GS LABS
GS GROUP

Публичный - L0

Программный комплекс «Система условного доступа DREGUARD»

Общее описание

Индекс	CAS-DREGUARD-GD
Конфиденциальность	Публичный - L0
Ревизия	1.1
Статус	Согласован

Содержание

1. Аннотация

Данный документ содержит общее описание Программного комплекса "Система условного доступа DREGUARD" (далее - CAS DREGUARD или Система). Основной акцент сделан на высокоуровневом описании структуры системы и её функционала. Документ предназначен для широкого круга специалистов как технического, так и гуманитарного профиля, а также для руководящего состава, которым необходимо составить общее представление о CAS DREGUARD, ознакомиться с основным функционалом и структурой.

За информацией, касающейся технических подробностей работы системы и её компонентов, следует обращаться к документам "Техническое описание" для соответствующих компонентов.

Данное описание является публичным документом.

2. Термины и сокращения

Термин	Сокращение	Определение
Абонент	-	Физическое или юридическое лицо, с которым оператор ТВ заключает договор на оказание услуг.
Авторизация	-	Процесс предоставления абоненту прав на использование услуг телевизионного оператора (просмотр телевизионных каналов и услуги интерактивных телевизионных сервисов).
Антишаринг	-	Подход, используемый в разработке технологий по противодействию нелегальному доступу к каналам, закрытым CAS DREGUARD, при котором распространяются ключи (CW), полученные от одной авторизованной смарт-карты.
Биллинговая система (Business Support System)	BSS	Сторонний по отношению к CAS DREGUARD компонент, отвечающий за сбор информации об использовании услуг, выставление счетов абонентам, обработку платежей. На основании этой информации биллинговая система выдает CAS DREGUARD команды на добавление, удаление или изменение подписок, сообщений Инфокас, или иных данных, хранящихся в CAS DREGUARD.
Головное оборудование	-	Оборудование головной станции оператора. В данном документе под головным оборудованием подразумевается та его часть, которая непосредственно взаимодействует с Системой Условного Доступа согласно стандарту DVB-SimulCrypt.
Класс	-	Единица доступа в CAS DREGUARD. С точки зрения пользователя CAS DREGUARD (оператора ТВ), класс определяет пакет телевизионных каналов, предоставляемых абоненту в качестве единой услуги. На базе управления правами на класс реализовано управление доступом абонента к пакету каналов. При оформлении подписки на класс, абоненту предоставляется доступ ко всем телевизионным каналам, входящим в его состав.
Контрольное слово (Control word)	CW	Ключи, используемые для скремблирования/дескремблирования транспортного потока алгоритмом CSA.
ПАК "Криптокипер" (Криптокипер, Cryptokeeper)	СК	Специализированное шифрующее устройство.
Криптопериод		Период времени, в течение которого скремблером используется один и тот же ключ скремблирования (CW).

Мастер-ключ	MK	Ключ, необходимый для декодирования операционных ключей, 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 (TV Provider)	-	Организация, предоставляющая услуги просмотра цифрового телевидения и использования дополнительных сервисов.
Операционный ключ	OPKEY	Ключ, используемый для шифрования и расшифровывания управляющих слов (CW). Операционные ключи передаются в зашифрованном виде в составе специальных команд в EMM сообщениях.
Пакет услуг	-	Данный термин используется в рамках функционала WHN. Совокупность прав на использование услуг оператора ТВ, предоставляемая абоненту при заключении договора. Подписка на пакет услуг определяет доступные для абонента типы услуг (Streaming, PVR и прочее), классы подключаемых устройств (например, планшеты GS), максимальное количество одновременно подключаемых устройств. Пакет услуг может иметь привязку к одному или нескольким каналам.
Подписка	-	Информация о правах доступа абонента к классам и услугам оператора ТВ (идентификатор класса, идентификатор пакета услуг и период, на который они предоставлены).
Приёмник (Set Top Box)	STB	Устройство абонента, принимающее и обрабатывающее сигнал цифрового телевидения и передающее его далее для воспроизведения (например, на телевизоре или планшете).
Оператор ТВ	-	Организация, предоставляющая услуги просмотра цифрового телевидения и использования дополнительных сервисов.
Система управления подписками (Subscriber Management System)	SMS	Система, принимающая, обрабатывающая и хранящая информацию о подписках абонентов.
Скремблер	SCR	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.
Смарт-карта	-	Версия внешней смарт-карты, реализованная на аппаратной платформе. Используется в CAS DREGUARD для идентификации пользователей, безопасного хранения приватных данных и защиты криптографических операций, необходимых для управления доступом.

Стриминг (Streaming)	-	Функция приёмника, позволяющая передавать контент с приёмника-сервера на устройство-клиент (приёмник, планшет). Различают следующие виды Streaming: • Mirror Streaming: на мобильное устройство транслируется контент, воспроизводимый на сервере; • Independent Streaming: на мобильное устройство транслируется контент по запросу клиента, независимо от контента, воспроизводимого на сервере.
Услуга	-	Дополнительная платная функциональность приёмного оборудования, доступ к которой ограничивается оператором цифрового телевидения в соответствии с разработанными им правилами использования данной функциональности (например, использование Streaming и т.д.).
Access criteria (Критерий доступа)	AC	Данные системы условного доступа, необходимые ECMG для формирования ECM сообщений. Состав и структура этих данных определяется разработчиком CAS DREGUARD и является закрытой информацией
Conditional access system (Система условного доступа)	CAS	Система условного доступа обеспечивает защиту контента, передаваемого по каналам вещания и распределения, от коммерческого пиратства.
CAS DREGUARD Library (далее по тексту - Library)	-	Система, представляющая собой промежуточное ПО, которое обеспечивает взаимодействие ПО приемника и эмулятора смарт-карты. Library управляет выделением служебных данных (например, ECM и EMM) из принятого транспортного потока, получением из них зашифрованных ключей и их передачу эмулятору смарт-карты для расшифровки.
DRE Account Manager (далее по тексту - Account Manager)	ACM	Сервис авторизации и распределения прав. CAS DREGUARD может обратиться к Account Manager (через свой фронтенд или API) для авторизации, передачи и проверки прав пользователя. Затем, при помощи WEB UI, пользователь CAS DREGUARD может создавать дополнительные учетные записи, назначать роли и создавать группы прав.
DRE Advanced Encryption Service	-	Программа, обеспечивает возможность дополнительной защиты контента при вещании в спутниковой и IP сетях.
DRE Config Manager (далее по тексту - ConfigManager)	CM	Сервис для хранения списка операторов и их конфигурационных данных. Сервис получает, агрегирует и выдает перечень операторов, которые используют DREAMPlatform, а также набор конфигурационных данных для каждого оператора. Таким образом, абонент, пользуясь одним клиентским приложением, может получать доступ к нескольким операторам.

DRE Messaging Service (далее по тексту - Hermes)	-	Система, реализующая функционал отправки уведомлений на оборудование абонентов.
DVB-Simulcrypt	-	DVB-стандарт архитектуры, позволяющей функционировать множеству Систем Условного Доступа в рамках единой головной станции. Этот стандарт определяет архитектуру головного оборудования и СУД, временные параметры взаимодействия компонентов, их интерфейсы и формат сообщений.
Electronic Program Guide, (электронный программный гид)	EPG	Электронный телегид. Сервер генерирует поток данных с файлами расписания телепередач, расписания показа фильмов и файлами обновления ПО, встроенного в приёмники.
Encoded Channel DRE	ECD	Дополнительная функция CAS DREGUARD, предназначенная для информирования абонента о причине ограничения доступа к телепередаче. Информирование производится через сообщения "Кодированный канал", которые содержат код статуса дескремблирования и краткую инструкцию по устранению проблемы.
Enhanced Common Scrambling Algorithm	ECSA	Технология аппаратного антишаринга, построенная на дополнительном шифровании CW до его шифрования алгоритмом смарт-карты. Требует аппаратной поддержки в процессоре STB, в который встраивается библиотека (CAS DREGUARD Library).
Entitlement Control Message	ECM	Сообщение CAS DREGUARD, содержащее в зашифрованном виде CW, дескремблирующие транслируемый поток.
Entitlement Management Message	EMM	Сообщение CAS DREGUARD, содержащее служебные данные, информацию о правах доступа и специальные команды (изменение подписки, обновление операционного ключа и другие).
InfoCAS	-	Дополнительная функция CAS DREGUARD, позволяющая оператору ТВ рассылать текстовые сообщения абонентам. Функция реализуется системой CAS DREGUARD или системой Сервисов. Сообщения принудительно отображаются на экране ТВ поверх основного изображения. Примеры использования сообщений - предупреждения об обновлении ПО, окончании подписки, оповещения населения и другие.
Lite mode	-	Режим работы ECMG. В данном режиме CW передаются в ECM в незашифрованном виде.

L-режим	-	Режим ограниченного просмотра, предназначенный для мотивации абонента продлить подписку. В данном режиме картинка телеканала пропорционально уменьшается, а в остальной области экрана выводится реклама.
Pairing	-	Режим CAS DREGUARD, обеспечивающий работу смарт-карты только с одним конкретным приёмником.
Scrambling Control Group	SCG	Логическое объединение каналов, скремблируемых едиными CW, создаваемое на головном оборудовании Оператора ТВ.
Simulcrypt синхронизатор	SCS	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.
Мультиплексор (Multiplexer)	MUX	Компонент головного оборудования, предназначенный для преобразования получаемой информации в TS с последующей передачей на спутник.
Common Scrambling Algorithm	CSA	Общий алгоритм скремблирования, используемый для защиты цифрового телевизионного потока от несанкционированного доступа
Transport Stream	TS	Формат медиаконтейнера, который инкапсулирует пакеты элементарных потоков и других данных.
TS Monitor	TSM	Набор программных средств, предназначенных для мониторинга транспортного потока.
Subscriber Management System	SMS	Компонент который позволяет управлять подписками/услугами /устройствами/каналами и т.д. Обеспечивает интеграцию с биллинг системами операторов.

3. Назначение системы

CAS DREGUARD представляет собой программно-аппаратный комплекс, включающий в себя основные компоненты системы условного доступа (CAS), обеспечивая защиту контента путем кодирования транспортного потока перед его передачей в канал вещания. Данные, 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.

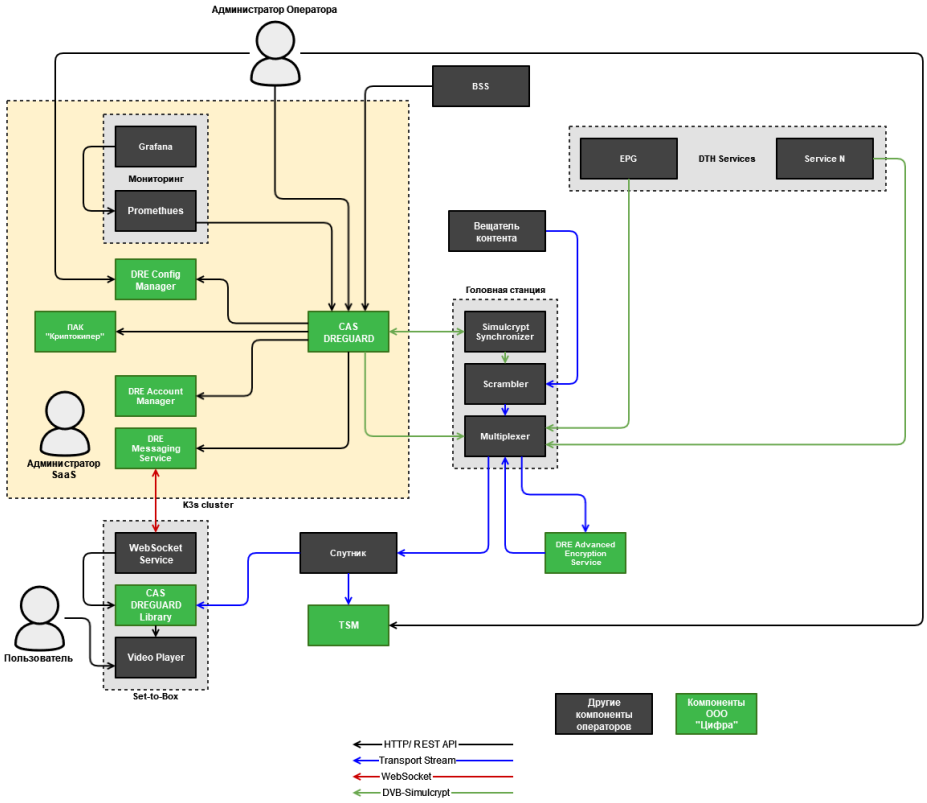
CAS DREGUARD отвечает за:

- прием и обработку информации от биллинговой системы (подписки, геокоды, сообщения);
- передачу абонентам ключей, необходимых для расшифровки защищенного транспортного потока, в зашифрованном виде в составе ECM и EMM сообщений;

CAS DREGUARD разработан в соответствии со стандартом DVB-Simulcrypt, что делает его совместимым с большинством головного оборудования, представленного сегодня на рынке.

4. Описание CAS DREGUARD

4.1. Структура взаимодействия CAS DREGUARD



Система	Исходящие взаимодействия (из CAS DREGUARD в другие системы)	Входящие взаимодействия (из других систем в CAS DREGUARD)
Головная станция оператора	Отправка в головную станцию сгенерированных ECM и EMM	Поддерживает DVB-Symulcrypt соединение, передает в него CW (Control Word) и AC (Access criteria)
BSS (Биллинг)	-	Отправка информации о создании подписок на услуги/классы в CAS DREGUARD по факту осуществления покупки клиентом оператора
DRE Account Manager	Обращения за валидацией пользователей-администраторов системы для определения существования их в системе и определения уровня доступа к системам	-

DRE Messaging Service	Получение информации необходимой для дальнейшей отправки на клиентские устройства операторов CAS DREGUARD	-
DRE Config Manager	Обращения за получением параметров конфигурации, разбитых индивидуально под каждого оператора	-
DRE Advanced Encryption Service	-	В CAS DREGUARD загружаются ключи ADEC /ECSA необходимые для дополнительной защиты элементарных потоков (защита применяется в дополнение к стандартному алгоритму (CSA))
ПАК "Криптокипер"	Обращается за получением дополнительной информации для формирования ECM/EMM	
TSM	-	Мониторинг транспортного потока в контексте CAS-атрибутики (APDU, ECSA, ADEC и т.п.)

4.2. Системы, взаимодействующие с CAS DREGUARD

Компоненты операторов:

- BSS - биллинговая система, сторонний по отношению к CAS DREGUARD компонент, отвечающий за обработку платежей, хранение информации о пользователях, формирование команд на операции с подписками и подсчет времени до окончания срока действия каждой подписки, а также за формирование команд на работу с сообщениями InfoCAS. Команды от BSS в виде HTTP запросов отправляются в CAS DREGUARD и в нем же обрабатываются.
- Головная станция:
  - Simulcrypt Synchronizer (SCS) - компонент головного оборудования, предназначенный для установления и поддержания соединения с CAS DREGUARD, передачи ему CW и AC, получения сгенерированных ECM сообщений и перенаправления их в Multiplexer;
  - Scrambler (SCR) - компонент головного оборудования, предназначенный для шифрования потока с помощью CW;
  - Multiplexer (MUX) - компонент головного оборудования, формирующий единый транспортный поток MPEG-2 из всех входных данных.
- Prometheus + Grafana:
  - Prometheus - агрегатор статистики. Показатели, по которым собирается статистика, задаются так называемыми "метриками". В соответствии с заданными метриками компоненты Системы собирают статистику о своей работе и отправляют её в Prometheus. Полученная статистика используется для мониторинга работы Системы.
  - Grafana - средство визуализации метрик, полученных Prometheus.
- EPG - электронный телегид. Сервер генерирует поток данных с файлами расписания телепередач, расписания показа фильмов и файлами обновления ПО, встроенного в приёмники.

Компоненты ООО "Цифра":

- DRE Config Manager - сервис для хранения списка операторов и их конфигурационных данных. Сервис получает, агрегирует и выдает перечень операторов, которые используют DREAMPlatform, а также набор конфигурационных данных для каждого оператора. Таким образом, абонент, пользуясь одним клиентским приложением, может получать доступ к нескольким операторам.
- ПАК "Криптокипер" – система, отвечающая за шифрование информации, передаваемой в ECM и EMM.
- DRE Account Manager - сервис авторизации и распределения прав. CAS DREGUARD может обратиться к Account Manager (через свой фронтенд или API) для авторизации, передачи и проверки прав пользователя. Затем, при помощи WEB UI, пользователь CAS DREGUARD может создавать дополнительные учетные записи, назначать роли и создавать группы прав.
- DRE Messaging Service - система, реализующая функционал отправки уведомлений на оборудование абонентов.
- DRE Advanced Encryption Service - программа обеспечивает возможность дополнительной защиты контента при вещании в спутниковой и IP сетях.
- CAS DREGUARD Library (далее по тексту - Library) - система, представляющая собой промежуточное ПО, которое обеспечивает взаимодействие ПО приемника и эмулятора смарт-карты. Library управляет выделением служебных данных (например, ECM и EMM) из принятого транспортного потока, получением из них зашифрованных ключей и их передачу эмулятору смарт-карты для расшифровки.
- TSM - набор программных средств, предназначенных для мониторинга транспортного потока.

5. Дополнительные функции CAS DREGUARD

Функциональность	Краткое описание
L-mode	В системе реализован режим работы (*L-режим*), позволяющий при окончании оплаченного срока подписки продлить возможность просмотра канала со следующим ограничениями: 1. Размер области картинки канала пропорционально уменьшается (до 70% экрана ТВ). 2. В свободной области экрана отображается реклама.
InfoCAS	Дополнительная функция CAS DREGUARD, позволяющая оператору ТВ рассылать текстовые сообщения абонентам. Функция реализуется системой CAS DREGUARD или системой Сервисов. Сообщения принудительно отображаются на экране ТВ поверх основного изображения. Примеры использования сообщений - предупреждения об обновлении ПО, окончании подписки, проведении профилактических работ, оповещения населения и другие
ECD	Отображение информации об ошибках на экране ТВ. Текст информирует абонента о возможной причине ограничения доступа на просмотр. Данная возможность используется службой поддержки оператора ТВ для локализации и устранения ошибок
Поддержка нескольких тюнеров	Поддержка нескольких транспортных потоков (т.е. использование в STB с несколькими тюнерами) Функция реализуется в CAS DREGUARD Library
Холодное резервирование	Метод повышения надёжности системы: резервные элементы не несут нагрузки до момента подключения их вместо отказавшего основного элемента
ECSA	Технология аппаратного антишаринга, построенная на дополнительном шифровании CW до его шифрования алгоритмом смарт-карты. Требует аппаратной поддержки в процессоре STB, в который встраивается библиотека (CAS DREGUARD Library)
Встроенная смарт-карта	В STB используется SC Emulator

6. Мониторинг CAS DREGUARD

Мониторинг работы системы осуществляется с помощью системы Prometheus и визуализацией метрик с помощью Grafana.

7. Требования и ограничения

7.1. Системные требования

CAS DREGUARD должен эксплуатироваться минимально на 2-х серверах.

Серверные приложения CAS DREGUARD разворачиваются в системе оркестрации K3s и должны удовлетворять минимальным требованиям:

- Процессор — 4 ядра (x64) или больше;
- Оперативная память — минимум 8 GB;
- Жесткий диск — 2 × 150 GB (зависит от количества клиентов);
- Сетевые интерфейсы – 2 x 1 Gb/s.

Сервер для работы СУБД PostgreSQL, к которому обращаются серверные приложения, должен удовлетворять минимальным требованиям:

- Процессор — 4 ядра (x64) или больше;
- Оперативная память — минимум 8 GB;
- Жесткий диск — 2 × 250 GB (зависит от количества клиентов);
- Сетевые интерфейсы – 2 x 1 Gb/s.

Также для работы CAS DREGUARD требуется головное оборудование, соответствующее стандарту DVB-Simulcrypt ver. 2.

7.2. Требования к квалификации обслуживающего персонала

Для настройки и администрирования CAS DREGUARD персонал должен удовлетворять следующим требованиям:

- обладать теоретическими знаниями и практическим опытом работы с СУБД PostgreSQL;
- иметь навыки работы и администрирования ОС сервера, а также опыт работы с Docker и Kubernetes;
- 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.

7.3. Ограничения

7.3.1. Аппаратные ограничения

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

7.3.2. Ограничения по безопасности

Для обеспечения безопасности важных данных, все компоненты системы 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.

8. Поддерживаемые стандарты

Следует учитывать, что здесь приведены основные стандарты, которым соответствует CAS DREGUARD. Каждый из них ссылается на несколько других.

1. ETSI TS 101 197 V1.2.1 DVB SimulCrypt; Part 1: Head-end architecture and synchronization
2. ETSI TS 103 197 V1.5.1 Head-end Implementation of SimulCrypt
3. ETSI TR 102 035 V1.1.1 Implementation Guidelines of the DVB Simulcrypt Standard
4. ETSI ETR 289: "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems
5. ISO/IEC 13818-1 (2000): "Information technology - Generic coding of moving pictures and associated audio information: Systems".
6. ETSI EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems".
7. ETSI ETR 162: "Digital Video Broadcasting (DVB); Allocation of Service Information (SI) codes for DVB systems"
8. ETSI ETR 289: "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems"
9. IETF RFC 791 (1981): "Internet Protocol".
10. IETF RFC 793 (1981): "Transmission Control Protocol"