Клиентская JAVA-библиотека для сервера ЭП с зарубежными алгоритмами

11485466.72.21.12.169

Инструкция по установке и эксплуатации

Содержание

1 Введение

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

2 Назначение и условия применения

2.1 Назначение системы

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

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

- Формирование электронной подписи в соответствии с алгоритмом RSA.
- Проверка электронной подписи.

2.2 Условия применения системы

«Клиентская JAVA-библиотека для сервера ЭП с зарубежными алгоритмами» 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 ЭП с зарубежными алгоритмами» необходим сетевой доступ к ПАК ФПСУ-IP, на котором установлено программное изделие «Сервер ЭП».

3 Установка программного изделия «Клиентская JAVA-библиотека для сервера ЭП с зарубежными алгоритмами»

Для того чтобы установить программное изделие «Клиентская JAVA-библиотека для сервера ЭП с зарубежными алгоритмами», следует скопировать содержимое

дистрибутива «Клиентская JAVA-библиотека для сервера ЭП с зарубежными алгоритмами» на жёсткий диск компьютера.

4 Удаление программного изделия «Клиентская JAVA-библиотека для сервера ЭП с зарубежными алгоритмами»

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

5 Описание библиотеки

5.1 Пакеты библиотеки «Клиентская JAVA-библиотека для сервера ЭП с зарубежными алгоритмами»

В состав библиотеки «Клиентская JAVA-библиотека для сервера ЭП с зарубежными алгоритмами» входит один пакет – ru.infocrypt. icrsa.

5.2 Классы пакета ru.infocrypt.icrsa

В состав пакета ru.infocrypt.icrsa входит один класс – ICRsa.

5.2.1 Класс ICRsa

```
java.lang.Object
        ru.infocrypt.icrsa.ICRsa
-----------------------------------------------------------------------

    public class ICRsa
    extends java.lang.Object
    implements java.lang.AutoCloseable
```

Описание

Работа с сервером электронной подписи на базе ФПСУ-IP (ключи RSA).

Конструкторы

ICRsa (java.lang.String ip, int port, int timeout) – формирование экземпляра класса на основании данных сервера ЭП.

```
public ICRsa(java.lang.String ip,
             int port,
             int timeout)
      throws ru.infocrypt.icrsa.exception.FpsuException
```

Параметры:

ip - ip адрес сервера

port - порт

timeout - таймаут

Исключения:

ru.infocrypt.fpsu.exception.FpsuException - возможные исключения

ICRsa (java.lang.String ip, int port, int timeout, ru.infocrypt.icrsa.enums.ProtocolType protocolType, ru.infocrypt.icrsa.TLSContext tlsContext) – формирование экземпляра класса на основании данных сервера ЭП.

```
public ICRsa(java.lang.String ip,
             int port,
             int timeout,
             ru.infocrypt.icrsa.enums.ProtocolType protocolType,
             ru.infocrypt.icrsa.TLSContext tlsContext)
      throws ru.infocrypt.icrsa.exception.FpsuException
```

Параметры:

ip - ip адрес сервера

port - порт

timeout - таймаут

protocolType - протокол, используемый для связи

tlsContext - контекст TLS сессии

Исключения:

ru.infocrypt.icrsa.exception.FpsuException - возможные исключения

Методы

Модификатор и тип	Метод и описание
void	close() Освободить ресурсы, занятые классом ICRsa
byte[]	decrypt(ru.infocrypt.icrsa.FpsuKey rsaKey, byte[] encrypted) Расшифровать данные

Модификатор и тип	Метод и описание
ru.infocrypt.icrsa.FpsuKey	getKey(short keyNo) Получить метаданные закрытого ключ сервера ЭП по номеру
ru.infocrypt.icrsa.DSInfo	signDigest(ru.infocrypt.icrsa.FpsuKey rsaKey, byte[] digest) Формирование ЭП
void	test() Тестирование сервера ЭП на основании проверки версии внутреннего ПО
boolean	verify(ru.infocrypt.icrsa.FpsuKey rsaKey, java.lang.String verifyAlg, byte[] sign, java.io.InputStream inStream) Проверить ЭП

Метод close

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

Назначение:

Освобождение ресурсов, занятых классом ICRsa

Исключения:

```
java.lang.Exception - возможные исключения
```

Метод decrypt

```
public byte[] decrypt(ru.infocrypt.icrsa.FpsuKey rsaKey,
                      byte[] encrypted)
               throws ru.infocrypt.icrsa.exception.FpsuException
```

Назначение:

Расшифровывание данных.

Параметры:

```
rsaKey - ключ на сервере ЭП (RSA)

encrypted - зашифрованный блок данных
```

Возвращаемое значение:

```
расшифрованный блок данных
```

Исключения:

```
ru.infocrypt.icrsa.exception.FpsuException - возможные исключения
```

Метод getKey

```
public ru.infocrypt.icrsa.FpsuKey getKey(short keyNo)
                      throws ru.infocrypt.icrsa.exception.FpsuException
```

Назначение:

Получение метаданных закрытого ключа сервера ЭП по номеру.

Параметры:

keyNo - номер ключа на сервере ЭП

Возвращаемое значение:

объект FpsuKey

Исключения:

ru.infocrypt.icrsa.exception.FpsuException - возможные исключения

Метод signDigest

```
public ru.infocrypt.icrsa.DSInfo signDigest(ru.infocrypt.icrsa.FpsuKey rsaKe
y,
                                            byte[] digest)
                          throws ru.infocrypt.icrsa.exception.FpsuException
```

Назначение:

Формирование ЭП для заранее вычисленного хеш-значения.

Параметры:

rsaKey - ключ на сервере ЭП (RSA)

digest- хеш-значение

Возвращаемое значение:

структура DSInfo, содержащая RAW ЭП и необходимые данные

Исключения:

ru.infocrypt.icrsa.exception.FpsuException - возможные исключения

Метод test

```
public void test()
          throws ru.infocrypt.icrsa.exception.FpsuException
```

Назначение:

Тестирование сервера ЭП на основании проверки версии внутреннего ПО.

Исключения:

ru.infocrypt.icrsa.exception.FpsuException - возможные исключения

Метод verify

```
public boolean verify(ru.infocrypt.icrsa.FpsuKey rsaKey,
                      java.lang.String verifyAlg,
                      byte[] sign,
                      java.io.InputStream inStream)
               throws ru.infocrypt.icrsa.exception.FpsuException
```

Назначение:

Проверить ЭП.

Параметры:

`rsaKey - ключ на сервере ЭП (RSA)`

`verifyAlg - алгоритм проверки ЭП`

`sign - ЭП в формате RAW`

`inStream - входящий поток с данными на проверку`

Возвращаемое значение:

`true в случае корректной ЭП, иначе false`

Исключения:

`ru.infocrypt.icrsa.exception.FpsuException - возможные исключения`