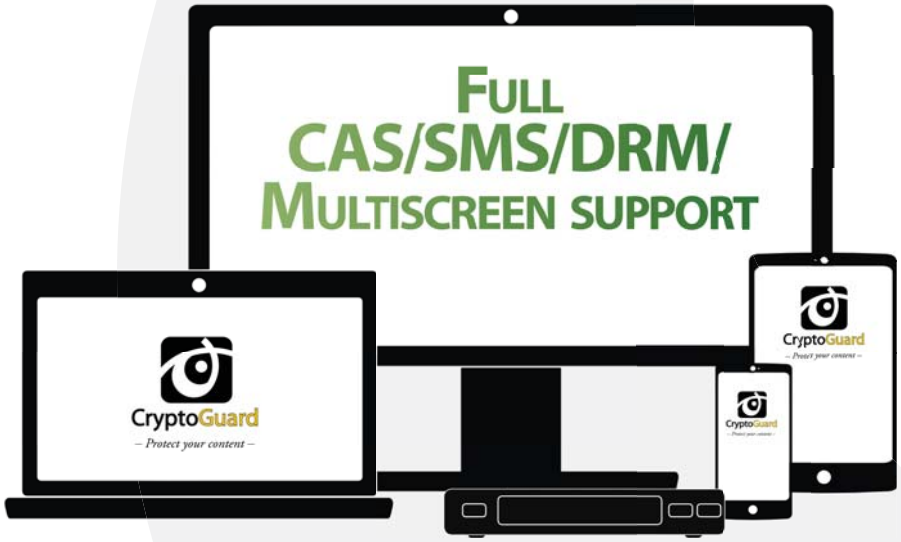
Для работы с 200 тысячами абонентов необходимо будет 4+1 серверов каждого из этих типов.

Однако, наиболее загружен Origin сервер. Например, 3000 пользовательских устройств получают каждый видеопоток, условно примем 2 Мб/с, суммарная нагрузка на сервер составит 6 Гбит/сек видео-трафика. Тут также надо внимательно определять требования к Интернет-каналу от головной станции. Если 3000 зрителей получают контент из недостаточно распределенной системы, следовательно надо внимательно смотреть на организацию и загрузку сети доставки контента (CDN).

Сеть доставки контента может быть просто компанией, которая разместила огромное количество стриминговых серверов повсюду, так чтобы зрители, например, в некотором небольшом городе, подключались к местному Origin серверу, а не получали контент по всему маршруту, начиная с центральной станции оператора.

Origin сервер самого оператора будет обеспечивать трафик только до серверов CDN, при этом полоса видео-трафика от центральной ГС будет разумно небольшой.

CryptoGuard имеет партнеров, являющихся лидерами решений для создания законченных OTT проектов. Часто поставщиками сегменторов, Origin серверов и в особенности мульти-профильных транскодеров являются те же самые вендоры, что уже поставляют оператору DVB оборудование, такое как мультиплексеры и скремблеры. В то же время выбор CDN сильно зависит от данного рынка. Оптимальный выбор OTT решения является серьезным вызовом.



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