GS LABS
GS GROUP

Публичный - L0

Система генерации ключей Keys Generation System (KGS)

Общее описание

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

Содержание

1. Аннотация

Данный документ содержит общее описание инфраструктуры для работы с ключами (KMI). Документ содержит назначение системы, общее описание системы и её составных частей, порядок взаимодействия между ними.

Документ предназначен для широкого круга специалистов как технического, так и гуманитарного профиля, а также для руководящего состава, которым необходимо составить общее представление о системе KMI, ознакомиться с основным функционалом и структурой.

Общее описание является публичным документом (public document), т.е. распространяемым среди сотрудников группы компаний GS Labs и партнеров компании.

2. Термины и сокращения

Термин	Определение
API	Набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) для использования во внешних программных продуктах. Используется программистами для написания всевозможных приложений.
AUX-keys	Вспомогательные ключи, используемые в работе внешних устройств и систем (Link Encryption, Cryptokeeper, CAS DB, смарт-карты).
CAS	Система Условного Доступа.
ChipBlackBox	Программно-аппаратный комплекс персонализации чипов.
Cryptokeeper	Устройство, используемое для хранения и шифрования приватных данных CAS (например, ключей).
Database Abstraction Layer (DAL)	Один из компонентов общей инфраструктуры, обеспечивающий интерфейс для доступа к единой базе данных всех прочих компонентов и приложений.
External Server (внешний сервер)	Любой сервер, на который экспортируются ключи из системы KMI (SignServer, ChipBlackBox и т.д.).
Firmware keys (fw keys, ключи прошивки)	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. Также ключи могут быть только общими и быть связанными с одной или несколькими сущностями: DeviceClass, PartType и STBModel.
Framework	Структура программной системы; программное обеспечение, облегчающее разработку и объединение разных компонентов большого программного проекта. Framework может включать вспомогательные программы, библиотеки кода, язык сценариев и другое ПО, облегчающее разработку и объединение разных компонентов большого программного проекта. Обычно объединение происходит за счёт использования единого API.

FTP	Протокол передачи файлов – стандартный протокол, предназначенный для передачи файлов по TCP-сетям (например, Интернет). Протокол построен на архитектуре "клиент-сервер" и использует разные сетевые соединения для передачи команд и данных между клиентом и сервером.
KMI (Key Management Infrastructure)	Инфраструктура для работы с ключами: генерация, экспорт, импорт, управление.
LE-набор	Набор ключей, хранящихся в системе и привязанных к одному из PartType.
LE-блок	Блок данных, содержащий ключи какого-либо LE-набора, зашифрованные одним из общих OTP ключей чипа и содержащий информацию о PartType, индексе OTP ключа и подпись SHA-256 для всего блока.
LE-комплект	Набор из двух LE-блоков, передаваемый на приемник. Ключи в каждом LE-блоке зашифрованы одним из OTP ключей соответствующего чипа (host / security) приемника.
Master Key	Основные ключи защиты служебных сообщений CAS. Ключи разделяются по функции обработки (шифрование, подпись) и адресации сообщения (индивидуальные, групповые, общие для партии Part Type, глобальные (общие) для экземпляра CAS).
OTP-keys (One Time Programmable)	Ключи, которые прошиваются в однократно программируемую область памяти в чипе.
Sign Server	Сервер, осуществляющий шифрование и подпись переданных на него прошивок для приемников.
SSL	Криптографический протокол, который обеспечивает защищенную передачу информации. Используется в тех случаях, когда нужно обеспечить должный уровень защиты информации, которую пользователь передает серверу. Для работы протокола требуется, чтобы на сервере был установлен SSL-сертификат.
SSL-набор	Несколько SSL-пакетов, предназначенных для записи в один STB. Каждый SSL-пакет из набора будет использоваться своим программным модулем в прошивке приемника. Т.е. SSL-пакет #1 - в Selene, SSL-пакет #2 - APlatform (Android) и т.д.
SSL-пакет	Два файла: SSL сертификат (как правило, в формате X.509) и связанный приватный ключ.
STB	Ресивер цифрового телевидения.

TDE (Transparent Database Encryption)	Компонент системы KMI, обеспечивающий шифрование "на лету" секретной информации в базе данных.
Workflow	Графическое представление потока задач в процессе и связанных с ним под-процессов, включая специфические работы, информационные зависимости и последовательность решений и работ.

Сокращение	Расшифровка
API	Application Programming Interface
AUX	Auxiliary
BBX	BlackBoX
DAL	Database Abstraction Layer
DB	Database
DRM	Digital Rights Management
FW	Framework
HES	Hybrid Encryption System
KMI	Key Management Infrastructure
LE	Link Encryption
OTP	One Time Programmable
SSL	Secure Sockets Layer
STB	Set-Top-Box
TDE	Transparent Database Encryption
TL	Transport Layer
БД	База Данных
ПО	Программное Обеспечение

3. Назначение

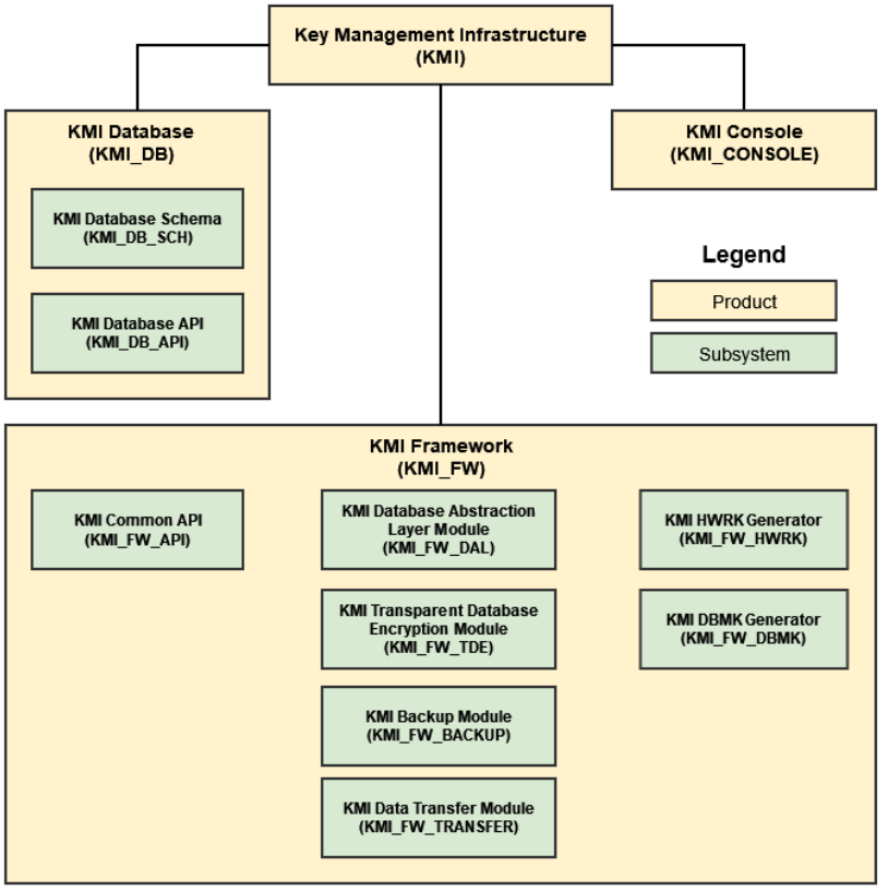
Продукт KMI предназначен для генерации, хранения и экспорта OTP-ключей для персонализации чипов. Главными преимуществами KMI являются:

- Реализация полноценной БД для управления и хранения ключами с возможностью её регулярного пополнения в процессе функционирования.
- Создание комплекта разработчика, стандартизирующего и упрощающего доступ к базе данных для создания различных приложений, поддерживающих необходимые рабочие процессы.
- Схема развёртывания (включая физическое расположение серверов), равно как база данных и комплект разработчика, проектируются максимально защищённым способом.

Перейти к Содержанию...

4. Описание KGS

4.1. Архитектура



4.1.1. KMI Database (KMI_DB)

Каждый из компонентов KGS DB представляет собой SQL-скрипт, выполняемый с помощью PostgreSQL-клиента и создающий определенный набор объектов в БД. Скрипт предназначен для однократной установки администратором системы.

Список реализованных компонентов:

Компонент	Описание
KMI_DB_SCH	Модель данных. Подсистема содержит только скрипт создания базы данных (таблицы, ключи, индексы, последовательности), включая начальное наполнение системных справочников.

KMI_DB_API	Серверная логика. Подсистема содержит только серверную (БД) логику (хранимые процедуры, представления, триггеры и т.п.) и является зависимой от KMI_DB_SCH.

4.1.2. KMI Framework (KMI_FW)

Каждый из компонентов инфраструктуры представляет собой HES-модуль, предоставляющий внешние интерфейсы для выполнения определенных операций, специфичных для данного модуля.

Под интерфейсами в данном случае понимается возможность приема сообщения (XML) с использованием возможностей HES-платформы (Transport Layer). В сообщении указывается информация, достаточная для вызова той или иной функции компонента. Формат сообщения (структура XML) фиксирован в рамках KMI. Результат выполнения функции также передается вызывающей стороне с помощью HES-сообщений.

Список реализованных компонентов:

Компонент	Описание
KMI_FW_API	Компонент, содержащий все интерфейсы KMI. Содержит запросы к остальным компонентам KMI Framework (при необходимости). В его задачи входят прием параметров, упаковка их в сообщение, передача требуемому модулю, получение ответа и возврат его вызывающей стороне.
KMI_FW_TDE	Компонент шифрования данных при записи в БД и чтении из нее. Содержит все алгоритмы шифрования, связанного с KMI и BlackBox. **Доступ к компоненту ограничен**. Применяется в KMI и на внешних серверах, использующих в своей работе лестницу ключей, генерируемую в KMI (ChipBlackBox, KMS и т.п.).
KMI_FW_DAL	Компонент, обеспечивающий взаимодействие с базой данных. Единственный компонент, взаимодействующий с БД. Остальные компоненты KMI_FW взаимодействуют с БД только через интерфейсы DAL.
KMI_FW_BACKUP	Компонент, обеспечивающий запуск бекапа базы данных по запросам пользователей.
KMI_FW_TRANSFER	Компонент, обеспечивающий передачу данных между сервером KMI и FTP-сервером, к которому имеют доступ пользователи.
KMI_FW_HWRK	Компонент, с помощью которого осуществляется генерация HWRK-ключа (используется в лестнице ключей).

KMI_FW_DBMK	Компонент, с помощью которого осуществляется генерация DBMK-ключа (используется в лестнице ключей).

4.1.3. KMI Console (KMI_CONSOLE)

KMI_Console содержит различные workflow-компоненты для реализации всех функций системы, перечисленных в главе 3.

Каждый из workflow-компонентов представляет собой Python-скрипт, содержащий в себе некоторую бизнес-логику, такую, как, например, генерация ключей или импорт результатов прошивки чипов.

Алгоритм работы скрипта в общем случае сводится к собственной логике и вызову функций из состава инфраструктурных компонентов. Вызов компонентов осуществляется через общую библиотеку (KMI_FW_API).

Компоненты KMI_Console имеют графический интерфейс (интерфейс командной строки), через который пользователь осуществляет выполнение операций в системе KMI.

4.1.4. HES platform

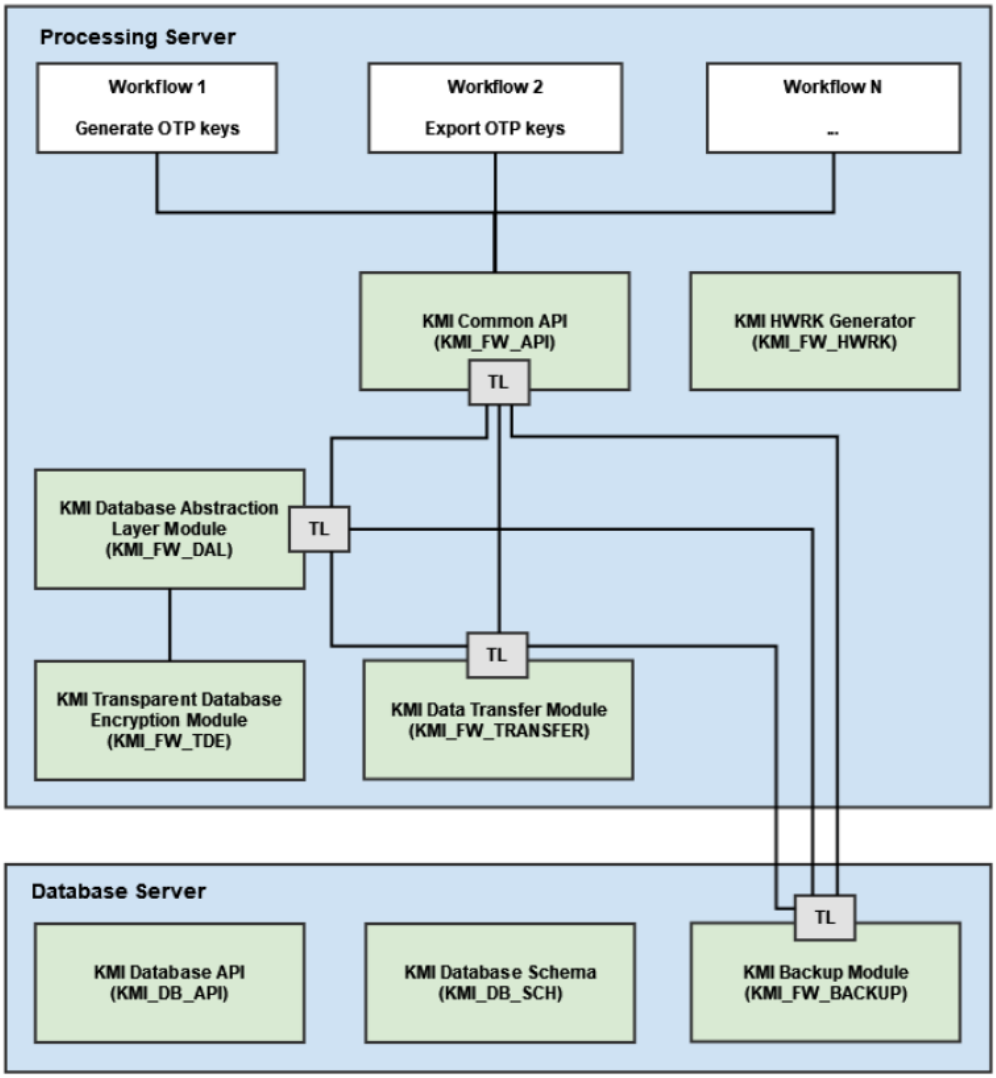
HES platform это продукт (платформа), на базе которого строятся модули KMI. HES обеспечивает интерфейс взаимодействия компонентов между собой. Составной частью HES являются TL (Transport Layer).

HES 3.0 сделан на базе библиотеки очереди сообщений ZeroMQ и предоставляет обёртку для её использования в продуктах. Библиотека служит для организации собственных очередей сообщений и простой их маршрутизации. Её использование в составе обновлённого HES позволяет отказаться от поддержки нестандартного протокола взаимодействия транспортного уровня, а заодно от службы маршрутизации сообщений посредством **прямого** обращения к желаемому сервису.

Перейти к Содержанию...

4.2. Взаимодействие компонентов

Схематично состав компонентов KMI и взаимосвязи между ними представлены на рисунке ниже.



Управление системой осуществляется посредством KVM. Оператор, используя KVM, подключается к Processing Server, а тот, в свою очередь, к серверу БД (Database Server). Для работы оператора с системой KGS используется пользовательский интерфейс (User Interface), который является частью KMI_CONSOLE.

Все компоненты Framework, за исключением подсистемы бекапирования (KMI_FW_BACKUP), устанавливаются на Processing Server (см. Схема развертывания). KMI_FW_BACKUP устанавливается вместе с компонентами БД (KMI_DB_API, KMI_DB_SCH) на Database Server (см. Схема развертывания).

⚠ Компонент KMI_FW_TDE помимо Processing Server (TDE(KMI)) также может быть установлен на внешний сервер? если тот использует лестницу ключей, сгенерированную системой KMI, например, на SignServer - TDE(SS).

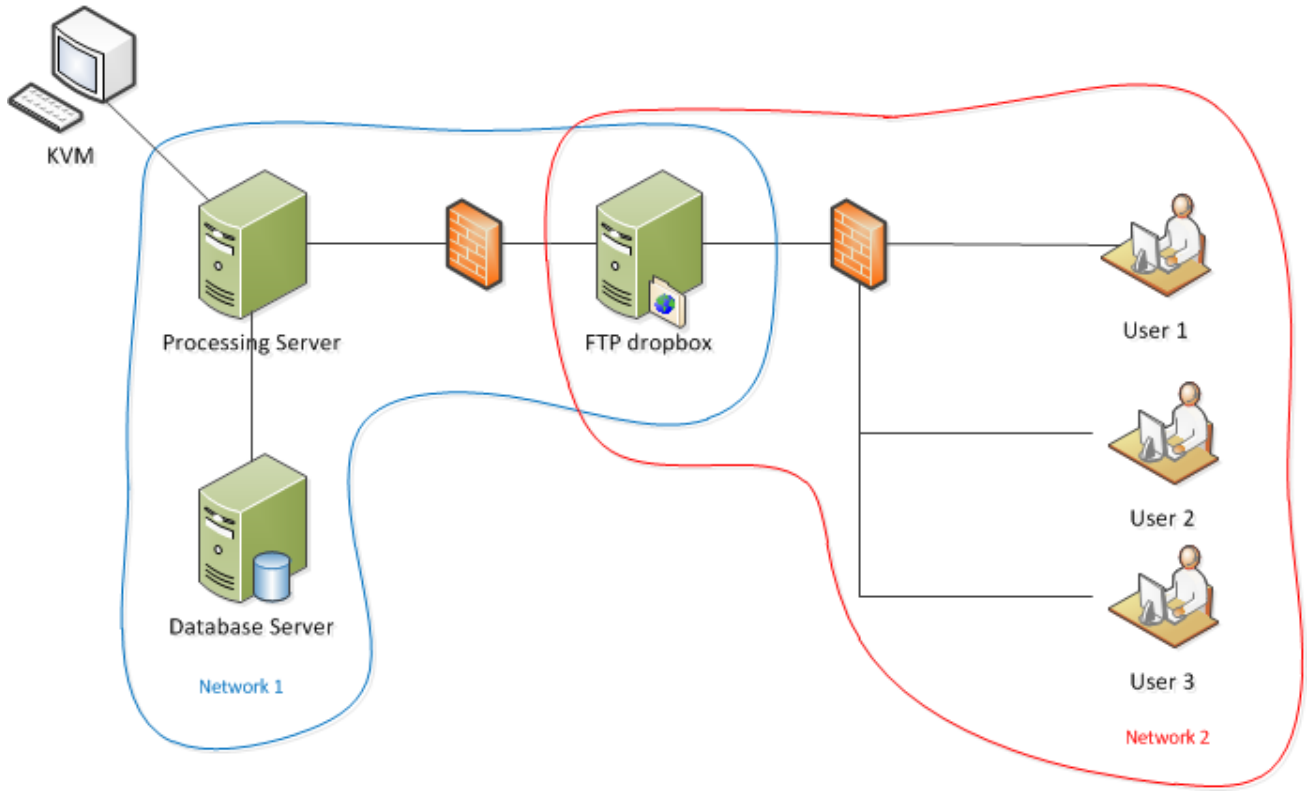
В основе компонентов KMI_FW, вне зависимости от места их установки, лежит платформа HES. Взаимодействие между компонентами осуществляется путем обмена сообщениями (XML) с использованием возможностей HES-платформы (Transport Layer).

Для выполнения задач, заданных оператором, используются рабочие процессы (workflows). Количество и состав workflows определяются версией ПО и типом решаемой задачи. При работе workflow вызываются функции из состава других инфраструктурных компонентов. Вызов компонентов осуществляется через общую библиотеку (KMI_FW_API).

Перейти к Содержанию...

4.3. Схема развертывания

Схема развертывания компонентов приведена на рисунке ниже.



На схеме используются следующие обозначения:

- **Database Server** – сервер, на котором развернута база данных (PostgreSQL). Входит в выделенную физическую сеть “Network 1”.

- **Processing Server** – сервер, на котором развернуты все компоненты (включая DAL) общей инфраструктуры (Framework), обеспечивающие выполнение определенных задач (workflows). Сервер входит в выделенную физическую сеть “Network 1”.
  Оба сервера (Database Server и Processing Server) расположены в отдельном защищенном помещении, доступ в которое ограничен.

  ⚠ На всех серверах используется ОС Debian / Ubuntu.

- **KVM** (keyboard, video, mouse) – **Терминал** – физическое оборудование, подсоединенное к Processing Server для запуска оператором определенных задач (workflows).

  ⓘ Фактически это ЭВМ/терминал, с которой(которого) пользователь управляет KGS (работает в KMI_CONSOLE).

  Предполагается, что пользователь имеет доступ к KGS только посредством KVM, который подключен к серверу в защищенном помещении.

- **FTP dropbox** – выделенный сервер для обмена информацией по FTP. Входит в две физические сети “Network 1” и “Network 2”. Сервер осуществляет соединения в рамках сети “Network 1” только с Processing Server и только по протоколу FTP (firewall). Сервер осуществляет соединения в рамках сети “Network 2” только с фиксированным набором рабочих станций и только по протоколу FTP (firewall).
- **User 1/2/3** – рабочие станции в рамках сети “Network 2”, которым разрешен доступ на FTP dropbox.

Передача данных в/из KGS осуществляется только посредством файлов. Все файлы, в свою очередь, пересылаются только через FTP dropbox.

Перейти к Содержанию...

4.4. Принцип работы

Программа KMI, получив введенные с помощью User Interface команды оператора (KVM), выполняет поставленные задачи. Сформировав команды и выполнив дополнительные действия (логирование событий, бекапирование системы и т.д.), Processing Server обращается к БД, расположенной на Database Server. Производится обмен данными с базой (извлечение данных, запись ключей в базу и т.д.). Результат выполнения операций отображается в пользовательском интерфейсе.

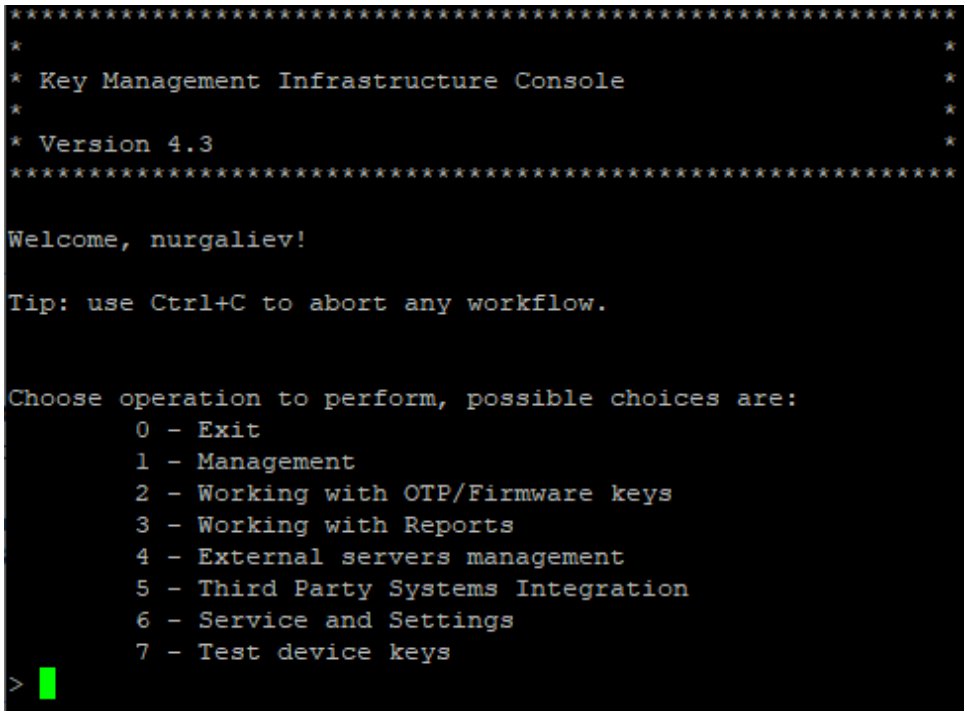
Экспорт/импорт ключей в БД осуществляется оператором с помощью сервера FTP dropbox: оператор экспортирует сгенерированные ключи на сервер, с которого, в свою очередь, их может забрать пользователь одной из рабочих станций в рамках сети “Network 2”, которым разрешен доступ на FTP dropbox. Для импорта ключей в БД пользователь рабочей станции сохраняет ключи на FTP dropbox; оператор забирает их с сервера и импортирует в базу KMI.

Перейти к Содержанию...

5. KMI Console (User Interface)

Управление KMI осуществляется посредством пользовательского интерфейса. Создание интерфейса реализовано, как и все компоненты Framework, с помощью Python-скрипта.

Пример интерфейса (русский язык) приведен на рисунке ниже.



KMI Console может быть представлена на двух языках: Русский, English.

Меню содержит основные операции, выполняемые системой и определяемые компонентами Workflow.

Работа в интерфейсе KMI подробно описана в документе "KMI x.x. Руководство пользователя".

Перейти к Содержанию...