Клиентская JAVA-библиотека для сервера LAU-ключевания

11485466.5014.051

Инструкция по установке и эксплуатации

Содержание

1 Введение

Настоящий документ содержит руководство по установке и эксплуатации программного изделия «Клиентская JAVA-библиотека для сервера LAU-ключевания». Руководство включает в себя справочную информацию по работе с библиотекой «Клиентская JAVA-библиотека для сервера LAU-ключевания».

2 Назначение и условия применения

2.1 Назначение системы

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

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

- LAU-ключевание блока данных.
- Проверка LAU-ключевания блока данных.

2.2 Условия применения системы

«Клиентская JAVA-библиотека для сервера LAU-ключевания» 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 LAU-ключевания» необходим сетевой доступ к ПАК ФПСУ-IP, на котором установлено программное изделие «Сервер LAU-ключевания».

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

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

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

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

5 Описание библиотеки

5.1 Пакеты библиотеки «Клиентская JAVA-библиотека для сервера LAU-ключевания»

В состав библиотеки «Клиентская JAVA-библиотека для сервера LAU-ключевания» входит один пакет – ru.infocrypt.fpsu.

5.2 Классы пакета ru.infocrypt.fpsu

В состав пакета ru.infocrypt.fpsu входят классы:

- LauParameters
- SbLau.

5.2.1 Класс LauParameters

```
java.lang.Object
        ru.infocrypt.fpsu.LauParameters
-----------------------------------------------------------------------
```

```
public class LauParameters
extends java.lang.Object
```

Описание

Класс, представляющий набор параметров LAU.

Конструкторы

LauParameters (java.lang.String service, java.lang.String profileCode, java.lang.String senderBic, java.lang.String receiverBic, java.lang.Boolean isPDE, java.lang.String digestAlgorithm) – конструктор параметров LAU.

```
public LauParameters(java.lang.String service,
                     java.lang.String profileCode,
                     java.lang.String senderBic,
                     java.lang.String receiverBic,
                     java.lang.Boolean isPDE,
                     java.lang.String digestAlgorithm)
```

Параметры:

`service - сервис SWIFT; "swift.fin" для сообщений FIN`

`profileCode - код профиля; доступен только в AMP!`

`senderBic - (11 знаков, т.е. без кода LT)`

`receiverBic - BIC получателя (11 знаков, т.е. без кода LT)`

`isPDE - индикация PDE`

`digestAlgorithm - алгоритм для вычисления хеша FIN; если не указано - используется SHA-1`

Методы

Модификатор и тип	Метод и описание
void	setDigestAlgorithm(java.lang.String value) Задать алгоритм для вычисления хеша FIN
void	setIsPDE(java.lang.Boolean value) Задать признак PDE
void	setProfileCode(java.lang.String value) Задать код профиля
void	setReceiverBic(java.lang.String value) Задать BIC получателя
void	setSenderBic(java.lang.String value) Задать BIC отправителя
void	setService(java.lang.String value) Задать сервис SWIFT

Метод setDigestAlgorithm

```
public void setDigestAlgorithm(java.lang.String value)
```

Назначение:

Задание алгоритма для вычисления хеша FIN.

Метод setIsPDE

```
public void setIsPDE(java.lang.Boolean value)
```

Назначение:
Задание признака PDE.

Метод setProfileCode

```
public void setProfileCode(java.lang.String value)
```

Назначение:
Задание кода профиля.

Метод setReceiverBic

```
public void setReceiverBic(java.lang.String value)
```

Назначение:
Задание кода BIC получателя.

Метод setSenderBic

```
public void setSenderBic(java.lang.String value)
```

Назначение:
Задание кода BIC отправителя.

Метод setService

```
public void setService(java.lang.String value)
```

Назначение:
Задание сервиса SWIFT.

5.2.2 Класс SbLau

```
java.lang.Object

        ru.infocrypt.fpsu.SbLau
-------------------------------------------------------------------------

     public class SbLau
     extends java.lang.Object
```

Описание

Класс SBLau.

Поля

Модификатор и тип	Поле и описание	Значение
static int	SHA_1_KEY_NUMBER	2000
static int	SHA_256_KEY_NUMBER	3000

Поле SHA_1_KEY_NUMBER

```
public static final int SHA_1_KEY_NUMBER
```

Поле SHA_256_KEY_NUMBER

```
public static final int SHA_256_KEY_NUMBER
```

Конструкторы

SbLau (java.lang.String addr, int port, int timeOut) – конструктор сущности с параметрами LAU сессии. Конструктор инициирует новую LAU сессию используя данные адреса, порта и таймаута сервера LAU.

```
public SbLau(java.lang.String addr,
             int port,
             int timeOut)
      throws ru.infocrypt.fpsu.SBLauException
```

Параметры:

addr - адрес LAU сервера

port - порт LAU сервера

timeOut - таймаут LAU сервера.

Исключения:

ru.infocrypt.fpsu.SBLauException - возможные исключения

SbLau (java.lang.String addr, int port, int timeOut, int mtuSize) – конструктор сущности с параметрами LAU сессии. Конструктор инициирует новую LAU сессию используя данные адреса, порта и таймаута сервера LAU.

```
public SbLau(java.lang.String addr,
             int port,
             int timeOut,
             int mtuSize)
      throws ru.infocrypt.fpsu.SBLauException
```

Параметры:

`addr - адрес LAU сервера`

`port - порт LAU сервера`

`timeOut - таймаут LAU сервера.`

`mtuSize - значение системного параметра MTU_SIZE.`

Исключения:

`ru.infocrypt.fpsu.SBLauException - возможные исключения`

Методы

Модификатор и тип	Метод и описание
java.lang.String	calculate(int keyNumber, byte[] data) Ключевание блока данных
java.lang.String	calculateLAU(int keyNumber, byte[] data, LauParameters lauParameters) Ключевание блока данных с указанием параметров LAU
java.lang.String	calculateLAUWithIdent(int keyNumber, byte[] data, java.lang.String absID, LauParameters lauParameters) Ключевание блока данных с учетом идентификатора АБС и параметров LAU
java.lang.String	calculateWithIdent(int keyNumber, java.lang.String absID, byte[] data) Ключевание блока данных с учетом идентификатора АБС
boolean	check(int keynumber, byte[] data, java.lang.String lau) Проверка LAU
boolean	checkLAU(int keynumber, byte[] data, java.lang.String lau, LauParameters lauParameters) Проверка LAU
boolean	checkWithIdent(int keynumber, byte[] data, java.lang.String lau, java.lang.String absID) Проверка LAU с учетом идентификатора АБС (поддержка, начиная с версии ФПСУ 0018)

Метод calculate

```
public java.lang.String calculate(int keyNumber,
                                  byte[] data)
                           throws ru.infocrypt.fpsu.SBLauException
```

Назначение:
Ключевание блока данных

Параметры:
keyNumber - номер ключа на ПАК «Сервер LAU-ключевания»

data - обрабатываемый массив байтов

Возвращаемое значение:
строка с рассчитанным LAU

Исключения:
ru.infocrypt.fpsu.SBLauException - возможные исключения

Метод calculateLAU

```
public java.lang.String calculateLAU(int keyNumber,
                                      byte[] data,
                                      LauParameters lauParameters)
                               throws ru.infocrypt.fpsu.SBLauException
```

Назначение:
Ключевание блока данных с указанием параметров LAU

Параметры:
keyNumber - номер ключа на ПАК «Сервер LAU-ключевания»

data - обрабатываемый массив байтов

lauParameters - параметры LAU

Возвращаемое значение:
строка с рассчитанным LAU

Исключения:
ru.infocrypt.fpsu.SBLauException - возможные исключения

Метод calculateLAUWithIdent

```
public java.lang.String calculateLAUWithIdent(int keyNumber,
                                               byte[] data,
                                               java.lang.String absID,
                                            LauParameters lauParameters)
                                 throws ru.infocrypt.fpsu.SBLauException
```

Назначение:
Ключевание блока данных с учетом идентификатора АБС и параметров LAU

Параметры:
keyNumber - номер ключа на ПАК «Сервер LAU-ключевания»

data - обрабатываемый массив байтов

```
absID - идентификатор АБС

lauParameters - параметры LAU
```

Возвращаемое значение:

```
строка с рассчитанным LAU (44 символа из алфавита [0-9A-Za-z./=])
```

Исключения:

```
ru.infocrypt.fpsu.SBLauException - возможные исключения
```

Метод calculateLAUWithIdent

```
public java.lang.String calculateWithIdent(int keyNumber,
                                           java.lang.String absID,
                                           byte[] data)
                                    throws ru.infocrypt.fpsu.SBLauException
```

Назначение:

Ключевание блока данных с учетом идентификатора АБС

Параметры:

```
keyNumber - номер ключа на ПАК «Сервер LAU-ключевания»

absID - идентификатор АБС

data - обрабатываемый массив байтов
```

Возвращаемое значение:

```
строка с рассчитанным LAU
```

Исключения:

```
ru.infocrypt.fpsu.SBLauException - возможные исключения
```

Метод check

```
public boolean check(int keynumber,
                     byte[] data,
                     java.lang.String lau)
              throws ru.infocrypt.fpsu.SBLauException
```

Назначение:

Проверка LAU

Параметры:

```
keyNumber - номер ключа на ПАК «Сервер LAU-ключевания»

data - обрабатываемый массив байтов

lau - проверяемый код LAU
```

Возвращаемое значение:

```
true в случае корректности кода, иначе false
```

Исключения:
ru.infocrypt.fpsu.SBLauException - возможные исключения

Метод checkLAU

```
public boolean checkLAU(int keynumber,
                        byte[] data,
                        java.lang.String lau,
                        LauParameters lauParameters)
                 throws ru.infocrypt.fpsu.SBLauException
```

Назначение:
Проверка LAU

Параметры:
keyNumber - номер ключа на ПАК «Сервер LAU-ключевания»

data - обрабатываемый массив байтов

lau - проверяемый код LAU

lauParameters – параметры LAU

Возвращаемое значение:
true в случае корректности кода, иначе false

Исключения:
ru.infocrypt.fpsu.SBLauException - возможные исключения

Метод checkLAUWithIdent

```
public boolean checkLAUWithIdent(int keynumber,
                                 byte[] data,
                                 java.lang.String lau,
                                 java.lang.String absID,
                                 LauParameters lauParameters)
                          throws ru.infocrypt.fpsu.SBLauException
```

Назначение:
Проверка LAU с учетом идентификатора АБС (поддержка, начиная с версии ФПСУ 0018).

Параметры:
keyNumber - номер ключа на ПАК «Сервер LAU-ключевания»

data - обрабатываемый массив байтов

lau - проверяемый код LAU

absID - идентификатор АБС

lauParameters - параметры LAU

Возвращаемое значение:
true в случае корректности кода, иначе false

Исключения:
ru.infocrypt.fpsu.SBLauException - возможные исключения

Метод checkWithIdent

```
public boolean checkWithIdent(int keynumber,
                              byte[] data,
                              java.lang.String lau,
                              java.lang.String absID)
                       throws ru.infocrypt.fpsu.SBLauException
```

Назначение:
Проверка LAU с учетом идентификатора АБС (поддержка, начиная с версии ФПСУ 0018).

Параметры:
keyNumber - номер ключа на ПАК «Сервер LAU-ключевания»

data - обрабатываемый массив байтов

lau - проверяемый код LAU

absID - идентификатор АБС

Возвращаемое значение:
true в случае корректности кода, иначе false

Исключения:
ru.infocrypt.fpsu.SBLauException - возможные исключения