IMAQLIQ

IMAQrypt

ОПИСАНИЕ

Содержание

Введение 3

Термины и сокращения 3

1. Общие сведения 4

1.1. Назначение ПК IMAQrypt 4

1.2. Стандарты 4

1.3. Общая схема функционирования ПК IMAQrypt в составе услуги IPTV 5

1.4. Состав ПК IMAQrypt 6

1.5. Внешние системы, с которыми взаимодействует ПК IMAQrypt 6

2. Описание принципов работы ПК IMAQrypt 7

2.1. Принципы ограничения доступа к потокам IPTV 7

2.2. Механизм формирования защищенных потоков 7

2.3. Механизм получения доступа к защищенным потокам 7

3. Ключевые особенности ПК IMAQrypt 8

4. Требования к эксплуатации 9

4.1. Требования к аппаратной платформе 9

4.2. Требования к операционной системе 9

4.3. Требования к обслуживанию ПК IMAQrypt 9

4.4. Требования к квалификации персонала 9

4.5. Требования к резервированию 10

Введение

Данный документ описывает структуру, основные модули системы условного доступа IMAQrypt и взаимосвязь между ними. Предназначен для технических специалистов операторов связи, предоставляющих услуги IPTV, OTT и VoD с помощью комплексных программных решений компании Имаклик Сервис.

Термины и сокращения

IPTV	Технология цифрового телевидения в сетях передачи данных по протоколу IP
OTT	Медиа-сервис, передаваемый через сеть Internet
VoD	Видео по запросу
STB	Абонентское устройство
MPEG-TS, TS	Транспортный поток IPTV
Middleware	Программное обеспечение оператора, описывающее услугу IPTV и доступ к ней абонента
ЦПУ	Центральное процессорное устройство
ПК	Программный комплекс
ПО	Программное обеспечение
Сеть ПД	Сеть передачи данных

1. Общие сведения

1.1. Назначение ПК IMAQrypt

Программный комплекс IMAQrypt является системой условного доступа, и предназначен для установки на сетях пакетной передачи данных с целью регулирования доступа абонентов к услуге IPTV, предоставляемой оператором связи.

1.2. Стандарты

ГОСТ Р 56948-2016 Телевидение вещательное цифровое. Алгоритмы скремблирования контента служб DVB-IPTV, использующих транспортные потоки MPEG2.

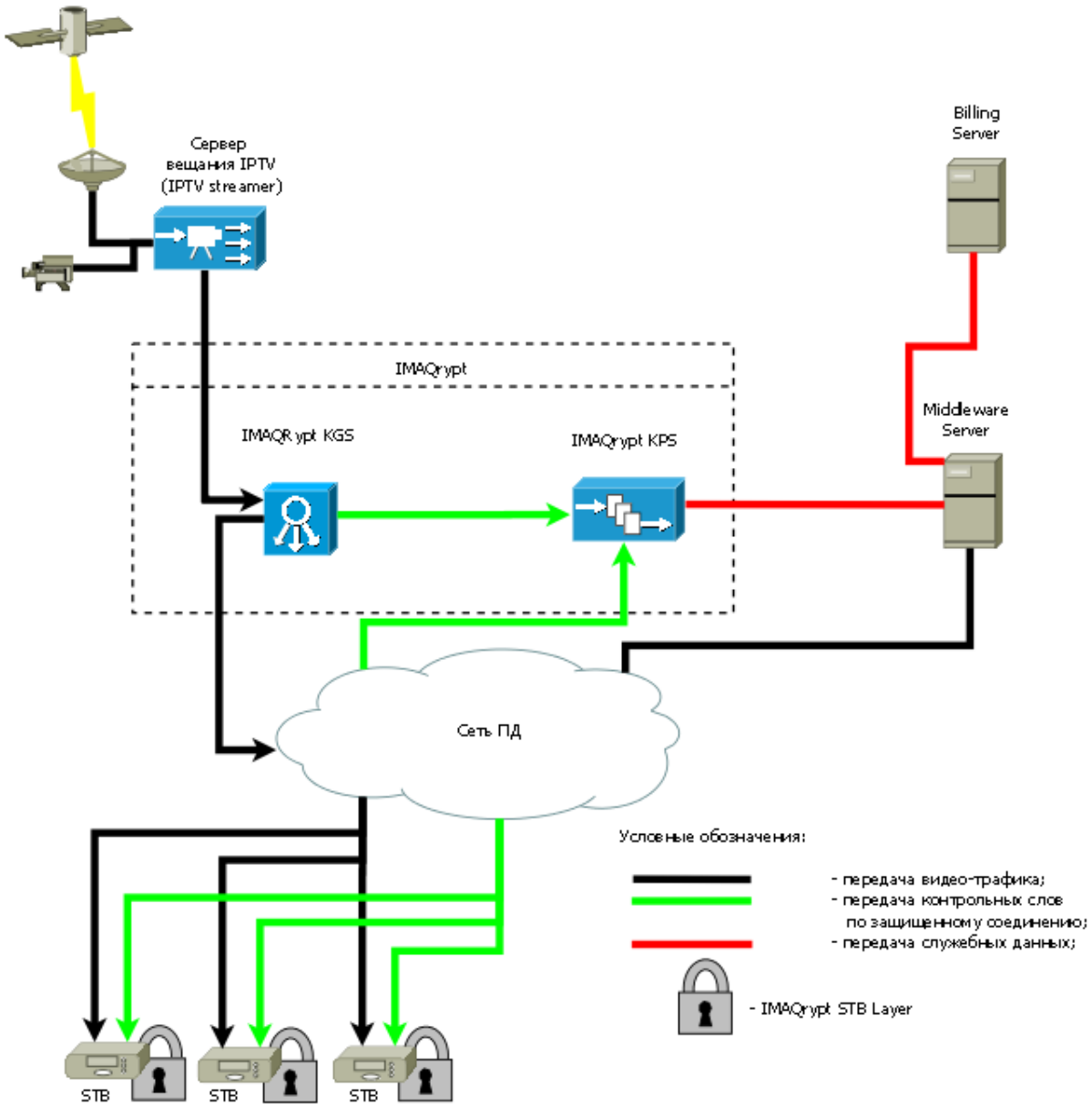
ETSI TS 103 127 V1.1.1 (2013-05) Digital Video Broadcasting (DVB); Content Scrambling Algorithms for DVB-IPTV Services using MPEG2 Transport Streams

RFC 768 User Datagram Protocol

RFC 793 TRANSMISSION CONTROL PROTOCOL

RFC 791 INTERNET PROTOCOL

1.3. Общая схема функционирования ПК IMAQrypt в составе услуги IPTV



1.4. Состав ПК IMAQrypt

IMAQrypt KGS – сервис, отвечающий за генерирование контрольных слов и организацию скремблирования. Принимает транспортные потоки медиа-данных от сервера вещания и передает их в скремблированном виде, пригодном для передачи по сетям ПД или Интернет.

IMAQypt KPS - сервис контрольных слов. Принимает решение о передаче главных контрольных слов пользовательскому оборудованию (STB) на основании данных, полученных от серверов Middleware или сервера биллинга.

IMAQrypt STB Layer - набор программных компонент, поставляемый вендору STB в виде исполняемой библиотеки, и позволяющий дескремблировать медиа-контент.

1.5. Внешние системы, с которыми взаимодействует ПК IMAQrypt

Billing server — сервер, обеспечивающий учет предоставленных телекоммуникационных услуг, их тарификацию, выставление счетов абонентам и обработку платежей.

Middleware server — сервер с установленным ПО Imaqliq Middleware или др., обеспечивающий преобразование и взаимодействие между интерфейсом пользовательского оборудования и оборудованием оператора связи по сети передачи данных оператора.

STB (set-top-box) — пользовательское устройство, обеспечивающее доступ потребителя услуг IPTV к медиа-контенту оператора связи.

IPTV Streamer - сервер, организующий вещание транспортных потоков IPTV в сеть IP.

2. Описание принципов работы ПК IMAQrypt

2.1. Принципы ограничения доступа к потокам IPTV

В ПК IMAQrypt разграничение доступа к услуге IPTV достигается за счет того, что для дескремблирования транспортного потока IPTV пользователю необходимо получать главные контрольные слова, без которых дескремблирование невозможно. Система условного доступа выдает главные контрольные слова только разрешенным пользователям и только на разрешенные потоки медиа-данных. Главное контрольное слово является индивидуальным для каждого потока и сменяется с настраиваемой периодичностью.

2.2. Механизм формирования защищенных потоков

IMAQrypt KGS захватывает данные (payload) из транспортного потока TS из сети IP, генерирует главные (Master-Key) и потоковые (In-Stream Key) контрольные слова, вычисляет результирующие контрольные слова, которые будут использоваться при скремблировании потока. Для скремблирования данных может использоваться любой внешний модуль (библиотека), поддерживающий общий программно-ориентированный алгоритм скремблирования IPTV (CISSA) версии 1 (ГОСТ Р 56948-2016) с использованием скремблирования на уровне TS. Скремблированные данные формируются в транспортный поток TS и транслируются в сеть, главные контрольные слова передаются модулю IMAQypt KPS.

Каждый экземпляр IMAQrypt KGS отвечает только за один поток медиа-данных, что позволяет оптимизировать распределение серверных ресурсов. При запуске экземпляра IMAQrypt KGS начинается приём потока медиа-данных и сразу же генерируются первичные контрольные слова.

2.3. Механизм получения доступа к защищенным потокам

Воспроизведение потокового видео-контента осуществляется пользовательским оборудованием STB, предоставленным ему оператором связи. STB, при старте воспроизведения потока, запрашивает у сервера IMAQypt KPS главные контрольные слова. Потоковые контрольные слова передаются непосредственно в медиа-контейнерах вместе с потоком медиа-данных. По заранее известному алгоритму из пары контрольных слов STB вычисляет результирующие контрольные слова. Полученные контрольные слова передаются на ЦПУ STB для дальнейшего дескремблирования потока стандартными средствами STB. Для того чтобы STB получил возможность работать с ПК IMAQrypt, необходима интеграция ПО STB с использованием специализированной библиотеки IMAQrypt STB Layer и наличие на

STB штатных аппаратных средств дескремблирования в соответствии со стандартом ГОСТ Р 56948-2016.

3. Ключевые особенности ПК IMAQrypt

- Масштабируемое решение - IMAQrypt позволяет наращивать производительность системы методом добавления серверных мощностей без перерыва предоставления услуг и остановки ключевых компонент.

- Высокая производительность - 1 типовой сервер начального уровня способен обрабатывать сотни каналов IPTV в режиме реального времени.

- IMAQrypt является современным решением, позволяющим безопасно передавать видео в любом качестве.

- Универсальность — ПК IMAQrypt одинаково хорошо подходит для предоставления услуг IPTV, VoD и OTT.

- Высокая защищенность — результирующие контрольные слова вычисляются из пары контрольных слов, которые передаются по разным соединениям.

- Взломостойкость — периодическая смена контрольных слов делает бессмысленным взлом ключей методом подбора. Частота смены ключей может настраиваться по желанию.

- Гибкость - для старта услуги достаточно 1-го сервера для развёртывания всей необходимой инфраструктуры ПК IMAQrypt.

- Все протоколы реализованы в строгом соответствии с принятыми стандартами.

- ПК IMAQrypt может быть интегрирован с любым устройством STB, установленном на сети оператора.

4. Требования к эксплуатации

4.1. Требования к аппаратной платформе

ПК IMAQrypt может работать на любом аппаратном обеспечении с архитектурой x86. По требованию возможно применение на платформах с иной архитектурой, например, PPC, ARM и т. п.

4.1.1. Пример конфигурации сервера IMAQrypt KGS, рассчитанного на обработку 100 транспортных потоков в разрешении SD:

- процессор Intel(R) Xeon(R) CPU L5630 (4 ядра);
- оперативная память 4ГБ;
- жесткий диск 200ГБ;
- два сетевых интерфейса Ethernet 1000BASE-T.

4.1.2. Пример конфигурации сервера IMAQrypt KPS, рассчитанного на обработку запросов от 100000 абонентских устройств:

- два процессора Intel(R) Xeon(R) CPU L5630 (4 ядра);
- оперативная память 16ГБ;
- жесткий диск 200ГБ;
- четыре сетевых интерфейса Ethernet 1000BASE-T.

4.2. Требования к операционной системе

ПК IMAQrypt может работать под управлением любой версии GNU/Linux.

4.3. Требования к обслуживанию ПК IMAQrypt

ПК IMAQrypt рассчитан на круглосуточный непрерывный режим работы без необходимости каких-либо регулярных воздействий. Данные, необходимые для функционирования системы, содержатся в конфигурационных файлах и оперативной памяти серверов. Требуется начальная конфигурация системы, мониторинг процессов, резервирование данных. Для получения более подробной информации см. “Руководство по эксплуатации”.

4.4. Требования к квалификации персонала

Для разворачивания и администрирования ПК IMAQrypt требуется инженерный персонал, обладающий следующими знаниями и квалификацией: сетевые протоколы TCP/IP, Ethernet; технология IPTV; администрирование ОС семейства Unix.

4.5. Требования к резервированию

Требуется холодное резервирование конфигурационных файлов при каждом изменении конфигурации системы.