GS LABS
GS GROUP

Публичный - L0

Система генерации ключей Keys Generation System (KGS)

Руководство пользователя

Индекс	KGS-UG
Конфиденциальность	Публичный - L0
Ревизия	1.0
Статус	Согласован

Содержание

1. Аннотация

Данный документ является руководством по использованию "Системы генерации ключей Keys Generation System (KGS)" (далее по тексту - KGS или Система). Руководство содержит общие сведения о продукте, системные требования, основные группы задач, решаемых Системой, процедуры работы с программой.

Документ предназначен для пользователей, осуществляющих работу в KGS. Руководство ориентировано на пользователей, обладающих подробными знаниями о системе KGS, имеющих практические навыки работы с консолью (KVM) и с FTP-сервером. Пользователи должны иметь доступ в закрытое помещение, в котором установлена система.

⚠ В связи с постоянным совершенствованием продукта, могут иметь место незначительные несоответствия описания и фактического функционирования/внешнего вида интерфейса у конечного пользователя, НЕ ВЛИЯЮЩИЕ НА ОСНОВНОЙ ФУНКЦИОНАЛ.

2. Термины и сокращения

⚠ Термины, используемые в интерфейсе KGS, подробно описаны в отдельном документе, **доступ к которому ограничен**.

Термин	Определение
ADEC	Технология дополнительного шифрования транспортного потока (TS).
ADEC ключи	Ключи, которые используются в алгоритме дополнительного шифрования TS.
Batch	Пачка – служебный термин, используемый для локализации пакетных операций в системе. Все операции, которые производятся с чипами, внутри системы выполняются в рамках какой-либо пачки. Пачки используются при откате отчетов о программировании чипов или производства STB устройств.
Black Box	Сервер передачи ключей Keys Transfer Server. С точки зрения системы KGS, это Внешний сервер с типом 'Black Box'.
CAS	Система Условного Доступа.
CAS Команды (CAS Commands)	Команды для БД CAS, используются при создании Мастер Ключей. Связь между CAS Командами и описанием Мастер Ключа - "один ко многим": для одной команды может использоваться несколько Мастер Ключей (например, с разным processing_type: _ENC и _MAC), но один Мастер Ключ не может использоваться одновременно для нескольких команд.
CoT ключи (chain-of-trust keys)	Ключи, используемые в цепочке secure boot чипа для подписи и шифрования прошивки или генерации производных ключей. Фактически функциональное назначение CoT ключа аналогично "Ключам прошивки", отличается только способ генерации. CoT-ключи генерируются на первом или втором уровне через KDF и являются "derived key".
Derived Key	Производный ключ, рассчитанный по алгоритму RK KDF.
DRM-ключи	Ключи, генерируемые с помощью Initialization Vector и выбранного OTP-ключа. Используются партнером (СпераСофт) для прошивки в игровые приставки, с целью защиты контента на базе произведенных устройств/чипов. На базе этих данных (DRM-ключи, Partner IV, OTP-ключ) партнер генерирует собственную лестницу ключей.
ECSA	Технология дополнительного шифрования контрольных слов (CW) для алгоритма CSA по лестнице ключей.
ECSA ключи	Ключи, которыми шифруются CW.

Fusemap конфигурация (Fusemap Config, FMC)	Подробное описание области OTP-памяти чипа с адресами, полями и их размерами, включая OTP-ключи и конфигурационные биты.
HWRK-ключи	Ключи (public + private), используемые в лестнице ключей. Генерируются (вместе с DBMK-ключами) подсистемой KMI_FW_DBMK (утилитой DBMK Generator), причем на том физическом сервере, на котором будут использоваться. ⚠ **Обратите внимание!** Здесь и далее используются внутренние системные обозначения компонентов (например, KMI_FW_DBMK). Соответствие между названиями компонентов (подсистем KGS) и внутренними обозначениями приведено в документе "Система генерации ключей Keys Generation System (KGS). Общее описание", в разделе "Архитектура". Public HWRK-ключ, сгенерированный на Внешнем сервере, используется при экспорте файла конфигурации на этот сервер.
Initialization Vector (также initVector, Partner IV)	Вектор инициализации - специально генерируемый массив данных (16 байт = 32 символа, в hex-формате), вместе с индексом OTP-ключа используется для подготовки DRM-ключей. Значение вектора уникально и постоянно в рамках Партнер+Тип партии.
JTAG-ключ	Уникальный ключ, привязанный к чипу (device). Представляет собой своеобразный пароль, который используется для тестирования чипа, т.е. чипы с данным ключом используются только для тестирования.
KDF (Key Derivation Function)	Функция (алгоритм), генерирующая ключи. KDF применяется: • для генерации JTAG ключа для SRISC (только для Типа Устройства = 'Secure SoC GS2'). • при обфускации OTP-ключей. • для генерации CoT ключей.
KOF (key obfuscation function)	Специальная функция (и алгоритм), которая действительно "запутывает" значения OTP-ключей и использует результат OVDF как входной параметр для некоторых задач (например, в качестве ключа обфускации и т.д.). Может быть настроена для Вида Партии.
KVM-переключатель (keyboard video mouse)	Устройство, предназначенное для коммутации одного комплекта устройств ввода-вывода между несколькими компьютерами.
LE-набор	Набор ключей, хранящихся в системе и привязанных к одному из Видов Партий.

LE-блок	Блок данных, содержащий ключи какого-либо LE-набора, зашифрованные одним из общих OTP ключей чипа и содержащий информацию о Виде Партии, индексе OTP ключа и подпись SHA-256 для всего блока.
OTP Карта ключей (Keymap, также OTP keymap)	Карта ключей – ключевой элемент, характеризующий определенный тип чипа. Карта ключей всегда привязана к какому-либо типу чипов и не существует вне его контекста. Карта ключей, по сути, является аналогом fuse map с тем отличием, что набор элементов в карте ключей может быть подмножеством fuse map, поскольку содержит только те элементы, для которых выполняется генерация и сохранение ключей в системе.
OTP-ключ	Ключ, персонализированный в OTP-память (One Time Programmable memory).
OTP Root key	OTP-ключ, который используется только как корневой ключ в лестнице ключей.
OVDF (obfuscation value derivation function)	Специальная функция (и алгоритм), результатом которой является некоторое сгенерированное значение, которое, в свою очередь, может быть использовано в качестве базы / ключа для обфускации ("запутывания") значений OTP-ключей. Сама по себе функция не выполняет обфускацию, она только генерирует значение для использования в реальных функциях обфускации (KOF). Может быть настроена для Вида Партии.
Pairing	Режим CAS, обеспечивающий работу смарт-карты только с одним конкретным приёмником.
PGP ключ пользователя (User key)	PGP-ключ, используемый системой KGS для шифрования данных при экспорте на FTP-сервер или дешифрования при импорте. PGP-ключ может быть сгенерирован в системе KGS (генерируются private + public части ключа) либо импортирован с FTP-сервера (импортируется и хранится только public-часть ключа).
RK KDF	Применение KDF к OTP-root-ключу перед лестницей ключей.
Sign Server	Сервер, осуществляющий шифрование и подпись переданных на него прошивок для приемников.
STB (Set Top Box)	Ресивер цифрового телевидения.
STB Модель (STB model)	Модель ресивера цифрового телевидения, в который устанавливается персонализированный чип.
Workflow (WF)	Пункт консольного меню KGS с шагами, обеспечивающими выполнение того или иного процесса работы с конфигурациями сущностей или ключами чипов.
БД CAS (CASDB)	Сущность, вокруг которой группируются параметры для поддержки генерации, хранения и экспорта ключей для системы условного доступа заданной версии. "Условная база данных CAS", для которой готовятся и затем экспортируются ключи и параметры.

Вид Партии	См. Тип Партии.
Внешний сервер (External Server)	Любой сервер, на который экспортируются ключи из системы KGS.
Вспомогательные Ключи (AUX keys)	Вспомогательные (auxiliary) ключи, используемые в работе внешних устройств и систем.
Класс устройств (Device class)	Модель чипа, в который прошиваются сгенерированные KGS ключи.
Ключи прошивки (Firmware keys, fw keys)	Ключ для защиты прошивки и обеспечения безопасной загрузки ПО чипа (Secure boot). Некоторые ключи относятся к OTP keys, некоторые не записываются в OTP. Все ключи, которые используются для шифрования и расшифрования прошивки, а также для создания и проверки подписи прошивки. Ключи прошивки могут как персонализироваться в чип, так и не персонализироваться.
Мастер Ключ (Мастер-ключ CAS, Master Key)	Основные ключи защиты служебных сообщений CAS. Ключи разделяются по функции обработки (шифрование, подпись) и адресации сообщения (индивидуальные, групповые, общие для Вида Партии, глобальные (общие) для экземпляра CAS).
Номер Партии (Part Number, PN)	Сущность, которая характеризует заказы чипов у производителя (чип-вендора). Как правило, в чипах используемое имя партии, выгравированное на корпусе. В KGS сущность кроме имени имеет внутренний идентификатор. В KGS имя задается пользователем и может не совпадать с маркировкой на чипе.
Обфускация (Obfuscation)	Необязательная операция, применяется, если чип не имеет защищенной области памяти для хранения ключей.
Оператор (Operator)	Оператор вещания, для трансляции программ которого предназначен произведенный приемник (STB Модель). Может быть привязан к чипу в процессе работы по факту обработки отчетов о производстве STB-устройств.
Описание Fusemap конфигурации (Fusemap config decription, FMCD)	Сущность в KGS для хранения описания FMC.
Партнер (Partner)	Производитель неких устройств на произведенных KGS чипах (в данный момент под устройствами подразумеваются игровые приставки), которые используют лестницу ключей, основанную на OTP-ключах, сгенерированных системой KGS.

Пользователь (User)	Пользователь системы KGS. Характеризуется именем, системным именем и внутренним идентификатором. Имя пользователя используется только для отображения в системе, системное имя используется для связки с учетной записью на Processing Server и FTPсервере. Для каждого пользователя в системе могут быть загружены один или несколько открытых (public) PGP-ключей (User keys), которые используются при выгрузке данных из системы на FTP-сервер. Администратор KGS задает всем остальным пользователям права доступа на отдельные операции (Workflows) в системе.
Помощник (Wizard)	"Помощник" для выгрузки данных из KGS. Помощник фактически представляет собой специальную операцию (пункт меню), которая объединяет в себе отдельные операции (пункты меню), используемые для экспорта данных (например, для персонализации чипов).
Поставщик (Vendor)	Производитель чипов.
Производитель (Manufacturer)	Производитель STB с персонализированными чипами. Характеризуется наименованием и внутренним идентификатором. Производитель может иметь одну или более моделей устройств (STB Модель).
Профиль RK KDF (RK KDF Profile)	Специальная сущность, созданная для хранения параметров профиля RK KDF. Под профилями RK KDF понимается именно настройка KDF для OTP Root Key в KGS.
Ресурс (Resource)	Ресурсы (объекты), используемые в KGS. Все ресурсы делятся на следующие категории: 1. **FTP-connection**. Параметры соединений с FTP-сервером: FTP_URL, port, login, password. 2. **Workflow**. Добавление новой операции (пункта меню) в консоль KGS. Используется для идентификации процесса (workflow) в системе, управления правами на их выполнение для отдельных пользователей и точечной настройки каждого процесса с помощью настроечных параметров. 3. **Component**. Подсистема в рамках KGS. Используется как контейнер для хранения настроечных параметров, уточняющих работу компонентов (например, режим отладки для каждого из компонентов).
Тестовые ключи (Test keys)	Нешифрованные значения ключей (OTP root-ключей и Ключей прошивки), требующихся для тестовых партий устройств (*тестовых Видов Партий*) и приемников.
Тип Партии (Part Type, PT, PTTP)	Сущность, которая характеризует набор общих OTP-ключей в чипах одной партии: у всех чипов одной PT одинаковые общие ключи. В чипах используется только идентификатор Вида Партии, в KGS также используется пользовательское имя Не путать его с Номером Партии.

Тип Устройства (Device type)	Тип чипа. Характеризует Класс устройств.

Сокращение	Расшифровка
ADEC	ADditional EnCryption
AUX	Auxiliary
BBX	Black Box
CAS	Conditional Access System
CoT	Chain-of-Trust
CW	Control Word
DRM	Digital Rights Management
ECSA	Enhanced CSA
FMC	Fuse Map Config
FMCD	Fuse Map Config Description
ID	Identifier
IV	Inintialization Vector
JTAG	Joint Test Action Group
KDF	Key Derivation Function
KOF	Key Obfuscation Funcion
KVM	Keyboard Video Mouse
LE	Link Encryption
MK	Master Key
OTP	One Time Programmable
OVDF	Obfuscation Value Derivation Function
PK	Pairing Key
PN	Part Number
PT	Part Type
PTTP	Part Type

RK KDF	Root Key KDF
STB	Set Top Box
TS	Transport Stream
WF	Workflow

3. Общие сведения

Система генерации ключей Keys Generation System (KGS) предназначена для работы с ключами, прошиваемыми в однократно программируемую область чипа в процессе его персонализации. Программа предоставляет инфраструктуру, необходимую разработчикам систем, использующих персонализированные ключи. Программа реализует механизмы генерации, безопасного хранения и экспорта ключей для возможности дальнейшего их использования в процессе персонализации чипов на производственной линии.

Тип ЭВМ: IBM PC-совмест. ПК; ОС: Debian.

Язык программирования: C++, Python 3

Общие сведения о Keys Generation System, такие как назначение, функциональные возможности, архитектура, схема развертывания, принцип работы, описаны в документе "Система генерации ключей Keys Generation System (KGS). Общее описание".

3.1. Требования к вводимым данным

На ввод данных через workflow (KMI_CONSOLE) и сохранение введенной информации в БД существуют ограничения. KGS возвращает ошибку либо не позволяет вставить данные в следующих случаях:

- при отправке 50 и более символов кириллицы (UTF-8);
- при вводе 100 и более символов латиницы (UTF-8);
- при вводе символов кириллицы (ANSI);
- при вводе 100 и более символов латиницы (ANSI).

Несмотря на возможность, в интерфейсе KGS НЕ РЕКОМЕНДУЕТСЯ использовать кириллицу при наименовании объектов и сущностей, поскольку эти наименования частично используются в отчетах, поступающих от производителей чипов и приемников, которые могут быть расположены в другой стране. Кроме того, кириллица занимает больший объем данных в системе и, таким образом, снижает допустимое количество символов при вводе. Если ввести значение, большее чем позволено в БД, то появится ошибка, т.е. система KGS не позволит оператору этого сделать.

Вводя имена файлов (особенно при экспорте-импорте данных), следует учитывать регистр файла: в ОС семейства Linux *file_ name* и *File_ Name* это два разных имени.

Перейти к Содержанию...

3.2. Настроечные параметры KGS

Для каждого из Ресурсов, независимо от их типа, в системе может быть сохранено произвольное количество настроечных параметров типа строка или число.

Параметр может отсутствовать в справочнике, в этом случае считается, что поведение системы соответствует случаю, когда он присутствует со значением, которое указано как значение по умолчанию.

Все поддерживаемые настроечные параметры для текущего наполнения Системы, а также их предназначение приведены в документе "Руководство администратора" (доступ предоставляется по запросу).

Для настройки параметров необходимо:

1. В KMI_CONSOLE перейдите в **Сервис и настройки -> Конфигурация -> Изменение параметра** и выберите соответствующий *Тип ресурса*.
2. На экране отобразится таблица параметров данного ресурса.
3. Введите идентификатор параметра, который нужно отредактировать.
4. Введите новое значение параметра, нажмите Enter.

Перейти к Содержанию...

4. Работа с программой

4.1. Ограничения

4.1.1. Разрешенные символы

1. При работе в KMI_CONSOLE, во всех запросах пользовательского ввода (**кроме создания /редактирования сущностей** - есть нюансы, которые описаны ниже), разрешены: **a-z A-Z 0-9 - _ . , @ ( ) [ ]** и **пробел**.
2. В названиях сущностей / именах файлов (при вводе пользователем):
    a. Запрещены следующие символы: **^ @ * & + = / ; : **
    b. Нельзя создавать объекты, начинающиеся на **.** (начинающиеся на точку), в остальных случаях символ **.** (точка) - разрешен.
3. Пробелы в именах файлов заменяются на подчёркивания с выводом сообщения вида:
File name 'some name#!%$' contains forbidden symbols. New name is 'some_name____'
4. Если введен неверный символ, то пользователю выводится сообщение с ошибкой:
Input contains invalid symbols. Please provide input again
5. В названиях сущностей и именах файлов рекомендуется использовать только большие и малые латинские буквы, цифры, подчеркивание "_" и дефис "-".
6. При экспорте-импорте данных следует учитывать регистр файла: в ОС семейства Linux *file_name* и *File_Name* это два разных имени.

4.1.2. PGP-шифрование импортируемых файлов

При работе с WF **Работа с ключами OTP/прошивки** -> **Импорт ключей OTP (устаревшие STB)**, **Работа с ключами OTP/прошивки** -> **Добавление значений для ключей прошивки (импорт)** и **Интеграция сторонних систем** -> **Шифрование SSL-сертификатов** система KGS выполняет принудительную расшифровку импортируемых файлов всеми private PGP-ключами всех пользователей, которые занесены в базу данных KGS. Принудительная расшифровка выполняется независимо от расширения имени файла. Если импортируемый файл не зашифрован или требуемый ключ не найден, то система выдаст ошибку, а WF будет прервано.

В остальных случаях файлы, которые планируется импортировать в KGS, могут быть как шифрованы PGP-ключом, так и не шифрованы им: система определяет необходимость расшифровки по расширению имени файла.

4.2. Запуск программы

Управление системой KGS осуществляется с консоли (KVM), расположенной в закрытой комнате с ограниченным доступом.

4.2.1. Автоматический запуск

Для запуска программы необходимо:

1. Открыть консоль (KVM).
2. Пройти авторизацию, введя имя пользователя и пароль, выданные администратором системы.

После запуска KMI_CONSOLE откроется главное меню программы.

4.2.2. Запуск консоли вручную

Если не настроен автоматический запуск KMI_CONSOLE, то для запуска программы необходимо:

1. Открыть консоль (KVM).
2. Пройти авторизацию, введя имя пользователя и пароль, выданные администратором системы.
3. Выполнить команду:
    a. для запуска консоли на русском языке:

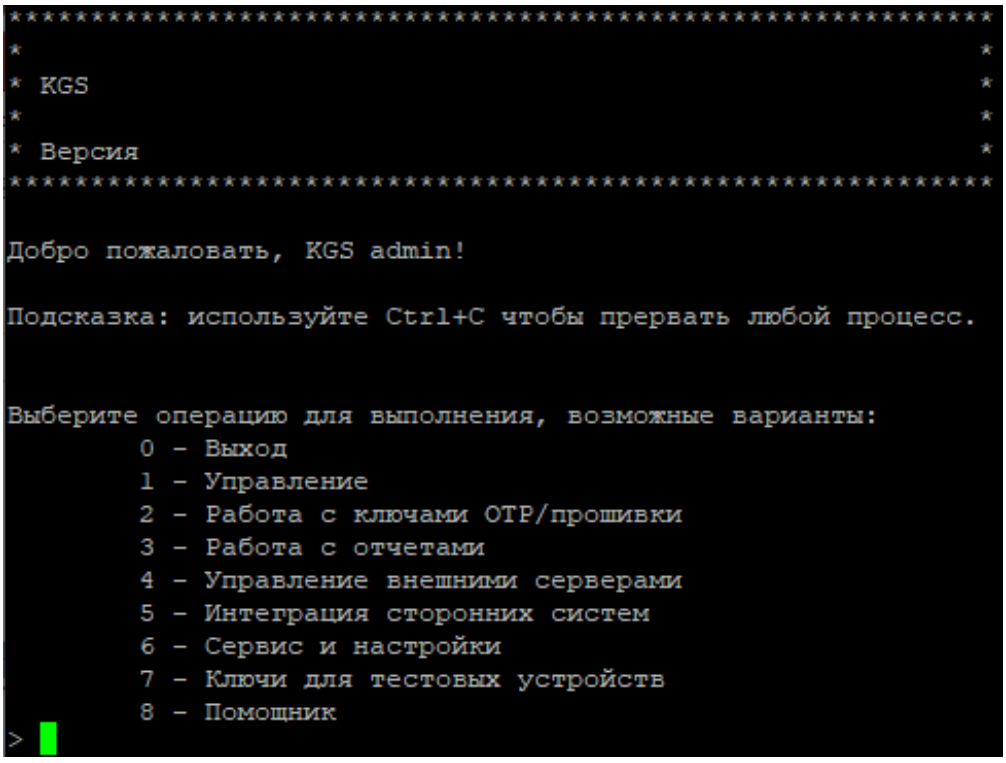
```
python3 /opt/kmi/console/kmi_console.py --lang=rus
```

    b. для запуска на английском языке:

```
python3 /opt/kmi/console/kmi_console.py --lang=eng
```

По умолчанию используется английский язык. Т.е. если не указать параметр *--land=<rus/eng>*, то будет запущена консоль на английском языке.

4.3. Главное меню



Главное меню программы содержит следующие пункты:

1. **Управление**.
   Операции управления (добавление/редактирование/удаление Операторов, Производителей, STB Моделей и т.д.).
2. **Работа с ключами OTP/прошивки**.
3. **Работа с отчетами**.

4. **Управление внешними серверами**.
5. **Интеграция сторонних систем**.
6. **Сервис и настройки**.
   Данный пункт главного меню должен быть доступен только пользователям с правами администратора.
7. **Ключи для тестовых устройств**.
8. **Помощник**.

Выбор пункта меню осуществляется нажатием соответствующей цифры и ввода (Enter). Выход из дочерних меню / рабочих процессов (workflows) в главное меню осуществляется выбором пункта **Выход** (клавиша **0**), выход из главного меню (завершение работы) программы - выбором пункта **Выход** и подтверждением операции (клавиша "**Y**"). Выход из главного меню приводит к автоматическому завершению работы с системой.

Прерывание (отмена) операции осуществляется нажатием комбинации клавиш **Ctrl+ C**.

4.3.1. Дерево меню

Меню структурировано следующим образом:

1. Управление
   a. Выход
   b. Операторы
      i. Выход
      ii. Получение списка сущностей Операторы
      iii. Добавление сущности Оператор
      iv. Изменение сущности Оператор
      v. Удаление сущности Оператор
   c. Внешние серверы
      i. Выход
      ii. Получение списка Внешних серверов
      iii. Добавление Внешнего сервера
      iv. Изменение Внешнего сервера
      v. Удаление Внешнего сервера
   d. Производители
      i. Выход
      ii. Получение списка сущностей Производители
      iii. Добавление сущности Производитель
      iv. Изменение сущности Производитель
      v. Удаление сущности Производитель
   e. STB Модели
      i. Выход
      ii. Получение списка STB Моделей
      iii. Добавление STB Модели
      iv. Изменение STB Модели
      v. Удаление STB Модели
      vi. Добавление связи STB Модели и Типа Партии
      vii. Удаление связи STB Модели и Типа Партии
   f. Поставщики
      i. Выход

Перейти к Содержанию...

4.4. Многопользовательский режим и блокировка Workflows

В KMI_CONSOLE используется многопользовательский режим: в консоли могут работать одновременно несколько пользователей (пользователи подключаются к консоли удаленно, например, по SSH). Если один пользователь работает в workflow, то указанный WF будет заблокирован для других пользователей. По окончании работы пользователя с WF блокировка снимается.

Если при попытке войти в меню Управление (вообще) либо запустить любое другое workflow 2 и более низкого уровня (например, войти в Работа с ключами OTP/прошивки и попытаться запустить любой пункт меню, кроме "Выход") пользователю выдается сообщение вида:

```
Error: Workflow #<workflow_id> is locked by user <username> at <date> <time>. Please, try later...
```

, то это означает, что Workflow в данный момент используется другим пользователем.

Рекомендации в случае блокировки WF:

1. Подождать некоторое время и повторить попытку доступа к WF. Время ожидания определяется субъективно: период исполнения WF может сильно различаться в зависимости от их типа и введенных данных (например, количества ключей в случае генерации).
2. Возможна ситуация, когда WF остается заблокированным в течение длительного времени. Возможные причины:
    a. WF еще не закончило выполнение операции (например, генерация огромного количества ключей).
    b. Пользователь после выполнения операции не вышел из workflow.
    c. Пользователь прервал выполнение workflow, нажав *Ctrl+Z*.
3. Последующие действия предпринимаются, если первый способ не сработал:
    a. Если есть возможность, связаться с пользователем, заблокировавшим WF, и решить проблему.

        > **ВАЖНО!** Принудительная разблокировка workflow (см. приведенные ниже способы, особенно с помощью перезапуска KMI_FW_DAL) может иметь негативные последствия. Например, одним из последствий может быть появление в БД данных, которые никак нельзя использовать.

    b. Обратиться к администратору KGS. Последний, используя WF "Разблокировать Workflow для пользователя", разблокирует WF.

        > Если администратор KGS прервет выполнение WF Разблокировать Workflow для пользователя, нажав *Ctrl+Z*, то данное workflow будет заблокировано для ВСЕХ пользователей (в т.ч. и для самого администратора KGS).
        >
        > Разблокировать WF "Разблокировать Workflow для пользователя" можно, только перезапустив службу KMI_FW_DAL.

    c. Если не удается решить проблему с помощью WF "Разблокировать Workflow для пользователя", администратор перезапускает службу KMI_FW_DAL.

Перезапуск KMI_FW_DAL выполняет только администратор KGS и **только в крайнем случае**.

Перейти к Содержанию...

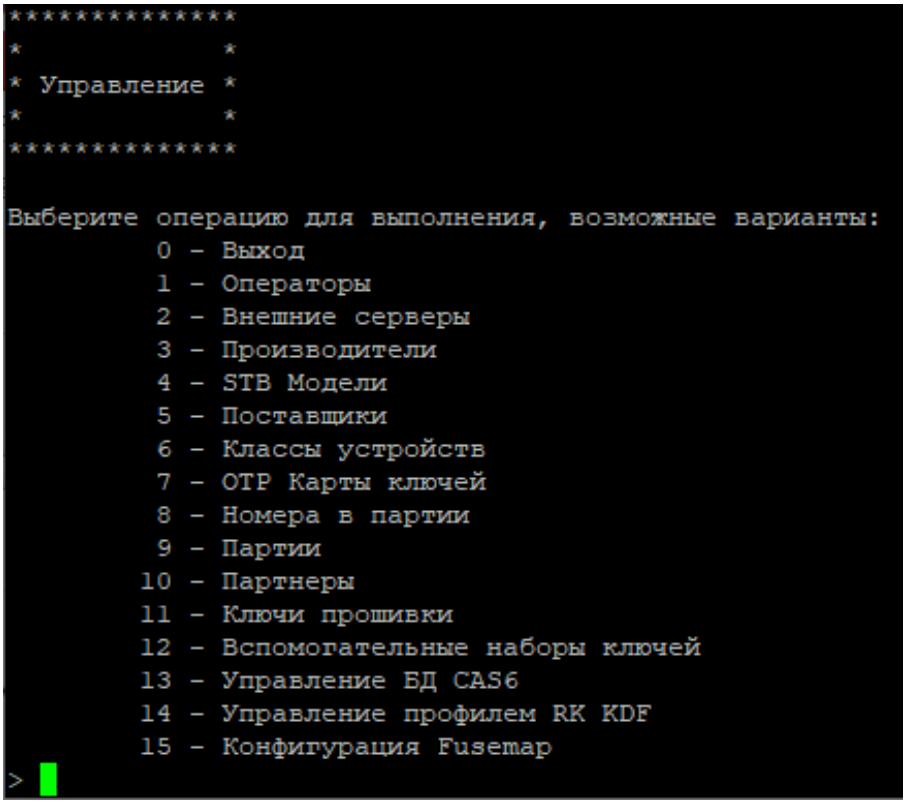
5. Описание workflows

В общем виде работа с workflow осуществляется следующим образом:

1. Выбрать workflow. Например, если требуется выполнить "Добавление сущности Оператор" (расположен в разделе "Управление", подраздел "Операторы" - см. "Дерево меню"), то Перейти в **Управление** -> **Операторы** -> **Добавление сущности Оператор**.
2. Следовать подсказкам workflow, отображаемым на экране.
3. В случае успешного выполнения - нажать Enter, чтобы вернуться в главное меню.

5.1. Управление

Для входа в меню управления необходимо в главном меню выбрать **Управление**.



Дерево меню для данного раздела:

1. Выход
2. Операторы
3. Внешние серверы
4. Производители
5. STB Модели
6. Поставщики
7. Классы устройств

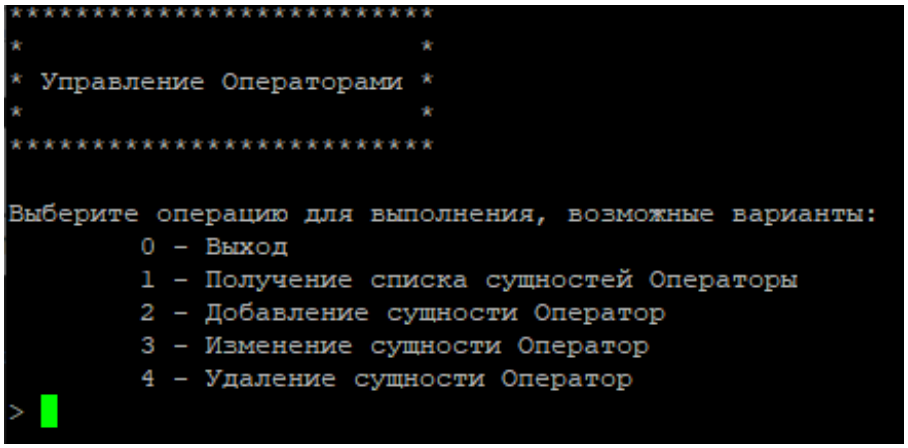
8. OTP Карты Ключей
9. Номера в партии
10. Партии
11. Партнеры
12. Ключи прошивки
13. Вспомогательные наборы ключей
14. Управление БД CAS
15. Управление профилем RK KDF
16. Конфигурация Fusemap

С помощью данного меню осуществляется управление и настройка данных в БД KGS (сведения об операторах, производителях, партиях ключей и т.д.).

Список возможных операций приведен в подразделах ниже.

С помощью меню "Управление" осуществляется ввод данных в базу данных KGS, а также установление зависимостей между этими данными. Настройка системы с помощью "Управление" осуществляется в первую очередь: при отсутствии определенных зависимостей между данными основные операции KGS (например, генерация и экспорт ключей, генерация отчетов) не будут выполняться или выполняться с ошибкой.

5.1.1. Операторы



Дерево меню для данного раздела:

1. Выход
2. Получение списка сущностей Операторы
3. Добавление сущности Оператор
4. Изменение сущности Оператор
5. Удаление сущности Оператор

5.1.1.1. Получение списка сущностей Операторы

Просмотр списка существующих операторов.

5.1.1.2. Добавление сущности Оператор

Добавление нового оператора в систему.

5.1.1.3. Изменение сущности Оператор

Изменение имени существующего оператора.

5.1.1.4. Удаление сущности Оператор

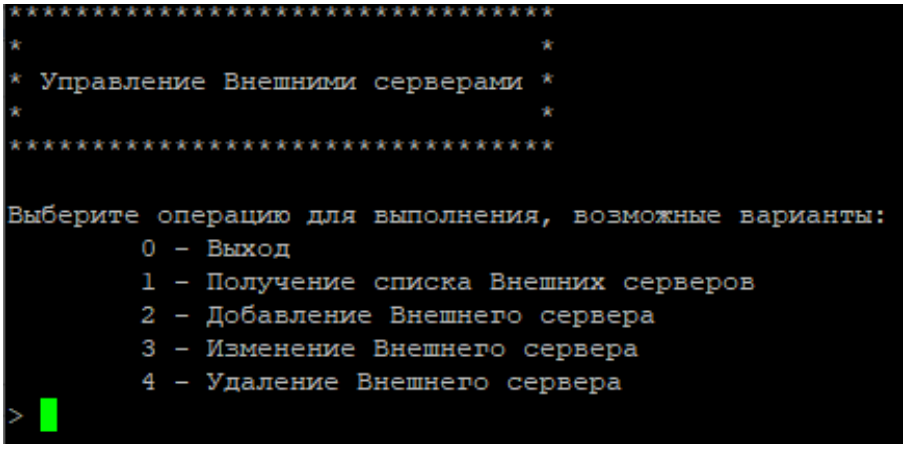
Удаление оператора из Системы.

Ограничения:

- Если для данного оператора был произведен хотя бы один приемник (и был обработан соответствующий отчет о производстве), удаление сущности Оператор будет невозможно.
- Если есть сущность "БД CAS", привязанная к выбранному оператору, то удаление оператора будет невозможно.

Перейти к Содержанию...

5.1.2. Внешние серверы



Дерево меню для данного раздела:

1. Выход
2. Просмотр списка Внешних серверов
3. Добавление Внешнего сервера
4. Изменение Внешнего сервера
5. Удаление Внешнего сервера

5.1.2.1. Просмотр списка Внешних серверов

Просмотр списка существующих внешних серверов с указанием их типа (Black Box, Sign Server, Generic).

5.1.2.2. Добавление Внешнего сервера

Добавление нового Внешнего сервера.

5.1.2.3. Изменение Внешнего сервера

Изменение имени существующего Внешнего сервера.

5.1.2.4. Удаление Внешнего сервера

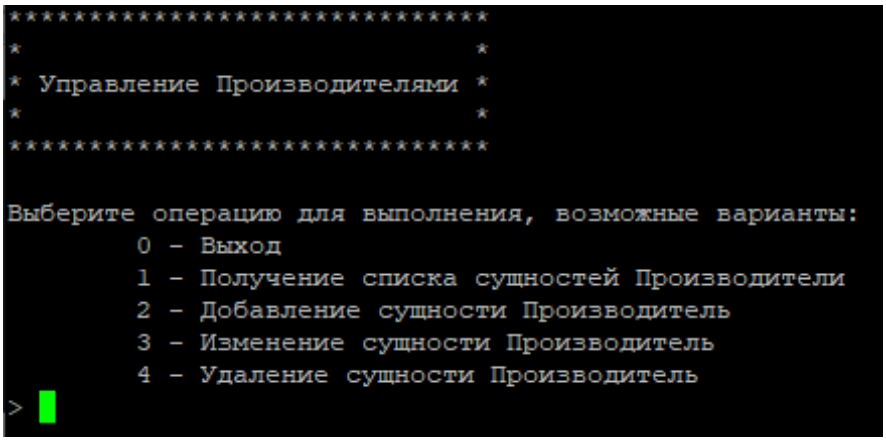
Удаление Внешнего сервера из Системы.

Ограничения:

- Удаление невозможно, если для выбранного Внешнего сервера был произведен хотя бы однократный экспорт ключей, либо есть привязка между Внешним сервером и каким-либо Видом Партии.

Перейти к Содержанию...

5.1.3. Производители



Дерево меню для данного раздела:

1. Выход
2. Получение списка сущностей Производители
3. Добавление сущности Производитель
4. Изменение сущности Производитель
5. Удаление сущности Производитель

5.1.3.1. Получение списка сущностей Производители

Просмотр списка существующих в системе Производителей.

5.1.3.2. Добавление сущности Производитель

Добавление нового Производителя в Систему.

5.1.3.3. Изменение сущности Производитель

Изменение имени выбранного Производителя.

5.1.3.4. Удаление сущности Производитель

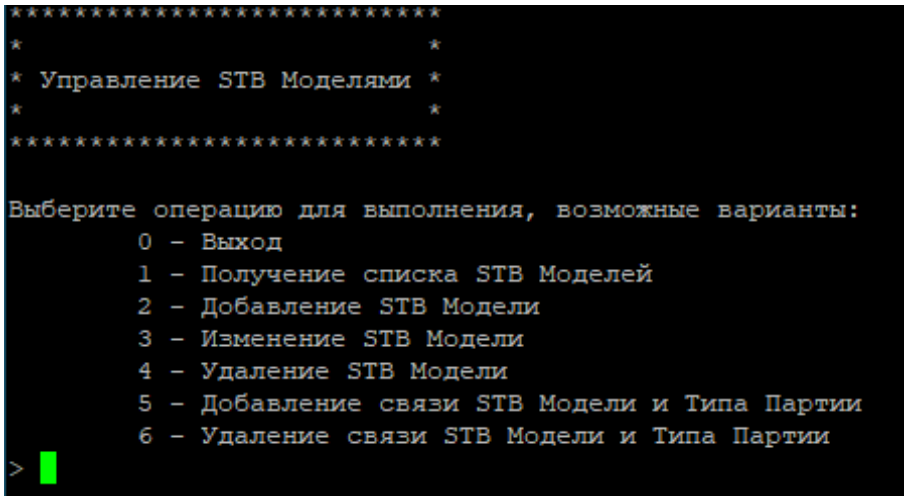
Удаление Производителя из Системы.

Ограничения:

- Удаление невозможно, если для выбранного Производителя существует хотя бы одна активная STB Модель.

Перейти к Содержанию...

5.1.4. STB Модели



Дерево меню для данного раздела:

1. Выход
2. Получение списка STB Моделей
3. Добавление STB Модели
4. Изменение STB Модели
5. Удаление STB Модели
6. Добавление связи STB Модели и Типа Партии
7. Удаление связи STB Модели и Типа Партии

Данное меню позволяет добавлять / изменять / удалять модели приемников цифрового телевидения (STB Моделей).

STB Модели должны быть привязаны к конкретному Производителю (Manufacturer Id).

5.1.4.1. Получение списка STB Моделей

Просмотр списка STB Моделей, привязанных к выбранному Производителю.

5.1.4.2. Добавление STB Модели

Добавление новой модели приемника (STB Модели) для выбранного Производителя.

Ограничения:

- одна модель (STB Модель) может быть привязана только к одному Производителю.

5.1.4.3. Изменение STB Модели

Изменение имени STB Модели.

5.1.4.4. Удаление STB Модели

Удаление модели приемника из Системы.

Особенности и ограничения:

- Удаление невозможно, если для выбранной модели хотя бы однократно была произведена загрузка и обработка отчета о производстве.
- Если STB Модель была привязана к Виду Партии, то при удалении модели приемника эта связь удаляется автоматически.

5.1.4.5. Добавление связи STB Модели и Типа Партии

Привязка STB Модели к Виду Партии.

Необходимые условия:

- Производитель.
- STB Модель.
- Класс устройств.
- Поставщик, привязанный к Классу устройств.
- Вид Партии, привязанный к Классу устройств.

> Особенности связи "STB Модель" <-> "Вид Партии": многие ко многим, без ограничений. Например, можно привязать одну и ту же модель STB (STB Модель) более чем 2 раза к разным Видам Партий разных Классов устройств, также можно привязать одну STB Модель к нескольким разным Видам Партий одного и того же Класса устройств.

5.1.4.6. Удаление связи STB Модели и Типа Партии

Отвязка STB Модели от Вида Партии.

Необходимые условия:

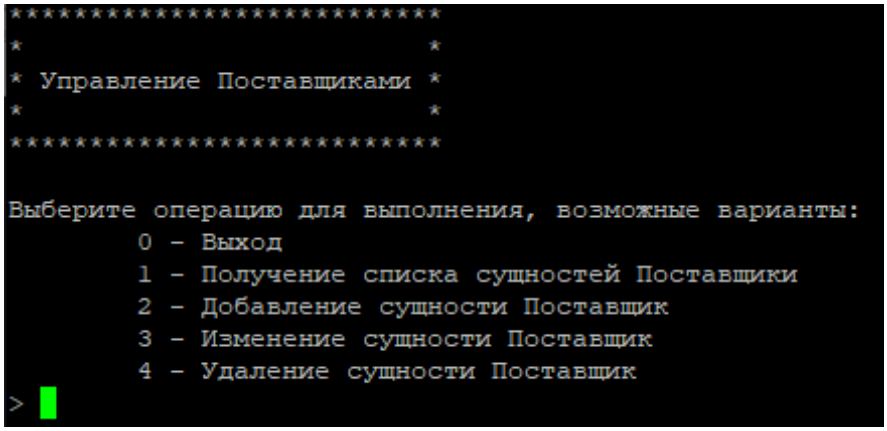
- STB Модель, привязанная к Виду Партии.
- Класс устройств.
- Поставщик, привязанный к Классу устройств.
- Вид Партии, привязанный к Классу устройств.

Ограничения:

- Если для выбранной пары "STB Модель" - "Вид Партии" уже загружены отчеты о производстве приемников, то удаление связи между ними невозможно.

Перейти к Содержанию...

5.1.5. Поставщики



Дерево меню для данного раздела:

1. Выход
2. Получение списка сущностей Поставщики
3. Добавление сущности Поставщик
4. Изменение сущности Поставщик
5. Удаление сущности Поставщик

5.1.5.1. Получение списка сущностей Поставщики

Просмотр списка существующих Поставщиков (vendors).

5.1.5.2. Добавление сущности Поставщик

Добавление Поставщика.

5.1.5.3. Изменение сущности Поставщик

Изменение имени существующего Поставщика в Системе.

5.1.5.4. Удаление сущности Поставщик

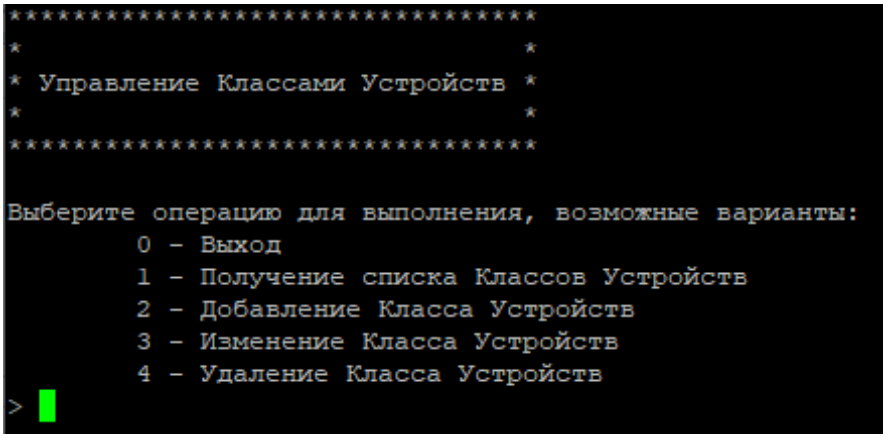
Удаление Поставщика из Системы.

Ограничения:

- Удаление невозможно, если для выбранного Поставщика существует хотя бы один актуальный Класс устройств.

Перейти к Содержанию...

5.1.6. Классы устройств



Дерево меню для данного раздела:

1. Выход
2. Получение списка Классов Устройств
3. Добавление Класса Устройств
4. Изменение Класса Устройств
5. Удаление Класса Устройств

Данное меню позволяет добавлять / изменять / удалять Классы устройств.

> Классы чипов должны быть привязаны к конкретному Поставщику.

5.1.6.1. Получение списка Классов Устройств

Просмотр списка Классов устройств. Отображается список существующих классов, их тип и соответствующих им поставщиков (графа *Поставщик*).

5.1.6.2. Добавление Класса Устройств

Добавление Класса устройств в Систему. Один Класс устройств может соответствовать нескольким Поставщикам.

5.1.6.3. Изменение Класса Устройств

Изменение имени Класса устройств.

5.1.6.4. Удаление Класса Устройств

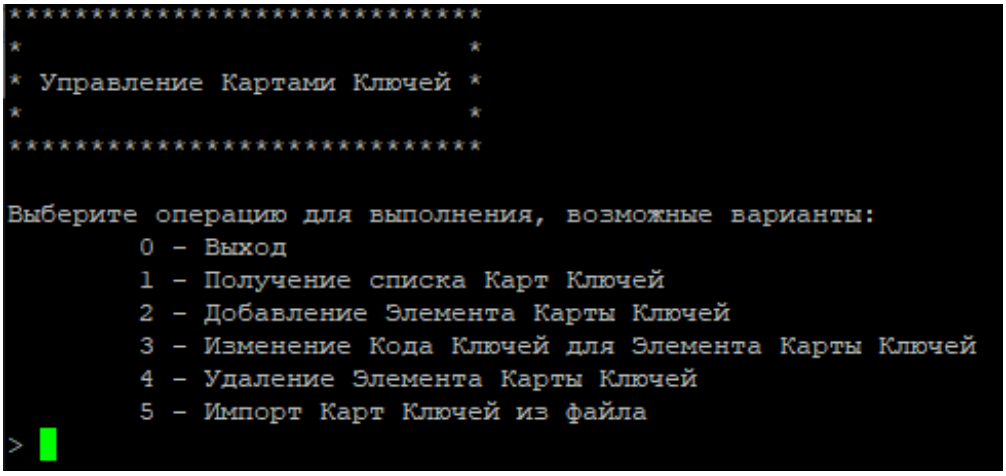
Удаление Класса устройств из Системы.

Ограничения:

- Удаление невозможно, если для выбранного типа чипов есть актуальная Карта Ключей, Вид Партии или Номер Партии.

Перейти к Содержанию...

5.1.7. OTP Карты Ключей



Дерево меню для данного раздела:

1. Выход
2. Получение списка Карт Ключей
3. Добавление Элемента Карты Ключей
4. Изменение Кода Ключей для Элемента Карты Ключей
5. Удаление Элемента Карты Ключей
6. Импорт Карт Ключей из файла

Данное меню позволяет создавать/удалять/просматривать OTP Карты ключей, а также редактировать названия ключей.

5.1.7.1. Получение списка Карт Ключей

Просмотр списка Карт Ключей.

Особенности отображения данных:

- Поля '*Прошивка*' и '*Характеристики*' заполняются только для Ключей прошивки. В случае root key ставится прочерк "-".
- Поле '*Характеристики*' будет заполнено только в том случае, если выполнена привязка Ключа прошивки к OTP Карте Ключей.
- *Прошивка* - флаг, определяющий, нужно ли зашить Ключ прошивки либо его часть в OTP (=Yes).
- *Характеристики* - параметры ключа прошивки, выгружаемого при экспорте в OTP.

5.1.7.2. Добавление Элемента Карты Ключей

Добавление Карты Ключей в Систему.

Необходимые условия:

- Наличие хотя бы одного Поставщика (см. Добавление сущности Поставщик).
- Наличие Класса устройств, привязанного к Поставщику (см. Добавление Класса Устройств).

5.1.7.3. Изменение Кода Ключей для Элемента Карты Ключей

Изменение названия ключей в Карте Ключей.

5.1.7.4. Удаление Элемента Карты Ключей

Удаление ключей из выбранной Карты Ключей.

Ограничения:

- Изменение карты ключей станет невозможно после того, как будет проведена первичная генерация ключей.

5.1.7.5. Импорт Карт Ключей из файла

Система осуществляет импорт файла с картой OTP-ключей с FTP-сервера, проверку формата и (в случае успеха) сохранение значения в БД для выбранного Класса устройств.

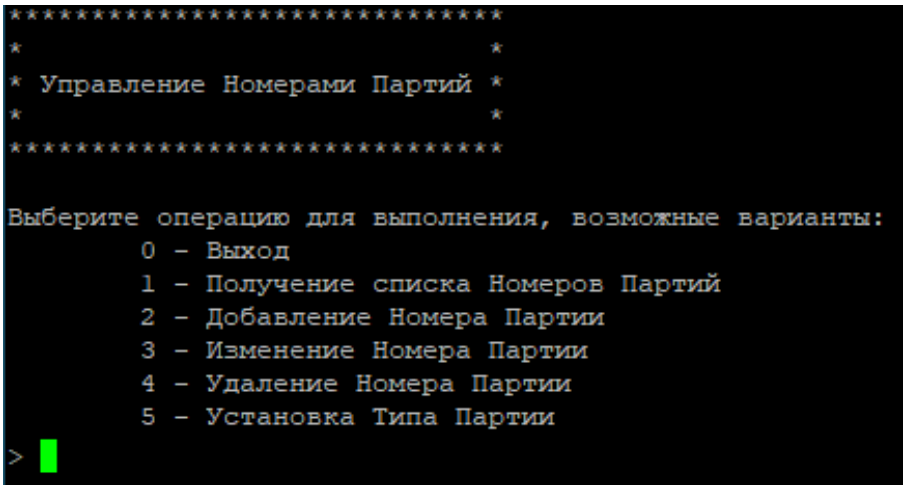
Файл импортируется из папки *in* **текущего** пользователя на FTP-сервере.

Особенности:

- При повторном импорте уже имеющиеся ключи в карте будут проигнорированы по индексу с соответствующим сообщением.
- Соответственно, импортировать карту ключей можно и по частям (например, оставить в файле только откорректированные строки, вызвавшие ошибку в предыдущий раз).

Перейти к Содержанию...

5.1.8. Номера в партии



Дерево меню для данного раздела:

1. Выход
2. Получение списка Номеров Партий
3. Добавление Номера Партии
4. Изменение Номера Партии
5. Удаление Номера Партии
6. Установка Типа Партии
7. Импорт Конфигурации Fusemap GS2

8. Экспорт Конфигурации Fusemap GS2

Данное меню позволяет добавлять / изменять / удалять Номера Партий (Part Numbers).

К Номеру Партии должен быть привязан Вид Партии. Сами же Номера Партий должны быть привязаны к конкретному Классу устройств.

5.1.8.1. Получение списка Номеров Партий

Просмотр списка Номеров Партий. В таблице приводятся Номера Партий + значения Видов Партии (+ идентификатор вида партии (в десятичном виде, в скобках)), привязанные к данному Номеру Партии + Описание конфигурации Fusemap, слинкованной с Номером Партии, + признак SRISC/SCEMU Конфигурации Fusemap.

5.1.8.2. Добавление Номера Партии

Добавление Номера Партии в Систему.

Особенности:

- Номер Партии должен быть привязан к Виду Партии. При отсутствии Вида Партии операция привязки проводится позже. Подробное описание приведено в Установка Типа Партии.

5.1.8.3. Изменение Номера Партии

Изменение имени сущности Номер Партии.

5.1.8.4. Удаление Номера Партии

Удаление Номера Партии из Системы.

5.1.8.5. Установка Типа Партии

Привязка Вида Партии к Номеру Партии. Одно значение Вида Партии может быть привязано к нескольким Номерам Партий.

5.1.8.6. Импорт Конфигурации Fusemap GS2

Система осуществляет импорт Конфигурации Fusemap из внешних источников, ввод значения ovdf3-context и привязку этих данных к выбранному Номеру Партии.

Если в базе данных KGS уже имеются данные по Конфигурации Fusemap и ovdf3-context для выбранного Номера Партии, то KGS осуществляет перезапись данных (старые данные заменяются импортируемыми).

Конфигурация Fusemap необходима для персонализации чипов. По сути, Конфигурация Fusemap это набор бит, который записывается в OTP вместе с OTP root-ключами в процессе персонализации и влияет на управление различными аппаратными блоками и функциональностью чипа. Примером таких бит могут быть индексы производных ключей от корневого ключа. Некоторые значения из Конфигурации Fusemap влияют на формирование производных ключей в сценариях с KDF.

Конфигурации Fusemap для SRISC и для SCEMU различны, так как отличается список конфигурационных бит, и представляют собой 2 **разных** файла.

Импортируемый файл с Конфигурацией Fusemap должен быть предварительно подготовлен пользователем в соответствующем формате, зашифрован PGP-ключом (private часть ключа должна храниться в системе KGS) и загружен на FTP-сервер, в папку *in* пользователя. После окончания работы файл удаляется с FTP-сервера.

5.1.8.7. Экспорт Конфигурации Fusemap GS2

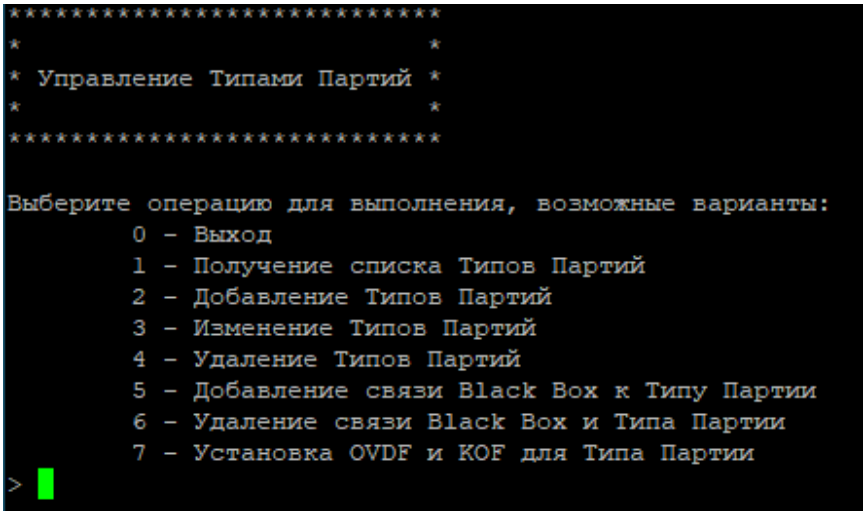
Система осуществляет экспорт файлов с Конфигурацией Fusemap и ovdf3-context, соответствующих выбранному Номеру Партии. Данные экспортируются в виде файлов на FTP-сервер в папку *out*, для текущего (осуществляющего операцию) пользователя либо пользователя, привязанного к выбранному Поставщику. При экспорте данные шифруются PGP-ключом пользователя, для которого осуществляется экспорт.

⚠ Конфигурация Fusemap необходима для персонализации чипов.

Конфигурацию Fusemap нельзя сгенерировать в системе KGS: файлы с Fusemap конфигурацией генерируются вне системы и впоследствии импортируются (см. Импорт Конфигурации Fusemap GS2). Т. е. при персонализации чипов данные по Fusemap конфигурации уже имеются у Заказчика. Значение ovdf3-context представляет собой hex string (8 символов) и используется при настройке OVDF для Вида Партии (см. Установка OVDF и KOF для Типа Партии). В связи с этим предполагается, что экспорт выполняется только по мере необходимости (например, при потере данных).

Перейти к Содержанию...

5.1.9. Партии



Дерево меню для данного раздела:

1. Выход
2. Получение списка Типов Партий
3. Добавление Типов Партий
4. Изменение Типов Партий
5. Удаление Типов Партий

6. Добавление связи Black Box к Типу Партии
7. Удаление связи Black Box и Типа Партии
8. Установка OVDF и KOF для Типа Партии

Данное меню позволяет добавлять / изменять / удалять Типы Партий (также обозначаются как Виды Партий).

> Вид Партии должен быть привязан к Классу устройств. Для выполнения основных операций также необходимо привязать Вид Партии к Номеру Партии, Black Box.

5.1.9.1. Получение списка Типов Партий

Просмотр списка Видов Партий.

Содержимое таблицы с параметрами зависит от того, был ли выбран (пользователем) или нет Класс Устройства.

5.1.9.2. Добавление Типов Партий

Добавление Вида Партии в Систему.

Особенности:

- Статус 'тестовый' для Вида Партии накладывает ограничения на работу с ключами и устройствами (см. **тестовые ключи**). Данный статус также **нельзя изменить**.

5.1.9.3. Изменение Типов Партий

Изменение имени Вида Партии и (при выполнении определенных условий) extended info.

5.1.9.4. Удаление Типов Партий

Удаление Вида Партии из Системы.

Ограничения:

- Если к "Поставщику - Классу устройств" не привязан ни один Вид Партии, то операция прервется сообщением об ошибке.
- Если для данного Вида Партии был сгенерирован вектор инициализации (см. Подготовка DRM ключей) либо к нему привязан хотя бы один LE-набор ключей (см. Добавление наборов общих вспомогательных ключей, с типом "Link Encryption"), либо сгенерированы общие root-ключи для Вида Партии, либо создано описание хоть одного ключа прошивки для Вида Партии, то операция также прервется сообщением об ошибке.

5.1.9.5. Добавление связи Black Box к Типу Партии

Привязка Black Box к Виду Партии. Одно значение Black Box может быть привязано к нескольким Видам Партий.

5.1.9.6. Удаление связи Black Box и Типа Партии

Отвязка Black Box от Вида Партии.

5.1.9.7. Установка OVDF и KOF для Типа Партии

Настройка OVDF и KOF для Вида Партии.

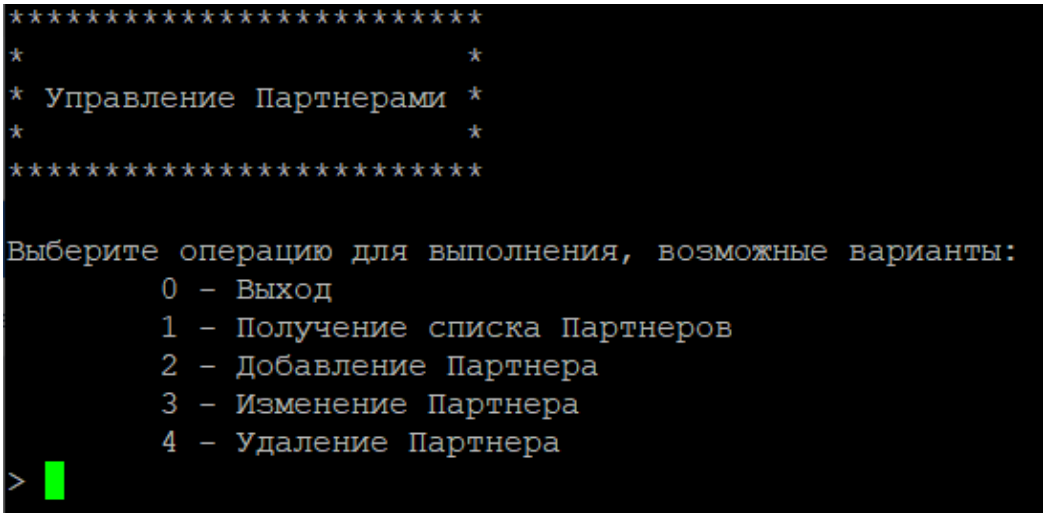
Необходимые условия:

- Класс устройств.
- Поставщик, привязанный к Классу устройств.
- Вид Партии, привязанный к Классу устройств.
- Карта Ключей, привязанная к Классу устройств и содержащая хотя бы один ключ, помеченный как obfuscation data.

> ⚠ Последнее условие не влияет на проведение процедуры, но если настроена обфускация и отсутствуют obfuscation data, то генерация OTP ключей завершится ошибкой.

Перейти к Содержанию...

5.1.10. Партнеры



Дерево меню для данного раздела:

1. Выход
2. Получение списка Партнеров
3. Добавление Партнера
4. Изменение Партнера
5. Удаление Партнера

5.1.10.1. Получение списка Партнеров

Просмотр списка Партнеров и их параметров.

5.1.10.2. Добавление Партнера

Добавление Партнера в Систему.

5.1.10.3. Изменение Партнера

Изменение имени Партнера.

5.1.10.4. Удаление Партнера

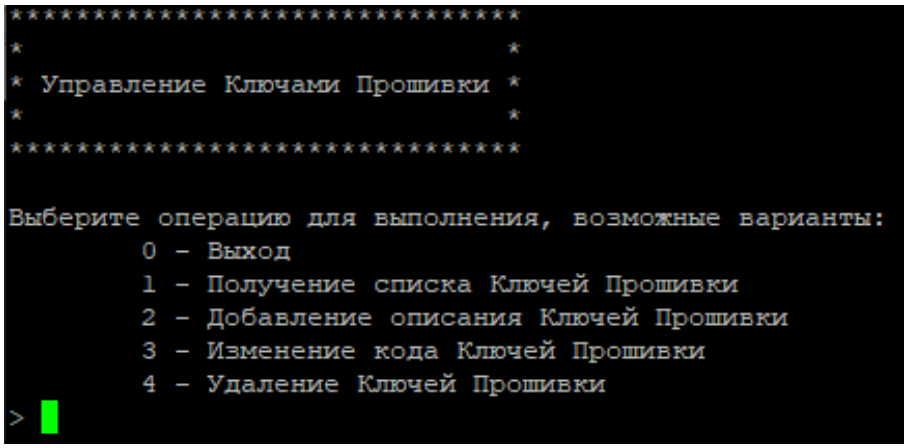
Удаление Партнера из Системы.

Ограничения:

- Если для выбранного Партнера существует вектор инициализации (initVector), то удаление невозможно. Вектор инициализации генерируется при подготовке DRM-ключей (см. Подготовка DRM ключей). Узнать о наличии вектора инициализации можно, просмотрев список Партнеров.
- Если к выбранному Партнеру прилинкован Пользователь, то удаление невозможно.

Перейти к Содержанию...

5.1.11. Ключи прошивки



Дерево меню для данного раздела:

1. Выход
2. Получение списка Ключей Прошивки
3. Добавление описания Ключей Прошивки
4. Изменение кода Ключей Прошивки
5. Удаление Ключей Прошивки

5.1.11.1. Получение списка Ключей Прошивки

Просмотр списка Ключей Прошивки, соответствующих введенным параметрам.

Для отображения данных по ключам необходимо указывать только те параметры (Класс устройств обязательно, Вид Партии и STB Модель опционально), к которым была выполнена привязка описаний ключей (см. Добавление описания Ключей Прошивки).

Таким образом, если Ключи Прошивки привязаны к Класс устройств + Вид Партии + STB Модель, то при выборе, например, только "Класс устройств" либо "Класс устройств + Вид Партии" процедура завершится **ошибкой**.

5.1.11.2. Добавление описания Ключей Прошивки

Выполняется создание описаний Ключей Прошивки, при этом ключи прошивки могут быть описаны в любой момент жизненного цикла класса устройств/партии. Если предполагается, что некоторые ключи прошивки могут персонализироваться, то необходимо карты таких ключей прошивки описать сначала в OTP Карте ключей устройства и после добавить их описание в карте ключей прошивки, указав ссылку на описание в OTP Карте ключей, выбрав ключ из списка существующих ключей, привязанных к заданной партии (Виду Партии). Если необходимо описать ключи, привязанные к STB Моделям, то до описания карты необходимо добавить в БД модели STB и связать их с Видом Партии.

5.1.11.3. Изменение кода Ключей Прошивки

Изменение имени Ключа Прошивки.

5.1.11.4. Удаление Ключей Прошивки

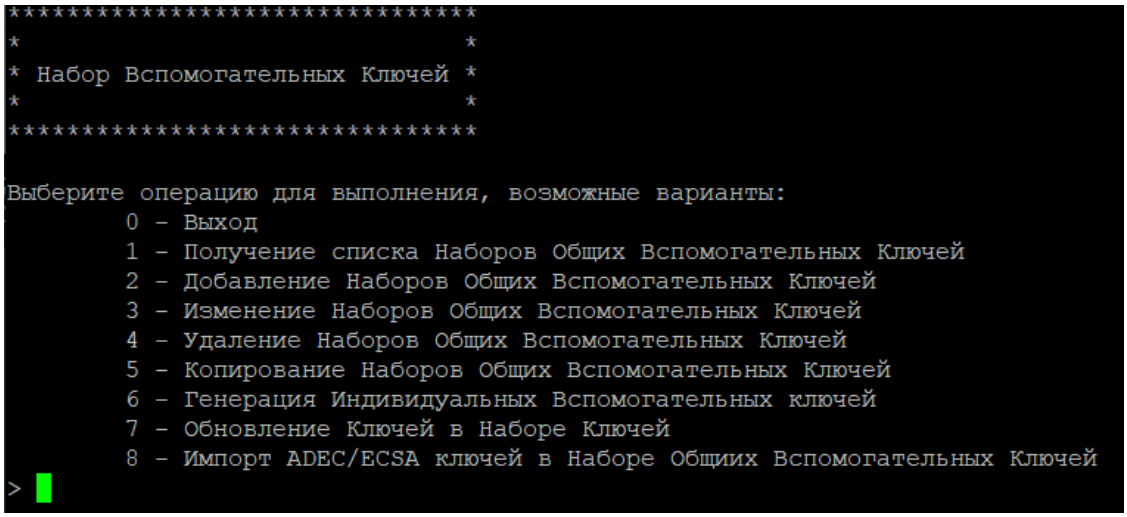
Удаление Ключа Прошивки из Системы.

Ограничения:

- При наличии связи профиля RK KDF с fwky_id (идентификатором Ключа Прошивки), в момент удаления Ключа Прошивки эта связь проверяется. Если связь есть, то удаление запрещено (в этом случае пользователю сначала надо удалить профиль RK KDF, а затем можно удалить сам Ключ Прошивки).
- Удаление невозможно, если ключ прошивки привязан к Виду Партии и установлена ссылка на таблицу KMI_DEVICE_KEYMAPS, т.е. если ключ выгружается и персонализируется через Black Box.

Перейти к Содержанию...

5.1.12. Вспомогательные наборы ключей



Дерево меню для данного раздела:

1. Выход
2. Получение списка Наборов Общих Вспомогательных Ключей
3. Добавление Наборов Общих Вспомогательных Ключей
4. Изменение Наборов Общих Вспомогательных Ключей
5. Удаление Наборов Общих Вспомогательных Ключей
6. Копирование Наборов Общих Вспомогательных Ключей

7. Генерация Индивидуальных Вспомогательных Ключей
8. Обновление Ключей в Наборе Ключей
9. Импорт ADEC/ECSA ключей в Наборе Общих Вспомогательных Ключей

Данное меню позволяет управлять Наборами Вспомогательных Ключей (Auxiliary (Aux) Keysets): просматривать / добавлять / редактировать / удалять / копировать Наборы Общих Вспомогательных Ключей (Common Auxiliary (Aux) Keysets), генерировать Индивидуальные Вспомогательные Ключи, обновлять ключи в наборах, а также импортировать ADEC/ECSA ключи.

5.1.12.1. Получение списка Наборов Общих Вспомогательных Ключей

Просмотр списка актуальных Наборов Общих Вспомогательных Ключей.

Поле "Тип Партии":

- Если набор не привязан к Виду Партии, то в столбце "Тип Партии" ячейка остается пустой (с прочерком).
- Если набор привязан к Виду Партии, то в столбце указывается имя Вида Партии и (в скобках) его идентификатор.

Поле "Источник" - источник значения Набора ключей:

- Generated
- Imported
- Cloned - для случаев, если набор склонирован без изменений (см. Копирование Наборов Общих Вспомогательных Ключей).
- Updated - для случаев замены одного или нескольких значений ключей в указанном наборе (см. Обновление Ключей в Наборе Ключей). При этом в поле "Копия" отображается идентификатор набора, с которого произведено обновление со сменой ключей.

Поле "Копия":

- в поле через запятую отображаются значения всех идентификаторов (по возрастанию) для наборов, которые являются копиями друг друга, т.е. у которых одинаковые ключи, включая исходный набор (см. Копирование Наборов Общих Вспомогательных Ключей). Наборы, помеченные как удаленные, не отображаются.
- поле будет пустым, если ключи набора сгенерированы случайным образом (т.е. не скопированы с другого набора или не были скопированы в другой набор).

5.1.12.2. Добавление Наборов Общих Вспомогательных Ключей

Создание Набора общих Вспомогательных Ключей.

5.1.12.3. Изменение Наборов Общих Вспомогательных Ключей

Переименование пользовательского имени набора ключей. Остальные атрибуты набора не меняются.

Переименовывать набор разрешается в любой момент, одинаковые имена наборов в рамках одного и того же Вида Партии запрещены.

5.1.12.4. Удаление Наборов Общих Вспомогательных Ключей

Удаление Набора Вспомогательных Ключей.

Ограничения:

- Если к Виду Партии не привязан ни один Набор Вспомогательных Ключей (который имеет тип отличный от ADEC/ECSA), то операция прервется сообщением об ошибке.
- Если выбранный Набор Вспомогательных Ключей был использован в экспорте (см. Экспорт общих вспомогательных ключей), то операция также прервется сообщением об ошибке.

5.1.12.5. Копирование Наборов Общих Вспомогательных Ключей

Копирование наборов ключей между разными Видами Партий.

Ограничения:

- Разрешено копировать только Общие Вспомогательные Ключи с типами CK_IPKeys и CK_IPKeys_Secure.
- Запрещено копировать наборы ключей с типом CK_IPKeys_Secure в другие наборы с типом CK_IPKeys.
- Запрещено копировать наборы из прод. Вида Партии в наборы test Вида Партии.

5.1.12.6. Генерация Индивидуальных Вспомогательных Ключей

Генерация новых индивидуальных Вспомогательных Ключей (Pairing Keys, PK) либо обновление существующих PK с привязкой к устройствам.

Список пользователей, которые могут быть получателями данных, определяется как текущий пользователь + внешние пользователи, привязанные к любой внешней сущности **кроме** Поставщика.

5.1.12.7. Обновление Ключей в Наборе Ключей

С помощью данного workflow выполняется замена одного или нескольких значений ключей в указанном наборе.

Ограничения и допущения:

- В процессе создается копия набора и его ключей, после чего в этой копии заменяются указанные значения, исходный набор, с которого сделана копия, запоминается в БД.
- Применимо только для ключей наборов с типами ADEC/ECSA.

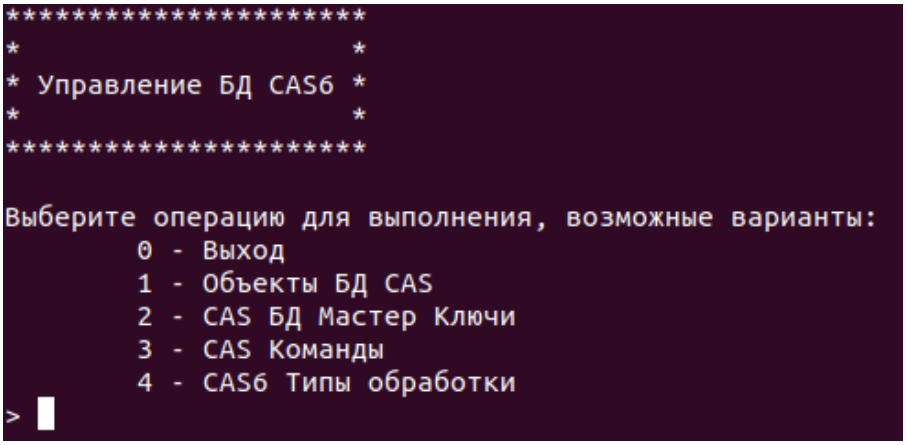
5.1.12.8. Импорт ADEC/ECSA ключей в Наборе Общих Вспомогательных Ключей

С помощью данного workflow осуществляется импорт (с FTP) значений ключей в Набор Общих Вспомогательных Ключей.

Импорт осуществляется с FTP-сервера, из папки *in* текущего (осуществляющего операцию) пользователя.

Перейти к Содержанию...

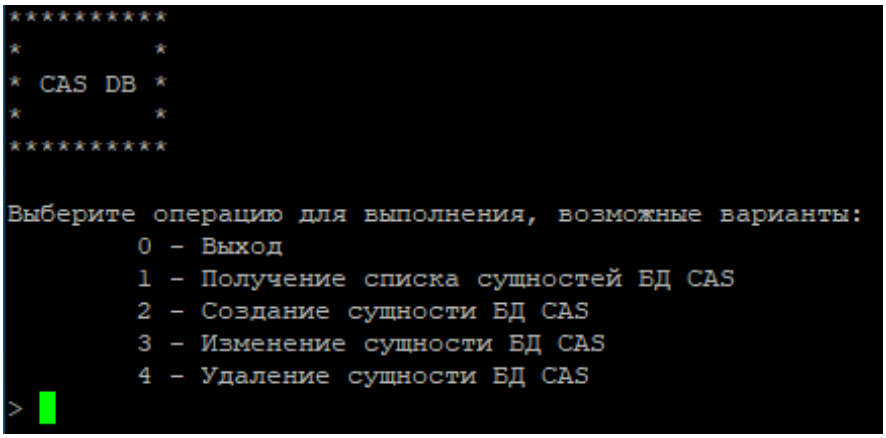
5.1.13. Управление БД CAS



Дерево меню для данного раздела:

1. Выход
2. Объекты БД CAS
3. CAS БД Мастер Ключи
4. CAS Команды
5. CAS6 Типы обработки

5.1.13.1. Объекты БД CAS



Дерево меню для данного раздела:

1. Выход
2. Получение списка сущностей БД CAS
3. Создание сущности БД CAS
4. Изменение сущности БД CAS
5. Удаление сущности БД CAS

Данное меню позволяет управлять (просматривать/создавать/удалять/редактировать) сущностями "БД CAS".

5.1.13.1.1. Получение списка сущностей БД CAS

Просмотр списка существующих БД CAS и операторов, к которым они привязаны.

5.1.13.1.2. Создание сущности БД CAS

Добавление сущности БД CAS в Систему. При добавлении сущность "БД CAS" привязывается к Оператору.

5.1.13.1.3. Изменение сущности БД CAS

Изменение БД CAS (пользовательского имени базы).

Ограничения:

- Редактирование привязанного Оператора невозможно.
- При ошибочном выборе Оператора, пользователь должен будет удалить сущность БД CAS и создать новую с правильным Оператором. Такое действие разрешено до момента первого экспорта ключей БД CAS.

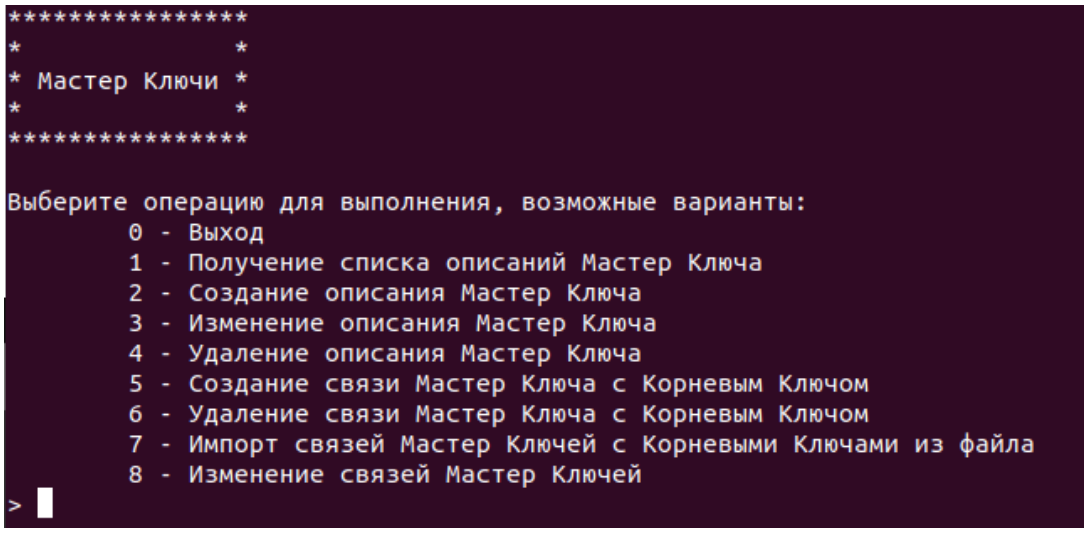
5.1.13.1.4. Удаление сущности БД CAS

Удаление БД CAS из Системы.

Ограничения:

- Если для БД CAS были успешно выгружены ключи, то операция прервется сообщением об ошибке.

5.1.13.2. CAS БД Мастер Ключи



Дерево меню для данного раздела:

1. Выход
2. Получение списка описаний Мастер Ключа
3. Создание описания Мастер Ключа
4. Изменение описания Мастер Ключа
5. Удаление описания Мастер Ключа
6. Создание связи Мастер Ключа с Корневым Ключом
7. Удаление связи Мастер Ключа с Корневым Ключом
8. Импорт связей Мастер Ключей с Корневыми Ключами из файла

9. Изменение связей Мастер Ключей

Данное меню позволяет управлять (создавать/удалять/просматривать) описания Мастер Ключей, редактировать названия ключей, а также добавлять и редактировать связи Мастер Ключей с Корневыми Ключами (в OTP Карте Ключей).

5.1.13.2.1. Получение списка описаний Мастер Ключа

Просмотр информации по Мастер Ключам и (опционально) экспорт файла, содержащего список Мастер Ключей и их связей с OTP-ключами, на FTP-сервер.

Экспортируемый файл загружается на FTP-сервер в папку *out* текущего (выполняющего операцию) пользователя. Файл шифрован одним или несколькими PGP-ключами пользователя, для которого осуществляется экспорт.

5.1.13.2.2. Создание описания Мастер Ключа

Добавление Мастер Ключа.

При создании описания Мастер ключа осуществляется его привязка к БД CAS.

5.1.13.2.3. Изменение описания Мастер Ключа

Изменение названия Мастер Ключа.

5.1.13.2.4. Удаление описания Мастер Ключа

Удаление описания Мастер Ключа.

Ограничения:

1. Удаление запрещено:
    a. только если уже был произведен успешный экспорт ключей базы данных CAS.
    b. если присутствует связь с OTP-ключами (хотя бы одним). Чтобы удалить описание МК, сначала следует удалить все связи (если допускается логикой, т.е. не было экспорта).

5.1.13.2.5. Создание связи Мастер Ключа с Корневым Ключом

Создание связи Мастер Ключа с Корневым Ключом.

> В случае ошибочного создания связи "Мастер Ключ - OTP Root Key", до момента генерации и экспорта ключей CAS6DB, пользователь должен будет удалить связь Мастер Ключа с OTP-ключом и создать её заново.

5.1.13.2.6. Удаление связи Мастер Ключа с Корневым Ключом

Удаление связи Мастер Ключа с Корневым Ключом.

Ограничения:

- Удаление связи запрещено, только если уже был произведен успешный экспорт ключей базы CAS.

5.1.13.2.7. Импорт связей Мастер Ключей с Корневыми Ключами из файла

Импорт (с FTP) связей Мастер Ключей с OTP-ключами.

Файл импортируется с FTP, из папки *in* **текущего** пользователя. Импортируемый файл шифрован PGP (PGP-ключ текущего пользователя, хранящийся в KGS, будет автоматически использоваться для расшифровки).

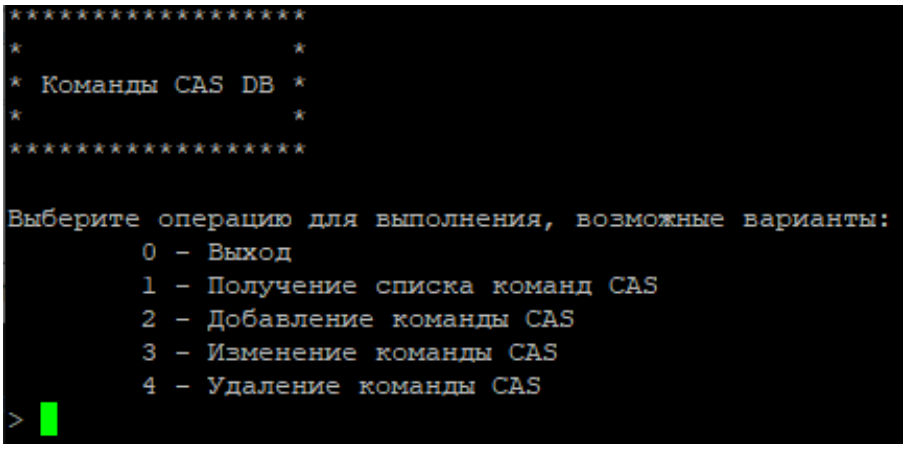
5.1.13.2.8. Изменение связей Мастер Ключей

Редактирование свойств связи отдельного выбранного Мастер ключа.

Редактирование доступно как до выполнения экспорта (WF 'Экспорт мастер ключей на CAS DB'), так и после выгрузки мастер ключей.

> Используется для упрощения работы и для снижения дублей CAS DB с Мастер ключами в KGS, появившихся из-за ошибок, внесенных при создании Мастер ключей и их связей с партиями.

5.1.13.3. CAS Команды



Дерево меню для данного раздела:

1. Выход
2. Получение списка команд CAS
3. Добавление команды CAS
4. Изменение команды CAS
5. Удаление команды CAS

Данное меню позволяет управлять (создавать/удалять/просматривать) CAS Команды - команды для БД CAS, которые используются при создании Мастер Ключей.

5.1.13.3.1. Получение списка команд CAS

Просмотр списка команд CAS. Отображаются все не удалённые (del_date = null) команды для БД CAS, сортировка выполнена по идентификатору команд (по возрастанию).

5.1.13.3.2. Добавление команды CAS

Добавление команды CAS.

5.1.13.3.3. Изменение команды CAS

Изменение имени команды CAS.

Ограничения:

1. Имя разрешено менять в любой момент.
2. Остальные свойства не редактируется: используется подход "удалить ошибочную - создать новую правильную".

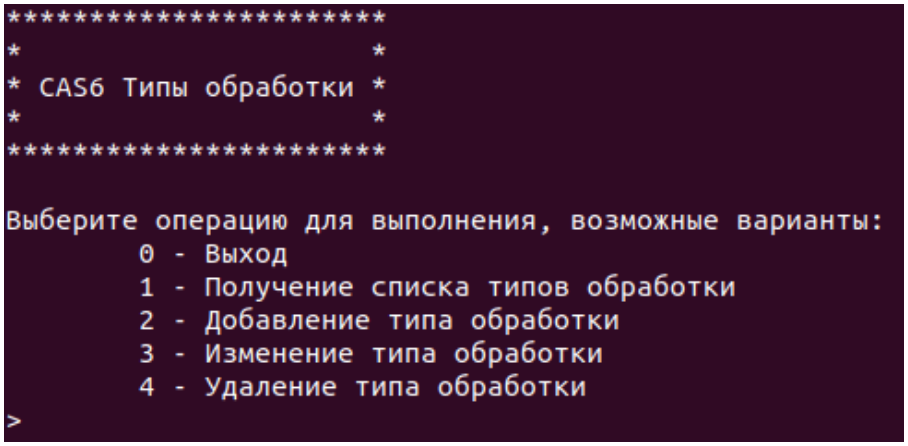
5.1.13.3.4. Удаление команды CAS

Удаление команды CAS из Системы.

Ограничения:

1. Удалять запись разрешено до того момента, пока не выгружена хоть одна БД CAS с Мастер Ключом, связанным с выбранной командой (с выбранным идентификатором удаляемой команды).

5.1.13.4. CAS6 Типы обработки



Дерево меню для данного раздела:

1. Выход
2. Получение списка типов обработки
3. Добавление типа обработки
4. Изменение типа обработки
5. Удаление типа обработки

5.1.13.4.1. Получение списка типов обработки

Просмотр списка типов операций обработки, для которых предназначены мастер ключи. Отображаются все не удалённые (del_date = null) операции для CAS6 DB, сортировка выполнена по идентификатору типа (по возрастанию).

5.1.13.4.2. Добавление типа обработки

Добавление команды CAS.

Ограничения:

1. Не могут существовать 2 записи, не удаленные логически, с одинаковыми наименованиями типа операции.
    a. Если запись удалена, то ее наименование не учитывается
2. Ограничение на допустимые символы аналогичны прочим WF.

5.1.13.4.3. Изменение типа обработки

Изменение имени (названия) типа обработки.

Ограничения:

1. Имя разрешено менять в любой момент.
2. Остальные свойства не редактируется: используется подход "удалить ошибочный - создать новый правильный".

5.1.13.4.4. Удаление типа обработки

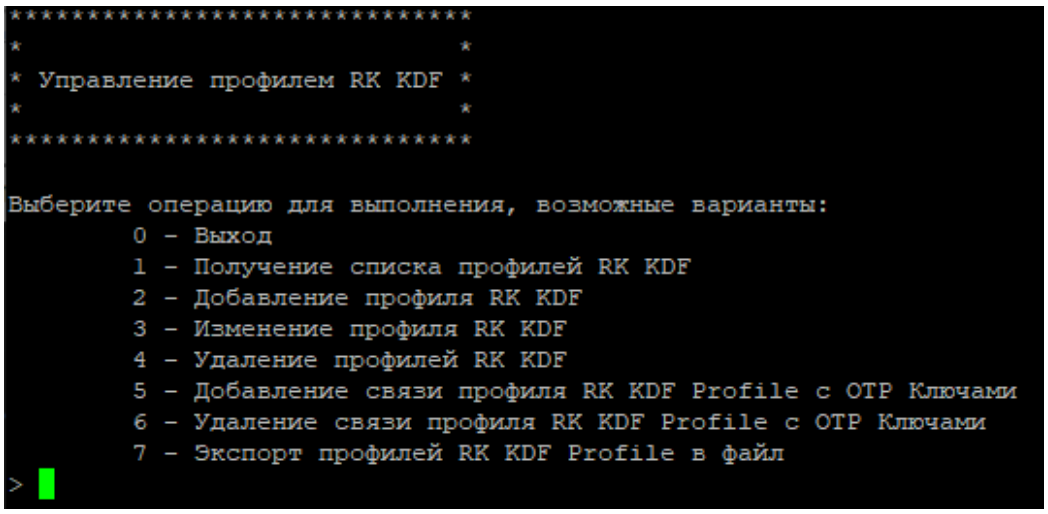
Удаление типа обработки из Системы.

Ограничения:

1. Удалять запись разрешено до того момента, пока не создана хоть одна запись с описанием Мастер Ключа, связанным с выбранным типом обработки (с выбранным идентификатором удаляемого типа).

Перейти к Содержанию...

5.1.14. Управление профилем RK KDF



Дерево меню для данного раздела:

1. Выход
2. Получение списка профилей RK KDF
3. Добавление профиля RK KDF
4. Изменение профиля RK KDF
5. Удаление профилей RK KDF
6. Добавление связи профиля RK KDF Profile с OTP Ключами
7. Удаление связи профиля RK KDF Profile с OTP Ключами

8. Экспорт профилей RK KDF Profile в файл

Данное меню позволяет управлять (создавать/редактировать/удалять/просматривать и т.п.) профилями RK KDF.

5.1.14.1. Получение списка профилей RK KDF

Просмотр списка существующих профилей RK KDF и их параметров.

5.1.14.2. Добавление профиля RK KDF

Добавление профиля RK KDF в Систему.

5.1.14.3. Изменение профиля RK KDF

Изменение имени и других параметров профиля RK KDF. **Если выбранный профиль не привязан к OTP ключу** (см. WF 'Добавление связи профиля RK KDF Profile с OTP Ключами'), то дополнительно можно изменить тип секретности профиля и производного ключа (secrecy).

Ограничения и допущения:

- Разрешено редактировать все параметры (кроме параметра *Секретность*) в любой момент времени.
- Параметр *Секретность* у выбранного профиля допускается редактировать до момента создания связи (линковки) этого профиля с любым из OTP-ключей.
- Шаблоны не используются, пользователь вводит данные вручную.

5.1.14.4. Удаление профилей RK KDF

Удаление профиля RK KDF из Системы.

Ограничения и допущения:

- Разрешено удалять профиль, связанный с OTP-ключом (каскадное удаление).
  - **НО**: если имеется связь хоть с одним Ключом Прошивки (т.е. если профиль RK KDF и OTP ключ использовались для генерации значения Ключа Прошивки (derived key)), то каскадное удаление профиля вместе со связью запрещено.
  - **НО**: если OTP-ключ связан с Мастер Ключом и профилем RK KDF, то каскадное удаление профиля вместе со связью запрещено.

    ⚠ Таким образом, профиль RK KDF нельзя удалить, если есть связь с Ключом Прошивки или Мастер Ключом.

5.1.14.5. Добавление связи профиля RK KDF Profile с OTP Ключами

Добавление связи профиля RK KDF Profile к OTP-ключу с выбранным индексом.

Ограничения и допущения:

- При выборе ключей из OTP-карты ограничения на тип ключа (is_block, is_scemu, is_otp_key) не накладываются.
- Длина выбранного OTP-ключа должна быть больше или равна 16 байт (128бит).
- При выборе профилей из списка отображаются все не удаленные профили независимо от существующих у них связей с другими OTP-ключами.

5.1.14.6. Удаление связи профиля RK KDF Profile с OTP Ключами

Удаление связи между профилем RK KDF и OTP-ключом с выбранным индексом.

Ограничения и допущения:

- Если имеется связь хоть с одним Ключом Прошивки (т.е. если профиль RK KDF и OTP ключ использовались для генерации значения Ключа Прошивки (derived key)), то удалять их связь (unlink) запрещено, каскадное удаление профиля вместе со связью также запрещается.

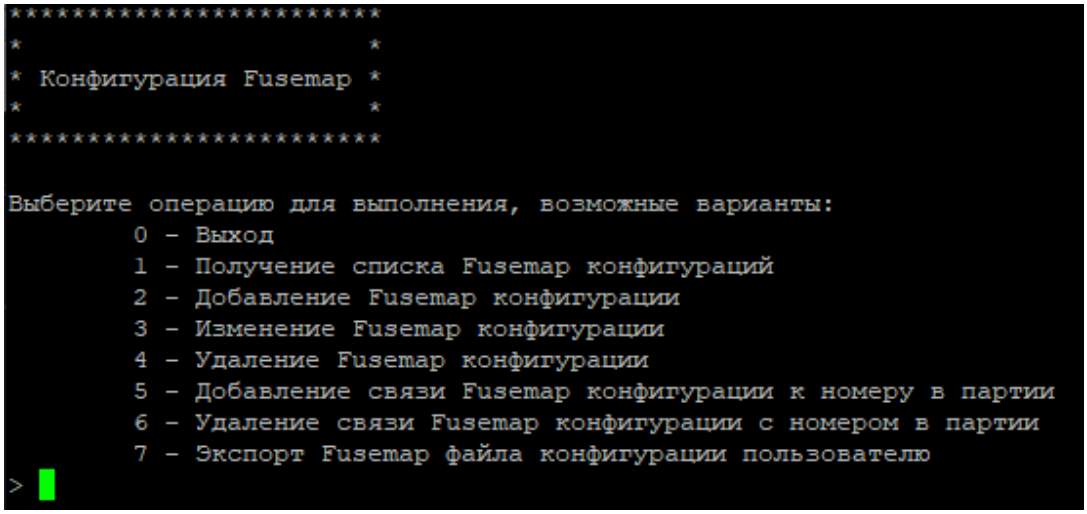
5.1.14.7. Экспорт профилей RK KDF Profile в файл

Экспорт всех RK KDF профилей, привязанных к выбранному Классу устройств, и их параметров в файл. В файл заносятся все неудаленные профили и их связи с OTP-ключами (при их наличии), при этом может существовать несколько связей одного профиля с OTP-ключами в рамках Класса устройств.

Экспортируемый файл загружается на FTP-сервер в папку *out* текущего (выполняющего операцию) пользователя. Файл шифрован одним или несколькими PGP-ключами.

Перейти к Содержанию...

5.1.15. Конфигурация Fusemap



Дерево меню для данного раздела:

1. Выход
2. Получение списка Fusemap конфигураций
3. Добавление Fusemap конфигурации
4. Изменение Fusemap конфигурации
5. Удаление Fusemap конфигурации
6. Добавление связи Fusemap конфигурации к номеру в партии
7. Удаление связи Fusemap конфигурации с номером в партии
8. Экспорт Fuseamp файла конфигурации пользователю

Данное меню позволяет управлять (создавать/редактировать/удалять/просматривать и т.п.) Fusemap конфигурации.

5.1.15.1. Получение списка Fusemap конфигураций

Просмотр списка существующих (неудаленных) описаний Fusemap конфигураций и их параметров.

5.1.15.2. Добавление Fusemap конфигурации

Добавление (импорт файла с FTP) Fusemap конфигурации.

Ограничения и допущения:

1. Импорт осуществляется из каталогов FTP (../in) для текущего (осуществляющего операцию) пользователя.
2. Импортируемый файл шифруется в pgp, KGS его автоматически расшифровывает, для чего текущему пользователю в KGS должен быть создан приватный PGP.
3. Импортируемый файл может быть размером до 4МБ. В противном случае, при выгрузке файла большего размера происходит ошибка.

5.1.15.3. Изменение Fusemap конфигурации

Изменение имени описания Fusemap конфигурации (Fusemap Config Description).

Ограничения и допущения:

1. Допускается редактировать только имя FMCD.

5.1.15.4. Удаление Fusemap конфигурации

Удаление Fusemap конфигурации из Системы.

5.1.15.5. Добавление связи Fusemap конфигурации к номеру в партии

Привязка Fusemap конфигурации к Номеру Партии.

5.1.15.6. Удаление связи Fusemap конфигурации с номером в партии

Удаление связи между Fusemap конфигурацией и Номером Партии.

5.1.15.7. Экспорт Fusemap файла конфигурации пользователю

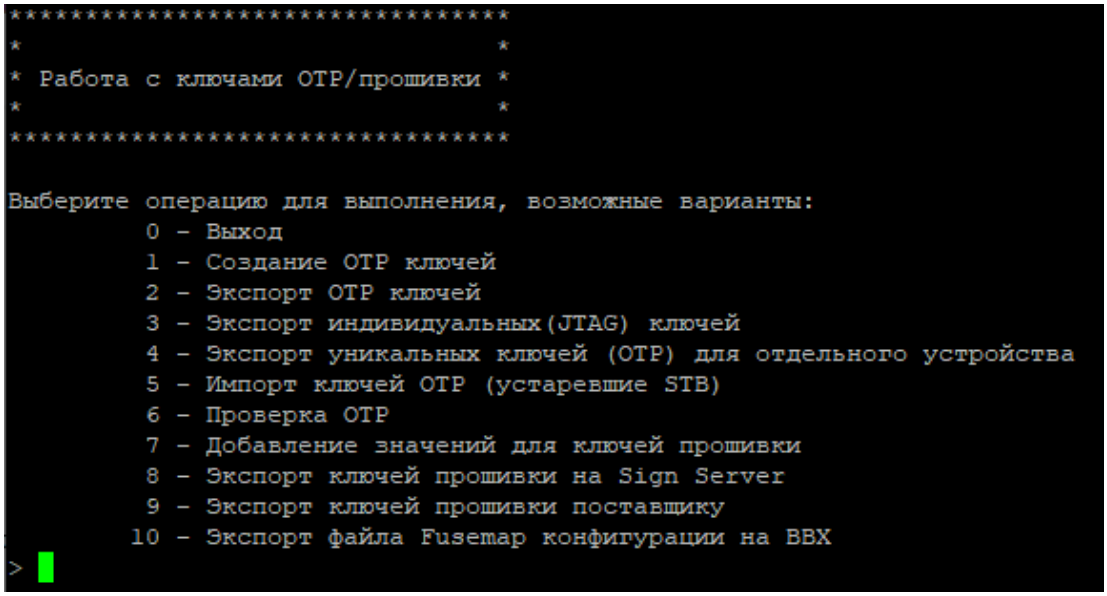
Экспорт файла с Fusemap конфигурацией, соответствующей выбранному Номеру Партии. Данные экспортируются в виде файла на FTP-сервер в папку *out* для текущего (осуществляющего операцию) пользователя.

Файл расшифровывается TDE, зашифровывается PGP-ключами и загружается на FTP в папку *out* текущего пользователя.

> ⚠ Fusemap конфигурацию нельзя сгенерировать в системе KGS: файлы с Fusemap конфигурацией генерируются вне системы и впоследствии импортируются (см. "Добавление Fusemap конфигурации").

Перейти к Содержанию...

5.2. Работа с ключами OTP/прошивки



Дерево меню для данного раздела:

1. Выход
2. Создание OTP ключей
3. Экспорт OTP ключей
4. Экспорт индивидуальных (JTAG) ключей
5. Экспорт уникальных ключей (OTP) для отдельного устройства
6. Импорт ключей OTP (устаревшие STB)
7. Проверка OTP
8. Добавление значений для ключей прошивки
9. Экспорт ключей прошивки на Sign Server
10. Экспорт ключей прошивки поставщику
11. Экспорт файла Fusemap конфигурации на BBX

5.2.1. Создание OTP ключей

Система генерирует OTP ключи для партии чипов (devices) заданного поставщика.

Ограничения:

- Максимальное количество ключей, которые могут быть сгенерированы для тестового Вида/Типа Партии, - 5000 шт.

Перейти к Содержанию...

5.2.2. Экспорт OTP ключей

Повторный экспорт ключей невозможен (кроме случая, если выгружаются чипы тестового Вида/Типа Партии). При попытке повторения данной операции будет выдано сообщение об ошибке.

Система осуществляет экспорт ВСЕХ ключей КАЖДОГО устройства (чипа) для заданного диапазона чипов. Ключи экспортируются в виде файлов на FTP-сервер в папку *out* пользователя. Список пользователей, которые могут быть получателями данных, определяется как текущий пользователь + внешние пользователи, привязанные к Поставщику или Black Box, которые будут выбраны в процессе работы.

Экспортируемый файл (с OTP ключами) шифрован одним или несколькими PGP-ключами (ключи выбираются при экспорте).

Перейти к Содержанию...

5.2.3. Экспорт индивидуальных (JTAG) ключей

Система осуществляет экспорт ОДНОГО УНИКАЛЬНОГО ключа (на выбор) либо для ОДНОГО устройства, либо для НЕСКОЛЬКИХ устройств из указанного списка/диапазона. Ключи экспортируются в рабочую папку текущего (осуществляющего операцию) пользователя на FTP-сервер.

Экспорт предназначен для устройств (чипов), которые впоследствии будут использоваться в тестировании (т.е. не будут использоваться в промышленной эксплуатации).

Экспортируемый файл (с JTAG ключом) шифрован одним или несколькими PGP-ключами.

Перейти к Содержанию...

5.2.4. Экспорт уникальных ключей (OTP) для отдельного устройства

Система осуществляет экспорт ВСЕХ индивидуальных OTP-ключей (либо производных ключей (от индивидуальных)) либо для ОДНОГО устройства, либо для НЕСКОЛЬКИХ устройств из указанного списка /диапазона. Ключи экспортируются для текущего (осуществляющего операцию) пользователя на FTP-сервер.

Особенности:

- Производные ключи могут быть сгенерированы как по тестовому, так и по прод. RK KDF профилям.

> ⚠ Если для выбранного в OTP-карте ключа указана необходимость обфускации и для Вида Партии, которой принадлежит чип, назначена функция OVDF/KOF, то несмотря на это, обфускация игнорируется и выгружается чистое значение ключа.

Экспорт предназначен для чипов, которые впоследствии будут использоваться в тестировании (т.е. не будут использоваться в промышленной эксплуатации).

Экспортируемые данные (zip-архив) шифрован одним или несколькими PGP-ключами.

Перейти к Содержанию...

5.2.5. Импорт ключей OTP (устаревшие STB)

Система осуществляет импорт ранее сгенерированных ключей из внешних источников.

Импортируемый файл в соответствующем формате должен быть подготовлен и загружен в папку *in* пользователя (текущего пользователя либо пользователя, привязанного к Поставщику) на FTP-сервере. Файл должен быть зашифрован PGP-ключом, привязанным к (выбираемому пользователем) Виду Партии.

Перейти к Содержанию...

5.2.6. Проверка OTP

С FTP-сервера импортируется файл с данными, блоки данных внутри файла шифруются (либо расшифровываются) с помощью OTP-ключа с заданным индексом и по заданному алгоритму, после чего формируется новый файл, содержащий результаты проведенной операции, и экспортируется на FTP-сервер. Формат выходного файла полностью соответствует формату входного файла, но дополнительно содержит результаты выполненной операции шифрования / расшифрования.

Импортируемый файл (архив) копируется с FTP-сервера на Processing Server, в папку **текущего** пользователя (т.е. пользователя, под которым в консоли выполняется данная операция). Этот файл является временным и удаляется после того, как содержащиеся в файле данные будут обработаны. **Экспортируемый** файл (архив) переносится (не копируется) на FTP-сервер, но уже в папку пользователя, для которого осуществляется экспорт (либо **текущего** пользователя, либо привязанного к выбранному **Поставщику**); файл шифрован одним или несколькими PGPключами.

Экспортируемый файл в дальнейшем анализируется (проводится валидация чипов): сравниваются результаты шифрования ключом из KGS и этим же ключом, прошитым непосредственно в чип. При этом OTP ключ не экспортируется в чистом виде. Если данные совпадают, то валидация чипов пройдена успешно (т.е. в чип прошиты нужные данные). Как правило, процедура используется для валидации ограниченной партии тестовых ключей: если проверка пройдена успешно, то осуществляется экспорт, персонализация и прошивка основной партии чипов.

Перейти к Содержанию...

5.2.7. Добавление значений для ключей прошивки

Система осуществляет генерацию ключа прошивки (генерация случайного значения (*генерация*) либо генерация производного ключа (*наследование*) на основе OTP-ключа) либо импорт файла с ключом из внешних источников.

В случае импорта файл в соответствующем формате должен быть подготовлен и загружен на FTP-сервер, в папку *in* пользователя (текущего пользователя либо пользователя, привязанного к Поставщику). Файл должен быть зашифрован одним или несколькими PGP-ключами (private часть хотя бы одного из этих PGP-ключей (ключ выбирается пользователем) должна храниться в системе KGS).

В случае генерации производного значения (*наследование*) существуют следующие **ограничения**:

1. Если выбранный Ключ Прошивки связан с OTP-картой, то выбор способа "*наследование*" отсутствует.
2. Генерация производных значений для Ключа Прошивки доступна только для следующих типов привязки Ключей Прошивки: Класс устройств + Тип Партии, Класс устройств + Тип Партии + STB Модель.
3. Ключ Прошивки и OTP ключ (key index в Карте Ключей) принадлежат одному и тому же Классу устройств, в качестве значения для OTP-ключа используется значение из того Типа Партии, к которому привязан Ключ Прошивки.
4. Ключ Прошивки, для которого нужно генерировать производное значение:
    a. не экспортируется на BBX и не пишется в OTP;
    b. не может иметь тип алгоритма crypto algo = 'kdf-aes-128' (GS2);
    c. не может иметь тип алгоритма crypto algo = 'RSA'.
    d. генерация производного ключа возможна только для ключей aes-128 и binary data до 128 бит.

Перейти к Содержанию...

5.2.8. Экспорт ключей прошивки на Sign Server

Система осуществляет экспорт ключей прошивки для заданного сервера подписи (в KGS обозначается как внешний сервер с типом 'Sign Server'). Ключи экспортируются на FTP-сервер, для текущего (осуществляющего операцию) пользователя либо пользователя, привязанного к Sign Server (ко Внешнему серверу с типом 'Sign Server'). Экспортируемый файл шифрован одним или несколькими PGP-ключами.

Экспортируемые ключи в дальнейшем используются на сервере для прошивки и подписи данных.

Перейти к Содержанию...

5.2.9. Экспорт ключей прошивки поставщику

Система осуществляет экспорт ключей прошивки Поставщику.

Ключи экспортируются на FTP-сервер, для текущего (осуществляющего операцию) пользователя либо пользователя, привязанного к выбранному Поставщику.

Каждый выбранный ключ прошивки экспортируется в отдельный файл. Файлы с ключами архивируются в zip-архив. Архив шифруется одним или несколькими PGP-ключами.

Перейти к Содержанию...

5.2.10. Экспорт файла Fusemap конфигурации на BBX

Система осуществляет экспорт файла с fusemap config (FMC), соответствующий выбранному Номеру Партии (PN), для выбранного Black Box (BBX).

При экспорте файл с FMC зашифровывается лестницей ключей для выбранного BBX. Файл дополнительно шифруется одним либо несколькими PGP-ключами.

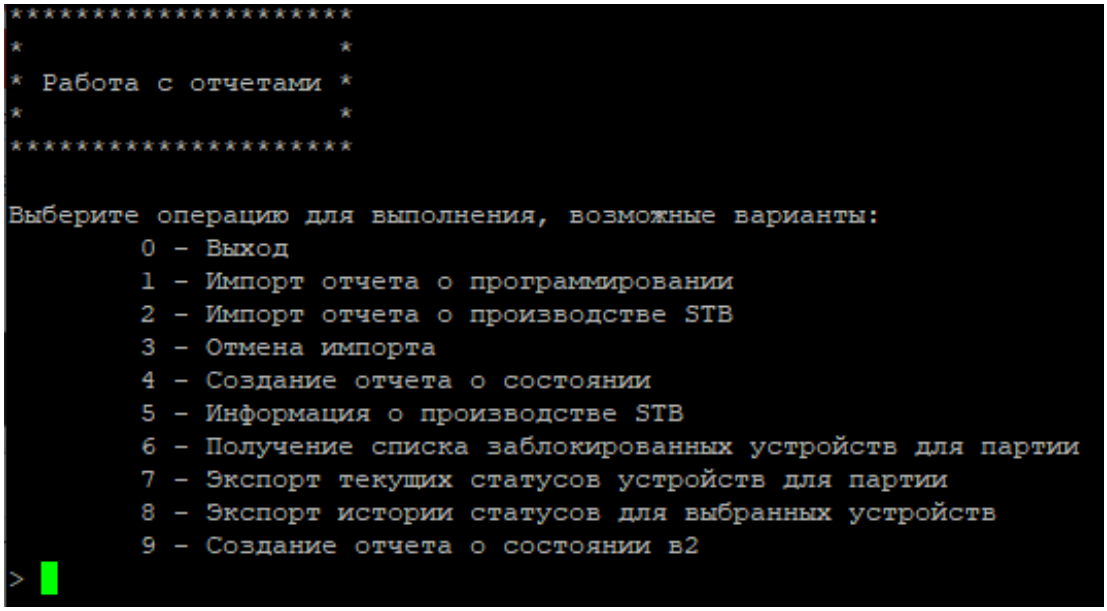
Экспорт осуществляется на FTP-сервер, в папку *out* пользователя. Список пользователей, которые могут быть получателями данных, определяется как текущий пользователь либо внешние пользователи, привязанные к выбранному Поставщику или Black Box (Внешнему серверу с типом 'Black Box').

⚠ Fusemap Config необходим для персонализации чипов.

Fusemap Config нельзя сгенерировать в системе KGS: файлы с fusemap config генерируются вне системы и впоследствии импортируются (см. "Добавление Fusemap конфигурации").

Перейти к Содержанию...

5.3. Работа с отчетами



Дерево меню для данного раздела:

1. Выход
2. Импорт отчета о программировании
3. Импорт отчета о производстве STB
4. Отмена импорта
5. Создание отчета о состоянии
6. Информация о производстве STB
7. Получение списка заблокированных устройств для партии
8. Экспорт текущих статусов устройств для типа партии
9. Экспорт истории статусов для выбранных устройств
10. Создание отчета о состоянии в2

5.3.1. Импорт отчета о программировании

Отчет о программировании какой-либо партии чипов предназначен для фиксации в системе результатов (успех / неуспех) прошивки чипов.

Отчет должен быть предварительно подготовлен внешним или текущим (осуществляющим импорт) пользователем и загружен на FTP-сервер, в папку *in* пользователя. В процессе работы файл с отчетом перемещается системой с FTP-сервера на Processing Server, проводится его валидация и обработка, результатом которой является обновление статусов программирования чипов, номера которых указаны в отчете.

Список пользователей, которые могут быть отправителем данных, определяется как текущий пользователь + внешние пользователи, привязанные к Поставщику или Black Box (Внешний сервер с типом 'Black Box'), которые будут выбраны в процессе работы.

Перейти к Содержанию...

5.3.2. Импорт отчета о производстве STB

Отчет с результатами производства STB устройств, содержащих персонализированные чипы, предназначен для фиксации в системе факта (успех / неуспех) производства, а также связей между произведенным чипом и другими сущностями системы (оператор, модель STB, ее серийный номер – вся эта информация содержится в отчете).

> ⚠ При загрузке отчета, содержащего 2 идентификатора чипов - основного SoC и сопроцессора CoPro, при сохранении в БД данных выполняются операции записи для двух чипов в одной транзакции. Таким образом, информация о статусе из отчета либо обновляется одновременно для двух чипов, либо откатывается до предыдущего состояния.

Отчет должен быть предварительно подготовлен текущим или внешним пользователем и загружен на FTP-сервер, в папку *in* пользователя. В процессе работы файл с отчетом перемещается системой с FTP-сервера на Processing Server, проводится его валидация и обработка, результатом которой является обновление статусов чипов, номера которых указаны в отчете, и сохранение в системе информации о том, в какую модель приемника был установлен данный чип. Кроме того, сохраняется информация об операторе, для которого был произведен данный приемник и его серийный номер.

Отчет о производстве STB должен генерироваться для каждой производственной партии (batch) и предоставляться в ООО "ПЦТ" до того, как STB будут отгружены операторам.

Каждый отчет должен содержать данные только по одной конкретной модели STB. Если Производитель выпускает больше моделей STB с CAS, то должны быть предоставлены отдельные отчеты по каждой модели STB.

Перейти к Содержанию...

5.3.3. Отмена импорта

Отмена результатов импорта отчета о программировании чипов или отчета о производстве STB (см. Импорт отчета о программировании, Импорт отчета о производстве STB). Используется, если загруженный отчет (отчет о программировании, отчет о производстве STB) содержит неверные данные.

Перейти к Содержанию...

5.3.4. Создание отчета о состоянии

Генерация и просмотр отчета с информацией о состоянии базы данных (количество ключей, их статус и т.п.) для заданного внутреннего номера партии и для заданного диапазона устройств.

Перейти к Содержанию...

5.3.5. Информация о производстве STB

Просмотр информации о произведенном STB, загруженной в KGS из отчета о производстве.

Поиск информации выполняется по любому из введенных идентификаторов: Серийный номер STB, CAS STB ID (для Main SoC) и CoProID (для CAS Co-Processor).

Перейти к Содержанию...

5.3.6. Получение списка заблокированных устройств для партии

Система осуществляет экспорт в файл списка номеров устройств (для выбранного Вида Партии), которые занесены в черный список KGS, а также их текущих статусов. В черный список KGS вносятся устройства, для которых выгружались индивидуальный (JTAG) ключ (см. Экспорт индивидуальных (JTAG) ключей) либо уникальные ключи для отдельного устройства (см. Экспорт уникальных ключей (OTP) для отдельного устройства).

> ⚠ Следует учитывать, что в файл экспортируются только blacklisted devices. Если для выбранного Вида Партии в статистике нет ни одного устройства, занесенного в черный список, то файл **не** экспортируется.

Данные экспортируются в виде файла на FTP-сервер, в папку *out* текущего (осуществляющего операцию) пользователя.

Экспортируемый файл шифрован одним или несколькими PGP-ключами.

Перейти к Содержанию...

5.3.7. Экспорт текущих статусов устройств для типа партии

Система осуществляет экспорт в файл списка всех устройств для выбранного Вида Партии (Типа Партии) вместе с подробной информацией об их текущих статусах и признаках (commit, backup, blacklist).

> ⚠ Следует учитывать, что если для выбранного Вида Партии в статистике нет ни одного устройства, то файл **не** экспортируется.

Данные экспортируются в виде файла на FTP-сервер в папку *out* текущего (осуществляющего операцию) пользователя.

Экспортируемый файл шифрован одним или несколькими PGP-ключами.

Перейти к Содержанию...

5.3.8. Экспорт истории статусов для выбранных устройств

Система осуществляет экспорт в файл всей информации из таблицы истории для выбранного устройства. Допускается выбор нескольких устройств из одной партии за один раз (количество устройств в файле **не** ограничено).

Данные экспортируются в виде файла на FTP-сервер, в папку *out* текущего (осуществляющего операцию) пользователя.

Экспортируемый файл упаковывается в zip-архив, который шифруется одним или несколькими PGP-ключами.

Перейти к Содержанию...

5.3.9. Создание отчета о состоянии в2

Генерация и просмотр отчета с информацией о состоянии базы данных (количество ключей, их статус и т.п.) для заданного внутреннего номера партии. В отличие от другого отчета (см. Создание отчета о состоянии) данный отчет содержит точный диапазон устройств, находящихся в разных статусах (*Generated / Exported / Released*).

В отчете отображается информация:

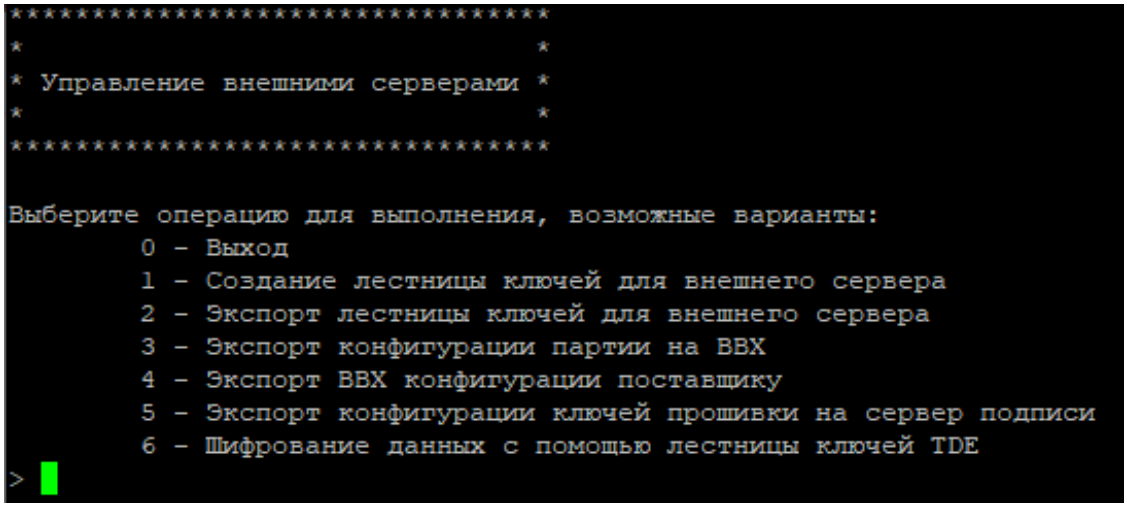
- либо только для устройств, входящих в задаваемый диапазон ***номер первого устройства ... номер последнего устройства***. По умолчанию этот диапазон может содержать **все** устройства для выбранных Класса устройств и Вида Партии.
- либо (если выбрана STB Модель) для **всех** устройств, относящихся к выбранной STB модели.

Дополнительно в отчете может быть отображена информация по соответствующим Номерам Партий.

Информация по количеству устройств с типом blacklisted, backed up, committed не отображается.

Перейти к Содержанию...

5.4. Управление внешними серверами



Дерево меню для данного раздела:

1. Выход
2. Создание лестницы ключей для внешнего сервера
3. Экспорт лестницы ключей для внешнего сервера
4. Экспорт конфигурации партии на ВВХ
5. Экспорт ВВХ конфигурации поставщику
6. Экспорт конфигурации ключей прошивки на сервер подписи
7. Шифрование данных с помощью лестницы ключей TDE

5.4.1. Создание лестницы ключей для внешнего сервера

Система генерирует лестницу ключей для выбранного Внешнего сервера (типы внешних серверов: 'Black Box', 'Sign Server').

Лестница ключей для заданного Black Box / Sign Server может быть сгенерирована только один раз (повторная генерация лестницы ключей для одного и того же Black Box / Sign Server не допускается). Набор ключей, согласно лестнице ключей для Black Box / Sign Server, генерируется и сохраняется в базе данных KGS с привязкой к этому Black Box / Sign Server. Ключи хранятся в зашифрованном виде.

В случае возникновения любых ошибок в процессе генерации производится откат базы данных в состояние, соответствующее началу работы.

Перейти к Содержанию...

5.4.2. Экспорт лестницы ключей для внешнего сервера

Система осуществляет экспорт лестницы ключей для выбранного внешнего сервера (типы внешних серверов: 'Black Box', 'Sign Server', 'Generic'). Данные экспортируются в виде файлов на FTP-сервер, в папку *out* для текущего (осуществляющего операцию) пользователя либо одного из Внешних пользователей.

Список пользователей, которые могут быть получателями данных, определяется как текущий пользователь либо внешние пользователи, привязанные ко Внешнему серверу, которые будут выбраны в процессе работы.

Для выполнения операции экспорта в систему KGS с FTP-сервера загружается **public HWRK-ключ**, сгенерированный на Внешнем сервере. Этим ключом шифруются данные в экспортируемых файлах. При отсутствии ключа на FTP экспорт лестницы ключей невозможен.

На FTP-сервер экспортируются ДВА файла - файл с ВВМК и файл вида ***<ExternalServerName>_keysladder.dat***, содержащий лестницу ключей.

Экспортируемые файлы шифрованы одним или несколькими PGPключами. Бинарный файл с ВВМК (относится к лестнице ключей) дополнительно шифруется HWRK-ключом выбранного Внешнего сервера. С FTP-сервера файлы забирает уполномоченный пользователь Системы, имеющий доступ к соответствующему Внешнему серверу.

Экспортируемые данные используются на Внешнем сервере для расшифровки ключей, поступающих из KGS.

Лестница ключей при штатной работе экспортируется только один раз.

Перейти к Содержанию...

5.4.3. Экспорт конфигурации партии на ВВХ

Система осуществляет экспорт конфигурации (ключа) для выбранного Black Box (Внешнего сервера с типом 'Black Box'). Данные экспортируются в виде файла на FTP-сервер, в папку *out* для текущего (осуществляющего операцию) пользователя либо одного из Внешних пользователей.

Список пользователей, которые могут быть получателями данных, определяется как текущий пользователь либо внешние пользователи, привязанные к Black Box, которые будут выбраны в процессе работы.

На FTP-сервер экспортируется файл, содержащий конфигурацию Вида Партии.

Экспортируемый файл шифрован одним или несколькими PGPключами. С FTP-сервера файлы забирает уполномоченный пользователь Системы, имеющий доступ к серверу Black Box.

Экспортируемые данные используются на сервере Black Box для последующей расшифровки ключей, поступающих из KGS (см. Экспорт OTP ключей), причем файл конфигурации экспортируется для каждого Вида Партии / Номера Партии, используемого в Black Box.

Перейти к Содержанию...

5.4.4. Экспорт BBX конфигурации поставщику

Система осуществляет экспорт конфигурации для выбранного Поставщика. Экспортируемый файл (файл конфигурации) шифрован одним или несколькими PGPключами. Файл экспортируется на FTP-сервер.

Список пользователей, которые могут быть получателями данных, определяется как текущий пользователь либо внешние пользователи, привязанные к Поставщику, которые будут выбраны в процессе работы.

Экспортируемый файл в дальнейшем используется ПО Поставщика при обращении последнего к API в Black Box. Таким образом, осуществляется интеграция данного Black Box в общий производственный процесс.

> ⚠ Файл конфигурации для Поставщика отличается от файла конфигурации для Black Box форматом файла и содержимым.

Перейти к Содержанию...

5.4.5. Экспорт конфигурации ключей прошивки на сервер подписи

Система осуществляет экспорт конфигурации для выбранного сервера подписи (Внешнего сервера с типом 'Sign Server'). Данные экспортируются в виде файла на FTP-сервер, в папку *out* для текущего (осуществляющего операцию) пользователя либо одного из Внешних пользователей.

Список пользователей, которые могут быть получателями данных, определяется как текущий пользователь либо внешние пользователи, привязанные к Sign Server (ко Внешнему серверу с типом 'Sign Server'), которые будут выбраны в процессе работы.

Экспортируемый файл шифрован одним или несколькими PGPключами. С FTP-сервера файл забирает уполномоченный пользователь Системы, имеющий доступ к серверу подписи.

Экспортируемые данные используются на сервере подписи для шифрования и расшифрования прошивки, а также для создания и проверки подписи прошивки, причем файл конфигурации экспортируется для каждого Вида Партии / Номера Партии (партии чипов), используемого на сервере подписи.

Перейти к Содержанию...

5.4.6. Шифрование данных с помощью лестницы ключей TDE

Система осуществляет загрузку произвольных данных с сервера FTP, шифрует эти данные по лестнице ключей выбранного Внешнего сервера и выгружает их обратно на FTP сервер без сохранения в KGS. Сервер, лестницей которого будут защищаться данные, должен быть предварительно создан в KGS в стандартных workflow для работы с Внешними серверами, также у сервера должна быть сгенерирована лестница ключей TDE.

Ограничения:

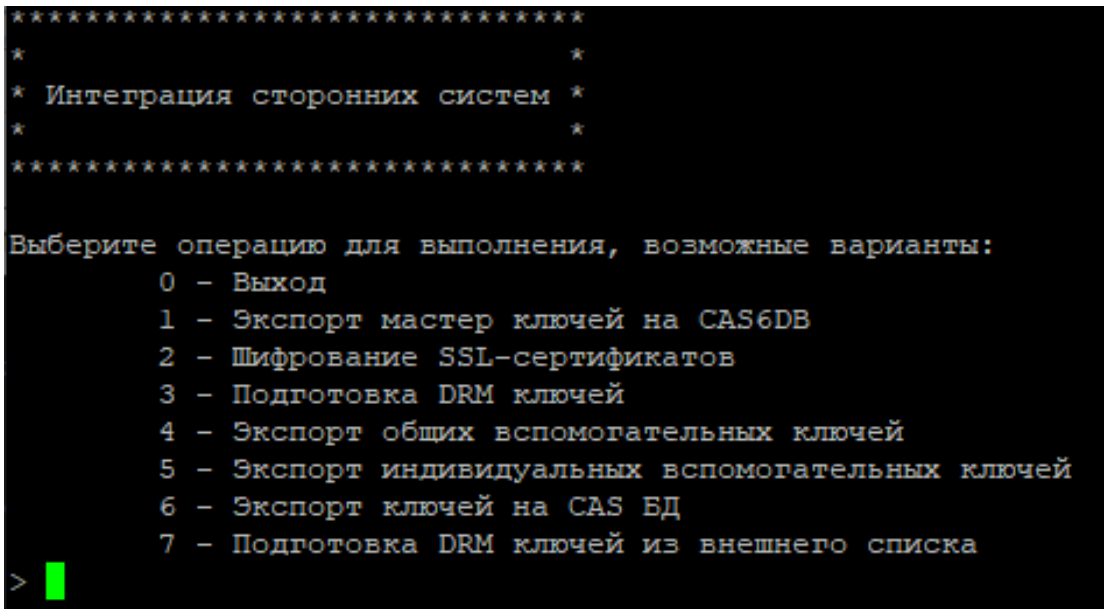
- Гарантируется обработка и шифрование (лестницей TDE) файлов размером до 100 Мб.
- При шифровании файл рассматривается в KGS как бинарные данные, и содержимое никаким образом не форматируется и не анализируется. Дополнительные данные при выгрузке не создаются, т.е. сервер, который использует защищенные с помощью TDE данные, должен предусматривать скрипты импорта данных в базу и использование их без привязки к каким-либо сущностям (DRM ключам, Виду Партии, root-ключам и т.п.).
- Список пользователей, которые могут быть получателями данных, определяется как текущий пользователь либо внешние пользователи, привязанные ко Внешнему серверу, которые будут выбраны в процессе работы.

Данные загружаются и экспортируются в виде файлов. При формировании имени экспортируемого файла к имени исходного файла добавляется ***.tde.gpg*** - ***<source_file_name>.tde.gpg***. Например, если <source_file_name> импортируемого файла - "wv_key.dat", то имя экспортируемого файла: "wv_key.dat.tde.gpg".

Экспортируемый файл шифрован одним или несколькими PGPключами. С FTP-сервера файл забирает уполномоченный пользователь Системы, имеющий доступ к соответствующему Внешнему серверу.

Перейти к Содержанию...

5.5. Интеграция сторонних систем



Дерево меню для данного раздела:

1. Выход
2. Шифрование SSL-сертификатов
3. Подготовка DRM ключей
4. Экспорт общих вспомогательных ключей
5. Экспорт индивидуальных вспомогательных ключей
6. Экспорт ключей на CAS БД
7. Подготовка DRM ключей из внешнего списка
8. Экспорт мастер ключей на CAS DB

5.5.1. Шифрование SSL-сертификатов

С FTP-сервера импортируется файл (архив) с SSL-сертификатами и закрытыми ключами (Personal Keys), архив распаковывается, каждый файл с PersonalKey (закрытый ключ) внутри распакованного архива шифруется, после чего формируется новый архив (.zip) и экспортируется на FTP-сервер. Экспортируемый архив содержит файлы, содержащие SSL-сертификаты (всегда) и PersonalKeys (опционально, в зависимости от типа SSL сертификата).

KGS не конвертирует форматы файлов с ключами и сертификатами. KGS лишь шифрует ключи (доступ к схеме шифрования строго ограничен, предоставляется по запросу), содержащиеся в импортируемых файлах.

Импортируемый файл (архив) копируется с FTP-сервера на Processing Server, в папку текущего пользователя (т. е. пользователя, под которым в консоли выполняется шифрование). Этот файл является временным и удаляется после того, как содержащиеся в файле данные будут обработаны. Импортируемый файл должен быть шифрован одним или несколькими PGP-ключами.

> ⚠ **Обратите внимание**! Система KGS автоматически попытается расшифровать импортируемый файл всеми имеющимися private PGP-ключами. Если файл не зашифрован или требуемый ключ не найден, то система выдаст ошибку.

Экспортируемый файл переносится (не копируется) на FTP-сервер, но уже в папку *out* **внешнего** пользователя, для которого осуществляется экспорт; файл шифрован одним или несколькими PGPключами.

Перейти к Содержанию...

5.5.2. Подготовка DRM ключей

Экспорт файла с конфигурацией и файла с DRM-ключами, зашифрованными OTP-ключом с выбранным индексом. Экспорт может осуществляться для нескольких OTP-ключей с выбранными индексами.

При этом DRM ключи можно генерировать в одном из следующих режимов:

1. для всех устройств, относящихся к выбранной модели приемника (STB Модель) и партии (Вид Партии).
2. для устройств из непрерывного диапазона (device ranges).
3. для списка устройств (hardwares list) - пользователь копирует в консоль список ID для генерации. При этом в KGS должны существовать устройства с введенными ID и все эти устройства должны относиться к одному Виду Партии, который тоже существует в KGS.

Экспортируемые файлы (файл конфигурации и файл с ключами) упаковываются в zip-**архив**, архив шифрован одним или несколькими PGPключами. Архив экспортируется на FTP-сервер, в папку *out* выбранного пользователя, для которого осуществляется экспорт (либо текущего пользователя, либо внешнего пользователя, привязанного к выбранному Партнеру).

Перейти к Содержанию...

5.5.3. Экспорт общих вспомогательных ключей

Экспортируются общие вспомогательные ключи. Экспортируется целиком набор (keyset) со всеми значениями, по отдельности значения из набора не выгружаются.

Обработка ключей при выгрузке, количество экспортируемых файлов, их объединение/нет в архив, форматы файлов и их дальнейшее использование определяется выбранным типом вспомогательных ключей. Сформированный файл/архив шифруется выбранным PGP ключом/ключами и экспортируется на FTP-сервер, в папку *out* **текущего** пользователя.

Перейти к Содержанию...

5.5.4. Экспорт индивидуальных вспомогательных ключей

Экспорт индивидуальных Вспомогательных Ключей (Pairing Keys). Ключи используются в смарт-картах.

Способы ввода идентификаторов чипов, для которых экспортируются вспомогательные ключи:

1. *Device range in console*. Пользователем задаются первый номер чипа (*device start number*) + количество чипов (*count of devices*).
2. *Hardwares list in console*. Пользователь вводит в консоль текст с идентификаторами. Список идентификаторов устройств вводится путем их копирования из буфера обмена или ввода с клавиатуры и двойного нажатия Enter (т.е. ввода пустой строки) для завершения ввода.
3. *External file in manufacturing report format*. Список идентификаторов устройств будет получен KGS после обработки импортируемого файла.

Выбранный способ имеет свои особенности и ограничения (дополнительно накладываемые требования к настройке, вводу и обработке данных, импортируемым и экспортируемым файлам).

Архив с экспортируемыми данными (с ключами) экспортируется на FTP-сервер, в папку *out* выбранного пользователя (текущий пользователь или внешний пользователь, привязанный к любой внешней сущности **кроме** Поставщика). Экспортируемый архив шифрован одним или несколькими PGPключами.

Перейти к Содержанию...

5.5.5. Экспорт ключей на CAS БД

Экспорт шифрованных ключей для базы CAS. Экспортируемые данные используются для работы с БД CAS.

Способы ввода идентификаторов чипов, для которых экспортируются ключи:

1. *Device range in console*. Пользователем задаются первый номер чипа (*device start number*) + количество чипов (*count of devices*).
2. *Hardwares list in console*. Пользователь вводит в консоль текст с идентификаторами. Список идентификаторов устройств вводится путем их копирования из буфера обмена или ввода с клавиатуры и двойного нажатия Enter (т.е. ввода пустой строки) для завершения ввода.
3. *External file in manufacturing report format*. Список идентификаторов устройств будет получен KGS после обработки импортируемого файла.

Выбранный способ имеет свои особенности и ограничения (дополнительно накладываемые требования к настройке, вводу и обработке данных, импортируемым и экспортируемым файлам).

Обработка ключей при выгрузке, количество экспортируемых файлов, форматы файлов и их дальнейшее использование зависят от выбранного пользователем Типа Устройства. Сформированный архив шифруется выбранными PGP ключами и экспортируется на FTP-сервер, в папку *out* **текущего** пользователя.

Перейти к Содержанию...

5.5.6. Подготовка DRM ключей из внешнего списка

Подготовка и экспорт данных, необходимых для работы с DRM ключами (экспорт файла с конфигурацией и файла с DRM-ключами, зашифрованными OTP-ключом с выбранным индексом). Экспорт может осуществляться для нескольких OTP-ключей с выбранными индексами. DRM ключи генерируются для списка устройств, который импортируется в KGS из внешнего источника (т.е. с FTP-сервера).

Импортируемые данные и их особенности:

1. Файл со списком устройств, для которых будет осуществляться генерация DRM ключей, должен быть предварительно подготовлен **текущим** пользователем и загружен на FTP-сервер в папку *in* текущего пользователя.
2. Особенности:
    a. Имя файла может быть любым.
    b. Импортируемый файл может содержать данные как по одному, так и по двум Видам Партий (автоматически определяется в workflow на основании анализа строк входного файла).
    c. Импортируемый файл **не** шифруется PGP ключами.

Экспортируемые данные и их особенности:

1. Для каждого индекса <idx> OTP-ключа в списке, заданном пользователем:
    a. Файл с конфигурацией.
    b. Файл с шифрованными значениями DRM ключей. Способ шифрования ключей и, как следствие, формат файла зависят от выбранного типа шифрования (***Light Encryption*** / ***TDE Encryption***).
2. Если выбрано шифрование ***TDE Encryption***, то дополнительно экспортируется файл, не зависящий от индексов и содержащий хэш лестницы ключей.
3. Приведенные выше файлы упаковываются в zip-архив, архив шифруется выбранными PGP-ключами и выгружается на FTP.
4. Если в файле со списком устройств было **два** Вида Партии (может быть одно или два значения - для HostCPU и CAS Co-Processor), то при экспорте будет создаваться **два архива** (для каждого из Видов Партий). Соответственно, каждый архив содержит только файлы для одного Вида Партии (#1 или #2).
5. Если в процессе обработки импортируемого файла со списком чипов произошли ошибки и DRM-ключи для каких-то устройств из списка не могут быть сгенерированы (например, Виды Партий не совпадают с обнаруженными в первой строке), то WF формирует файл с ошибками, в котором для каждого устройства описана причина ошибки. Файл с ошибками экспортируется **отдельно** (не включается в архив(ы)), шифруется выбранными PGP-ключами. Имя файла - **<input_filename>_errors.txt**, где <input_filename> - имя импортируемого файла (без расширения), скачанного с FTP.
6. Все файлы экспортируются на FTP-сервер в папку **текущего** пользователя.

Перейти к Содержанию...

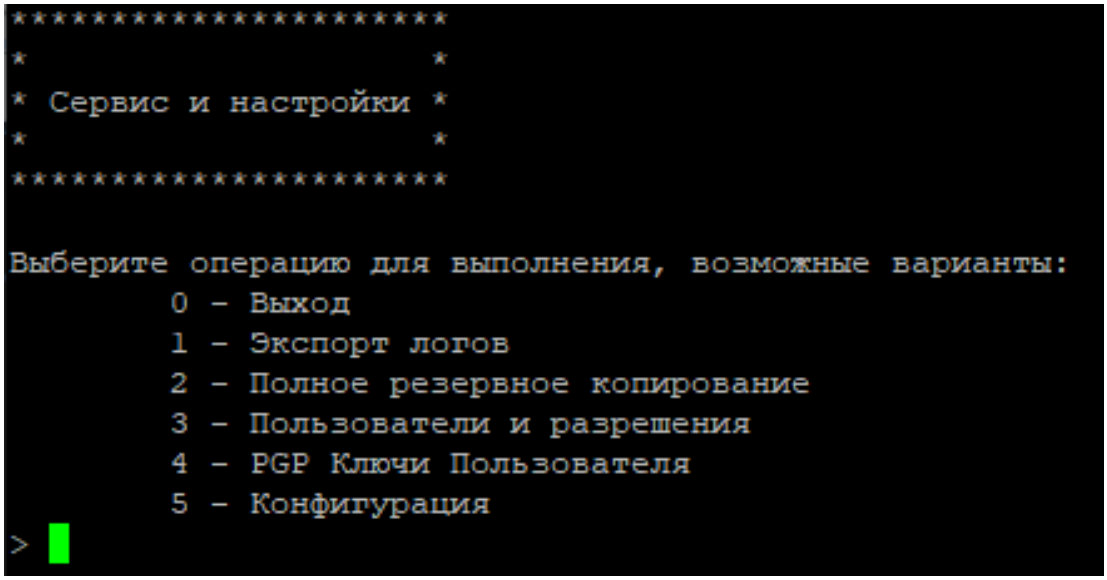
5.5.7. Экспорт мастер ключей на CAS DB

Экспорт шифрованных Мастер Ключей для БД CAS. Экспортируемые данные используются для работы с БД CAS.

Сформированные данные упаковываются в архив. Архив с данными экспортируется на FTP-сервер, в папку *out* **текущего** (осуществляющего операцию) пользователя. Архив шифруется GPG.

Перейти к Содержанию...

5.6. Сервис и настройки



Дерево меню для данного раздела:

1. Выход
2. Экспорт логов
3. Полное резервное копирование
4. Пользователи и разрешения
5. PGP ключи
6. Конфигурация

С помощью данного меню осуществляется настройка системы (настройка пользователей и прав доступа, управление PGP-ключами, настройка параметров консоли), а также выполнение служебных действий (экспорт логов, резервное бекапирование всей БД). **Данный пункт главного меню должен быть доступен только пользователям с правами администратора**.

Список возможных операций приведен в подразделах ниже.

5.6.1. Экспорт логов

Экспорт event logs и debug logs. Log-файлы копируются на FTP-сервер, в папку текущего пользователя без какого-либо шифрования.

Event logs содержит журнал бизнес-операций в системе, меняющих ее состояние (добавление нового Поставщика, экспорт ключей, создание нового пользователя).

Debug logs является журналом отладки и предназначен для использования при пуско-наладке системы либо при анализе ошибок.

Перейти к Содержанию...

5.6.2. Полное резервное копирование

Резервное копирование всей БД. Применяется после выполнения значительного объема работ, когда бекапирование после каждой операции невыгодно или неудобно.

Файл с архивом будет выгружен на FTP-сервер в папку специального пользователя, предназначенного для выполнения этих операций. Сформированный архив будет зашифрован выбранными PGP-ключами. Пользователь создается автоматически при установке системы (скрипт начального наполнения), его идентификатор прописывается в настроечных параметрах подсистемы и используется автоматически. Имя создаваемого пользователя по умолчанию – backup.

В процессе выполнения workflow пользователь выбирает тип бекапа. Возможны следующие типы:

1. ***Полное резервное копирование***. Полный бекап (файловый бекап). Используется функция *pg_start_backup*, создающая контрольную точку Postgres.
   Имя файла с бекапом - **YYYYMMDD-HH24MI-<BackupName>.tar.bz2**.

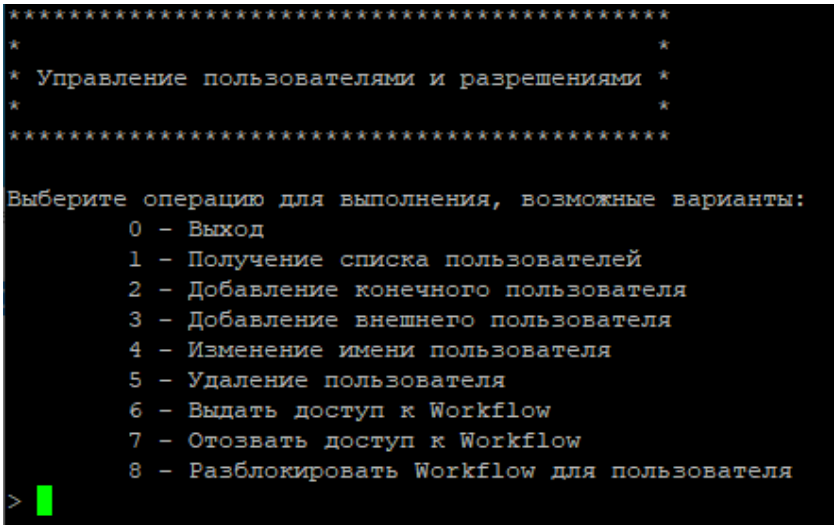
   > ⚠ **Обратите внимание!** Все workflows (WFs), предлагающие выполнить бекап в процессе работы (большинство WFs, меняющих БД), в случае согласия пользователя вместо Полного резервного копирования (*full backup*) выполняют Резервное копирование схемы (*scheme backup)*. Полный бекап (*full backup*) можно выполнить только в WF ***Сервис и настройки*** -> ***Полное резервное копирование***.

2. ***Резервное копирование схемы***. SQL-бекап. Бекапирование выполняется на уровне создания sql-скрипта, с помощью входящей в комплект Postgres утилиты *pg_dumpall*.
   Имя файла с бекапом - **YYYYMMDD-HH24MI-<BackupName>.tar.gz**.

> ⓘ Резервное копирование схемы (*Scheme backup*) выполняется медленнее, а файл бекапа будет больше, чем при выполнении Полного резервного копирования (*Full backup*). Тем не менее, в отличие от *Полного резервного копирования*, *Резервное копирование схемы* не привязано жестко к версии ОС и СУБД PostgreSQL.
>
> В связи с этим ***рекомендуется***:
>
> 1. Во всех стандартных случаях применять *Полное резервное копирование*.
> 2. *Резервное копирование схемы* применять при портировании системы (например, при портировании с ОС CentOS на ОС Debian).

Перейти к Содержанию...

5.6.3. Пользователи и разрешения



Дерево меню для данного раздела:

1. Выход
2. Получение списка пользователей
3. Добавление конечного пользователя
4. Добавление внешнего пользователя
5. Изменение имени пользователя
6. Удаление пользователя
7. Выдать доступ к Workflow
8. Отозвать доступ к Workflow
9. Разблокировать Workflow для пользователя

Данное меню позволяет создавать/удалять пользователей, менять имена пользователей и менять им права доступа.

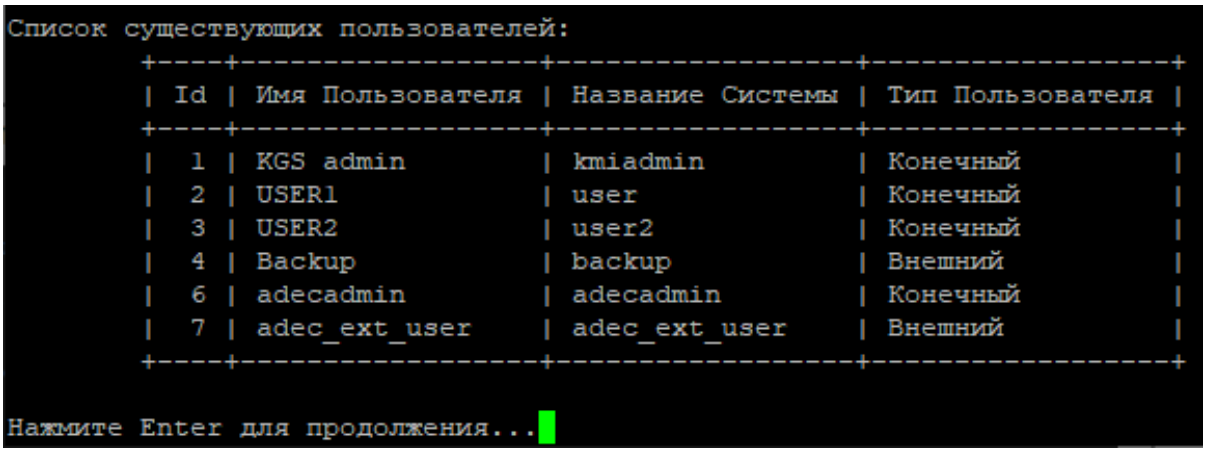
После создания нового пользователя необходимо обратиться к администратору KGS, который ОБЯЗАН:

1. Для Конечного пользователя: создать пользователя на FTPсервере и Processing Server, выдать ему права, создать директории пользователя на этих серверах.
2. Для Внешнего пользователя: создать пользователя на FTPсервере, выдать ему права, создать директории пользователя на FTPсервере.

В противном случае выполнение операций для данного пользователя приведет к ошибке.

5.6.3.1. Получение списка пользователей

Просмотр списка существующих пользователей и их тип (графа *Тип Пользователя*).



5.6.3.2. Добавление конечного пользователя

Добавление конечного пользователя (Terminal User).

Конечные пользователи - операторы Системы, имеющие физический доступ к KGS. Примером таких пользователей могут быть сотрудники, осуществляющие настройку Системы и/или генерацию и экспорт ключей.

5.6.3.3. Добавление внешнего пользователя

Добавление внешнего пользователя (External User).

Внешние пользователи - потребители Системы, они не имеют физического доступа к KGS, но имеют доступ к FTP-серверу для получения данных из Системы или загрузки туда данных для обработки Системой.

Внешние пользователи при создании привязываются к одной из сущностей:

- Поставщик;
- Оператор;
- Производитель;
- Внешний сервер;
- Партнер.

5.6.3.4. Изменение имени пользователя

Изменение имени пользователя. Под этим именем пользователь значится в Системе.

5.6.3.5. Удаление пользователя

Удаление пользователя из Системы.

Ограничения:

- В случае если Поставщик / Оператор / Производитель / Внешний сервер / Партнер, с которым связан удаляемый пользователь, является активным, то операция удаления будет прервана.

5.6.3.6. Выдать доступ к Workflow

Выдача выбранному пользователю прав доступа к одному или нескольким workflow.

5.6.3.7. Отозвать доступ к Workflow

Удаление для выбранного пользователя прав доступа к одному или нескольким workflow.

5.6.3.8. Разблокировать Workflow для пользователя

> В KMI_CONSOLE используется многопользовательский режим: в консоли могут работать одновременно несколько пользователей (пользователи подключаются к консоли удаленно, например, по SSH). Если один пользователь работает в workflow, то указанное WF будет заблокировано для других пользователей. По окончании работы пользователя с WF блокировка снимается. См. Многопользовательский режим и блокировка Workflows.
>
> Данное workflow используется для принудительной разблокировки workflow.

Особенности:

- Если пользователь передумал и не хочет снимать блокировку с workflow, то для выхода он должен **нажать *Ctrl+C***.
- Если пользователь прервет выполнение WF "**Разблокировать Workflow для пользователя**", нажав *Ctrl+Z*, то данное workflow будет заблокировано для ВСЕХ пользователей (в т.ч. и для самого администратора KGS).
- Разблокировать WF "**Разблокировать Workflow для пользователя**" можно, только перезапустив службу KMI_FW_DAL.

Перейти к Содержанию...

5.6.4. PGP Ключи Пользователя

```
*************
*           *
* PGP ключи *
*           *
*************

Выберите операцию для выполнения, возможные варианты:
         0 - Выход
         1 - Получение списка ключей
         2 - Импорт открытых PGP ключей
         3 - Создание пары PGP ключей
         4 - Экспорт открытых PGP ключей
         5 - Удаление PGP ключа
         6 - Получение списка групп PGP Ключей
         7 - Добавление группы PGP Ключей
         8 - Удаление группы PGP Ключей
         9 - Получение списка связей группы с PGP Ключом
        10 - Создание связи группы с PGP Ключом
        11 - Удаление связи группы с PGP Ключом
>
```

Дерево меню для данного раздела:

1. Выход
2. Получение списка ключей

3. Импорт открытых PGP ключей
4. Создание пары PGP ключей
5. Экспорт открытых PGP ключей
6. Удаление PGP ключа
7. Получение списка групп PGP Ключей
8. Добавление группы PGP Ключей
9. Удаление группы PGP ключей
10. Получение списка связей группы с PGP Ключом
11. Создание связи группы с PGP Ключом
12. Удаление связи группы с PGP Ключом

Данное меню позволяет управлять PGP-ключами пользователей (просмотр, импорт с FTP, генерация, экспортирование, удаление).

Ключи используются для шифрования данных при экспорте.

5.6.4.1. Получение списка пользовательских ключей

Просмотр списка PGP-ключей (public + private) (ключей, привязанных к выбранному Виду Партии, либо всех PGP ключей) и их атрибутов (название и тип ключа).

Если PGP-ключ недействителен (expire_time > current_time), то такой ключ в таблице не отображается.

5.6.4.2. Импорт открытых PGP ключей

Импорт с FTP файла с public PGP-ключом, с помощью которого будет осуществляться шифрование данных.

Особенности:

- Имя ключа (Key Name), под которым public PGP-ключ будет обозначаться в системе, считывается из файла. При миграции имя ключа, уже хранившегося на момент миграции в системе, будет сформировано следующим образом: <имя pgp> (<имя из KGS до миграции>).

5.6.4.3. Создание пары PGP ключей

Генерация пары PGP-ключа (public+private) в системе KGS. В процессе генерации предоставляется выбор: ключ с привязкой к Виду Партии (для специальной сторонней системы, с подписью) или без привязки (без подписи).

Ограничения:

- Ограничений на количество ключей без привязки к Виду Партии - нет.
- Ключ, привязанный к Виду Партии, может быть только один.

Приватный ключ, сгенерированный в KGS, используется для расшифровки различных данных, импортируемых в KGS на обработку (SSL-сертификаты, ключи прошивки (AES/RSA ключи), импорт отчетов и т.д.). Защита (формирование подписи в комментарии) публичного ключа не требуется, так как ключи прошивки в настоящий момент доступны в открытом виде и шифрование в PGP необходимо только для безопасного импорта ключей через FTP-сервер.

5.6.4.4. Экспорт открытых PGP ключей

Экспорт public-части PGP-ключа на FTP-сервер. В процессе экспорта предоставляется выбор, какой ключ экспортировать: ключ с привязкой к Виду Партии или без привязки.

В БД KGS осуществляется поиск PGP-ключа, привязанного к указанным параметрам; ключ должен быть **парным** (т.е. существуют public и private ключи, связанные между собой) и **актуальным** (т.е. не истек срок использования *expire_date*, включая обе части). Из полученной пары public-часть PGP-ключа экспортируется на FTP-сервер в папку *out* **текущего** пользователя без дополнительного шифрования.

Если был выбран экспорт ключа с привязкой к Виду Партии, то в дальнейшем public PGP-ключ экспортируется в специальную стороннюю систему, где используется для шифрования файлов, импортируемых в KGS.

Если был выбран экспорт ключа без привязки к Виду Партии, то в дальнейшем public PGP-ключ экспортируется вовне для шифрования файлов, импортируемых в KGS (например, SSL-сертификатов, отчетов о программировании и т.д.).

> **Обратите внимание**: PGP-ключи, доступные для экспорта, сгенерированы в KGS (см. Создание пары PGP ключей). Как следствие, private-часть экспортированного PGP-ключа хранится только в системе KGS (т.е. данные, шифрованные **только** экспортированным PGP-ключом, можно расшифровать только в системе KGS).

5.6.4.5. Удаление PGP ключа

Удаление PGP ключа из Системы.

Особенности:

- Если у выбранного ключа есть связанная public или private часть, то будет выведено предупреждение. При подтверждении операции будут удалены обе (public+private) части PGP-ключа.

5.6.4.6. Получение списка групп PGP Ключей

Просмотр списка групп PGP ключей (только групп).

5.6.4.7. Добавление группы PGP Ключей

Создание группы PGP ключей.

5.6.4.8. Удаление группы PGP ключей

Удаление группы PGP ключей.

Ограничения:

1. Если к группе привязаны ключи, то удаление запрещено.

5.6.4.9. Получение списка связей группы с PGP Ключом

Просмотр списка PGP-ключей, входящих в выбранную группу, и их (ключей) параметров.

5.6.4.10. Создание связи группы с PGP Ключом

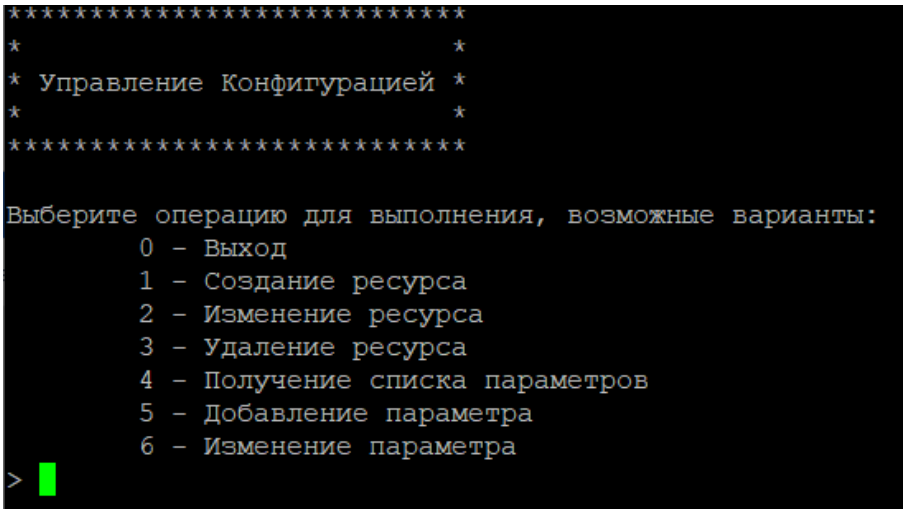
Добавление PGP ключа в группу.

5.6.4.11. Удаление связи группы с PGP Ключом

Удаление PGP ключа из группы.

Перейти к Содержанию...

5.6.5. Конфигурация



Дерево меню для данного раздела:

1. Выход
2. Создание ресурса
3. Изменение ресурса
4. Удаление ресурса
5. Получение списка параметров
6. Добавление параметра
7. Изменение параметра

Данное меню позволяет (частично) настраивать интерфейс: добавлять/удалять/редактировать источники данных (resources) и их параметры.

5.6.5.1. Создание ресурса

Добавление источника данных (ресурса):

- Workflow.
- FTP connection.

5.6.5.2. Изменение ресурса

> Настоятельно не рекомендуется изменять источники данных (ресурса), с тем чтобы в дальнейшем не возникла ошибка при обновлении консоли.

Изменение имени источника данных (ресурса).

5.6.5.3. Удаление ресурса

Удаление источника данных (ресурса).

5.6.5.4. Получение списка параметров

Просмотр списка параметров для ресурса указанного типа.

5.6.5.5. Добавление параметра

Добавление нового параметра для ресурса указанного типа.

Особености:

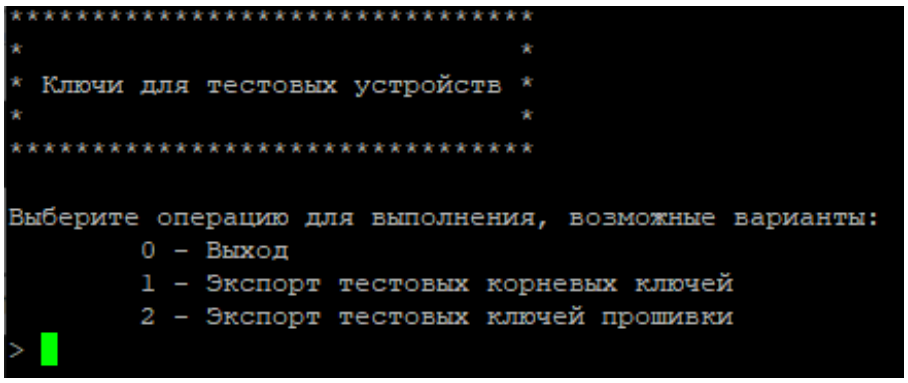
- Имя параметра (parameter code) не может быть изменено впоследствии.

5.6.5.6. Изменение параметра

Изменение параметра (тип данных, значение) для ресурса указанного типа.

Перейти к Содержанию...

5.7. Ключи для тестовых устройств



Дерево меню для данного раздела:

1. Выход
2. Экспорт тестовых корневых ключей
3. Экспорт тестовых ключей прошивки

5.7.1. Экспорт тестовых корневых ключей

Экспорт нешифрованных значений ВСЕХ OTP-ключей, описанных в OTP карте ключей, либо производных (от этих) ключей, требующихся для **тестовых** партий устройств и приемников.

Особенности:

- Разрешено экспортировать только тестовые производные ключи, т.е. сформированные только по тестовому RK KDF профилю.
- В OTP-карте не все ключи могут иметь связанные RK KDF профили. В этом случае ключ не выгружается.

Максимальное количество устройств (чипов) для тестового Вида Партии - 5000 шт.

Ключи экспортируются в виде файлов на FTP-сервер в папку *out* для текущего (осуществляющего операцию) пользователя либо одного из Внешних пользователей.

Список пользователей, которые могут быть получателями данных, определяется как текущий пользователь либо внешние пользователи, привязанные к Поставщику, связанному с выбранным Классом устройств.

Экспортируются следующие данные:

1. если RK KDF не используется (не привязан/не выбран):
    a. Экспортируются файл с ключами и (в случае обфускации) файл с обфусцированными значениями ключей.
    b. Экспортируемый файл (с OTP ключами) шифрован одним или несколькими PGP-ключами.
    c. Если у выбранного Вида Партии назначены функции OVDF/KOF и в карте ключей имеются ключи, которые необходимо обфускировать, то во второй файл выгружаются обфускированные значения ключей (но нешифрованные лестницами).
2. если выбрано "использовать KDF":
    a. 1 файл:
        i. Для каждого ключа, для которого выбран профиль RK KDF, применяется выбранный алгоритм RK KDF к OTP-ключу, после чего производный ключ записывается в первый файл. Т.е. файл содержит производные ключи.
        ii. При выгрузке производных ключей обфускация (KOF/OVDK) к выгружаемому производному ключу не применяется.
        iii. Если найдены ключи, к которым не привязан профиль RK KDF, но при этом выбрано "использовать KDF", то для этих ключей значение не выгружается (в файле ключей ставятся точки с запятой подряд ";;").
    b. 2 файл:
        i. Второй файл (RK KDF config) - конфиг с описанием для каждого OTP-ключа, номера и имени профиля RK KDF, использованных при экспорте.
        ii. В файл конфига добавляются только строки для тех RK KDF профилей, которые были выбраны пользователем при выполнении workflow.
    c. Оба файла (с ключами и конфигом) добавляются в zip-архив, который шифруется PGP-ключами и экспортируется на FTP.

Перейти к Содержанию...

5.7.2. Экспорт тестовых ключей прошивки

Экспорт нешифрованных значений ВСЕХ Ключей Прошивки, требующихся для **тестовых** партий устройств и приемников.

Ключи прошивки экспортируются в виде файлов на FTP-сервер в папку *out* для текущего (осуществляющего операцию) пользователя либо одного из Внешних пользователей.

Список пользователей, которые могут быть получателями данных, определяется как текущий пользователь либо внешние пользователи, привязанные к Поставщику, связанному с выбранным Классом устройств.

Экспортируемый архив шифрован одним или несколькими PGP-ключами пользователя, для которого осуществляется экспорт.

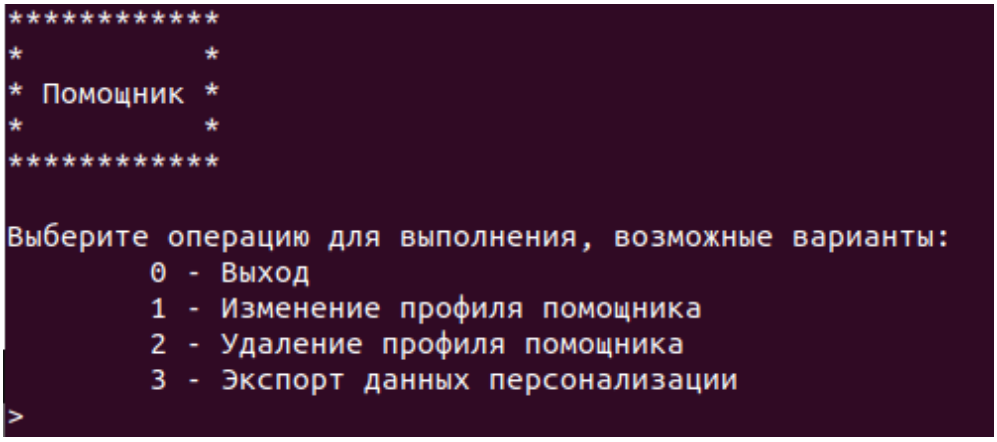
Особенности:

- Выгружаются симметричные ключи и приватные ключи RSA (включающие также публичную часть).

- Обфускация к ключам прошивки при выгрузке не применяется.

Перейти к Содержанию...

5.8. Помощник



Дерево меню для данного раздела:

1. Выход
2. Изменение профиля помощника
3. Удаление профиля помощника
4. Экспорт данных персонализации

Данное меню позволяет работать с Помощниками (переименовывать/удалять/создавать и экспортировать данные и т.п.).

5.8.1. Изменение профиля помощника

Переименование профиля Помощника.

5.8.2. Удаление профиля помощника

Удаление профиля Помощника.

Допущения и ограничения:

1. Связи профилей Помощников отсутствуют, удаление возможно в любой момент времени.
2. Удаление логическое, как в других сущностях (устанавливается актуальное del_date вместо NULL).

5.8.3. Экспорт данных персонализации

Система осуществляет выбор либо создание профиля Помощника (с типом 1 - "personalization data"), а затем (с помощью этого профиля) - подготовку и экспорт **всех** данных, необходимых для персонализации чипов в системе KTS.

> Данный помощник объединяет шаги следующих отдельных сценариев (сценарии представлены в порядке их блокировки на время выполнения данного помощника):

1. Проверка OTP (тестовые вектора для проверки OTP-ключей для завода)
2. Экспорт файла Fusemap конфигурации на BBX (конфигурации OTP-бит чипов партии для записи на заводе через BBX)
3. Экспорт конфигурации партии на BBX (конфигурация Типа Партии / Номера Партии для BBX)
4. Экспорт OTP ключей (OTP-ключи чипов партии для записи на заводе через BBX)

Перейти к Содержанию...