GS LABS

DRECRYPT

Общее описание

Содержание

Аннотация

Данный документ содержит общее описание комплекса DRECRYPT. Документ предназначен для широкого круга специалистов как технического, так и гуманитарного профиля, которым необходимо составить общее представление о комплексе DRE Crypt, ознакомиться с основным функционалом и структурой.

За информацией, касающейся технических подробностей работы комплекса и его компонентов, следует обращаться к "DRECRYPT. Техническое описание".

Термины и сокращения

Термин	Определение
Абонент	Физическое или юридическое лицо, с которым оператор ТВ заключает договор на оказание услуг.
Антишаринг	Подход, используемый в разработке технологий по противодействию кардшарингу.
Биллинговая система	Сторонний по отношению к DRE Crypt компонент, отвечающий за сбор информации об использовании услуг, выставление счетов абонентам, обработку платежей. На основании этой информации биллинговая система выдает SMS команды на добавление, удаление или изменение подписок, или иных данных, хранящихся в SMS.
Головное оборудование	Оборудование головной станции оператора ТВ, используемое для мультиплексирования, скремблирования и модуляции сигнала. Как правило, имеется в виду та его часть, которая непосредственно взаимодействует с системой условного доступа.
Кардшаринг	Способ нелегального доступа к каналам, закрытым системой условного доступа, при котором распространяются ключи (CW), полученные от одной авторизованной смарт-карты.
Класс	Единица контента, доступ к которой контролируется системой условного доступа. В данном документе под классом понимается пакет телеканалов, на который абонент может приобрести подписку.
Контрольное слово	Ключ, используемый для скремблирования/дескремблирования транспортного потока алгоритмом CSA.
Криптопериод	Период времени, в течение которого скремблером используется один и тот же ключ скремблирования (CW).
Мастер-ключ	Ключ, необходимый для декодирования CW_enc_keys, получаемых из EMM сообщений. Мастер-ключ относится к самому верхнему уровню иерархии ключей и хранится в самой защищённой области энергонезависимой памяти смарт-карты. Этот ключ получается легальным пользователем вместе со смарт-картой и никогда не меняется.
Подписка	Информация о правах доступа абонента к классам и услугам оператора ТВ (идентификатор класса, идентификатор пакета услуг и период, на который они предоставлены).
Оператор ТВ	Организация, предоставляющая услуги просмотра цифрового телевидения и использования дополнительных сервисов.
Система условного доступа	Система, которая обеспечивает защиту контента, передаваемого по каналам вещания и распределения, от коммерческого пиратства. Защита осуществляется путем кодирования транспортного потока перед его передачей в канал вещания. Ключи, необходимые для расшифровки транспортного потока, передаются в этом же транспортном потоке в составе ECM и EMM сообщений только тем абонентам, которые оплатили услуги оператора ТВ. Получив ключи, приемник абонента расшифровывает поступающий транспортный поток.

Скремблер	Устройство шифрования транспортного потока, входящее в состав головного оборудования. В терминологии стандарта DVB-Simulcrypt обозначает функциональный логический блок, ответственный за шифрование MPEG2 транспортного потока. Для выполнения данной функции должен обеспечивать прием CW от компонента SCS.
Access criteria	Данные системы условного доступа, необходимые ECMG для формирования ECM сообщений. Состав и структура этих данных определяется разработчиком системы условного доступа.
CW_enc_key	Ключ, используемый для шифрования и расшифровывания контрольных слов (CW). Данные ключи передаются в зашифрованном виде в составе EMM сообщений.
ECM	Сообщение, которое передается ресиверу абонента и содержит в зашифрованном виде CW, дескремблирующие транслируемый поток.
EMM	Сообщение, которое передается ресиверу абонента и содержит CW_enc_key/служебные данные/информацию о правах доступа/специальные команды. Разные типы EMM передают разную информацию.
Simulcrypt синхронизатор	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.
STB	Устройство абонента, принимающее и обрабатывающее сигнал цифрового телевидения и передающее его далее для воспроизведения (например, на телевизоре или планшете). STB состоит из программного (STB library) и аппаратного обеспечения.

Сокращение	Расшифровка
AC	Access criteria, критерий доступа
CSA	Common Scrambling Algorithm, общий алгоритм скремблирования
CW	Control word, контрольное слово
ECM	Entitlement Control Message, ECM-сообщение
EMM	Entitlement Management Message, EMM-сообщение
CAS	Conditional access system, система условного доступа
MK	Master key, мастер-ключ
MOD	Modulator, модулятор
MQS	Messages Queuing System, система обмена сообщениями
MUX	Multiplexer, Мультиплексор
OPKEY	Operational Key, операционный ключ
SCR	Scrambler, скремблер

SCS	Simulcrypt Synchronizer, Simulcrypt синхронизатор
SMS	Subscriber Management System, система управления подписками
STB	Set Top Box, приемник цифрового телевидения
ИС оператора	Информационные системы Оператора
СУД	Система условного доступа

1. Введение

1.1. Назначение DRECRYPT

DRECRYPT представляет собой программный комплекс, являющийся частью системы условного доступа (СУД).

В рамках СУД комплекс DRECRYPT отвечает за организацию сборки ECM и EMM сообщений, передаваемых абоненту и необходимых для расшифровки защищенного транспортного потока. Таким образом, DRE Crypt совместно с головным оборудованием позволяет оператору ТВ управлять доступом абонентов к своим сервисам для реализации услуг платного телевидения.

Комплекс DRE Crypt разработан в соответствии со стандартами DVB-Simulcrypt (см. Поддерживаемые стандарты), что делает его совместимым с большинством представленных на рынке моделей головного оборудования, а также допускает одновременное использование оператором ТВ нескольких экземпляров DRE Crypt на одной головной станции.

1.2. Область применения

DRE Crypt может использоваться в следующих системах цифрового телевидения:

- спутниковое цифровое ТВ (DVB-S/DVB-S2);
- эфирное ТВ (DVB-T/DVB-T2);
- кабельное ТВ (DVB-C/DVB-C2).

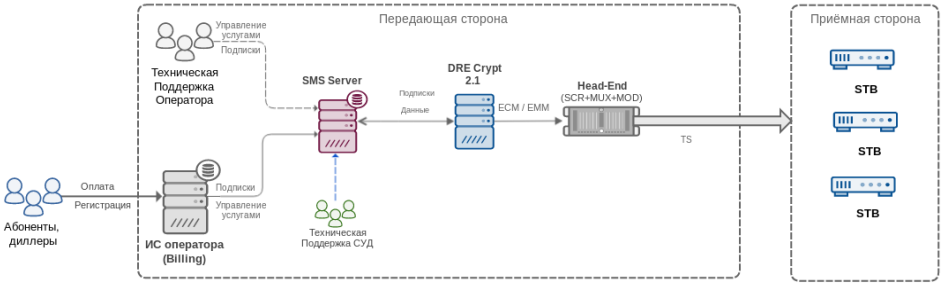
1.3. Поддерживаемые стандарты

ⓘ Следует учитывать, что здесь приведены основные стандарты, которым соответствует комплекс DRE Crypt. Каждый из них ссылается на несколько других.

1. ГОСТ Р 53527-2009. Телевидение вещательное цифровое. Требования к реализации системы ограничения доступа DVB Simulcrypt на головных станциях. Основные параметры. Технические требования
2. ГОСТ Р 53531-2009. Телевидение вещательное цифровое. Требования к защите информации от несанкционированного доступа в сетях кабельного и наземного телевизионного вещания. Основные параметры. Технические требования
3. ETSI TS 101 197 V1.2.1 DVB SimulCrypt; Part 1: Head-end architecture and synchronization
4. ETSI TS 103 197 V1.5.1 Head-end Implementation of SimulCrypt
5. ETSI TR 102 035 V1.1.1 Implementation Guidelines of the DVB Simulcrypt Standard
6. ETSI ETR 289: "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems
7. ISO/IEC 13818-1 (2000): "Information technology - Generic coding of moving pictures and associated audio information: Systems".
8. ETSI EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems".
9. ETSI ETR 162: "Digital Video Broadcasting (DVB); Allocation of Service Information (SI) codes for DVB systems"
10. ETSI ETR 289: "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems"
11. IETF RFC 791 (1981): "Internet Protocol".
12. IETF RFC 793 (1981): "Transmission Control Protocol"

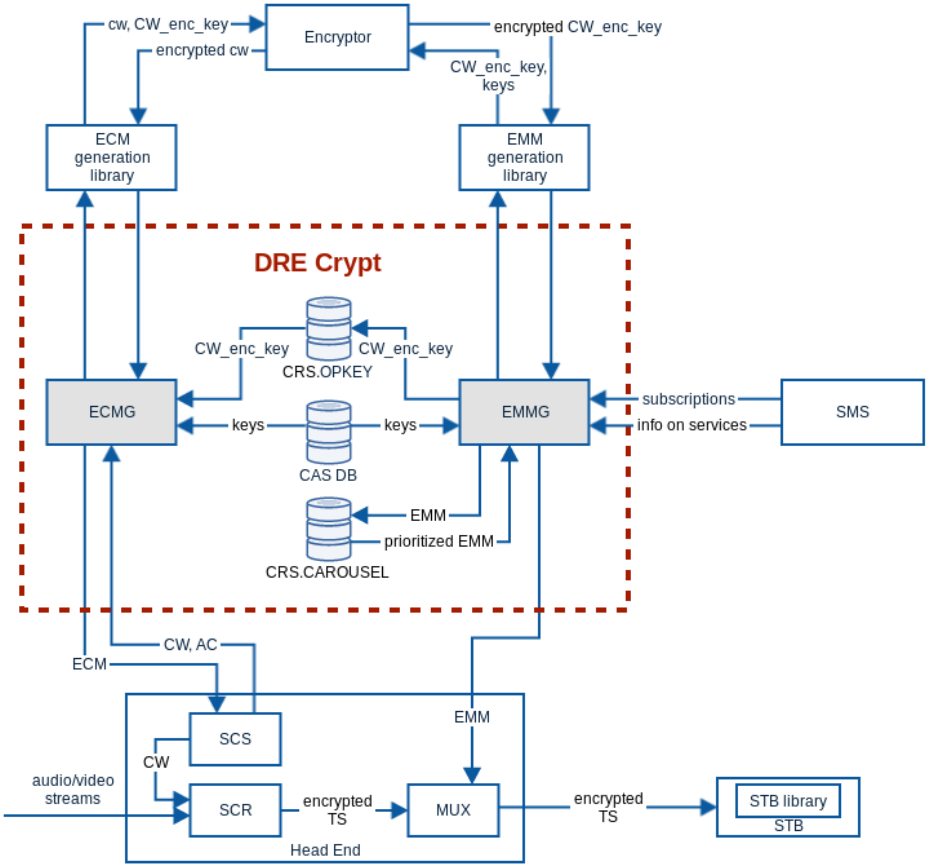
1.4. Схема работы

Общая схема работы DRECRYPT приведена на рисунке ниже.



2. Описание DRECRYPT

2.1. Структура DRECRYPT



2.2. Основные компоненты DRECRYPT

Основными компонентами DRECRYPTявляются:

- Entitlement Control Message Generator (ECMG) - компонент, управляющий генерацией ECM сообщений (ECM содержат в зашифрованном виде CW, расшифровывающие транспортный поток). ECMG принимает от SCS информацию, необходимую для генерации ECM, и, распределяя нагрузку оптимальным образом, вызывает функции ECM generation library. Получив собранное ECM, ECMG передает его SCS.
- Entitlement Management Message Generator (EMMG) - компонент, управляющий генерацией EMM сообщений (EMM содержат CW_enc_keys, необходимые для расшифровки CW). В соответствии с заданным расписанием EMMG опрашивает SMS и, распределяя нагрузку оптимальным образом, вызывает функции EMM generation library. Получив собранное EMM, EMMG помещает его в CRS. CAROUSEL для организации цикличной рассылки в соответствии с заданным приоритетом. Также EMMG генерирует CW_enc_keys в соответствии с заданным расписанием.
- CRS.OPKEY - схема БД CRS под управлением Postgres Pro, которая хранит CW_enc_keys, используемые для шифрования CW, а также настройки расписания и задач DRECRYPT.

- CAS DB - БД под управлением Postgres Pro, которая хранит ключи, используемые для дополнительного шифрования ECM и EMM. Конечная структура данной базы зависит от реализации библиотек по сборке ECM/EMM, поскольку именно данные библиотеки используют ключи из CAS DB.
- CRS.CAROUSEL - схема БД CRS под управлением Postgres Pro, используемая для организации цикличной рассылки EMM в соответствии с их приоритетом.

2.3. Внешние компоненты, взаимодействующие с DRECRYPT

- SMS – система управления информацией о пользователях, подписках на классы и услуги, сообщениях и др. Представляет собой БД под управлением Postgres Pro. SMS получает информацию от биллинга или от веб-интерфейса, хранит, обрабатывает и передает её в нужном формате EMMG.

  ⚠ В дополнение к Postgres Pro комплекс DRE Crypt может быть настроен для взаимодействия с SMS, работающей под управлением СУБД MSSQL и Oracle.

- ECM / EMM generation library - библиотеки по генерации ECM и EMM сообщений. Данные библиотеки осуществляют непосредственную сборку ECM/EMM необходимого формата, а также операции шифрования этих сообщений с помощью шифрующего устройства. Собранные ECM/EMM передаются ECMG/EMMG для отправки в CRS.CAROUSEL. Данные библиотеки могут быть предоставлены Заказчиком, что позволяет построить собственную логику защиты контента, а также определить дополнительные услуги, которые может предоставлять комплекс DRE Crypt (конечная реализация библиотек должна зависеть от аппаратного (STB) и программного (STB library) обеспечения, которое Заказчик планирует использовать на Приёмной стороне).
- Encryptor – система, отвечающая за шифрование информации, передаваемой в ECM и EMM. Encryptor-ом может быть любое шифрующее устройство, которое Заказчик желает использовать совместно со своими библиотеками по генерации ECM / EMM.
- Головное оборудование:
  - SCS - компонент головного оборудования, предназначенный для установления и поддержания соединения с ECMG, передачи ему CW и AC, получения сгенерированных ECM сообщений и перенаправления их в MUX;
  - SCR - компонент головного оборудования, предназначенный для шифрования потока с помощью CW;
  - MUX - компонент головного оборудования, формирующий единый транспортный поток из всех входных данных.
- STB library - библиотека приёмника, которая обрабатывает поступающие ECM и EMM.

3. Требования и ограничения

3.1. Системные требования

Для установки DRE Crypt желательно выделить отдельный сервер. Рекомендуется устанавливать сервер в локальной сети, защищенной от доступа извне.

3.1.1. Аппаратное обеспечение

- Процессор — 2 или 4 ядра;
- Оперативная память — 2 GB (рекомендуется 4 GB);
- Жесткий диск — 2 × 150 GB (зависит от объема БД);
- Головное оборудование, соответствующее стандарту DVB-Simulcrypt ver. 2.

3.1.2. Программное обеспечение

- ОС Debian 8 x64

3.2. Требования к квалификации обслуживающего персонала

Для настройки и администрирования DRE Crypt персонал должен удовлетворять следующим требованиям:

- обладать теоретическими знаниями и практическим опытом работы с СУБД Postgres Pro;
- иметь навыки работы и администрирования ОС Debian: создание разделов дисков, установка пакетов, создание и настройка сетевых подключений, запуск служб, настройка автозапуска служб, установка и настройка Postgres Pro, настройка работы с БД под управлением Postgres Pro;
- иметь общие понятия о функционировании спутникового и цифрового кабельного телевидения;
- знать структуру и принципы работы СУД и головного оборудования в соответствии со стандартами семейства DVB.

3.3. Ограничения

3.3.1. Аппаратные ограничения

В соответствии со стандартом DVB-Simulcrypt, DRECRYPT взаимодействует с головным оборудованием по протоколу TCP. Соответственно, серверы, на которых установлены компоненты СУД, должны иметь 10Base-T или полностью совместимый сетевой адаптер.

3.3.2. Ограничения по безопасности

Для обеспечения безопасности важных данных, все компоненты DRE Crypt рекомендуется устанавливать в одной локальной сети, защищенной от доступа извне.

Если выполнение данного требования невозможно ввиду географической удаленности компонентов друг от друга, рекомендуется использовать VPN соединения, туннелирование, защищенные протоколы связи.

4. Основные характеристики DRECRYPT

Параметр	Значение
Основные параметры	
Назначение	Для систем вещания
Алгоритм скремблирования	DVB Common Scrambling Algorithm
Регистрация в DVB	Есть
Поддержка DVB Simulcrypt 2.0	Есть
Количество необходимых PID	1 EMM PID на транспортный поток (TS) 1 ECM PID на пакет
Максимальное количество скремблируемых транспортных потоков	Не ограничено
Максимальное количество сервисов, которые можно скремблировать	Предел устанавливается скремблером
Максимальное количество подписчиков (пользователей)	Предел устанавливается аппаратными возможностями приёмного оборудования и соответствующими форматами ECM и EMM.
Максимальное количество классов	Предел устанавливается аппаратными возможностями приёмного оборудования и соответствующими форматами ECM и EMM.
Количество скремблеров	2 (проверено на практике), больше (вплоть до 32) - опционально (зависит от производительности аппаратного обеспечения)
Обработка широковещательных EMM	50 - 1 000 Kbps
Безопасность	
Дополнительное шифрование потока	Есть (опционально)*
Тип дескремблирующего оборудования на стороне пользователя	встроенная в приЁмник карта доступа либо внешняя смарт-карта
Функциональность	
Резервное копирование	Есть
Тип резервирования	Холодное

*Требуется система, которая предоставляет технологию дополнительного шифрования элементарных потоков, применяемую в дополнение к стандартному алгоритму шифрования (CSA).