GS LABS
GS GROUP

Публичный - L0

DRE Advanced Encryption Service

Общее описание

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

Содержание

1. Аннотация . . . 3
2. Термины и сокращения . . . 4
3. Назначение и структура системы . . . 6
3.1. Назначение . . . 6
3.2. Структурная схема . . . 6
3.3. Основные компоненты . . . 6
3.4. Внешние системы, взаимодействующие с ADEC Scrambler . . . 7
4. ADECScramblerIP (instance) . . . 8
4.1. Общее описание . . . 8
4.2. Логическая структура . . . 8
4.3. Общая структура взаимодействия . . . 9
4.3.1. Взаимодействие ADECScramblerIP с приемной стороной . . . 9
4.4. Функциональные возможности . . . 9
5. ADEC Scrambler WEB (UI) . . . 11

1. Аннотация

Документ содержит общее описание системы "DRE Advanced Encryption Service" (далее по тексту - ADECScrambler или Система) и предназначен для широкого круга специалистов. Подробнее работа системы описана в других документах по продукту.

2. Термины и сокращения

Термин	Определение
AGS	Продукт DRE Defender.
Транспортный поток (TS)	Набор объединенных элементарных потоков, используемый для передачи аудио, видео и других данных в системах цифрового вещания. Структура транспортного потока определена в стандарте ISO/IEC 13818-1.
Элементарный поток	Поток данных одного типа, передающийся в составе транспортного потока. Примеры: аудиодорожка, видео, телетекст, служебная информация.
Скремблер (Scrambler)	Устройство шифрования транспортного потока, входящее в состав головного оборудования. В терминологии стандарта DVB-Simulcrypt обозначает функциональный логический блок, ответственный за шифрование MPEG2 транспортного потока. Конкретная функциональность зависит от реализации.

Сокращение	Расшифровка
ACM	(Account Manager) - продукт DRE Account Manager. Сервис авторизации и распределения прав. Компоненты системы авторизуются через Account Manager. В интерфейсе Account Manager прописываются права того или иного компонента. Также в Account Manager хранятся, создаются новые, редактируются учетные записи пользователей, через специальный WEB UI назначаются права, создаются роли и группы прав для учетных записей пользователей.
AGS	API Gateway System
ADEC	(ADvanced EnCryption) - система шифрования транспортного потока, применяемая в дополнение к стандартному алгоритму шифрования (CSA).
MPEG	(от Moving Picture Experts Group - Группа Экспертов по Движущемуся Изображению) – название системы кодирования набора сжатых цифровых телевизионных видеосигналов, звуковых сигналов и данных пользователя телевизионной информации в поток цифровых пакетов
IP	(Internet Protocol) - протокол передачи данных по сети Интернет
PID	Идентификатор пакетов, относящихся к одному элементарному потоку. Уникален в пределах транспортного потока.
TS	Transport Stream, Транспортный поток (см. таблицу терминов)
TSoIP	(TS over IP) – передача транспортного потока цифрового телевидения по протоколу IP
UI	(User Interface) - пользовательский интерфейс

GbE (GigE)	(Gigabit Ethernet) - технология передачи данных по сети Ethernet со скоростью до 1 гигабит /сек
СУД	Система Условного Доступа

3. Назначение и структура системы

3.1. Назначение

Программа DRE Advanced Encryption Service (далее - ADECScrambler или Система) обеспечивает возможность дополнительной защиты контента при вещании в спутниковой и IP сетях. Для поддержки этой функциональности доступны следующие возможности:

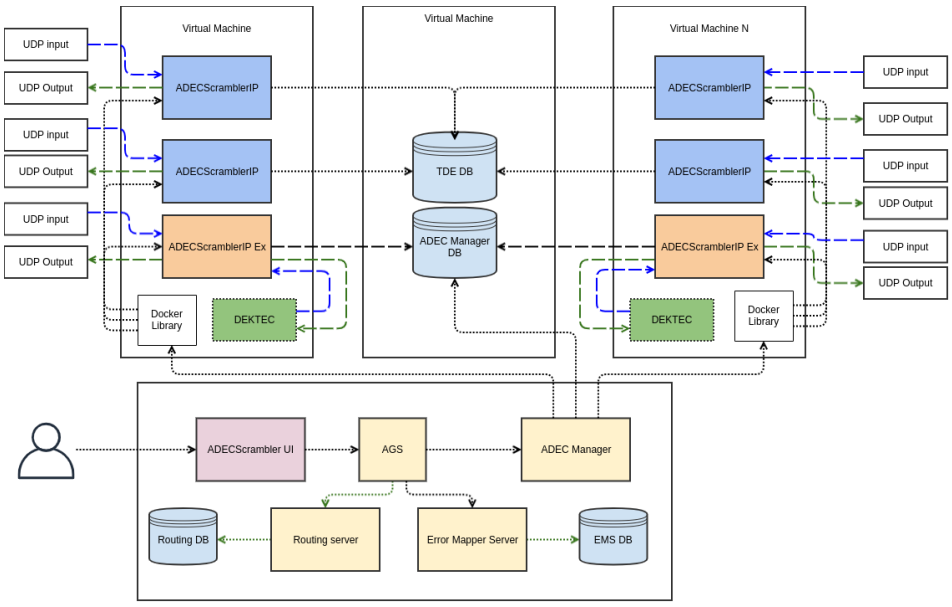
- Возможность выбора каналов для включения дополнительной защиты из списка каналов входящего транспортного потока.
- Возможность выбора различных алгоритмов дополнительной защиты, включая алгоритм S17.
- Предоставление набора метрик для мониторинга бесперебойной работы.

ADECScrambler обеспечивает:

- высокоскоростное шифрование транспортных потоков из следующих источников:
  - порт Gigabit Ethernet (порт Ethernet находится непосредственно на сетевой плате)
  - платы производителя DekTec, обеспечивающие функции ввода-вывода и обработки DVB /MPEG-2 цифровых видеосигналов
  - файл с сохраненным транспортным потоком
- сигнализацию о возникающих в работе ошибках
- мониторинг статистики работы по заданным показателям
- возможность отключения шифрования и прямой передачи транспортного потока на приемник
- возможность управления и настройки экземплярами скремблера через веб-интерфейс

3.2. Структурная схема

Структурная схема продукта ADECScrambler представлена на рисунке:



3.3. Основные компоненты

Система состоит из следующих компонентов:

- ADECScramblerIP - сервис для скремблирования TS потока с заданной конфигурацией.
- ADECScramblerIP Ex - аналог сервиса ADECScramlberIP с дополнительным функционалом для возможности захвата видео потока с DekTec плат.

  ⚠ Фактически ADECScramblerIP и ADECScramblerIP Ex - разные инстансы одной и той же сборки (adec_scrambler_go), с разными параметрами работы.

- ADEC Manager - сервис для управления и автоматизированного разворачивания экземпляров сервисов ADECScramblerIP и ADECScramblerIP Ex.
- ADEC Manager DB - база данных для работы ADEC Manager.
- TDE DB (в сборках обозначена как ADEC_DB) - база данных для хранения adec ключей, которыми шифруется поток.
- ADECScrambler UI (в сборках обозначен как ADEC Scrambler WEB) - доступная через web-браузер консоль (web-интерфейс) для управления конфигурациями ADECScramblerIP и ADECScramblerIP Ex.
- DRE Defender (далее по тексту - AGS) - API Gateway System - "proxy" для ADECScrambler UI: перенаправляет запрос в ADEC Manager и получает от него ответ:
  - в случае успеха - передает ответ в ADEC Scrambler UI.
  - в случае возникновения ошибки - на AGS формируется запрос на Error Mapper Server для переопределения внутреннего кода ошибки на внешний числовой код ошибки.
- EMS - Error Mapper Server - микросервис для сопоставления системных ошибок и внутренних ошибок Системы, для различных сценариев.
- EMS DB (в деплое разделена на два компонента - ems_db_sch и ems_db_api) - БД под управлением PostgreSQL, которая хранит данные для EMS (коды ошибок). База имеет начальное наполнение (в деплое называется adec_scrambler_error_maps_i18n).
- Routing Server (в деплое называется routing_server) - менеджер запросов для ADECScrambler UI (web). Работает в связке с AGS.
- Routing DB (в деплое разделена на два компонента - routing_db_sch и routing_db_api) - БД под управлением PostgreSQL, которая хранит данные (routings) для Routing Server.

3.4. Внешние системы, взаимодействующие с ADEC Scrambler

- **Только при использовании web-интерфейса ADECScrambler (ADEC Scrambler WEB / ADECScrambler UI)**:
  DRE Account Manager (ACM) (далее - Account Manager) - это сервис авторизации и распределения прав. Сторонний сервис (в данном случае - ADECScrambler) может обратиться к Account Manager (через свой фронтенд или API) для авторизации, передачи и проверки прав пользователя. Затем, при помощи WEB UI, пользователь стороннего сервиса может создавать дополнительные учетные записи, назначать роли и создавать группы прав.

4. ADECScramblerIP (instance)

4.1. Общее описание

Система ADECScramblerIP (далее - Система) представляет собой серверное приложение, реализующее скремблирование TS-потока adec-ключами. Входной (открытый) поток может быть захвачен из следующих источников:

- udp unicast socket
- udp multicast socket
- плата производителя DekTec, обеспечивающая ввод и обработку DVB/MPEG-2 цифровых видеосигналов
- file - данный режим работы в текущей версии предназначен только для целей тестирования, т.к нет регулировки по битрейту в данном режиме

Результирующий (шифрованный) поток передается в один из следующих приемников:

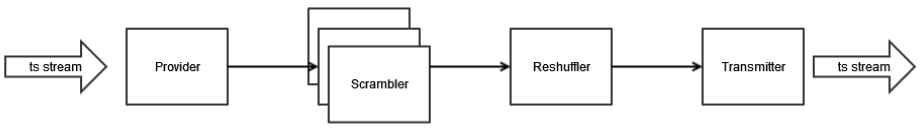
- udp unicast socket
- udp multicast socket
- плата производителя DekTec, обеспечивающая вывод и обработку DVB/MPEG-2 цифровых видеосигналов

Особенности ADECScramblerIP:

- Работа по IP протоколу через сетевую плату.
- Поддержка алгоритма S17.
- Поддержка хранения ключей в шифрованном виде.

4.2. Логическая структура

Структурная схема ADECScramblerIP представлена на рисунке:



ADECScramblerIP представляет собой конвейер с последовательной обработкой на каждом из узлов входного потока. Конвейер состоит из следующих компонентов:

- Provider - обеспечивает забор данных из источника и парсинга их в структуру ts-пакета.
- Scrambler - обеспечивает шифрование ts-пакета заданным алгоритмом.
- Reshufler - обеспечивает выстраивание ts-пакетов в правильном порядке следования после шифрования.
- Transmitter - обеспечивает передачу данных к приемнику.

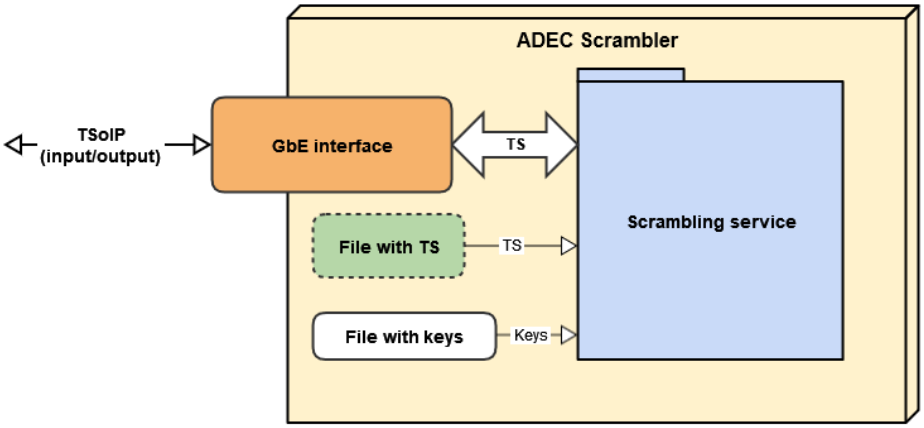
⚠ **Обратите внимание!** Описанное выше деление на компоненты - это логическое деление в рамках одного исполняемого файла adec_scrambler_go, т.е физически запускается одна служба.

4.3. Общая структура взаимодействия

ADECScramblerIP представляет собой выделенный сервер на ОС Debian 8 64 бит, снабженный интерфейсом Gigabit Ethernet. Входной и и выходной потоки поступают по IP, через сетевую плату. Исходный незашифрованный сигнал может быть получен не только по входному интерфейсу, но и из файла с сохраненным TS.

Используемые для скреблирования ключи могут храниться в зашифрованном виде, для их применения нужно знать пароль.

Взаимодействие частей Системы представлено на рисунке:



4.3.1. Взаимодействие ADECScramblerIP с приемной стороной

Настройка взаимодействия передающей и приемной стороны заключается в уведомлении приемной стороны об использовании дополнительного шифрования и настройках его режима.

4.4. Функциональные возможности

Основные задачи, выполняемые ADECScramblerIP:

- высокоскоростное шифрование транспортных потоков, получаемых из следующих источников:
  - через порт Gigabit Ethernet (порт Ethernet находится непосредственно на сетевой плате)
  - из файла с транспортным потоком
- сигнализация об ошибках
- возможность прямой передачи потока со входа на выход (отключение/включение скреблирования)

ADECScramblerIP обладает следующими характеристиками:

1) Основные:

- возможность одновременного скремблирования нескольких PID
- любой PID может быть привязан к любому ключу
- поддержка следующих алгоритмов шифрования: TDES, S17
- вывод потока осуществляется на один IP-порт

2) Входные и выходные интерфейсы:

- Gigabit Ethernet:
  - Вход/выход: транспортные потоки по протоколу IP
- ASI (только при использовании платы Dektec):
  - вход: транспортный поток через ASI-интерфейс
  - выход: транспортный поток через ASI-интерфейс
  - через один ASI-порт может передаваться один транспортный поток

3) Мониторинг:

- в логах указываются изменения в работе служб шифрования, ошибки, остановки, перезапуски и т.п.

  ⚠ Чтобы посмотреть логи, надо выполнить команду *docker logs container_name*

- собирает статистику о своей работе. Показатели, по которым собирается статистика (например, количество успешно зашифрованных байт), задаются так называемыми "метриками".

4) Безопасность:

- от неавторизованного доступа скремблер защищается средствами ОС
- набор ключей хранится в отдельном файле. Для шифрования файла используется специальная утилита (предоставляется по запросу заказчика).

5. ADEC Scrambler WEB (UI)

Web-интерфейс позволяет быстрее и легче настраивать основные параметры, необходимые при эксплуатации ADECScrambler.

Внешний вид графического интерфейса приведен на рисунке: