GS LABS
GS GROUP

Публичный - L0

Сервер передачи ключей Keys Transfer Server (KTS)

Общее описание

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

Содержание

1. Аннотация . . . 3
2. Термины и сокращения . . . 4
3. Назначение и общая характеристика системы . . . 5
3.1. Вид деятельности, для которой предназначена система . . . 5
4. Описание системы . . . 6
4.1. Структура системы и назначение ее частей . . . 6
4.2. Условия, необходимые для безопасной эксплуатации системы . . . 7
4.3. Функционирование системы . . . 7

1. Аннотация

Данный документ содержит общее описание Сервера передачи ключей Keys Transfer Server (KTS) (далее по тексту - KTS 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 KTS, 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.
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.
KGS	Система генерации ключей Keys Generation System (KGS). Продукт ООО "ПЦТ" для работы с ключами: генерация, экспорт, импорт, управление.
OTP-ключи	Ключи, которые прошиваются в однократно программируемую область памяти в чипе.
Персонализационные данные	Данные, которые программируются (персонализируются) в чип в OTP-память. К ним относятся: секретные ключи, несекретные значения (например, идентификатор чипа и пр.), а также конфигурационные настройки чипа (значения конфигурационных бит).

Сокращение	Расшифровка
ПД	Персонализационные данные
БД	База данных
API	Application Programming Interface, Интерфейс программирования приложений
FTP	File Transfer Protocol
OTP	One-Time Programmable
TDE	Transparent Database Encryption

3. Назначение и общая характеристика системы

3.1. Вид деятельности, для которой предназначена система

Сервер передачи ключей Keys Transfer Server предназначен для доставки ключей на производственную линию и занесения их уникального набора в однократно-программируемую область чипа в процессе его персонализации.

Программное обеспечение предоставляет инфраструктуру для персонализации, с возможностью:

- импорта ключей из системы KGS для партии чипов, их загрузки и сохранения в системе;
- настройки структуры базы данных в зависимости от типа устройства, для которого предназначены ключи;
- персонализации различных типов чипов путем конфигурирования системы;
- хранения ключей в зашифрованном виде;
- фиксации текущего статуса персонализации и сохранения результатов персонализации для каждого чипа;
- формирования отчетности.

Язык программирования: C++, Go

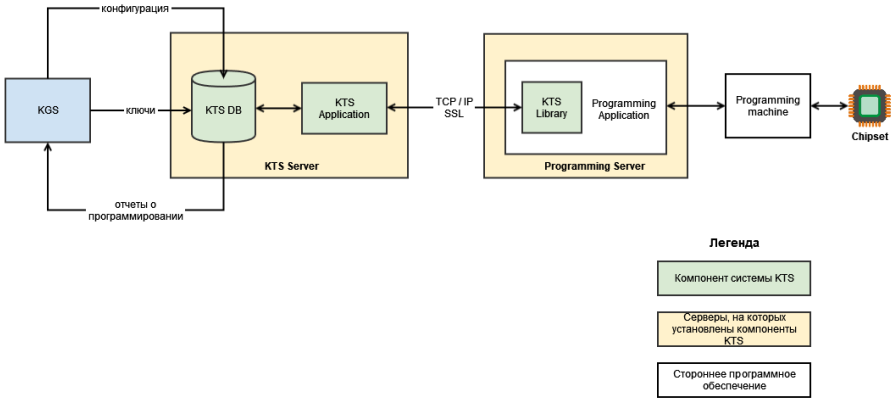
4. Описание системы

4.1. Структура системы и назначение ее частей

Система реализована на базе 3 основных компонентов (подсистем), каждый из которых включает в себя более мелкие структуры:

- **KGS** - продукт ООО "ПЦТ", предназначенный для генерации ключей, формирования требуемой конфигурации и импорта отчетов о программировании. Обмен данными осуществляется с помощью загрузки и выгрузки файлов на выделенный FTP-сервер.
- **KTS Server** - выделенный сервер на площадке завода, где происходит персонализация. Сервер развертывается в безопасной зоне, доступ к нему должен быть предоставлен только уполномоченным пользователям Системы. Сервер предназначен для хранения персонализационных данных (ключей).
  - **KTS DB (Database)** - SQL-база данных, предназначенная для хранения передаваемых из KGS ключей и конфигураций, развертывается на KTS Server, на зашифрованном разделе.
  - **KTS Application (название компонента в KTS - bbx_server_go)** - приложение-сервер, являющееся посредником между библиотекой-клиентом и базой данных, принимает запросы со стороны клиента по TCP/IP, обеспечивает шифрование данных между KTS Application и KTS Library, развертывается на KTS Server.
- **Programming Server** - выделенный сервер на площадке завода, где происходит персонализация. Сервер подключается непосредственно к оборудованию для персонализации (Programming Machine).
  - **KTS Library (название компонента в KTS - BBX_CHIP_CLIENT)** - библиотека-клиент, предназначенная для доступа к базе данных с ключами с помощью KTS Application и обеспечивающая интерфейсы для получения ключей и сохранения результатов персонализации, используя защищенный протокол обмена с KTS Application.
  - **Programming Application** - внешнее клиентское приложение, взаимодействующее непосредственно с оборудованием для персонализации чипов, и интегрированное с KTS Library. Использует своё API для запроса количества оставшихся устройств на KTS Server, для запроса ключей и тестовых векторов для наборов чипов, для записи статусов персонализации в KTS. В комплект поставки не входит.

Ниже представлена общая схема системы персонализации:



4.2. Условия, необходимые для безопасной эксплуатации системы

1. KTS Server развертывается на операционной системе Debian в виде виртуальной машины на зашифрованном разделе диска. На этой же машине находится и база данных. Для хранения БД с персонализационной информацией используется СУБД PostgreSql.
2. К серверам с ПД должен быть обеспечен доступ по защищенному каналу. Все внешние сетевые соединения также должны быть защищены специальным ПО (файрвол и т.п.).
3. Сервера с ПД должны располагаться в помещении, к которому предъявляются повышенные требования безопасности.
4. Пользователям (со стороны Programming Server) предоставляется прямой доступ только к библиотеке-клиенту.
5. Библиотека-клиент и клиентское приложение устанавливаются на компьютеры, которые работают непосредственно с программаторами чипов (Programming Machine).

4.3. Функционирование системы

Для обеспечения повышенной информационной безопасности, применяется многоступенчатое шифрование ПД, а также их хранение в зашифрованном виде.

Процесс подготовки ПД и персонализации состоит из следующих основных этапов:

1. Инициализация системы KTS:
    a. генерация фрагментов ключей защиты данных TDE на сервере KTS.
    b. KGS: генерация полной лестницы ключей TDE на основе фрагментов ключей, полученных при инициализации KTS-сервера.
    c. импорт полной лестницы TDE в систему KTS из KGS.
2. Генерация конфигурации ПД для модели чипа (разовая операция):
    a. KGS: создание конфигурации модели чипа в KGS, списка ключей и их экспорт из системы KGS.
    b. KGS: генерация файла с конфигурационными настройками(*) модели чипа и их экспорт из системы KGS.
    c. KTS: импорт конфигурации модели чипа со списком ключей и файла с конфигурационными настройками(*) с помощью скриптов из состава KTS.
3. Генерация ПД для партии чипов и загрузка их в KTS (повторяется по мере формирования заказов на производство партий чипов):
    a. KGS: генерация OTP-ключей для требуемой партии чипов и проверочных значений(*).
    b. Перенос ключей и проверочных значений(*) в систему KTS с помощью скриптов из состава KTS.
4. Альтернатива шагам 3 и 4:
    a. KGS: создание профиля "помощника", имеющего параметры для данного экземпляра KTS, и другие необходимые параметры.
    b. KGS: генерация и экспорт (из системы KGS) "кумулятивного архива", содержащего необходимый объем данных для персонализации партии чипов.
    c. KTS: обработка (и импорт) "кумулятивного архива" с персонализационными данными (с помощью скрипта из состава KTS).
5. Персонализация партий чипов для сконфигурированной модели чипа, формирование отчетов о программировании:
    a. Получение ключей (а также опционально файла с конфигурационными настройками и проверочных значений (*)) для необходимого числа чипов (число определяется возможностями Programming machine): по запросу с Programming Application библиотека KTS

Library обращается к KTS Application, которое считывает из KTS DB необходимые ПД, перешифровывает с помощью модуля TDE и отправляет в библиотеку по защищенному протоколу. Библиотека возвращает ПД в Programming Application.

b. Непосредственно программирование чипов: Programming Application, в свою очередь, посылает полученные ПД в Programming machine на запись их в OTP-память чипа (выполняется программирование чипа - персонализация).
c. Формирование отчетов о программировании: после записи ПД в чип результат программирования каждого чипа пересылается по цепочке Programming machine - Programming Application - KTS Library в KTS Application, которое сохраняет его в KTS DB. По мере накопления данных со статусами персонализации, уполномоченный пользователь Систем KTS и KGS экспортирует с помощью скриптов отчет из системы KTS и загружает его в систему KGS.

Примечание: (*) - генерация и использование файла с конфигурационными настройками и проверочных значений опциональны и определяются конкретной моделью чипа.