ЭЛЕКТРА

Система условного доступа
CAS Электра

Индекс	**2020-CASELECTRA**
Секретность	**Публичный**
Версия	**1.0**
Компания	**Электра**

Содержание

Оглавление

ЭЛЕКТРА

Аннотация

Данный документ содержит краткое описание программного комплекса CAS Электра, где описаны его структура и основной функционал.

ЭЛЕКТРА

Глоссарий

Термин	Определение
Система условного доступа (СУД) – CAS (Conditional Access System)	Система или комплекс программно-аппаратных систем, обуславливающий доступ к кодированным (этой системой) каналам или радиостанциям. Иными словами, это система управления получением разрешений на доступ к транслируемому контенту.
IP-технологии	Маршрутизируемый протокол сетевого уровня стека TCP/IP. Именно IP стал тем протоколом, который объединил отдельные компьютерные сети во всемирную сеть Интернет. Неотъемлемой частью протокола является адресация сети.
“Видео по запросу” - Video on demand (VOD)	Система индивидуальной доставки абоненту телевизионных программ и фильмов по цифровой кабельной, спутниковой или эфирной телевизионной сети с мультимедиасервера в различных мультимедиаконтейнерах. Фильм можно в любое время заказать из каталога, при этом часто поддерживаются дополнительные функции: перемотка, пауза, закладки.
Широковещательные каналы	Метод передачи данных в компьютерных сетях, при котором поток данных (каждый переданный пакет в случае пакетной передачи) предназначен для приёма всеми участниками сети.
Видеосервер	В системах телевизионного вещания видеосерверы используются для плановой выдачи заранее подготовленных видеоматериалов в эфир. В большинстве случаев видеосерверы находятся под управлением системы автоматизации телевизионного вещания.
Мультиплексор (MUX)	Устройство, позволяющее выбирать, комбинировать и передавать с более высокой скоростью один или несколько низкоскоростных аналоговых или цифровых входных сигналов на одной общей среде или в пределах одного общего устройства. Таким образом, несколько сигналов могут совместно использовать одно устройство или проводник передачи, такой как медный провод или оптоволоконный кабель.
Simulcrypt	Компонент головного оборудования, предназначенный для установления и поддержания соединения с ECMG, передачи ему CW и AC, получения сгенерированных ECM сообщений и перенаправление их в MUX.
Клиентская библиотека	Интерфейс прикладного программирования (API), предназначенный для использования при написании клиентских приложений. Клиентская библиотека пр едоставляет общие строительные блоки для построения распределенных клиентских приложений, включая приложения, не связанные с базой данных.
Hybrid Broadcast Broadband TV (HbbTV)	ТВ-стандарт для передачи дополнительных предложений из интернета на телевизор. Для приёма специально подготовленных веб-страниц в формате CE-HTML необходимо

	интернет-соединение, а также специально оборудованное ТВ-устройство или дополнительный HbbTV-приёмник. Также возможен приём сигнала через спутник. «Hybrid Broadcast Broadband Television» наряду с информацией о программах имеет также возможность скачивания содержимого передачи и интерактивные компоненты.
IPTV или Телевидение по протоколу интернета (Интерактивное телевидение)	Технология (стандарт) цифрового телевидения в сетях передачи данных по протоколу IP, используемая операторами цифрового кабельного телевидения, новое поколение телевидения.
Инфраструктура открытых ключей (ИОК, англ. PKI — Public Key Infrastructure)	Термин, подразумевающий набор мер и политик, позволяющих развертывать и управлять одной из наиболее распространенных форм онлайн-шифрования — шифрованием с открытым ключом.
Цифровые сертификаты X.509	Цифровые документы, которые представляют пользователя, компьютер, службу или устройство. Центр сертификации (ЦС), подчиненный ЦС или центр регистрации выдает сертификаты X.509. Сертификаты содержат открытый ключ субъекта сертификата.
Advanced Encryption Standard (AES)-128	Симметричный алгоритм блочного шифрования.
Водяной знак Watermarking	Технология, созданная для защиты авторских прав мультимедийных файлов. Обычно цифровые водяные знаки невидимы. Однако ЦВЗ могут быть видимыми на изображении или видео. Обычно это информация представляет собой текст или логотип.
Broadcast Encryption Manager (BEM)	Компонент структуры СУД, отвечающий за шифрование передаваемого видеоконтента.
Entitlement Control Message Generator (ECMG)	Компонент структуры СУД, управляющий генерацией ECM сообщений.
Real Time Encryption Server (RTES)	Сервер шифрования в реальном времени.
Remote Key Extractor (RKE)	Обеспечивает возможность передачи ключей «видео по запросу» от дистрибьютера к ретейлеру.
Remote Stream Manager (RSM)	Обеспечивает возможность передачи ключей шифрования широковещательных потоков от дистрибьютера к ретейлеру.
Certificate Authority (CA)	Центр сертификации - управляет созданием и обслуживанием всех сертификатов PKI, необходимых для работы системы.
Key Server (KS)	Сервер ключей - генерирует ключи шифрования.
Client Protection (CP)	Накапливает информацию о транзакциях, используемую для возможного обнаружения дублирующих устройств.
Automatic Redundancy Controller (ARC)	Компонент сетевого управления для контроля резервирования модуля RTES.
SOAP Agent (SA)	Предоставляет сервисы Simple Object Access Protocol (SOAP) для интеграции со сторонними приложениями.

Web Services Engine (WSE)	Обеспечивает функциональность SA сервиса CAS Электра.
CAS Электра GUI	Обеспечивает доступ к графическому интерфейсу CAS Электра.
Video Pre-Processor (VPP)	Управляет автономным шифрованием видеофайлов перед их публикацией на VOD-сервере.
Remote Stream Manager (RSM)	Обеспечивает возможность передачи ключей шифрования.
Remote Key Extractor (RKE)	Обеспечивает возможность передачи ключей «видео по запросу» от дистрибьютера к ретейлеру.

ОПИСАНИЕ

CAS Электра представляет собой программный комплекс, являющийся частью системы условного доступа (СУД) и технических средств защиты авторских прав (ТСЗАП).

Программный комплекс применяется для защиты телевизионного контента, передаваемого с использованием IP-технологий. От традиционных форматов вещания, таких как эфирное, спутниковое и кабельное телевидение, IP-телевидение отличается тем, что использует преимущества двустороннего канала связи, доступного в IP-сетях. Услуги IP-телевидения могут применяться как для “видео по запросу” Video on demand (VOD), так и для традиционного вещательного ТВ-контента.

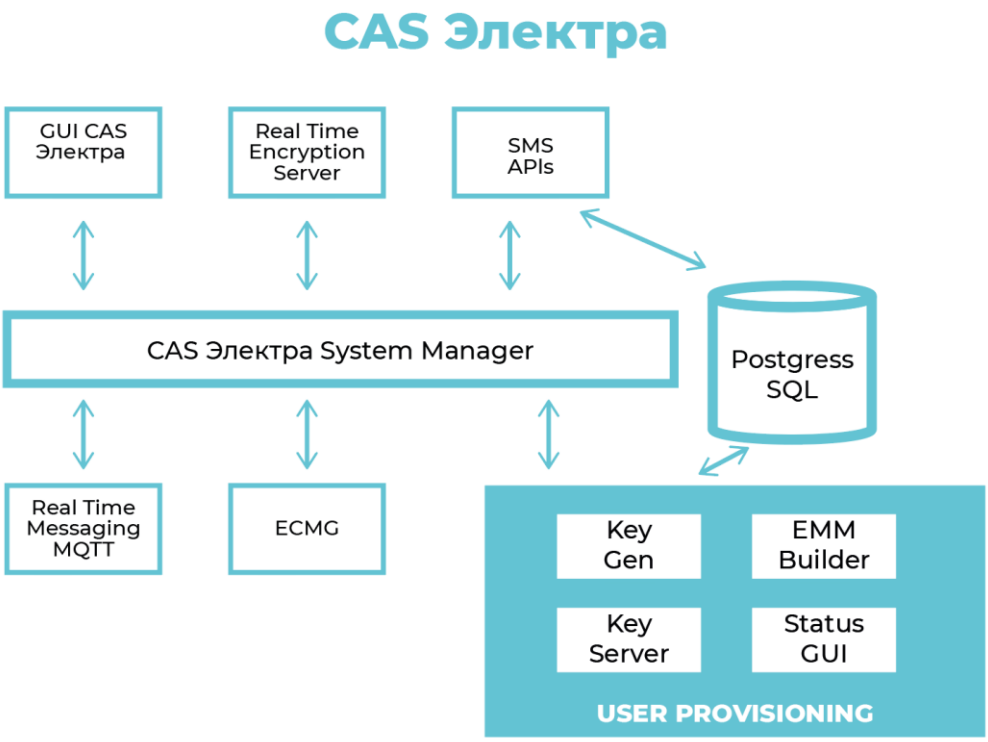
CAS Электра поддерживает:

- Стандартизированные двусторонние протоколы безопасности, используемые в IP-среде;
- Шифрование широковещательных каналов, где источником видеоканалов является внешний многопотоковый видеосервер;
- Шифрование широковещательных потоков через внешний IP-стример/мультиплексор (MUX) с поддержкой технологии Simulcrypt;
- Ручное или автоматическое шифрование видеофайлов для реализации услуги видео по запросу (VOD);
- Клиентская библиотека CAS Электра для абонентских устройств IPTV и Hybrid Broadcast Broadband TV (HbbTV);
- Система пар открытых и закрытых ключей Public Key Infrastructure (PKI), а также цифровые сертификаты X.509, использующие проверенные методы управления ключами CAS Электра;
- Возможность программного и аппаратного шифрования с использованием надежного алгоритма Advanced Encryption Standard (AES)-128;
- Многочисленные стандарты кодеков и видеоформатов: SD, HD, Ultra HD (UHD);
- Специальный водяной знак Watermarking с уникальным и высоконадежным идентификатором, который можно отследить до конечного пользователя.

СЕРВЕР И ЕГО ПРОГРАММНЫЕ КОМПОНЕНТЫ

CAS Электра состоит из различных модулей, включая абонентские устройства и серверные компоненты. Архитектура разработана с учетом возможности масштабирования, гибкости и резервирования.

Программный компонент – это программный сервис, работающий на сервере и выполняющий определенную функцию. Конфигурация сервера определяется программными компонентами, работающими на этом сервере. В CAS Электра программные компоненты могут быть включены по отдельности, а при необходимости могут быть перемещены с одного сервера на другой.



Настоящее описание соответствует классической организации архитектуры системы CAS Электра. В случае необходимости архитектура решения может быть пересмотрена в соответствии с нуждами конкретного заказчика.

- ***Компонент Broadcast Encryption Manager (BEM)*** может состоять либо из ECMG с шифратором/мультиплексором стороннего производителя, либо из RTES, но, как правило, не из обоих;

- ***Компоненты Remote Key Extractor (RKE) и Remote Stream Manager (RSM)*** предназначены только для развертывания FRM и могут быть развернуты на отдельном сервере или на удаленном Content Security Manager (CSM);

- ***Site Manager (SM)*** является опциональным компонентом.

В таблице приведены конфигурации сервера и программные компоненты, которые могут присутствовать в развертывании CAS Электра. Не все конфигурации/компоненты развернуты в каждой среде, и некоторые развертывания могут содержать иные конфигурации/компоненты; фактическая конфигурация развертывания зависит от нужд конкретного заказчика.

Конфигурация Сервера	Программный Компонент	Функция компонента
Content Security Manager (CSM)	CA	Certificate Authority (Центр сертификации): управляет созданием и обслуживанием всех сертификатов PKI, необходимых для работы системы.
	CI	Client Interface (Интерфейс пользователя): осуществляет защищенный обмен информацией между абонентскими устройствами и компонентами основного сервера
	KS	Key Server (Сервер ключей): генерирует ключи шифрования
	CP	Client Protection (Защита пользователей): накапливает информацию о транзакциях, используемую для возможного обнаружения дублирующих устройств
Broadcast Encryption Manager (BEM)	RTES	Real Time Encryption Server (Сервер шифрования в реальном времени): модуль шифрования в реальном времени многопоточных/однопоточных

		инкапсулированных видеопотоков для услуг вещания
	ECMG	Entitlement Control Message Generator (компонент, управляющий генерацией ECM сообщений): реализует спецификацию протокола Simulcrypt, который позволяет шифровать широковещательные потоки с помощью мультиплексоров сторонних производителей
	ARC	Automatic Redundancy Controller: Компонент сетевого управления для контроля резервирования модуля RTES
Operator Management Interface (OMI)	SA	SOAP Agent: предоставляет сервисы Simple Object Access Protocol (SOAP) для интеграции со сторонними приложениями
	WSE	Web Services Engine: обеспечивает функциональность SA сервиса CAS Электра
	CAS Электра GUI (GUI)	Реализует графический интерфейс CAS Электра
Video Encryption Manager (VEM)	VPP	Video Pre-Processor: управляет автономным шифрованием видеофайлов перед их публикацией на VOD-сервере
	RUN	RUN: автоматизирует обработку видеофайлов
Remote Stream Manager	RSM	Обеспечивает возможность передачи ключей шифрования широковещательных потоков от дистрибьютера к ретейлеру
Remote Key Extractor	RKE	Обеспечивает возможность передачи ключей «видео по запросу» от дистрибьютера к ретейлеру

Content Security Manager (CSM)

CSM является основным компонентом решения CAS Электра. Он реализует безопасную аутентификацию и авторизацию абонентских устройств, и распределение ключей в реальном времени. CSM также поддерживает развертывание современных интерактивных функций платного телевидения, таких как Personal Video Recorder (PVR) и Network PVR (nPVR).

CSM выступает в роли корневого центра сертификации (CA) в иерархии PKI при развертывании данной системы. Сертификаты X.509 используются для проверки и авторизации всех устройств в сети платного телевидения, защиты протоколов обмена сообщениями между программными компонентами CAS Электра и между системой головной станции и аутентифицированными абонентскими устройствами.

Реализация CSM может быть масштабирована под любой размер развертывания оператора путем распределения процессов компонентов CSM по кластерам физических серверов с использованием балансировки нагрузки и поддержки обхода отказа для каждого компонента.

CSM обеспечивает взаимодействие с абонентскими устройствами, который включает в себя:

- аутентификацию абонентов;
- инициализацию абонентских устройств;
- управление сеансами;
- безопасное распределение ключей абонентских устройств;
- проверку прав доступа.

Как правило, CSM содержит следующие программные компоненты:

CA - управляет созданием и обслуживанием всех сертификатов PKI

- Выступает в качестве главного компонента сертификации для сервисов CAS Электра

- Выдает новые сертификаты абонентским устройствам

- Хранит пользовательские сертификаты в базе данных CAS Электра

- Осуществляет отзыв сертификатов для отключения определенных абонентских устройств

- Использует сертификаты X.509 для проверки всех абонентских устройств и контента

- Предотвращает неавторизованное вмешательство в работу системы CAS Электра

KS - генерирует ключи для вещательных каналов

- Передает ключи вещания непосредственно на ТВ-приставки, ECMG и RTES

- Контролирует срок действия ключей

- Выполняет запросы к базе данных в режиме реального времени

- Предоставляет ключи ECMG, которые затем используются для шифрования контрольных слов control words (CW)

CI - Передает запросы сертификатов и ключей VOD между абонентскими устройствами и CSM

- Обеспечивает единую точку связи всех абонентских устройств с системой CAS Электра

- Предоставляет абонентским устройствам файл конфигурации при использовании загрузочного сервера

- Обеспечивает распределение запросов абонентских устройств между службами KS.

Operator Management Interface (OMI)

OMI представляет собой унифицированный SOAP-интерфейс для сторонних приложений, обеспечивающий создание и управление устройствами и услугами.

OMI предоставляет единый интерфейс для развертывания головных станций, распространяющих контент через различные сети и различные абонентские устройства. В результате OMI упрощает интеграцию головных станций и обеспечивает однородное управление правами для гетерогенных сетей и устройств.

В состав OMI также входит GUI CAS Электра - защищенный графический веб-интерфейс пользователя, поддерживающий основные функции, связанные с управлением функциями защиты контента в системе платного телевидения. GUI CAS Электра поддерживает такие функции, как определение сетей, управление устройствами, определение каналов, управление пользователями и подписками.

С помощью OMI операторы могут:

- Определять и управлять широкополосным вещанием и VOD-контентом;
- Определять и управлять абонентскими устройствами;
- Определять и управлять правами и политиками абонентов;
- Отправлять сообщения на абонентские устройства.

OMI состоит из следующих программных компонентов:

Web Services Engine - Обеспечивает функциональность SA сервиса CAS Электра

- Обеспечивает единую точку интеграции для всех приложений сторонних производителей

- Обеспечивает безопасный, аутентифицированный пользователем интерфейс для управления услугами

- Предоставляет SOAP-интерфейс к SMS-системам для синхронизации прав доступа

- Предоставляет SOAP-интерфейс к системам управления контентом

- Предоставляет SOAP API, поддерживающий многие популярные языки программирования

SOAP Agent - Внутренний SOAP-агент CAS Электра

- Обеспечивает безопасный интерфейс для управления системой

- Взаимодействует с компонентом Web Services Engine (WSE)

- Обеспечивает управление устройствами и контентом как для VOD, так и для вещательного контента

Broadcast Encryption Manager (BEM)

Конфигурация сервера BEM содержит программные компоненты, необходимые для обработки широковещательного контента. Она может состоять либо из ECMG с шифратором/мультиплексором стороннего производителя, либо из RTES, но, как правило, не из обоих.

Real Time Encryption Server (RTES)

RTES выполняет форматирование потока и шифрование видеоконтента для многоканальной и многопоточной передачи в рамках развертывания IPTV. В сочетании с CSM, RTES выполняет шифрование в реальном времени многоадресных транспортных IP-потоков transport streams (TS), содержащих сжатое видео в стандартах MPEG. Внутри каждого потока в ECM находится информация об управлении, которая может быть извлечена и использована клиентскими библиотеками для запроса соответствующего ключа дешифрования.

RTES взаимодействует с сетевым промежуточным ПО (Middleware) для управления правами подписчиков. В качестве опции RTES может также поддерживать систему, основанную на классах обслуживания, которая предлагает доступ к контенту на каждом канале по событиям (PayPerView), а также ограничения на просмотр на основе возрастного рейтинга.

RTES поддерживает кластерную работу, позволяющую масштабировать систему от одного до сотен одновременных каналов и обеспечивать автоматическое восстановление после отказа для обеспечения непрерывности обслуживания.

RTES обеспечивает следующие функциональные возможности:

- Шифрование многопоточного IP-контента в режиме реального времени;
- Поддержка гибких конфигураций шифрования для каждого канала с помощью графического интерфейса CAS Электра или OMI API;
- Поддержка настраиваемых интервалов смены ключей и интеграции ECM для обеспечения гибкого соотношения производительности и безопасности;
- Шифрует любой поток, независимо от скорости потока, разрешения и т.п., при условии, что он инкапсулирован в MPEG TS.

Entitlement Control Message Generator (ECMG)

ECMG генерирует ECM для шифрования в реальном времени широковещательных или многоадресных потоков с помощью мультиплексоров сторонних производителей, использующих Simulcrypt протокол.

ECMG обеспечивает следующие функциональные возможности:

- Получает контрольные слова и критерии доступа от мультиплексора. Вставляет (CW) и критерии доступа в ECM, затем шифрует ECM с помощью ключа;
- Отправляет ECM на мультиплексор для вставки в транспортный поток (TS);
- Получает ключи для шифрования (CW) от программного компонента KS, входящего в состав CSM;
- Поддерживает алгоритмы шифрования Digital Video Broadcasting (DVB)-CSA и AES.

Video Encryption Manager (VEM)

В CAS Электра сервер VEM выполняет прием незашифрованного видеоконтента (в формате MPEG-TS) и выполняется его шифрование перед отправкой на сервер VOD.

VEM содержит следующие компоненты:

VPP

Программный компонент VPP представляет собой интегрированный и очень гибкий механизм генерации зашифрованных файлов контента для подготовки к передаче VOD. Он поддерживает автоматизацию процесса ввода контента от получения промежуточных файлов и метаданных до инициализации VOD-сервера и системы прав доступа абонентов.

Взаимодействуя с CSM для генерации ключей, VPP шифрует видеоконтент с использованием алгоритма скремблирования AES. В CAS Электра реализован полностью MPEG-совместимый процесс шифрования видео, что позволяет сохранять поля заголовков ключей и поддерживать самый широкий спектр утилит индексирования, например, используемых для обеспечения функций VOD “trick play”. Использование транспортных потоков MPEG и форматов ECM стандарта DVB позволяет безопасно вставлять в каждый поток гибкий набор управляющих данных, включая контроль копирования, управление водяными знаками и рейтинговую оценку контента (родительский контроль).

В VPP используются протоколы шифрования и управления ключами, симметричные тем, которые применяются в компонентах шифрования RTES и ECMG системы CAS Электра. Такой подход повышает гибкость развертываемых конфигураций системы и обеспечивает практически бесшовную поддержку функций PVR и nPVR.

Кроме того, VPP:

- шифрует любой файл при условии, что он инкапсулирован в MPEG TS (на стандартном оборудовании может обрабатывать около 1 Гб в минуту);
- Инжектирует VOD-контент через SOAP API (OMI API) либо через модуль автоматизации RUN, либо вручную через графический интерфейс CAS Электра GUI;
- Обеспечивает настраиваемый процент шифрования; независимое управление аудио и видео шифрованием;
- Обеспечивает опциональную вставку видео-меток в поток контента с помощью системы Watermarking.

RUN

Программный компонент RUN позволяет гибко автоматизировать шифрование и прием VOD-контента. Он используется только в тех случаях, когда система SMS/VOD не передает инструкции по шифрованию VOD с помощью SOAP.

В отличие от VPP, RUN отслеживает один или несколько каталогов на предмет поступления видеофайлов. При обнаружении видеофайла он выполняет определенный набор инструкций для шифрования и авторизации.

Программный компонент RUN:

- Поддерживает автоматический прием и шифрование VOD;
- Предоставляет гибкие возможности конфигурирования;
- Поддерживает импорт VOD-контента с локального диска, блока серверных сообщений (SMB) или сетевой файловой системы (NFS).

Site Manager (SM)

SM является дополнительным компонентом системы CAS Электра. Данный компонент может:

- Управлять всеми лицензиями и сертификатами в рамках развертывания CAS Электра; значительно упрощать развертывание, управление и отслеживание серверных лицензий и сертификатов абонентских устройств;
- Отслеживание всех локальных копий VCM на конкретной площадке;
- Поддержка балансировки нагрузки для избыточности и/или масштабирования.

Remote Stream Manager (RSM)

RSM устанавливается на основной станции оператора-ретейлера и выступает в роли абонентского устройства для безопасного получения ключей вещательного контента, на которые имеет право оператор-ретейлер. Затем он хранит эти ключи в локальной базе данных CAS Электра. Устройства абонентов запрашивают эти ключи контента у локального CI, как и при запросе местного вещательного контента.

Remote Key Extractor (RKE)

RKE устанавливается на основной станции оператора-ретейлера и выступает в роли абонентского устройства для безопасного получения ключей VOD-контента, на который имеет право оператор-ретейлер. Затем эти ключи хранятся в локальной базе данных CAS Электра. Абонентские устройства запрашивают эти ключи контента у локального CI, как и при запросе локального VOD-контента. RKE на основной станции оператора-ретейлера размещается на сервере с конфигурацией VEM.

Базовые программные компоненты

Существует два компонента, являющихся базовыми для платформы CAS Электра:

CAS Control Monitor (CM)

- Запускает, контролирует, останавливает и автоматически перезапускает другие компоненты CAS Электра

- Настраивается на автоматический запуск сервисов

- Отображает информацию о версии, состоянии компонентов и использовании системы для каждого компонента

CAS Logging Service (LS)

- Собирает служебные сообщения от всех компонентов CAS Электра на локальной машине

- Управляет ротацией лог-файлов, размером файлов и продолжительностью записи

- Имеет настраиваемые уровни детализирования сообщений.

Дополнительные программные компоненты/функциональные возможности

Помимо вышеупомянутых серверных конфигураций и программных компонентов, оператор могут выбрать для развертывания в своей среде дополнительные функциональные возможности/программные компоненты. Все эти компоненты требуют определенной конфигурации для их развертывания.

Менеджер шифрования ключей SoC (SoCKEM)

System-on-Chip Key Encryption Manager (SoCKEM) является дополнительной функцией CAS Электра. Это программный модуль, обеспечивающий надежное хранение ключей шифрования контрольных слов (CWE) и управляющий дополнительным шифрованием ключей контента на всем пути передачи данных. CWE - это концепция безопасности, которая используется для более эффективной защиты ключей и расширения пути шифрования ключей за пределы клиентской библиотеки до аппаратного декриптора на абонентском устройстве (SoC), присутствующей в большинстве современных ТВ и ТВ-приставок.

Модуль SoCKEM в CAS Электра предназначен для взаимодействия с программным компонентом KS, присутствующим на сервере CSM. Рекомендуется развертывать модуль SoCKEM на собственном сервере, отдельно от всех остальных серверов.

Система Watermarking

Система CAS Электра может быть развернута с дополнительной технологией защиты водяными знаками, известной как система Watermarking. Это передовая технология защиты контента, которая позволяет вставлять в видеоконтент, отображаемый на каждом абонентском устройстве системы, незаметный водяной знак. Библиотека Watermarking, установленная на абонентском устройстве, распознавая его, запрашивает у основной станции CAS Электра уникальную метку. Она незаметно и прозрачно для зрителя встраивается в информацию о видеоизображении при его отображении на абонентском устройстве.

Entitlement Management Messages (EMM)

В зависимости от потребностей среды в CAS Электра могут быть реализован Entitlement Management Messages (EMM). EMM используются для передачи инструкций и/или сообщений на абонентские устройства. Например, EMM могут использоваться для отправки инструкций устройству для обновления кэша ключей или для вывода сообщений на экран.

В IPTV-сетях EMM доставляются на абонентские устройства используя широковещательные IP потоки непосредственно с CSM (OutOfBand). В гибридной IPTV/DVB-среде эти EMM сообщения могут доставляться тем же способом (OutOfBand) или используя мультиплексор и протокол Simulcrypt (InBand). При желании CAS Электра может быть настроен на доставку EMM обоими способами.

При выборе CAS Электра для доставки EMM потребуются следующие дополнительные программные компоненты: EMM Spooler и EMM Generator (EMMG).

EMM Spooler

- Генерирует EMM, которые запускаются по запросу EMM от OMI

- Доставляет EMM одним из трех способов: непосредственно на абонентские устройства IPTV (OutOfBand), в службу EMMG для доставки DVB, или обоими способами.

- Опционально. Отправляет сконфигурированное оповещение на абонентские устройства; если абонентское устройство теряет оповещение, дешифрование на устройстве блокируется.

EMMG

- Функционирует как внутриполосный (InBand) канал передачи сигнала абонентским устройствам

- Передача EMM внутриполосно (по сети DVB, а не IPTV) на внешний мультиплексор через Simulcrypt

- Мультиплексор внедряет EMM в шифрованный вещательный поток

- Требуется клиентская библиотека 3.x или более поздней версии

Экранный дисплей (OSD)

Экранный дисплей (OSD) выводит на экран абонентского устройства ТВ-приставок изображение или текст одного из выбранных типов, определенных в головной станции CAS Электра. Изображение/текст формируется в соответствии с требованием владельцев контента о возможности быстрого изолирования и отключения источников ретрансляции каналов с помощью мгновенно появляющихся трассировочных сообщений.

Реализация OSD в CAS Электра предполагает вставку директив OSD через графический интерфейс CAS Электра и/или SOAP-интерфейсы OMI на основе каждого канала. Типы сообщений определяются в процессе интеграции абонентского устройства, но должны включать минимальную возможность отображения:

- Идентификатор оборудования абонента (MAC-адрес или другой уникальный идентификатор, используемый системой CAS Электра);
- Локальное время абонентского устройства;
- Информация о версии и сборке клиентской библиотеки;
- Сетевой или другой графический логотип.

Сообщение должно отображаться абонентским устройством поверх видеоконтента в течение настраиваемого периода времени и размещаться в определенном месте на экране. Никакие действия пользователя не могут отменить это отображение.

Управление контролем выходного интерфейса

В некоторых случаях владельцы контента могут потребовать, чтобы на аналоговых и цифровых выходах абонентского устройства применялись защитные меры для предотвращения копирования кодированного и декомпрессированного сигнала. Такая возможность реализована в текущей версии CAS Электра и предполагает вставку защищенных правил в потоки вещательного и VOD-контента, управление которыми осуществляется через графический интерфейс CAS Электра и OMI API.

В число механизмов контроля копирования, которые могут быть задействованы, входят:

- Copy Generation Management System – Analog (CGMS-A), имплементированный в аналоговые интерфейсы (NTSC/PAL) абонентского устройства;
- Macrovision Analog Copy Protection (ACP);
- Dwight Cavendish ACP;
- Digital Only Trigger (DOT);
- High-bandwidth Digital Content Protection (HDCP) защита от копирования цифровых выходов Digital Visual Interface (DVI) и High-Definition Multimedia Interface (HDMI).

Абонентские устройства должны быть способны поддерживать и контролировать через свои аппаратные и программные подсистемы любой механизм контроля копирования, требуемый CAS Электра. В каждой системе контроля копирования подробные лицензионные требования определяют необходимое поведение абонентского устройства, если конкретное правило защиты не может быть полностью реализовано.

Client Protection (CP)

CP - это дополнительный компонент, обычно развертываемый на серверной конфигурации CSM для сбора подробной информации об абонентских устройствах. Он предназначен для получения информации о дублированных или неавторизованных абонентских устройствах IPTV. Информация об устройствах собирается в лог-файлы CP и затем анализируется с помощью инструмента анализатора обнаружения дублируемых устройств (CDA).

Компонент CP используется для обнаружения различных аномалий, которые могут возникать при использовании неавторизованных абонентских устройств, включая, в частности, следующие:

- Два или более абонентских устройств с одинаковым MAC-адресом;
- Абонентские устройства, часто меняющие IP-адреса;
- Абонентские устройства со слишком большим количеством попыток аутентификации или получения ключа;
- Повторяющиеся ошибки сеансового ключа.

Собранные сообщения сжимаются и шифруются с помощью инструмента обнаружения дублируемых устройств (CDET), а затем вручную экспортируются в инструмент CDA. Инструмент CDA может быть использован для поиска аномального поведения в файлах журнала. Для работы СР требуется специальная лицензия CAS Электра.

Клиентская библиотека

В состав CAS Электра входит клиентская библиотека для различных потребительских платформ. Клиентская библиотека CAS Электра представляет собой встроенный в абонентские устройства, такие как "умные" телевизоры и приставки, программный клиент, реализующий функции безопасности CAS Электра. Клиентская библиотека обеспечивает возможность безопасной расшифровки видеоконтента, VOD и линейного вещания, в системе платного телевидения.

Клиентская библиотека CAS Электра не зависит от платформы и может работать практически на любой операционной системе. Она также может работать на новых моделях STB, оснащенных специализированным аппаратным обеспечением для дешифрования, что позволяет ускорить и повысить эффективность дешифрования контента и обеспечить поддержку UHD 4K.

Клиентская библиотека CAS Электра разработана таким образом, чтобы требовать минимального количества ресурсов от аппаратного обеспечения STB и среды исполнения, а также использовать стандартизированный набор интерфейсов для взаимодействия с промежуточным (middleware) ПО.

Клиентская библиотека CAS Электра, являясь программным решением для обеспечения безопасности, работает без использования смарт-карт. Она предлагает функции защиты контента, включающие подписание, многоуровневую проверку целостности, обнаружение отладчиков, обфускацию ключей и возобновляемость основных функций безопасности.

При гибридном развертывании DVB-IP клиентская библиотека CAS Электра также взаимодействует с DVB-потоком и дескремблером DVB-CSA, от которых получает ECM, относящиеся к DVB-услугам. Она анализирует права абонента, определяя, какие ECM необходимо расшифровать, и возвращает дескремблеру контрольные слова для тех услуг, которые абонент имеет право просматривать.

Клиентская библиотека CAS Электра тесно взаимодействует с системой Watermarking - защищенным решением для отслеживания контента, позволяющим осуществлять маркировку видео на каждом абонентском устройстве ТВ-приставке в системе платного телевидения.

Несколько важных замечаний о клиентской библиотеке CAS Электра:

- Она разработана для распространения среди производителей абонентских устройств;
- Она спроектирована таким образом, чтобы требовать минимальных ресурсов от платформы абонентского устройства;
- Работает без использования смарт-карт и другого периферийного оборудования;
- Поставщик абонентского устройства осуществляет интеграцию в платформу абонентского устройства;
- Электра помогает производителю абонентских устройств в интеграции;
- После завершения интеграции проверяется общая безопасность.

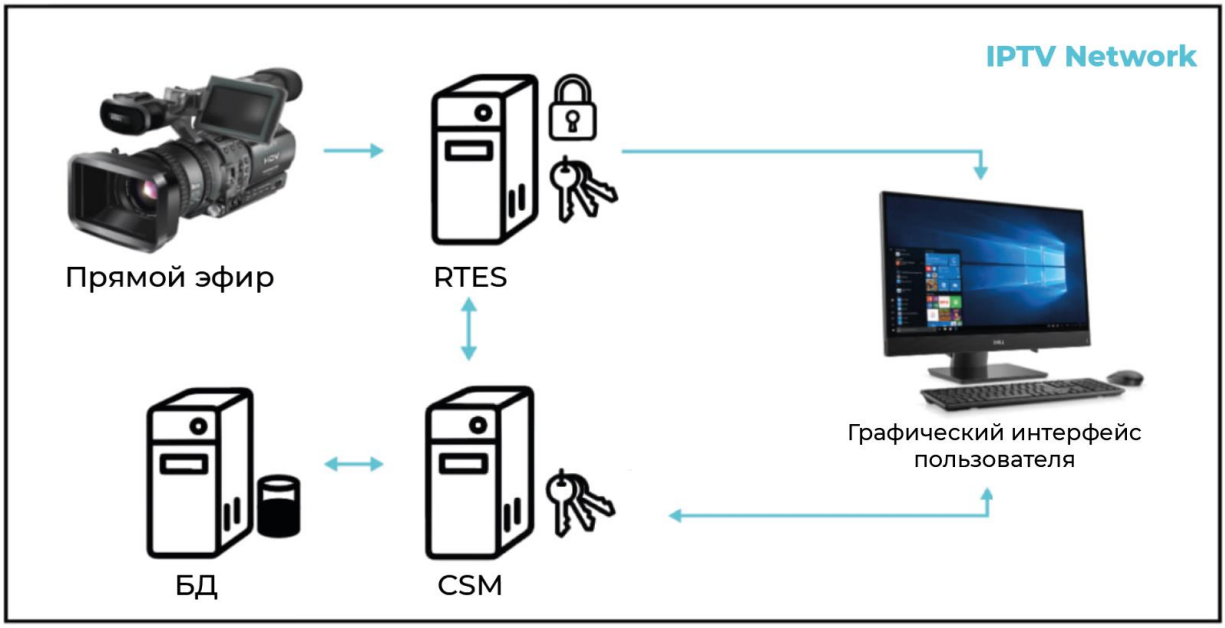
Обработка и доставка контента

Система CAS Электра использует схожую методику для обеспечения корректной расшифровки и отображения контента как для вещания, так и для VOD. Во всех случаях ключевые запросы проверяются на соответствие данным о правах абонента, связанным с соответствующим абонентским устройством.

В данном разделе представлен обзор процессов, используемых для распространения вещательного и VOD-контента.

Вещательный контент

Далее описан процесс обработки вещательного контента и его последующей доставки на абонентские устройства CAS Электра.



1) На вход RTES подается незашифрованный поток контента в формате MPEG-2 Single Program Transport Stream (SPTS). Принимаются различные форматы сжатия, включая MPEG-2, MPEG-4 SP, MPEG-4 AVC/H.264 и H.265. MPEG-2 SPTS транспортный поток должен быть инкапсулирован в пакеты UDP или RTP.

   На входе в RTES каждому каналу контента назначается IP-адрес и номер порта многоадресной рассылки. В графическом интерфейсе CAS Электра каналу также будет назначена комбинация выходного многоадресного адреса/номера порта и соответствующие параметры шифрования. Это также можно сделать с помощью OMI API.

2) RTES периодически (по умолчанию через каждые 24 часа) запрашивает смену ключа шифрования канала у сервера CSM для каждого определенного канала. Номер канала, применимый период времени и ключ шифрования канала надежно хранятся в базе данных CSM.

   Каждый поток вещания обрабатывается RTES с использованием ключа шифрования канала, в результате чего создается зашифрованный многоадресный транспортный поток MPEG-2, содержащий пакеты ECM. ECM-пакеты идентифицируют поток контента по номеру канала и содержат дополнительные правила дешифрования контента, используемые в процессе отображения.

   Такой подход к шифрованию сохраняет достаточную информацию о ключевых кадрах, необходимую для индексации потока при записи в приложениях PVR.

3) Каждое аутентифицированное абонентское устройство CAS Электра в развертывании устанавливает защищенное соединение с CSM на периодической основе (в том же цикле, в котором обновляются ключи в процессе шифрования) и запрашивает набор обновленных ключей для текущего канала.

   Абонентское устройство получает блок ключей, содержащий все актуальные ключи для каналов, которые абонентское устройство имеет право декодировать.

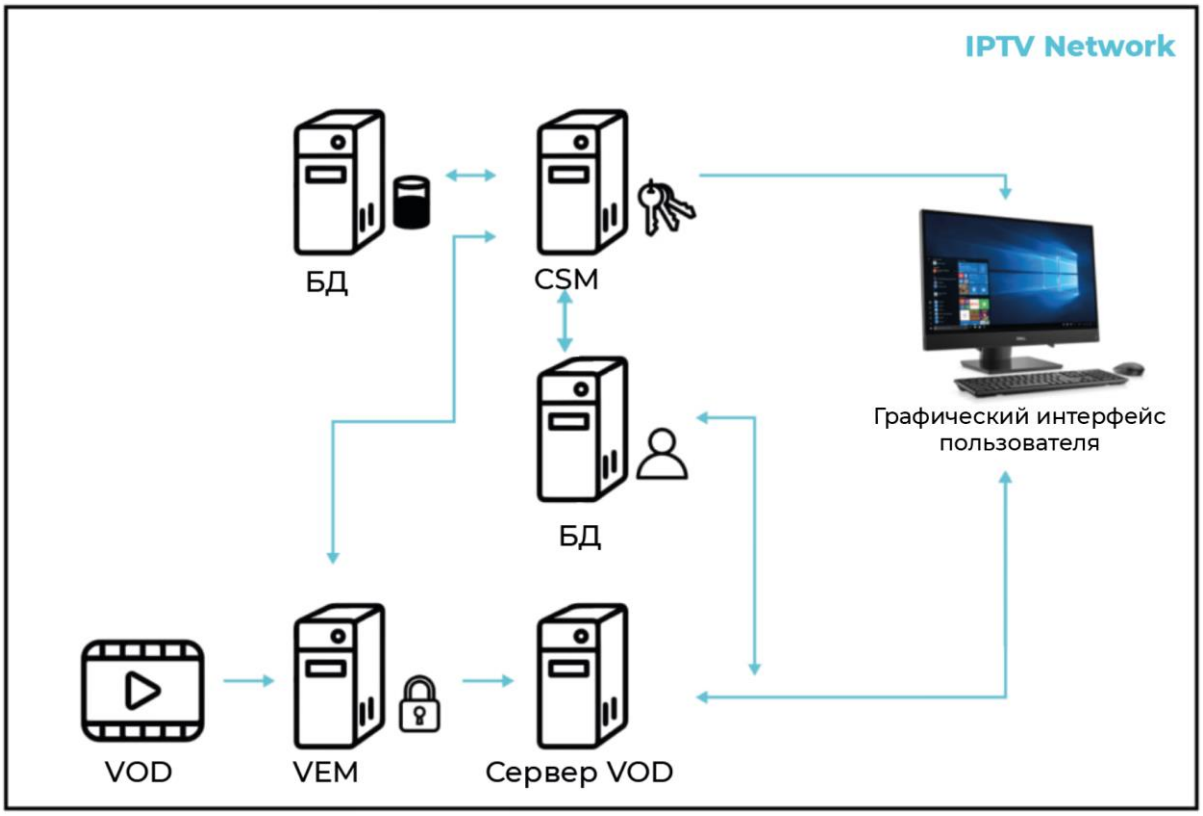
4) Когда абонент настраивается на определенный поток вещания, на абонентское устройство начинают поступать пакеты зашифрованного потока. Клиентская библиотека обнаруживает и считывает ECM-пакеты для определения номера канала.

5) Если соответствующий ключ канала уже находится в кэше абонентского устройства в результате регулярных запросов на обновление ключа, то он используется для расшифровки потока контента. Если требуется дополнительный ключ, выполняется защищенный запрос к CSM на получение требуемого ключа канала.

6) Канальный ключ разблокирует информацию в ECM-пакетах и позволяет расшифровать поток контента.

VOD-контент

Далее описан процесс обработки VOD-контента и его последующей доставки на абонентские устройства CAS Электра.



1) Для подготовки контента к предоставлению услуг VOD входящие медиа-файлы контента принимаются в незашифрованном виде в формате MPEG-2 SPTS. Принимаются различные форматы сжатия, включая HEVC, MPEG-2, MPEG-4 SP, MPEG-4 AVC/H.264 и H.265.

   Одновременно могут быть получены метаданные, связанные с файлом MPEG, для использования промежуточным ПО развертывания.

2) Программный компонент VPP на серверной роли VEM шифрует информацию в формате MPEG в файл, защищенный CAS Электра.

   В этой же итерации генерируется ключ шифрования для данного фрагмента содержимого.

3) С помощью назначенного идентификатора содержимого и ключа шифрования исходный файл шифруется с использованием интеллектуального алгоритма шифрования. Этот интеллектуальный подход сохраняет достаточную информацию о ключевых кадрах (I-frame) для индексирования зашифрованного файла с целью поддержки "trick play".

   ECM-пакеты вставляются в файл транспортного потока через равные промежутки времени. Эти пакеты идентифицируют файл содержимого и предоставляют дополнительные правила расшифровки содержимого, используемые в процессе отображения видеоматериалла на абонентском устройстве.

   После того как исходный файл будет полностью обработан VPP, он удаляется, а зашифрованный файл перемещается на сервер развертывания VOD. В это же время отдельный процесс добавляет описание содержимого в базу данных SMS. Связь между идентификатором контента и связанным с ним ключом шифрования сохраняется в базе данных CSM.

4) Абонент просматривает перечень VOD-контента, отображаемый на его абонентском устройстве. Когда он выбирает услугу просмотра контента, на основном узле системы выполняется запрос для предоставления прав доступа к просмотру, включая формирование платежной транзакции при необходимости. При успешном выполнении запроса (успешная покупка прав на просмотр), в базе данных CAS формируется соответсвующая запись.

5) Клиентское устройство запрашивает VOD поток с CDN платформы.

6) Как только поток зашифрованного контента поступает на абонентское устройство, происходит обнаружение встроенного идентификатора контента, который используется для создания защищенного соединения с базой ключей CSM.

   Эта операция запрашивает необходимые ключи для данного конкретного файла контента, и эти ключи передаются обратно абонентскому устройству, если внутрення проверка показывает, что данному абонентскому устройству были предоставлены соответствующие права.

7) При успешном получении ключа контента абонентское устройство расшифровывает поток контента с использованием ключа, после чего представляет видеоданные декодеру MPEG.