101000, г. Москва,
Армянский переулок д. 9 стр.1, оф.505
Тел.: +7 (495) 780-52-68
www.afinserv.ru

КРИПТО-СЕРВИС «AFS-CRYPTOGATE»

Руководство администратора

Версия: 1.0

Листов: 8

101000, г. Москва,
Армянский переулок д. 9 стр.1, оф.505
Тел.: +7 (495) 780-52-68
www.afinserv.ru

СОДЕРЖАНИЕ

ИЗМЕНЕНИЯ

Версия	Дата	Автор	Изменения
1.01	12.10.2018	Ходырев Н.А.	Первая версия документа

ТЕРМИНЫ/СОКРАЩЕНИЯ

Термин/сокращение	Описание
Поставщик	Организация-владелец электронного сервиса
СМЭВ	Система межведомственного электронного взаимодействия
ЭП	Электронная подпись
SOAP	Simple Object Access Protocol - протокол обмена структурированными сообщениями в распределённой вычислительной среде.
XML	eXtensible Markup Language — расширяемый язык разметки.
XSD	XML Schema definition - язык описания структуры XML документа.
WSDL	Web Services Description Language — язык описания веб-сервисов.
XMLDSIG	Цифровая подпись в формате XML

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Руководящие документы

Нормативно-правовые документы:

- Приказ ФСБ России от 13 ноября 1999 г. № 564 «Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия».

Технологические стандарты:

- Методические рекомендации по работе с Единой системой межведомственного электронного взаимодействия версия 3.4.0.3. М.: 2017, 151 с. (URL: https://smev3.gosuslugi.ru/portal).
- W3C. Latest SOAP versions. URL: https://www.w3.org/TR/soap/.
- W3C. XML Signature WG. URL: https://www.w3.org/Signature/.

1.2 Описание крипто-сервиса «AFS-CryptoGate»

Наименование:	Крипто-сервис «AFS-CryptoGate» (далее - Сервис)
Назначение:	Сервис предназначен для: • формирование хэша xml-документа, • наложение электронной подписи (ЭП) на xml-документ направляемый в СМЭВ, • проверку ЭП xml-документа, получаемого от СМЭВ.
Условия применения	Для функционирования сервса необходимы следующие прикладное программное обеспечение: – Операционная система поддерживающая спецификации Sun Java 2 ™ Virtual Machine и установку КриптоПро JCP 2.0 (Linux, Microsoft Server) – КриптоПро JCP 2.0 – Установленная JVM 1.7 и выше

1.3 Уровень подготовки администратора

Администратор системы должен обладать навыками, позволяющими проводить установку и настройку Сервиса, и соответствующие навыки в администрировании операционных систем и прикладного программного обеспечения.

Для поддержки функционирования Сервиса администратор должен обладать знаниями в области информационных и сетевых платформ, на которых реализуется Сервис.

Квалификация администратора Сервиса должна позволять выполнять следующие функции:

- управление конфигурацией (настройку) специального программного обеспечения Сервиса
- запуск, мониторинг и контроль работоспособности специального программного обеспечения Сервиса;

1.4 Перечень эксплуатационной документации, с которой необходимо ознакомиться администратору

Перед началом работы пользователю необходимо ознакомиться со следующими документами:

- Руководство администратора Сервиса (настоящий документ).

1.5 Условия, при соблюдении которых обеспечивается применение Системы в соответствии с назначением

До установки системы должны быть выполнены работы по обеспечению рабочей аппаратной конфигурации с топологией связей и настроенными протоколами взаимодействия.

Требования к программному обеспечению, установленному до развертывания Системы, приведены в разделе 1.2.

2 ПОДГОТОВКА К РАБОТЕ

2.1 Состав и содержание дистрибутивного носителя данных

Состав дистрибутива приведен в таблице 1.

Таблица 1. Состав дистрибутива системы

Имя сборки	Описание	Имя файла	Описание файла
eds.zip	Крипто-сервис «AFS-CryptoGate»	eds.jar	
		wss4j-1.6.3.jar	Библиотека Apache WSS4J - Web Services Security for Java

		config.xml	Настроечный файл сервиса
		eds-service.bat	Файл запуска криптосервиса

Список дистрибутивов смежных систем, необходимых для работоспособности системы:

- КриптоПро JCP 2.0;
- Java JRE 1.7 и выше.

2.1.1 Порядок проверки работоспособности

Проверка работоспособности Сервиса выполняется после его запуска. После запуска необходимо убедиться в том, что на экране окна интернет-браузера отобразилась WSDL сервиса по адресу указанному в config.xml.

3 ОПИСАНИЕ ОПЕРАЦИЙ ПО УСТАНОВКЕ И КОНФИГУРИРОВАНИЮ СИСТЕМЫ

3.1 Развертывание Сервиса

3.1.1 Установка JRE

Необходимо загрузить инсталлятор JDK по адресу http://www.oracle.com/technetwork/java/javase/downloads/index.html

Для Windows - запустить инсталлятор.

Для Linux (установка из-под пользователя root):

1. Скопировать bin-файл в /root.
2. Дать ему права на исполнение (chmod +x).
3. Запустить установку (по умолчанию ведется в каталог /usr/java).

3.1.2 Установка CryptoPro для Java

Установка и настройка выполняется согласно документу ЖТЯИ.00091-01 90 01. Руководство администратора безопасности.pdf, поставляемого в комплекте с CryptoPro JCP 2.0.

3.1.3 Установка дополнительных библиотек в Java

Необходимо скопировать следующие библиотеки:

- Из jcp-2.x\dependencies\ в Java\jre \lib\ext\
- Из дистрибутива библиотеку wss4j-1.6.3.jar в в Java\jre \lib\ext\

3.1.4 Настройка парметров Сервиса

Настройка Сервиса осуществляется следующими способами:

- Редактирование конфигурационного файла config.xml
- Через приложение GUI Конфиг AFS //todo описать после завершения разработки

Параметр	Описание	Пример значения	Комментарий
CRL\	Список отозванных сертифкатов	-	Certificate revocation list
check	Проверять список отозванных сертифкатов при выполнении операции Сервиса VerifySMEV3_EPOV	true|false	да/нет
remote	Испольовать интернет для получения актуального crl	true|false	да/нет Адрес CRL берется из сертифк
path	Локальное хранилище CRL	C:\confForWork\crl1\ или /opt/cs/crl	Настроечный файл сервиса
pathTrusted	Локальное хранилище доверенных/аккредитованны х УЦ	C:\confForWork\crl\CAList.xml	Файл доступен по адресу https://e-trust.gosuslugi.ru/CA
cryptoPro\	Параметры используемые при обращении сервиса к cryptoPro		
defaultCert\	Хранилище ключей используемое по умолчанию	-	
name	Имя хранилища	1-CIT-TEST	
key	Идентифкатор хранилища	1-CIT-TEST	
password	Пароль к хранилиц	12345678	
keystore	Тип используемого хранилища	HDImageStore или FloppyStore	
certs	Список ключей досутпных Сервису для наложения ЭП		
cert\	Хранилище ключа		Параметры аналогчнные defaultCert: name key password keystore
http	Сетевые парметры		Описание (wsdl) Сервиса будет

			доступно по адресу вида http:{host}:{port}{path}?wsdl
host	IP адрес сервиса	127.0.0.1	Если указать 127.0.0.1, то сервис будет доступен только с локальной машины
port	Порт по которому сервив слущает обращения	8300	
path	Префикс имени после IP и порта	/EDSService	

3.2 Запуск Сервиса

Запуск Сеервиса осуществляется вызовом JVM с параметрами, минимально необходимо указать расположение конфигурационного файла.

Пример вызова сервиса для Windows

```
chcp 1251
"c:\Program Files\Java\jre7\bin\java.exe" -jar "c:\data\crypto\t3\eds.jar"
"c:\data\crypto\t3\config2.xml"
pause
```

Пример вызова сервиса для Linux

```
nohup /opt/eds/jre1.6.0_43/bin/java -jar /opt/eds/eds.jar >> /opt/eds/eds.jar.out &
```

4 АВАРИЙНЫЕ СИТУАЦИИ

4.1 Действия по восстановлению Сервиса при отказе магнитных носителей или обнаружении ошибок в работоспособности

В случае необходимости восстановления Сервиса, Системный администратор проводит процедуру восстановления копии с резервного носителя.