GS LABS
GS GROUP

Публичный - L0

Система условного доступа DRECRYPT

Общее описание

Индекс	CASDRECRYPT-GD
Конфиденциальность	Публичный - L0
Ревизия	1.0
Статус	Согласован

Содержание

1. Аннотация

Данный документ содержит общее описание "Системы условного доступа DRECRYPT" (CAS DRECRYPT) (далее по тексту – DRECRYPT или Система). Документ предназначен для широкого круга специалистов как технического, так и гуманитарного профиля, которым необходимо составить общее представление о комплексе DRECRYPT, ознакомиться с основным функционалом и структурой.

2. Термины и сокращения

Термин	Определение
Абонент	Физическое или юридическое лицо, с которым оператор ТВ заключает договор на оказание услуг.
Биллинговая система	Сторонний по отношению к DRECRYPT 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.
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.
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.
Оператор ТВ	Организация, предоставляющая услуги просмотра цифрового телевидения и использования дополнительных сервисов.
Подписка	Информация о правах доступа абонента к классам и услугам оператора ТВ (идентификатор класса, идентификатор пакета услуг и период, на который они предоставлены).
Система управления подписками	Система, принимающая, обрабатывающая и хранящая информацию о подписках абонентов и иную служебную информацию.
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.

Транспортный поток	Набор объединенных элементарных потоков, используемый для передачи и хранения аудио, видео и других данных в системах цифрового вещания. Структура транспортного потока определена в стандарте ISO/IEC 13818-1.
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.
DRECRYPT	Система условного доступа DRECRYPT (CAS DRECRYPT) - 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, DRECRYPT совместно с головным оборудованием позволяет оператору ТВ управлять доступом абонентов к своим сервисам для реализации услуг платного телевидения.
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
БД	База данных
ОС	Операционная Система
ИС оператора	Информационные системы Оператора
СУД	Система условного доступа
AC	Access criteria, критерий доступа
CAS	Conditional access system, система условного 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
MK	Master key, мастер-ключ
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
TS	Transport Stream, транспортный поток

3. Введение

3.1. 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, DRECRYPT совместно с головным оборудованием позволяет оператору ТВ управлять доступом абонентов к своим сервисам для реализации услуг платного телевидения.

Комплекс DRECRYPT 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 DRECRYPT на одной головной станции.

3.2. Область применения

DRECRYPT 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).

3.3. Поддерживаемые стандарты

ⓘ Следует учитывать, что здесь приведены основные стандарты, которым соответствует комплекс DRECRYPT. 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"

3.4. Ключевые особенности

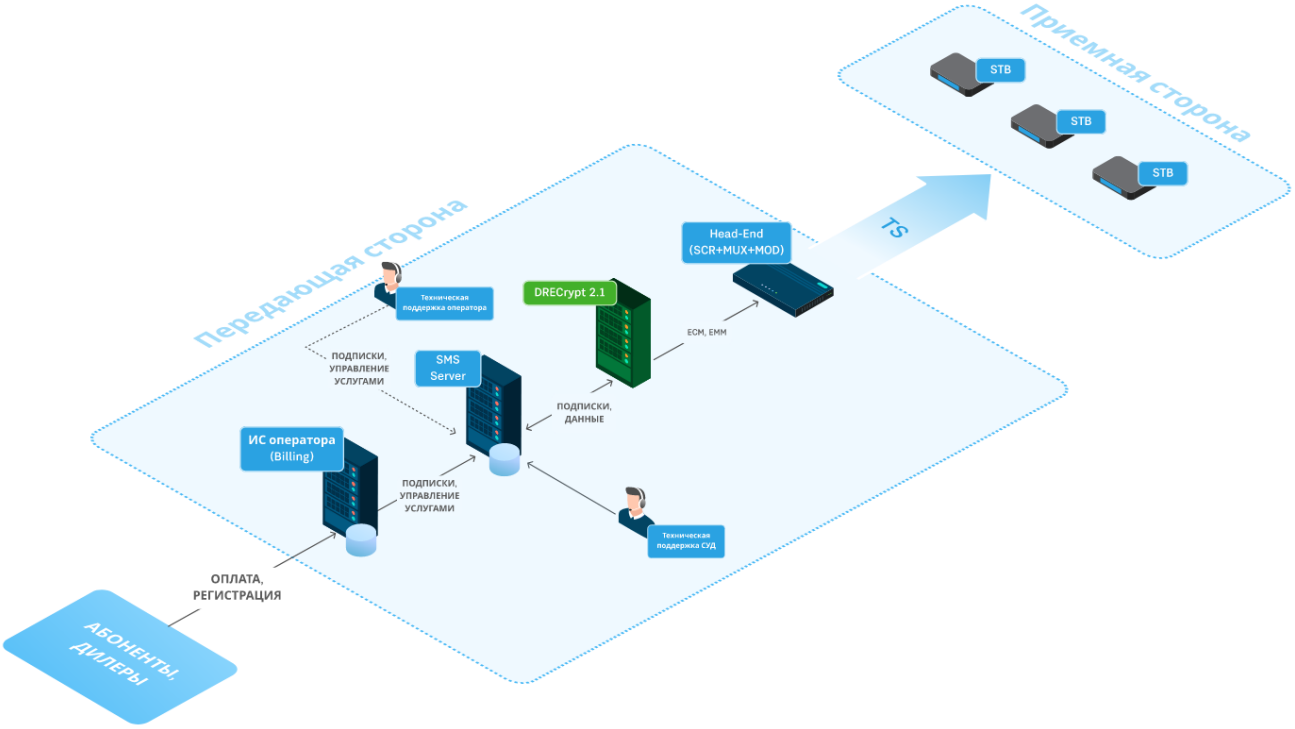
DRECRYPT обладает следующими достоинствами:

- Защита на надежном аппаратном обеспечении
  Технологии защиты контента постоянно совершенствуются, осуществляется активное сотрудничество с операторами по предупреждению, анализу и обработке актуальных проблем безопасности в сети оператора.
- Гибкость подхода к бизнес-моделям
  DRECRYPT работает как в системах крупных спутниковых операторов, так и в системах небольших кабельных операторов, с разными моделями ведения бизнеса - PayTV, PPV, VoD, Streaming и другими моделями.
- Разные модели внедрения
  DRECRYPT поддерживает разные модели внедрения (с использованием смарт-карт или без них, локальное или облачное развертывание, использование как услуги или как продукта) - можно подобрать оптимальное решение, в зависимости от потребности и технического оснащения.
- Контроль качества и аудит
  Для гарантии максимальной защищенности системы 2 раза в год проводится внешний аудит безопасности у лидера этой области – Farncombe Security Audit by Cartesian.
- Регулярное обновление
  В настоящее время используется 5 поколение систем условного доступа.
- Соблюдение сроков поставки
  Всегда в наличии готовые к отгрузке приемники и CAM модули, а так же оборудование для Системы Условного Доступа.

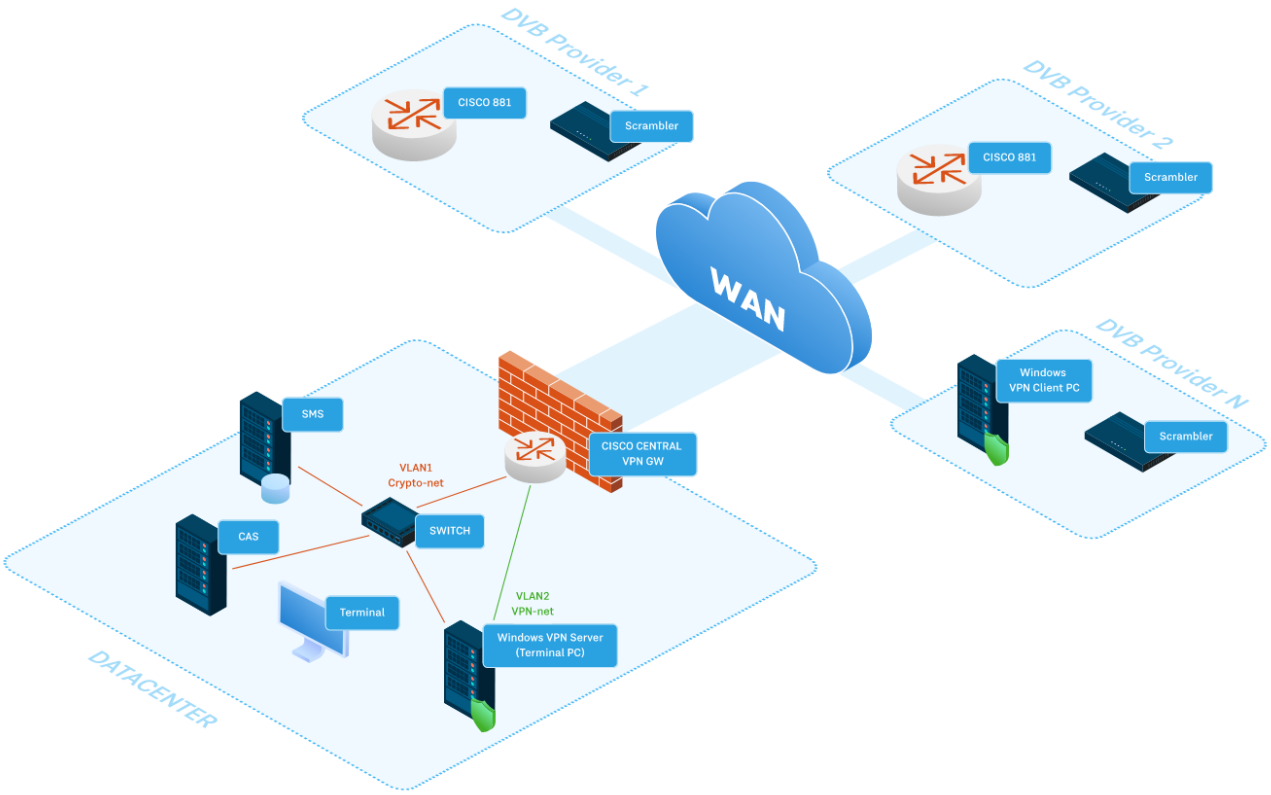
3.5. Схема работы

DRECRYPT может быть развернута локально или в облаке. Схемы работы DRECRYPT для каждого из этих решений приведены на рисунках ниже.

3.5.1. Локальное развертывание



3.5.2. Облачное развертывание



Особенности облачного решения:

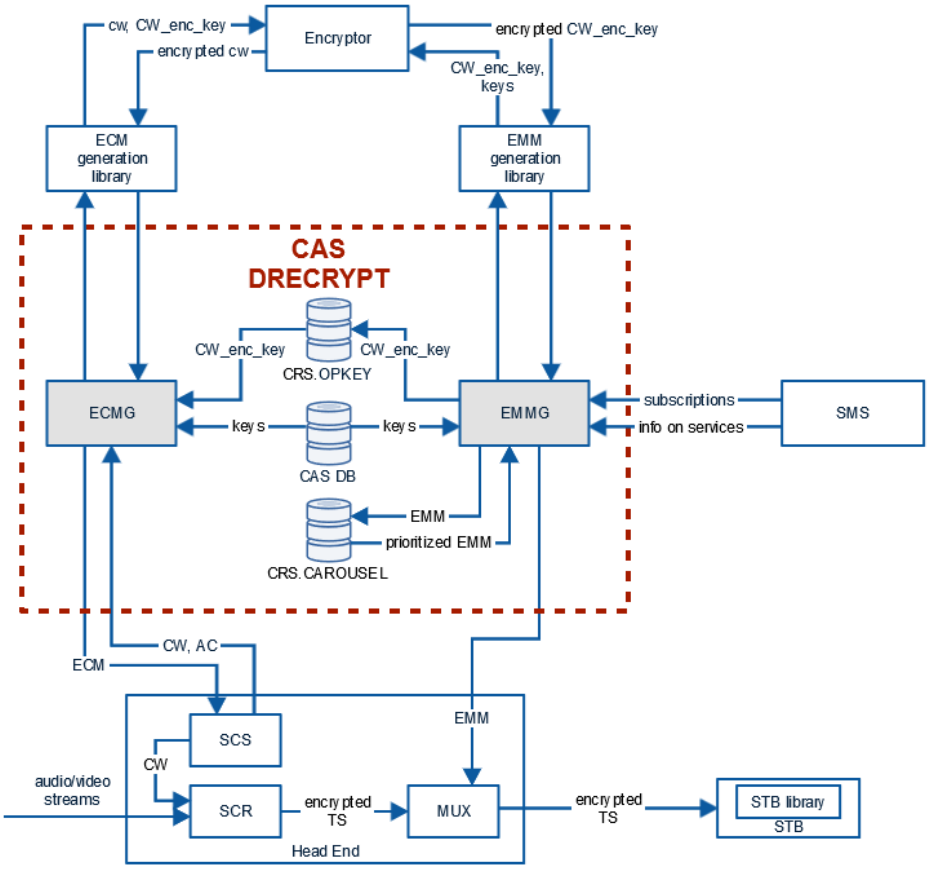
- Возможность проведения предварительного тестирования решения.

  ⚠ Для тестирования необходимо наличие на головной станции оператора скремблера с поддержкой DVB SimulCrypt.

- Преимущества и функциональность СУД аналогичны локальной версии.
- Оптимизация затрат на содержании аппаратной части СУД.

4. Описание DRECRYPT

4.1. Структура DRECRYPT



4.2. Составные части DRECRYPT

Основными компонентами DRECRYPT являются:

- 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.

4.3. Связи с другими программами

Комплекс DRECRYPT взаимодействует со следующими программами:

- 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 DRECRYPT может быть настроен для взаимодействия с SMS, работающей под управлением другой СУБД.

- 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 DRECRYPT (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.

5. Алгоритм работы DRECRYPT

5.1. Сценарии работы

- Пользователь оплатил доступ к определенному классу каналов. В этом случае:
  - Через биллинг или веб-интерфейс подписка на определенный срок добавляется в БД SMS.
  - По запросу EMMG процедура SMS формирует ответ, содержащий ID всех абонентов, у которых на момент запроса есть активные подписки, а также даты начала и окончания этих подписок. ID нашего абонента также попадает в данный ответ и будет попадать в него в течение всего времени жизни подписки.
  - Всем ID, информацию о которых получил EMMG, рассылаются EMM сообщения с CW_enc_keys, которые необходимы для расшифровки CW, передаваемых в ECM.
  - ECM рассылаются постоянно всем пользователям, но CW, содержащиеся в них, могут быть расшифрованы только теми пользователями, которые получили и расшифровали CW_enc_keys из EMM. С помощью расшифрованных CW приемник абонента может расшифровать поступающий транспортный поток и открыть каналы.
- У пользователя закончилась подписка на класс каналов. В этом случае:
  - По запросу EMMG процедура SMS формирует ответ, в котором находятся ID всех абонентов, у которых на момент запроса есть активные подписки. ID нашего абонента не попадает в данное представление, поскольку его подписка закончилась.
  - Данному абоненту не будет отослано EMM с CW_enc_keys, поэтому его приемник не сможет расшифровать CW и открыть каналы.

> ⚠ Необходимо заметить, что данная схема работы SMS и EMMG не является обязательной. В зависимости от нужд Заказчика, процедуры SMS могут возвращать разные данные. Например, одна процедура возвращает ID всех абонентов, у которых на момент запроса есть активные подписки, а другая возвращает ID всех абонентов, у которых подписки закончились. На каждый из этих ответов библиотека по сборке может генерировать разные типы EMM:
>
> - содержащее действительные CW_enc_keys (для активных подписок)
>
> - содержащее ненастоящие CW_enc_keys (для истекших подписок, такими CW_enc_keys приёмник абонента не сможет расшифровать CW и открыть каналы для просмотра)
>
> Т.е. логика работы процедур SMS и собираемые типы EMM индивидуальны для каждого Заказчика.

5.2. ECMG

Основная задача ECMG - передача CW в зашифрованном виде в составе ECM. Частота смены CW намного выше частоты смены CW_enc_keys, поэтому один и тот же CW_enc_key может использоваться для многих CW. ECMG забирает новый CW_enc_key из CRS.OPKEY и начинает использовать его для шифрования CW только после того, как EMMG скоординирует генерацию нового CW_enc_key, поместит его в CRS.OPKEY и сообщит ECMG, что новый CW_enc_key помещен в CRS.OPKEY.

Упрощенно алгоритм формирования ECM выглядит следующим образом:

1. SCS генерирует пару CW: для текущего криптопериода и для следующего.
2. SCS передает SCR сгенерированные CW.
3. SCR шифрует поступающий аудио/видео поток с помощью текущего CW. Для расшифровки потока приемнику пользователя необходимо передать данные CW. CW должны быть переданы в зашифрованном виде, чтобы нелегальный пользователь не смог получить их и расшифровать поступающий зашифрованный поток.
4. С целью шифрования SCS передает два CW (текущий и следующий) и AC компоненту ECMG.
5. ECMG получает CW_enc_key из CRS.OPKEY, после чего передает все необходимые данные (CW, AC, CW_enc_key) библиотеке по сборке ECM.
6. Используя CW_enc_key, библиотека с помощью Encryptor шифрует два CW по правилам, заданным в AC.
7. Библиотека формирует ECM, содержащее два зашифрованных CW и служебную информацию. При формировании ECM производится дополнительное шифрование его содержимого ключами из CAS DB (ключи поступают в библиотеку через ECMG).

   > ⓘ Почему в ECM отсылается сразу 2 (два) CW?
   >
   > Приемник пользователя должен расшифровывать поступающий сигнал непрерывно. После окончания текущего криптопериода головное оборудование начинает применять следующий CW. Если у приёмника нет данного CW, и он будет ждать ECM с новым CW, может произойти прерывание в расшифровке сигнала. Именно поэтому в ECM рассылается сразу 2 CW.

8. Библиотека по генерации сообщений передает сформированное ECM компоненту ECMG.
9. ECMG отправляет ECM сообщение в SCS.
   После мультиплексирования ECM отправляется пользователю. ECM рассылаются постоянно с заданным интервалом и для всех пользователей (broadcast сообщения).

5.3. EMMG

CW_enc_key, с помощью которого зашифрованы CW, также необходимо передать приемнику в зашифрованном виде. Аналогично ситуации с CW, приемнику необходимо передать текущий и следующий CW_enc_key. EMMG координирует периодическую генерацию CW_enc_keys в соответствии с заданным расписанием и помещает их в CRS.OPKEY. EMM с новыми CW_enc_keys начинают рассылаться пользователю только после того, как ECMG сообщил EMMG, что новые ключи получены из CRS.OPKEY.

Упрощенно алгоритм формирования EMM выглядит следующим образом:

1. После получения ответа от ECMG, что новые ключи получены из CRS.OPKEY, для шифрования обоих CW_enc_keys EMMG забирает ключи из CAS DB. Такие же ключи хранятся у пользователя в защищенной области памяти смарт-карты.
2. EMMG передает необходимые данные библиотеке по сборке EMM.
3. Библиотека передает два CW_enc_key и ключи Encryptor-у и получает обратно зашифрованные CW_enc_keys.
4. Библиотека формирует EMM заданного формата, содержащее зашифрованные CW_enc_keys и дополнительную служебную информацию. EMM генерируются периодически в соответствии с заданным расписанием независимо от ECM.

> Почему в EMM отсылается сразу 2 (два) CW_enc_key?
>
> Время действия CW_enc_key гораздо больше криптопериода CW. Одним и тем же CW_enc_key может быть зашифровано от нескольких сотен до нескольких тысяч сменяющихся CW. Когда время действия текущего CW_enc_key заканчивается, EMMG начинает использовать следующий, заранее сгенерированный CW_enc_key, для шифрования CW. На принимающей стороне уже должен быть данный CW_enc_key. В противном случае невозможно расшифровать CW, а без CW – транспортный поток. Поэтому в EMM передается два CW_enc_key.

При формировании EMM производится дополнительное шифрование его содержимого ключами из CAS DB.

5. Библиотека по генерации сообщений передает сформированные EMM компоненту EMMG.
6. EMMG помещает сгенерированные EMM сообщения в CRS.CAROUSEL.
7. CRS.CAROUSEL формирует единую очередь EMM в соответствии с их приоритетом.
8. EMMG забирает отсортированные EMM из CRS.CAROUSEL и передает их в MUX.

5.4. Обработка потока на приемной стороне

> Чтобы дескремблировать транспортные потоки (открыть ТВ каналы) на стороне абонента, в общем случае необходимо:
>
> - получить и обработать ECM (содержит CW);
> - получить и обработать EMM (содержит все ключи, необходимые для расшифровки CW);
> - расшифровать CW и передать их в дескремблер.

Приемник абонента производит обработку ECM и EMM, полученных через TS (Transport Stream), в следующем порядке:

1. Из полученного EMM два CW_enc_keys передаются смарт-карте.
2. Смарт-карта расшифровывает CW_enc_keys с помощью хранящихся в её памяти ключей.
3. Смарт-карта сохраняет расшифрованные CW_enc_keys в собственной памяти.
4. Из полученного ECM два CW передаются смарт-карте.
5. Смарт-карта расшифровывает CW с помощью текущего CW_enc_key.
6. CW передаются дескремблеру и используются для расшифровки потоков.

6. Требования и ограничения

6.1. Системные требования

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

6.1.1. 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.

6.1.2. Программное обеспечение

- ОС Debian 8 x64

6.2. Требования к квалификации обслуживающего персонала

Для настройки и администрирования DRECRYPT 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.

6.3. Ограничения

6.3.1. 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.

6.3.2. Ограничения по безопасности

Для обеспечения безопасности важных данных, все компоненты DRECRYPT 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.

7. 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).