Клиентская JAVA-библиотека для сервера кодов аутентификации

11485466.5014.053

Инструкция по установке и эксплуатации

Содержание

1 Введение

Настоящий документ содержит руководство по установке и эксплуатации программного изделия «Клиентская JAVA-библиотека для сервера кодов аутентификации» (далее «Клиентская JAVA-библиотека для сервера КА»). Руководство включает в себя справочную информацию по работе с библиотекой «Клиентская JAVA-библиотека для сервера КА».

2 Назначение и условия применения

2.1 Назначение системы

«Клиентская JAVA-библиотека для сервера КА» представляет собой библиотеку JAVA, которая предназначена для предоставления удобного мультиплатформенного программного интерфейса к программному изделию «Сервер кодов аутентификации» в составе ПАК ФПСУ-IP.

В программном изделии «Клиентская JAVA-библиотека для сервера КА» реализовано выполнение с помощью программного изделия «Сервер кодов аутентификации» следующих основных функций:

- Создание кодов аутентификации.
- Проверка кодов аутентификации.

2.2 Условия применения системы

«Клиентская JAVA-библиотека для сервера КА» должна работать под управлением ОС, поддерживающих среду JVM версий 1.6, 1.7 и 1.8.

Для работы программного изделия «Клиентская JAVA-библиотека для сервера КА» необходим сетевой доступ к ПАК ФПСУ-IP, на котором установлено программное изделие «Сервер кодов аутентификации».

3 Установка программного изделия «Клиентская JAVA-библиотека для сервера КА»

Для того чтобы установить программное изделие «Клиентская JAVA-библиотека для сервера КА», следует скопировать содержимое дистрибутива «Клиентская JAVA-библиотека для сервера КА» на жёсткий диск компьютера.

4 Удаление программного изделия «Клиентская JAVA-библиотека для сервера КА»

Для того чтобы удалить программное изделие «Клиентская JAVA-библиотека для сервера КА», необходимо удалить с жёсткого диска компьютера ранее установленные файлы дистрибутива «Клиентская JAVA-библиотека для сервера КА».

5 Описание библиотеки

5.1 Пакеты библиотеки «Клиентская JAVA-библиотека для сервера КА»

В состав библиотеки «Клиентская JAVA-библиотека для сервера КА» входит один пакет – ru.infocrypt.sbk3j.

5.2 Классы пакета ru.infocrypt.sbk3j

В состав пакета ru.infocrypt.sbk3j входят классы:

- AuthentificationCode,
- SBKARetCode,
- ServerKA.

5.2.1 Перечисление SBKARetCode

```
java.lang.Object
  java.lang.Enum<SBKARetCode>
      ru.infocrypt.sbk3j.SBKARetCode
-----------------------------------------------------------------------
      public enum SBKARetCode
      extends java.lang.Enum<SBKARetCode>
```

Описание

Коды возврата.

Константы

Константа	Описание
SBK3J_EC_BAD_PACKET	public static final SBKARetCode SBK3J_EC_BAD_PACKET
SBK3J_EC_CONNECT	public static final SBKARetCode SBK3J_EC_CONNECT
SBK3J_EC_LENGTH	public static final SBKARetCode SBK3J_EC_LENGTH
SBK3J_EC_TIMEOUT	public static final SBKARetCode SBK3J_EC_TIMEOUT
SBKA_EC_BAD_PACKET	public static final SBKARetCode SBKA_EC_BAD_PACKET
SBKA_EC_BAD_PARAM	public static final SBKARetCode SBKA_EC_BAD_PARAM
SBKA_EC_BAD_RNG	public static final SBKARetCode SBKA_EC_BAD_RNG
SBKA_EC_BAD_TEST	public static final SBKARetCode SBKA_EC_BAD_TEST
SBKA_EC_DEVICE_IS_EMPTY	public static final SBKARetCode SBKA_EC_DEVICE_IS_EMPTY
SBKA_EC_DEVICE_NOT_FOUND	public static final SBKARetCode SBKA_EC_DEVICE_NOT_FOUND
SBKA_EC_DRIVER_INTERNAL	public static final SBKARetCode SBKA_EC_DRIVER_INTERNAL
SBKA_EC_DRIVER_NOT_FOUND	public static final SBKARetCode SBKA_EC_DRIVER_NOT_FOUND
SBKA_EC_INVALID_ADDRESS	public static final SBKARetCode SBKA_EC_INVALID_ADDRESS
SBKA_EC_INVALID_IMI	public static final SBKARetCode SBKA_EC_INVALID_IMI
SBKA_EC_INVALID_KA	public static final SBKARetCode SBKA_EC_INVALID_KA
SBKA_EC_INVALID_PIN	public static final SBKARetCode SBKA_EC_INVALID_PIN
SBKA_EC_INVALID_VERSION	public static final SBKARetCode SBKA_EC_INVALID_VERSION
SBKA_EC_LIB_NOT_INIT	public static final SBKARetCode SBKA_EC_LIB_NOT_INIT
SBKA_EC_NO_KEY	public static final SBKARetCode SBKA_EC_NO_KEY

Константа	Описание
SBKA_EC_NO_REGION	public static final SBKARetCode SBKA_EC_NO_REGION
SBKA_EC_NO_RESOLVE	public static final SBKARetCode SBKA_EC_NO_RESOLVE
SBKA_EC_NO_RESPONSE	public static final SBKARetCode SBKA_EC_NO_RESPONSE
SBKA_EC_NO_SESSION	public static final SBKARetCode SBKA_EC_NO_SESSION
SBKA_EC_NO_SOCKET	public static final SBKARetCode SBKA_EC_NO_SOCKET
SBKA_EC_NO_TCPIP	public static final SBKARetCode SBKA_EC_NO_TCPIP
SBKA_EC_NOT_IMPLEMENTED	public static final SBKARetCode SBKA_EC_NOT_IMPLEMENTED
SBKA_EC_OK	public static final SBKARetCode SBKA_EC_OK
SBKA_EC_SIZE_NOT_ENOUGH	public static final SBKARetCode SBKA_EC_SIZE_NOT_ENOUGH

Методы

Модификатор и тип	Метод и описание
static SBKARetCode	get(int error) Возвращает определенный объект SBKARetCode
java.lang.String	getInfo() Возвращает информацию об ошибке
int	getValue() Возвращает внутренний порядковый номер ошибки
static SBKARetCode	valueOf(java.lang.String name) Возвращает константу перечисления данного типа с указанным именем
static SBKARetCode[]	values() Возвращает массив констант в порядке, в котором они были указаны в перечислении данного типа

Метод get

```
public static SBKARetCode get(int error)
```

Метод getInfo

```
public java.lang.String getInfo()
```

Метод getValue

```
public int getValue()
```

Метод valueOf

```
public static SBKARetCode valueOf(java.lang.String name)
```

Описание:

Возвращает константу перечисления данного типа с указанным именем. Строка должна точно соответствовать идентификатору константы, указанному в перечислении данного типа. (Лишние пробелы недопустимы.)

Параметры:
`name – возвращаемое имя константы перечисления.`

Возвращаемое значение:

константа перечисления данного типа с указанным именем

Исключения:
`java.lang.IllegalArgumentException – если перечисление данного типа не содержит константу с указанным именем`

`java.lang.NullPointerException – если аргумент равен null`

Метод values

```
public static SBKARetCode[] values()
```

Описание:

Возвращает массив констант в порядке, в котором они были указаны в перечислении данного типа. Данный метод позволяет перебрать константы следующим образом:

```
for (SBKARetCode c : SBKARetCode.values())
    System.out.println(c);
```

Возвращаемое значение:

Массив констант в порядке, в котором они были указаны в перечислении данного типа.

5.2.2 Класс AuthentificationCode

```
java.lang.Object

        ru.infocrypt.sbk3j.AuthentificationCode
-----------------------------------------------------------------------

     public class AuthentificationCode

     extends java.lang.Object
```

Описание

Код аутентификации.

Конструкторы

AuthentificationCode (byte[] input) – структурирование кода аутентификации (КА).

```
public AuthentificationCode(byte[] input)
```

Параметры:

```
input - сериализованный КА
```

Методы

Модификатор и тип	Метод и описание
byte[]	getByteArray() Сериализованный КА
byte	getDirection() Направление передачи КА (от сервера к клиенту или от клиента к серверу)
int	getFromNumber() Номер отправителя (номер устройства, которое создаёт КА)
byte[]	getHash() Хеш
byte[]	getRand() Случайный набор байтов (3 байта)
short	getRegion() Номер региона
int	getToNumber() Номер получателя (номер устройства, которое будет проверять КА)
short	getVersion() Версия ключа для данного КА
boolean	isVisualize() Визуализация
byte[]	serialize() Сериализовать структуру

Метод getByteArray

```
public byte[] getByteArray()
```

Назначение:
Получение сериализованного КА.

Возвращаемое значение:
массив байтов

Метод getDirection

```
public byte getDirection()
```

Назначение:
Получение направления передачи КА (от сервера к клиенту или от клиента к серверу).

Возвращаемое значение:
число

Метод getFromNumber

```
public int getFromNumber()
```

Назначение:
Получение номера отправителя (номера устройства, которое создаёт КА).

Возвращаемое значение:
номер

Метод getHash

```
public byte[] getHash()
```

Назначение:
Получение значения хеш-функции.

Возвращаемое значение:
массив байтов

Метод getRand

```
public byte[] getRand()
```

Назначение:
Получение случайного набора байтов (3 байта).

Возвращаемое значение:
массив байтов

Метод getRegion

```
public short getRegion()
```

Назначение:

Получение номера региона.

Возвращаемое значение:
`номер`

Метод getToNumber

```
public int getToNumber()
```

Назначение:
Получение номера получателя (номер устройства, которое будет проверять КА).

Возвращаемое значение:
`номер`

Метод getVersion

```
public short getVersion()
```

Назначение:
Получение версии ключа для данного КА.

Возвращаемое значение:
`версия`

Метод isVisualize

```
public boolean isVisualize()
```

Назначение:
Визуализация.

Возвращаемое значение:
`значение`

Метод serialize()

```
public byte[] serialize()
```

Назначение:
Сериализация структуры.

Возвращаемое значение:
`сериализованная в набор байтов структура`

Метод getServerKA

```
public ServerKA getServerKA()
```

Назначение:
Получение структуры с маскированным ключом.

Возвращаемое значение:

ServerKA структура с маскированным ключом.

Метод getPublicKey

```
public byte[] getPublicKey()
```

Назначение:

Получение открытого ключа.

Возвращаемое значение:

```
открытый ключ в виде набора байтов
```

Метод getSerializedServerKA

```
public byte[] getSerializedServerKA()
```

Сериализованная структура с маскированным ключом

Возвращаемое значение:

```
набор байтов
```

5.2.3 Класс ServerKA

```
java.lang.Object

         ru.infocrypt.sbk3j.ServerKA
-----------------------------------------------------------------------

      public class ServerKA

      extends java.lang.Object
```

Описание

Сервер расчета кодов аутентификации.

Конструкторы

ServerKA(java.lang.String serverIP, int port, int timeout) – инициализация рабочей сессии с сервером кодов аутентификации на основе ФПСУ-IP

```
public ServerKA(java.lang.String serverIP,
                int port,
                int timeout)
         throws ru.infocrypt.sbk3j.SbkaException
```

Методы

Модификатор и тип	Метод и описание
AuthentificationCode	calculate(int region, int toNumber, byte[] data) Устаревший
AuthentificationCode	calculateToClient(int region, int toNumber, byte[] data) Сформировать КА для клиента
java.util.List<AuthentificationCode>	calculateToClientGroup(int region, int[] groupMembers, byte[] data) Сформировать коды аутентификации для группы клиентов
AuthentificationCode	calculateToServer(int region, int toNumber, byte[] data) Сформировать КА для сервера
boolean	check(byte[] data, AuthentificationCode ac) Проверка КА для блока данных
ru.infocrypt.sbk3j.Info	getInfo() Получить информацию об устройстве КА
java.util.List<ru.infocrypt.sbk3j.RegionsInfo>	getRegionsInfo() Список регионов

Метод calculate

```
@Deprecated
public AuthentificationCode calculate(int region,
                                       int toNumber,
                                       byte[] data)
```

Назначение:
Устаревший

Метод calculateToClient

```
public AuthentificationCode calculateToClient(int region,
                                               int toNumber,
                                               byte[] data)
                                        throws ru.infocrypt.sbk3j.SbkaException
```

Назначение:
Формирование КА для клиента.

Параметры:

region - номер региона

toNumber - номер получателя

data - данные

Возвращаемое значение:
структура AuthentificationCode - код аутентификации

Исключения:
ru.infocrypt.sbk3j.exception.Sbk3jException - возможные исключения

Метод calculateToClientGroup

```
public java.util.List<AuthentificationCode> calculateToClientGroup(
                                                        int region,
                                                        int[] groupMembers,
                                                        byte[] data)
                                          throws ru.infocrypt.sbk3j.SbkaException
```

Назначение:
Формирование кодов аутентификации для группы клиентов.

Параметры:
region - номер региона

groupMembers - номера получателей

data - данные

Возвращаемое значение:
список структур AuthentificationCode - кодов аутентификации

Исключения:
ru.infocrypt.sbk3j.exception.Sbk3jException - возможные исключения

Метод calculateToServer

```
public AuthentificationCode calculateToServer(int region,
                                               int toNumber,
                                               byte[] data)
                                        throws ru.infocrypt.sbk3j.SbkaException
```

Назначение:
Формирование КА для сервера.

Параметры:
region - номер региона

toNumber - номер получателя

data - данные

Возвращаемое значение:
структура AuthentificationCode - код аутентификации

Исключения:
ru.infocrypt.sbk3j.exception.Sbk3jException - возможные исключения

Метод check

```
public boolean check(byte[] data,
                     AuthentificationCode ac)
              throws ru.infocrypt.sbk3j.SbkaException
```

Назначение:
Проверка КА для блока данных.

Параметры:
data – данные

ac - проверяемый КА

Возвращаемое значение:
результат проверки

Исключения:
ru.infocrypt.sbk3j.exception.Sbk3jException - возможные исключения

Метод getInfo

```
public ru.infocrypt.sbk3j.Info getInfo()
                                throws ru.infocrypt.sbk3j.SbkaException
```

Назначение:
Получение информации об устройстве КА.

Возвращаемое значение:
Info структура с информацией

Исключения:
ru.infocrypt.sbk3j.exception.Sbk3jException - возможные исключения

Метод getRegionsInfo

```
public java.util.List<ru.infocrypt.sbk3j.RegionsInfo> getRegionsInfo()
                                    throws ru.infocrypt.sbk3j.SbkaException
```

Назначение:
Получение списка регионов.

Возвращаемое значение:
RegionsInfo список структур с информацией по каждому из регионов, поддерживаемых сервером КА

Исключения:
ru.infocrypt.sbk3j.exception.Sbk3jException - возможные исключения