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 . . . 3
2. Термины и сокращения . . . 4
3. Назначение . . . 6
4. Описание KGS . . . 7
4.1. Архитектура . . . 7
4.1.1. KGS Database (KMI_DB) . . . 7
4.1.2. KGS Framework (KMI_FW) . . . 8
4.1.3. KGS Console (KMI_CONSOLE) . . . 9
4.2. Взаимодействие компонентов . . . 9
4.3. Схема развертывания . . . 11
4.4. Принцип работы . . . 12
5. Пользовательский интерфейс . . . 13

1. Аннотация

Данный документ содержит общее описание "Системы генерации ключей Keys Generation System (KGS)" (далее по тексту - KGS или Система). 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 KGS, ознакомиться с основным функционалом и структурой.

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.
DAL	Один из компонентов общей инфраструктуры, обеспечивающий интерфейс для доступа к единой базе данных всех прочих компонентов и приложений.
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.
TDE	Компонент системы KGS, 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.
Внешний сервер (External Server)	Любой сервер, на который экспортируются ключи из системы KGS.

Сокращение	Расшифровка
API	Application Programming Interface
DAL	Database Abstraction Layer
DB	Database
FW	Framework
TDE	Transparent Database Encryption
TL	Transport Layer

БД	База Данных
ПО	Программное Обеспечение

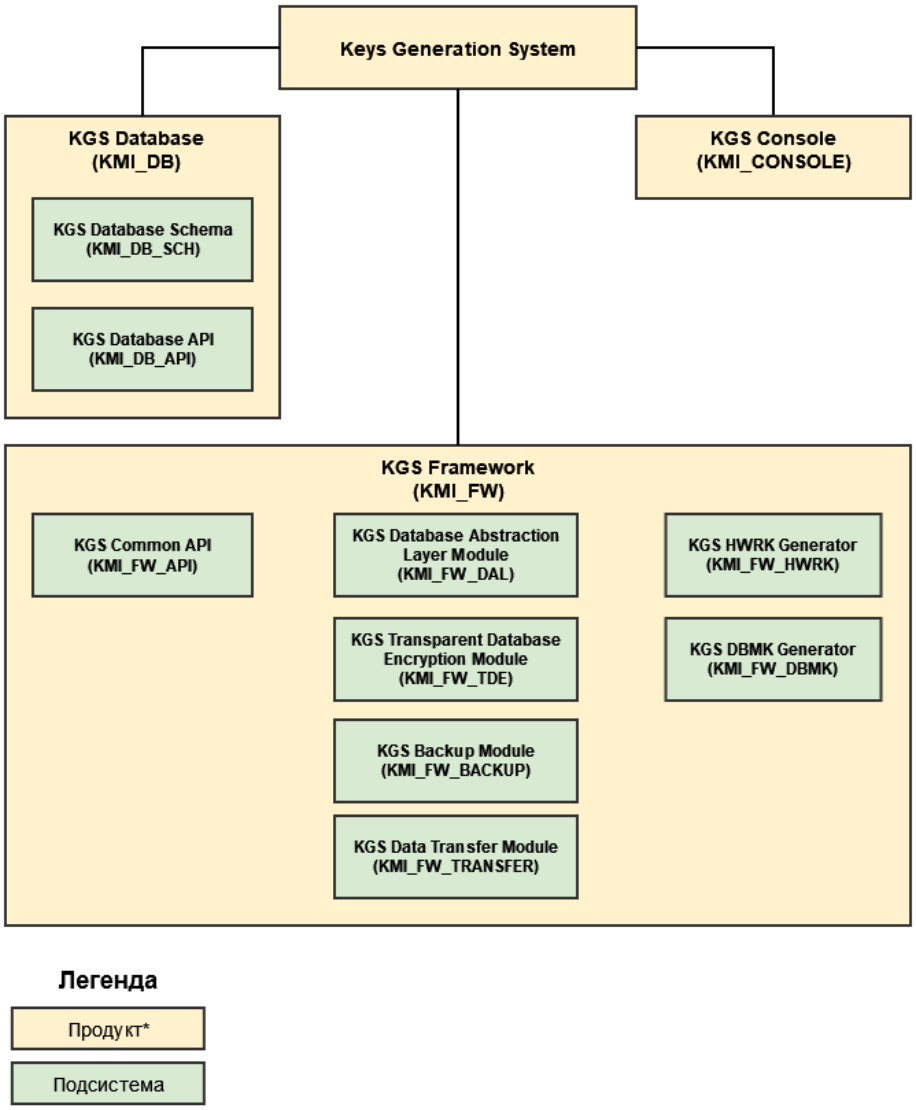
3. Назначение

Система 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.

Перейти к Содержанию...

4. Описание KGS

4.1. Архитектура



* В скобках указываются внутренние системные обозначения компонентов

4.1.1. KGS 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
Название	**Внутреннее обозначение**	
KGS Database Schema	KMI_DB_SCH	Модель данных. Подсистема содержит только скрипт создания базы данных (таблицы, ключи, индексы, последовательности), включая начальное наполнение системных справочников.
KGS Database API	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. KGS Framework (KMI_FW)

Каждый из компонентов инфраструктуры представляет собой модуль, предоставляющий внешние интерфейсы для выполнения определенных операций.

Под интерфейсами в данном случае понимается возможность приема сообщения (XML). В сообщении указывается информация, достаточная для вызова той или иной функции компонента. Формат сообщения (структура XML) фиксирован в рамках KGS. Результат выполнения функции передается вызывающей стороне с помощью зашифрованных сообщений.

Список реализованных компонентов:

Компонент		Описание
Название	**Внутреннее обозначение**	
KGS Common API	KMI_FW_API	Компонент, содержащий все интерфейсы KGS. Содержит запросы к остальным компонентам KGS Framework (при необходимости). В его задачи входят прием параметров, упаковка их в сообщение, передача требуемому модулю, получение ответа и возврат его вызывающей стороне.
KGS Transparent Database Encryption Module	KMI_FW_TDE	Компонент шифрования данных при записи в БД и чтении из нее. Содержит все алгоритмы шифрования, связанного с KGS. **Доступ к компоненту ограничен**. Применяется в KGS и на внешних серверах, использующих в своей работе лестницу ключей, генерируемую в KGS.

KGS Database Abstraction Layer Module	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.
KGS Backup Module	KMI_FW_BACKUP	Компонент, обеспечивающий запуск бекапа базы данных по запросам пользователей.
KGS Data Transfer Module	KMI_FW_TRANSFER	Компонент, обеспечивающий передачу данных между сервером KGS и FTP-сервером, к которому имеют доступ пользователи.
KGS HWRK Generator	KMI_FW_HWRK	Компонент, с помощью которого осуществляется генерация HWRK-ключа (используется в лестнице ключей).
KGS DBMK Generator	KMI_FW_DBMK	Компонент, с помощью которого осуществляется генерация DBMK-ключа (используется в лестнице ключей).

4.1.3. KGS Console (KMI_CONSOLE)

KGS Console содержит различные workflow-компоненты для реализации всех функций системы.

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

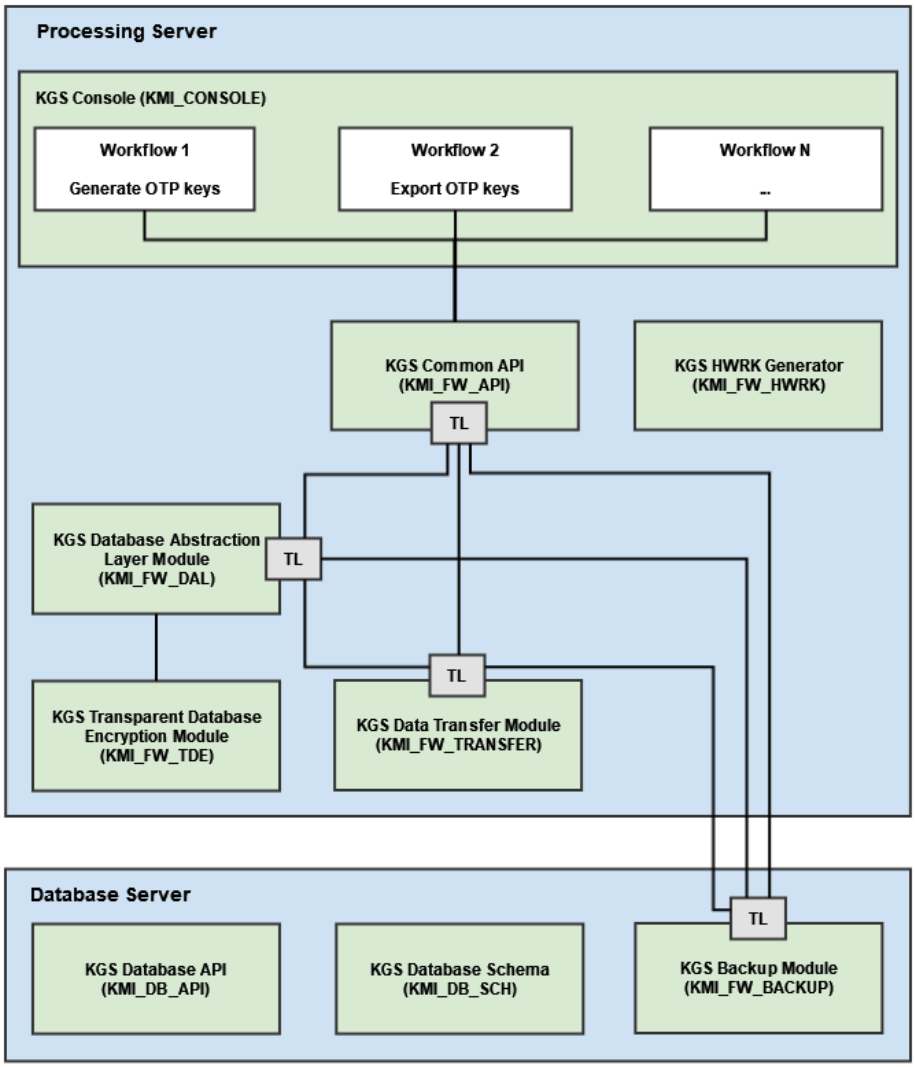
Алгоритм работы скрипта в общем случае сводится к собственной логике и вызову функций из состава инфраструктурных компонентов. Вызов компонентов осуществляется через общую библиотеку (KMI_FW_API).

Компоненты KGS Console имеют графический интерфейс (интерфейс командной строки), через который пользователь осуществляет выполнение операций в Системе.

Перейти к Содержанию...

4.2. Взаимодействие компонентов

Схематично состав компонентов KGS 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 также может быть установлен на Внешний сервер, если тот использует лестницу ключей, сгенерированную системой KGS.

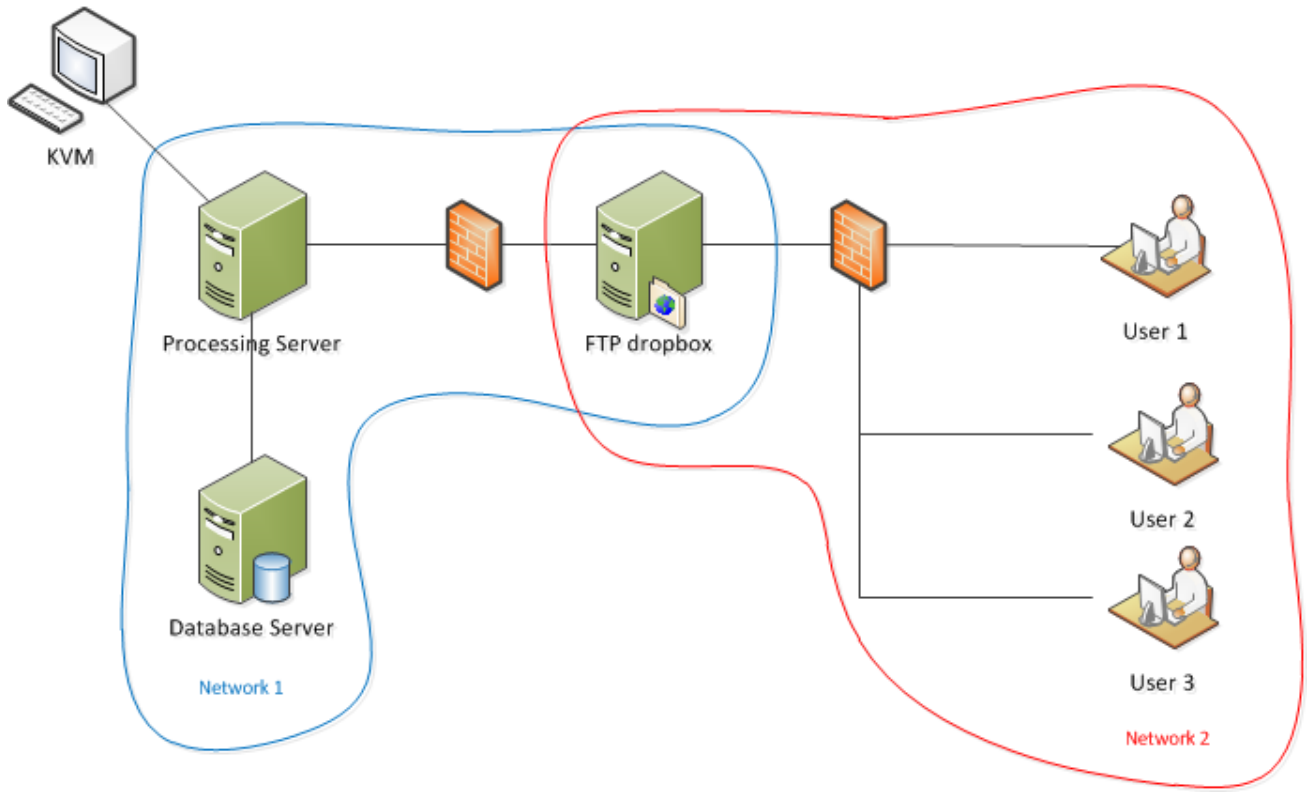
Взаимодействие между компонентами осуществляется путем обмена зашифрованными сообщениями (XML).

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

KGS, 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.

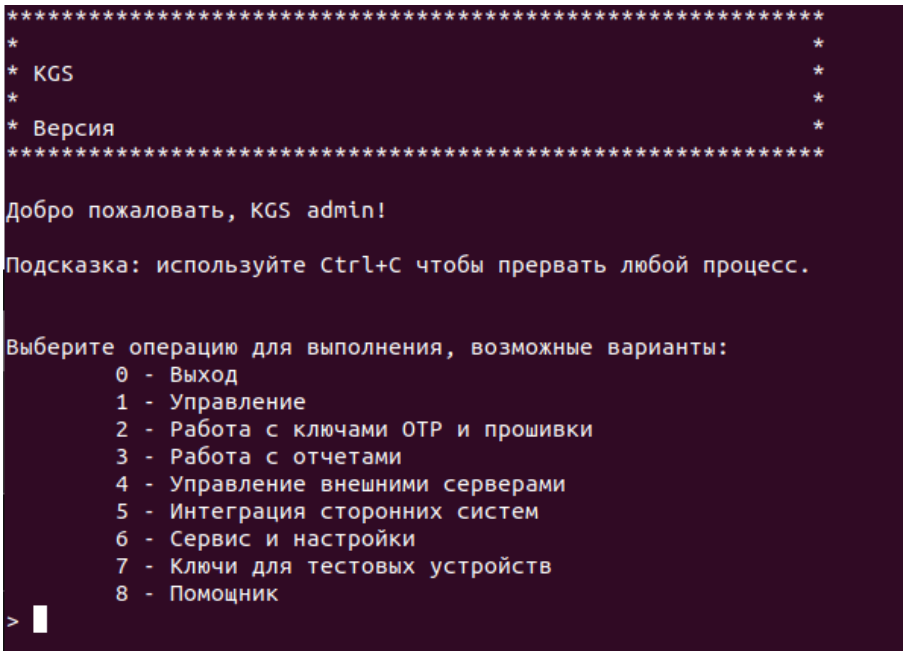
Экспорт/импорт ключей в БД осуществляется оператором с помощью сервера FTP dropbox: оператор экспортирует сгенерированные ключи на сервер, с которого, в свою очередь, их может забрать пользователь одной из рабочих станций в рамках сети “Network 2”, которым разрешен доступ на FTP dropbox. Для импорта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

Перейти к Содержанию...

5. Пользовательский интерфейс

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

Пример интерфейса (русский язык) приведен на рисунке ниже.



Пользовательский интерфейс может быть представлен на двух языках: Русский, English.

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

Работа в интерфейсе KGS подробно описана в документе "Руководство пользователя".

Перейти к Содержанию...