

АО «СИГНАЛ-КОМ»

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС
SIGNAL-COM CLOUD DSS
Версия 1.0

Руководство системного программиста

ШКНР.00051-01 32 01
Листов 28

АННОТАЦИЯ

Настоящий документ содержит руководство системного программиста программно-аппаратного комплекса Signal-COM Cloud DSS, предназначенного для централизованного дистанционного создания, обслуживания и применения ключей электронной подписи.

СОДЕРЖАНИЕ

| | |
|---|----|
| Аннотация | 2 |
| Содержание | 3 |
| 1. Общие сведения о программе..... | 5 |
| 1.1. Назначение программы | 5 |
| 1.2. Список сокращений | 5 |
| 1.3. Термины и определения | 5 |
| 1.4. Характеристики программы | 6 |
| 1.5. Аппаратные требования | 6 |
| 1.6. Требования к программному окружению..... | 7 |
| 2. Структура программы | 8 |
| 2.1. Сведения о структуре программы | 8 |
| 2.2. Сведения о составных частях программы | 8 |
| 2.3. Сведения о связях между составными частями программы | 9 |
| 3. Настройка программы..... | 11 |
| 3.1. Подготовка окружения..... | 11 |
| 3.1.1. Установка разделяемых библиотек | 11 |
| 3.2. Файл конфигурации..... | 11 |
| 3.3. Настройка ПАКМ «Сигнал-КОМ HSM» | 11 |
| 3.4. Настройка сервера электронной подписи..... | 11 |
| 3.5. Настройка сервера управления ключевой информацией..... | 11 |
| 3.6. Настройка веб-сервера идентификации..... | 12 |
| 3.6.1. Быстрый старт | 12 |
| 3.6.2. Дескриптор развёртывания | 12 |
| 3.6.3. Параметры конфигурации..... | 12 |
| 3.6.4. Требования по безопасности | 13 |
| 3.7. Настройка веб-приложения идентификации | 13 |
| 3.7.1. Быстрый старт | 13 |
| 3.7.2. Дескриптор развёртывания | 13 |
| 3.7.3. Параметры конфигурации..... | 14 |
| 3.7.4. Требования по безопасности | 15 |
| 3.8. Настройка веб-сервиса администратора..... | 15 |
| 3.8.1. Быстрый старт | 15 |
| 3.8.2. Дескриптор развёртывания | 15 |
| 3.8.3. Требования по безопасности | 16 |
| 3.9. Настройка веб-сервиса оператора | 16 |
| 3.9.1. Быстрый старт | 16 |
| 3.9.2. Дескриптор развёртывания | 16 |
| 3.9.3. Параметры конфигурации..... | 16 |
| 3.9.4. Требования по безопасности | 17 |
| 3.10. Настройка веб-сервиса пользователя..... | 17 |
| 3.10.1. Быстрый старт | 17 |
| 3.10.2. Дескриптор развёртывания | 17 |
| 3.10.3. Параметры конфигурации..... | 17 |
| 3.10.4. Требования по безопасности | 18 |
| 3.11. Настройка клиентских веб-приложений..... | 18 |
| 3.11.1. Настройка веб-приложения администратора | 19 |
| 3.11.2. Настройка веб-приложения оператора | 20 |
| 3.11.3. Настройка веб-приложения пользователя | 21 |
| 3.11.4. Требования по безопасности | 22 |
| 3.12. Настройка сервера оповещений | 23 |
| 3.12.1. Быстрый старт | 23 |
| 3.12.2. Дескриптор развёртывания | 23 |
| 3.12.3. Требования по безопасности | 24 |
| 3.13. Настройка сервера аудита событий | 24 |
| 3.13.1. Быстрый старт | 24 |
| 3.13.2. Дескриптор развёртывания | 24 |
| 3.13.3. Создание базы данных сервера аудита событий..... | 25 |
| 3.13.4. Требования по безопасности | 25 |

| | | |
|------------|---|----|
| 3.14. | Настройка базы данных | 25 |
| 3.14.1. | Создание базы данных | 25 |
| 3.14.2. | Настройка Hibernate..... | 26 |
| 3.15. | Управление приложениями | 26 |
| 5. | Сообщения системному программисту | 27 |
| Литература | | 28 |

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1. Назначение программы

Программно-аппаратный комплекс Signal-COM Cloud DSS (далее Cloud DSS) предназначен для централизованного дистанционного создания, хранения, обслуживания и применения ключей электронной подписи и сертификатов ключей проверки электронной подписи.

Cloud DSS позволяет выполнять операции создания и проверки электронных подписей в форматах CMS, CAdES, PAdES, XMLDSig, Office OpenXML. Дополнительно реализована возможность зашифрования и расшифрования данных в формате CMS.

В Cloud DSS реализован интерфейс взаимодействия с Удостоверяющими центрами, облегчающий пользователям регистрацию и получение сертификатов ключей проверки электронной подписи.

Cloud DSS реализован в виде веб-сервисов и предоставляет программный интерфейс по протоколам SOAP [1] и REST.

1.2. Список сокращений

В настоящем руководстве используются следующие сокращения:

- БД – база данных;
- ПАК - программно-аппаратный комплекс;
- ПАКМ – программно-аппаратный криптографический модуль;
- СУБД – система управления базами данных;
- ТК – технический комитет;
- ЭП – электронная подпись;
- CAdES – CMS Advanced Electronic Signature;
- CMS – Cryptographic Message Syntax;
- CRL – Certificate Revocation List;
- DSS – Digital Signature Service;
- HTTP – Hypertext Transfer Protocol;
- HSM – Hardware Security Module;
- ITU-T – International Telecommunication Union - Telecommunication sector;
- MITM – Man in the Middle;
- OASIS – Organization for the Advancement of Structured Information Standards;
- RFC – Request for Comments;
- SOAP – Simple Object Access Protocol;
- TSP – Time-Stamp Protocol;
- VPN – Virtual Private Network;
- XML – eXtensible Markup Language;
- XMLDSig – XML Digital Signature.

1.3. Термины и определения

В настоящем руководстве используются следующие термины:

- веб-сервис – реализация интерфейса взаимодействия между различными приложениями по протоколам REST и SOAP;
- ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи;
- удостоверяющий центр – юридическое лицо, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей;
- сертификат ключа проверки электронной подписи – документ в электронном виде или документ на бумажном носителе, выданные Удостоверяющим центром либо доверенным лицом Удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

- электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

1.4. Характеристики программы

ПАК Cloud DSS реализован в виде веб-сервисов и предоставляет программный интерфейс по протоколам REST и SOAP.

В ПАК Cloud DSS поддерживаются следующие криптографические алгоритмы:

- алгоритм создания ключей электронной подписи ГОСТ Р 34.10-2012 [4];
- алгоритм электронной подписи ГОСТ Р 34.10-2012 [4];
- алгоритм шифрования ГОСТ 28147-89 [15].

ПАК Cloud DSS позволяет формировать запросы на создание сертификатов в формате PKCS #10 [5] и CMC [6].

ПАК Cloud DSS реализует следующие протоколы электронной подписи:

- CMS;
- CAdES;
- PAdES;
- XMLDSig;
- OOXML.

ПАК Cloud DSS реализует следующие протоколы шифрования данных:

- CMS.

Протокол CMS реализован в соответствии с RFC 5652 [7] и рекомендациями ТК 26 [8].

Протокол CAdES реализован в соответствии с RFC 5126 [11].

Протокол PAdES реализован в соответствии с [16].

Протокол XMLDSig реализован в соответствии с [9] и рекомендациями ТК 26 [10].

Протокол подписи документов OOXML реализован в соответствии с [17].

В ПАК Cloud DSS реализована возможность добавления меток доверенного времени в подпись в соответствии с CAdES [11], PAdES [16] и RFC 3161 [12].

ПАК Cloud DSS использует сертификаты ключей проверки ЭП в формате ITU-T X.509 [13] и рекомендаций ТК 26 [14].

1.5. Аппаратные требования

Минимальная аппаратная конфигурация ПАК Cloud DSS включает ПАКМ «Сигнал-КОМ HSM» и два сервера для программных компонентов (внутренних и внешних). Минимальные аппаратные требования к этим устройствам приведены ниже.

Таблица 1 – Требования к серверу для размещения внутренних компонентов

| Оборудование | Минимальные требования |
|--------------------|------------------------|
| Процессор | 64 бита, 4 ядра, 3 ГГц |
| Оперативная память | 16 ГБ |
| Жесткий диск | 2 ТБ |
| Сетевые адаптеры | Два сетевых адаптера |

Таблица 2 – Требования к серверу для размещения внешних компонентов

| Оборудование | Минимальные требования |
|--------------|------------------------|
| Процессор | 64 бита, 4 ядра, 3 ГГц |

| | |
|--------------------|----------------------|
| Оперативная память | 16 ГБ |
| Жесткий диск | 2 ТБ |
| Сетевые адаптеры | Два сетевых адаптера |

1.6. Требования к программному окружению

Все программные компоненты ПАК Cloud DSS реализованы для выполнения в виртуальной машине Java 8 (JRE 8). Рекомендуется использовать самую новую на момент установки версию Java 8.

Программные компоненты ПАК Cloud DSS могут быть установлены на любых серверных ОС, которые поддерживаются для Java 8 (<https://www.oracle.com/technetwork/java/javase/certconfig-2095354.html>). Рекомендуемая ОС – CentOS 7 и выше.

Программные компоненты ПАК Cloud DSS выполнены в виде Java EE приложений. Рекомендуемый сервер приложений – Apache Tomcat версии 8.5 и выше.

Рекомендуемая версия СУБД – MariaDB 10.4 и выше.

2. СТРУКТУРА ПРОГРАММЫ

2.1. Сведения о структуре программы

Программно-аппаратный комплекс Cloud DSS состоит из следующих слоёв:

- веб-интерфейс – предназначен для обеспечения доступа участников к функциям ПАК через графическую оболочку;
- программный интерфейс – предназначен для доступа к функциям ПАК через API;
- набор внутренних сервисов – скрытые от пользователей ПАК функциональные компоненты;
- хранилище ключей (HSM) – также скрытый от пользователей ПАК компонент, в котором осуществляется хранение ключей ЭП и выполнение операций с их использованием (например, создание ЭП).

Рисунок 1 – Архитектура ПАК Cloud DSS



2.2. Сведения о составных частях программы

В состав программно-аппаратного комплекса Cloud DSS входят следующие обязательные компоненты:

- ПАКМ «Сигнал-KOM HSM»;
- сервер электронной подписи DSS Server;
- сервер управления ключевой информацией DSS Key Manager;
- веб-сервер идентификации DSS Identity Server;
- веб-приложение идентификации DSS Identity Web;
- веб-сервис администратора DSS Administrator API;
- веб-сервис оператора DSS Operator API;
- веб-сервис пользователя DSS Customer API;
- сервер оповещений DSS Notification Server;
- сервер аудита событий DSS Audit Server;

- база данных ПАК Cloud DSS.

Дополнительно в состав ПАК Cloud DSS могут быть включены следующие компоненты:

- веб-приложение администратора DSS Administrator Web;
- веб-приложение оператора DSS Operator Web;
- веб-приложение пользователя DSS Customer Web.

2.3. Сведения о связях между составными частями программы

Рисунок 2 – Типовая схема размещения компонентов ПАК Cloud DSS

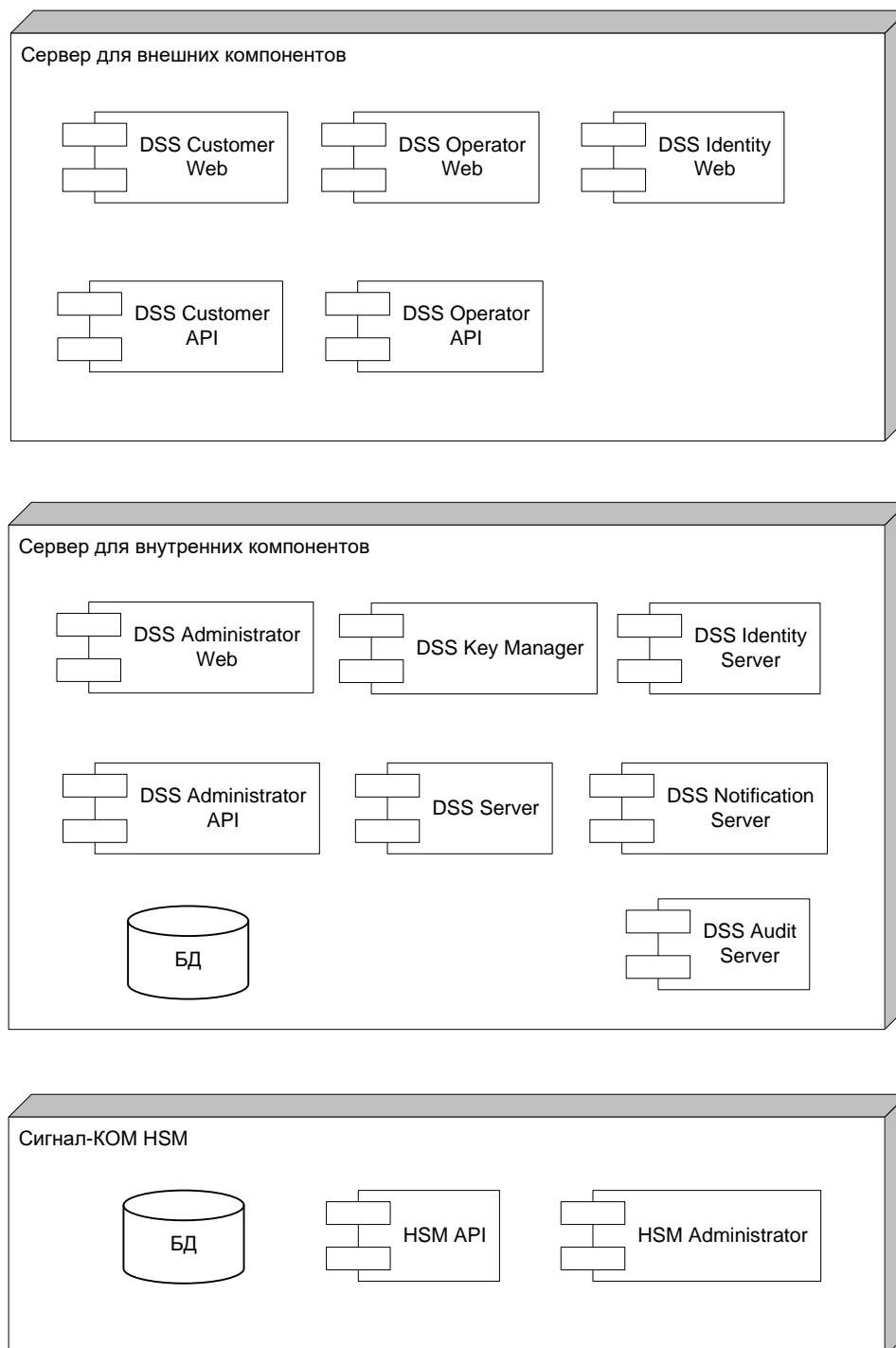


Схема размещения компонентов ПАК Cloud DSS при необходимости может быть изменена (при соблюдении принципа разделения компонентов типовой схемы) в следующих случаях:

- при размещении отдельных компонентов на выделенных серверах (например, БД);
- при увеличении количества (масштабировании) отдельных компонентов (например, DSS Server, ПАКМ «Сигнал-КОМ HSM»).

3. НАСТРОЙКА ПРОГРАММЫ

Установка и конфигурирование компонентов ПАК Cloud DSS рассмотрены на примере использования контейнера сервлетов Apache Tomcat 8 (<http://tomcat.apache.org>).

Конфигурирование компонентов ПАК Cloud DSS осуществляется путём редактирования файлов web.xml и файла конфигурации ПАК Cloud DSS (см. п. 3.2).

3.1. Подготовка окружения

Для развёртывания внешних компонентов ПАК Cloud DSS необходимо предварительно установить:

- JRE/JDK 1.8 (рекомендуется использовать самую новую на момент установки версию);
- Apache Tomcat 8 (рекомендуемая версия - 8.5 и выше);
- Java-архивы (jar) разделяемых библиотек (см. п. 3.1.1).

Подробные инструкции по установке и настройке Apache Tomcat 8 см. <http://tomcat.apache.org/tomcat-8.0-doc/setup.html>.

Для развёртывания внутренних компонентов ПАК Cloud DSS необходимо дополнительно установить:

- СУБД MariaDB (рекомендуемая версия - 10.4 и выше).

3.1.1. Установка разделяемых библиотек

Для установки разделяемых библиотек необходимо выполнить следующие действия:

- в корневом каталоге Apache Tomcat (\$CATALINA_HOME) создать подкаталог shared/lib;
- поместить содержимое поставляемого в составе дистрибутива файла архива shared.lib.zip в каталог \$CATALINA_HOME/shared/lib;
- в файле \$CATALINA_BASE/conf/catalina.properties задать

```
shared.loader=${catalina.home}/shared/lib/*.jar
```

3.2. Файл конфигурации

Файл конфигурации ПАК Cloud DSS представляет собой обычный файл свойств Java (Properties File Format), в котором параметры компонентов ПАК Cloud DSS задаются парами propertyName=propertyValue.

В составе дистрибутива имеется тестовый пример конфигурации (файл dss-webserver.properties), который необходимо скопировать в каталог \$CATALINA_BASE/conf.

Описание отдельных параметров файла конфигурации приводится в соответствующих разделах описания настройки компонентов ПАК Cloud DSS.

3.3. Настройка ПАКМ «Сигнал-КОМ HSM»

Установка и настройка компонента ПАКМ «Сигнал-КОМ HSM» описаны в [3].

3.4. Настройка сервера электронной подписи

Установка и настройка компонента сервер электронной подписи DSS Server описаны в [1].

3.5. Настройка сервера управления ключевой информацией

Установка и настройка компонента сервер управления ключевой информацией DSS Key Manager описаны в [2].

3.6. Настройка веб-сервера идентификации

3.6.1. Быстрый старт

В составе дистрибутива ПАК Cloud DSS имеется файл эталонной конфигурации (conf/dss-webserver.properties), в котором необходимо указать актуальные адреса серверов компонентов Cloud DSS:

```
...
ru.signalcom.dss.idp.service.address=http://idp_hostname:[port]
ru.signalcom.dss.service.address=http://dss_hostname:[port]
ru.signalcom.dss.keyman.service.address=http://keyman_hostname:[port]
...
```

где

- idp_hostname - имя (ip адрес) веб-сервера идентификации (DSS Identity Server);
- dss_hostname - имя (ip адрес) сервера электронной подписи (DSS Server, п.3.4.);
- keyman_hostname - имя (ip адрес) сервера управления ключевой информацией (DSS Key Manager, п. 3.5.);

При типовом размещении компонентов Cloud DSS адреса их серверов совпадают и равны:

http://localhost:[port]

Для быстрого старта приложения необходимо выполнить следующие действия:

- скопировать файл эталонной конфигурации conf/dss-webserver.properties в каталог \$CATALINA_BASE/conf;
- стартовать сервер Apache Tomcat;
- скопировать файл dss-identity-service.war в каталог \$CATALINA_BASE/webapps.

Приложение будет автоматически развёрнуто и загружено на выполнение в контексте /dss-identity-service (т.е. доступно по URL, например, http://localhost[:port]/dss-identity-service).

3.6.2. Дескриптор развёртывания

Дескриптор развёртывания (файл web.xml) располагается в каталоге /WEB-INF приложения.

В дескрипторе развёртывания задаётся путь к файлу конфигурации в параметре приложения с именем configFileName, например:

```
...
<context-param>
  <param-name>configFileName</param-name>
  <param-value>${catalina.base}/conf/dss-webserver.properties</param-value>
</context-param>
...
```

3.6.3. Параметры конфигурации

Файл конфигурации \$CATALINA_BASE/conf/dss-webserver.properties представляет собой текстовый файл, содержащий значения параметров в формате:

Имя_параметра=Значение_параметра

Веб-сервер идентификации настраивается следующими параметрами:

```
...
ru.signalcom.dss.confirmation.timeout=<confirmation_timeout>
...
ru.signalcom.dss.identity.max_token_cache=<token_cache_size>
ru.signalcom.dss.identity.token_expiration_time=<token_lifetime>
ru.signalcom.dss.identity.user_otp_expiration_time=<otp_lifetime>
ru.signalcom.dss.identity.user_otp_max_cache_size=<otp_cache_sizer>
ru.signalcom.dss.identity.user_otp_failed_attempts_max=<otp_failed_attempts>
...
```

где

- <confirmation_timeout> - максимальная продолжительность процесса подтверждения операции с OTP (сек);
- <token_cache_size> - максимальный размер кеша для хранения маркеров доступа;
- <token_lifetime> - продолжительность валидности маркера доступа (сек);
- <otp_lifetime> - продолжительность валидности OTP (сек);
- <otp_cache_size> - максимальный размер кеша для хранения OTP;
- <otp_failed_attempts> - количество неудачных попыток ввода OTP для блокирования;

3.6.4. Требования по безопасности

Каналы взаимодействия веб-сервера идентификации со смежными системами должны быть защищены от активного несанкционированного вторжения, включая атаку MITM.

Доступ к веб-серверу идентификации должен быть ограничен (средствами сервера приложений, использованием VPN и т. д.).

Защите от несанкционированного изменения подлежит файл дескриптора развёртывания веб-сервера идентификации (/WEB-INF/web.xml) и файл конфигурации ПАК Cloud DSS (\$CATALINA_BASE/conf/dss-webserver.properties).

Меры обеспечения безопасности сервера приложений описаны в соответствующем разделе документации (для Apache Tomcat 8 – <http://tomcat.apache.org/tomcat-8.0-doc/security-howto.html>).

3.7. Настройка веб-приложения идентификации

3.7.1. Быстрый старт

В составе дистрибутива ПАК Cloud DSS имеется файл эталонной конфигурации (conf/dss-webserver.properties), в котором необходимо указать актуальные адреса серверов компонентов Cloud DSS. Для работы DSS Identity Web необходимо указать адрес DSS Identity Server:

```
...  
ru.signalcom.dss.idp.service.address=http://idp_hostname:[port]  
...
```

где

idp_hostname - имя (ip адрес) веб-сервера идентификации (DSS Identity Server, п. 3.6.);

При типовом размещении компонентов Cloud DSS это адрес сервера из п.3.6.1, и к нему должен быть обеспечен сетевой доступ.

Для быстрого старта приложения необходимо выполнить следующие действия:

- скопировать файл эталонной конфигурации conf/dss-webserver.properties в каталог \$CATALINA_BASE/conf;
- стартовать сервер Apache Tomcat;
- скопировать файл dss-identity-sp.war в каталог \$CATALINA_BASE/webapps.

Приложение будет автоматически развёрнуто и загружено на выполнение в контексте /dss-identity-sp (т.е. доступно по URL, например, http://localhost[:port]/dss-identity-sp).

3.7.2. Дескриптор развёртывания

Дескриптор развёртывания (файл web.xml) располагается в каталоге /WEB-INF приложения.

В дескрипторе развёртывания задаётся путь к файлу конфигурации в параметре приложения с именем configFileName, например:

```
...  
<context-param>
```

```
<param-name>configFileName</param-name>
<param-value>${catalina.base}/conf/dss-webserver.properties </param-value>
</context-param>
...
```

3.7.3. Параметры конфигурации

Настройки безопасности веб-приложения идентификации основаны на механизме java spring security и сконфигурированы в xml-файле \$CATALINA_BASE/webapps/dss-identity-sp/WEB-INF/classes/securityContext.xml. Этот файл не подлежит изменению.

Для настройки параметров клиентов веб-приложения идентификации предназначен xml-файл конфигурации \$CATALINA_BASE/webapps/dss-identity-sp/WEB-INF/classes/applicationContext.xml, содержащий значения параметров зарегистрированных OAuth 2.0 клиентов. Элементы этого файла, доступные для редактирования, описаны ниже:

3.7.3.1 Элемент <property name="dssIDPClientList">

Список зарегистрированных OAuth 2.0 клиентов:

```
...
<property name="dssIDPClientList">
  <list>
    <ref bean="dssIdpClientName" />
  </list>
</property>
...
```

где

- dssIdpClientName – имя java класса OAuth 2.0 клиента (см. п. 3.7.3.2.) в списке зарегистрированных клиентов;

3.7.3.2 Элемент <bean id="dssIdpClientName" class="ru.signalcom.dss.identity.sp.DssIDPClient">

```
...
<bean id="dssIdpClientName" class="ru.signalcom.dss.identity.sp.DssIDPClient">
  <property name="clientId" value="<ID>" />
  <property name="clientPass" value="<PASSWORD>" />
  <property name="authnUrl" value="/idp/oauth/authorize" />
  <property name="issuer" value=""/>
  <property name="logoutUrl" value="http://client_hostname:[post]/logout-url" />
  <property name="backpostUrl" value="http://client_hostname:[post]/backpost-url" />
  <property name="authnProtocol" value="IDP" />
  <property name="uniqueAttribute" value=""/>
  <property name="redirectUri" value="http://client_hostname:[post]/redirect-url" />
  <property name="displayName" value="<CLIENT-APP-DISPLAY-NAME>" />
</bean>
...
```

где

- dssIdpClientName – имя java класса OAuth 2.0 клиента (см. п. 3.7.3.1.);
- <ID> - идентификатор OAuth 2.0 клиента;
- <PASSWORD> - секрет OAuth 2.0 клиента;
- <property name="authnUrl" value="/idp/oauth/authorize" /> - URL в приложении DSS Identity Web для редиректа браузера при аутентификации OAuth 2.0 клиента (в текущей реализации значение фиксировано);
- <property name="issuer" value=""/> - имя сервиса-издателя маркера доступа (в текущей реализации игнорируется);
- <property name="logoutUrl" value="http://client_hostname:[post]/logout-url" />- URL в приложении OAuth 2.0 клиента для редиректа браузера после завершения сессии в DSS Identity Web;

- `<property name="backpostUrl" value="http://client_hostname:[post]/<backpost-url>"/>` - URL в приложении OAuth 2.0 клиента для редиректа браузера в других случаях (кроме аутентификации и завершения сессии);
- `<property name="authnProtocol" value="IDP"/>` - внутреннее обозначение типа сервера идентификации;
- `<property name="uniqueAttribute" value=""/>` - уникальный атрибут при аутентификации OIDC и SAML 2.0 (в текущей реализации игнорируется);
- `<property name="redirectUri" value="http://client_hostname:[post]/<redirect-url>"/>` - URL в приложении OAuth 2.0 клиента для редиректа браузера при аутентификации OAuth 2.0 клиента;
- `<property name="displayName" value="<CLIENT-APP-DISPLAY-NAME>"/>` - видимое имя приложения OAuth 2.0 клиента при аутентификации в приложении DSS Identity Web;

3.7.4. Требования по безопасности

Каналы взаимодействия веб-приложения идентификации со смежными системами должны быть защищены от активного несанкционированного вторжения, включая атаку MITM.

Доступ к веб-приложению идентификации должен быть ограничен (средствами сервера приложений, использованием VPN и т. д.).

Защите от несанкционированного изменения подлежат следующие файлы:

- дескриптор развёртывания /WEB-INF/web.xml;
- файл конфигурации безопасности /WEB-INF/classes/securityContext.xml;
- файл конфигурации клиентов /WEB-INF/classes/applicationContext.xml;
- файл конфигурации общих параметров ПАК Cloud DSS \$CATALINA_BASE/conf/dss-webserver.properties;

Меры обеспечения безопасности сервера приложений описаны в соответствующем разделе документации (для Apache Tomcat 8 – <http://tomcat.apache.org/tomcat-8.0-doc/security-howto.html>).

3.8. Настройка веб-сервиса администратора

Конфигурирование веб-сервиса администратора осуществляется путём редактирования файла дескриптора развёртывания веб-сервиса администратора.

3.8.1. Быстрый старт

Для развёртывания и старта веб-сервиса администратора необходимо выполнить следующие действия:

- убедиться, что сервер Apache Tomcat загружен;
- скопировать файл конфигурации dss-webserver.properties в каталог \$CATALINA_BASE/conf;
- скопировать файл dss-administrator-api.war в каталог \$CATALINA_BASE/webapps.

Веб-сервис администратора будет автоматически развёрнут и загружен на выполнение в контексте /dss-administrator-api (WSDL веб-сервиса будет доступен по URL <http://localhost:8080/dss-administrator-api/DSSAdministratorWebService?wsdl>).

3.8.2. Дескриптор развёртывания

Дескриптор развёртывания веб-сервиса администратора (файл web.xml) располагается в каталоге /WEB-INF приложения.

В дескрипторе развёртывания задаётся путь к файлу конфигурации ПАК Cloud DSS в параметре приложения с именем configFileName, например:

```
...  
<context-param>
```

```
<param-name>configFileName</param-name>
<param-value> ${catalina.base}/conf/dss-webserver.properties </param-value>
</context-param>
...
```

3.8.3. Требования по безопасности

Каналы взаимодействия веб-сервиса администратора со смежными системами должны быть защищены от активного несанкционированного вторжения, включая атаку MITM.

Доступ к веб-сервису администратора должен быть ограничен (средствами сервера приложений, использованием VPN и т. д.).

Защите от несанкционированного изменения подлежит файл дескриптора развёртывания веб-сервиса администратора (/WEB-INF/web.xml) и файл конфигурации ПАК Cloud DSS (\$CATALINA_BASE/conf/dss-webserver.properties).

Меры обеспечения безопасности сервера приложений описаны в соответствующем разделе документации (для Apache Tomcat 8 – <http://tomcat.apache.org/tomcat-8.0-doc/security-howto.html>).

3.9. Настройка веб-сервиса оператора

Конфигурирование веб-сервиса оператора осуществляется путём редактирования файла дескриптора развёртывания веб-сервиса оператора и файла конфигурации ПАК Cloud DSS.

3.9.1. Быстрый старт

Для развёртывания и старта веб-сервиса оператора необходимо выполнить следующие действия:

- убедиться, что сервер Apache Tomcat загружен;
- скопировать файл конфигурации dss-webserver.properties в каталог \$CATALINA_BASE/conf;
- скопировать файл dss-operator-api.war в каталог \$CATALINA_BASE/webapps.

Веб-сервис оператора будет автоматически развёрнут и загружен на выполнение в контексте /dss-operator-api (WSDL веб-сервиса будет доступен по URL <http://localhost:8080/dss-operator-api/DSSOperatorWebService?wsdl>).

3.9.2. Дескриптор развёртывания

Дескриптор развёртывания веб-сервиса оператора (файл web.xml) располагается в каталоге /WEB-INF приложения.

В дескрипторе развёртывания задаётся путь к файлу конфигурации ПАК Cloud DSS в параметре приложения с именем configFileName, например:

```
...
<context-param>
  <param-name>configFileName</param-name>
  <param-value> ${catalina.base}/conf/dss-webserver.properties </param-value>
</context-param>
...
```

3.9.3. Параметры конфигурации

Веб-сервис оператора использует следующие параметры файла конфигурации ПАК Cloud DSS:

- «ru.signalcom.dss.confirmed.actions» - задает список операций оператора, которые требуют подтверждения с помощью двухфакторной аутентификации, по умолчанию значение не задано; данный параметр используется, если значение параметра «ru.signalcom.dss.allow.confirmation.policy.override» (см. ниже) равно false или в профиле оператора не задан список этих операций;

- «ru.signalcom.dss.allow.confirmation.policy.override» - задает уровень использования параметра «ru.signalcom.dss.confirmed.actions» (см. выше), по умолчанию значение равно true; если значение параметра «ru.signalcom.dss.allow.confirmation.policy.override» равно false, то будет использоваться список операций, заданных параметром «ru.signalcom.dss.confirmed.actions»; если равно true, то может использоваться список операций, заданных в профиле оператора;
- «ru.signalcom.dss.confirmation.timeout» - задает период (в секундах), в течение которого оператор должен подтвердить операцию, по умолчанию значение равно 30;
- «ru.signalcom.dss.transaction.timeout» - задает период (в секундах), в течение которого оператор должен завершить операцию, по умолчанию значение равно 30;
- «ru.signalcom.dss.psk.validity.period» - задает период действия общего секретного ключа (в сутках), по умолчанию значение равно 455.

3.9.4. Требования по безопасности

Каналы взаимодействия веб-сервиса оператора со смежными системами должны быть защищены от активного несанкционированного вторжения, включая атаку MITM.

Доступ к веб-сервису оператора должен быть ограничен (средствами сервера приложений, использованием VPN и т. д.).

Защите от несанкционированного изменения подлежит файл дескриптора развёртывания веб-сервиса оператора (/WEB-INF/web.xml) и файл конфигурации ПАК Cloud DSS (\$CATALINA_BASE/conf/dss-webserver.properties).

3.10. Настройка веб-сервиса пользователя

Конфигурирование веб-сервиса пользователя осуществляется путём редактирования файла дескриптора развёртывания веб-сервиса пользователя и файла конфигурации ПАК Cloud DSS.

3.10.1. Быстрый старт

Для развёртывания и старта веб-сервиса пользователя необходимо выполнить следующие действия:

- убедиться, что сервер Apache Tomcat загружен;
- скопировать файл конфигурации dss-webserver.properties в каталог \$CATALINA_BASE/conf;
- скопировать файл dss-customer-api.war в каталог \$CATALINA_BASE/webapps.

Веб-сервис пользователя будет автоматически развёрнут и загружен на выполнение в контексте /dss-customer-api (WSDL веб-сервиса будет доступен по URL <http://localhost:8080/dss-customer-api/DSSCustomerWebService?wsdl>).

3.10.2. Дескриптор развёртывания

Дескриптор развёртывания веб-сервиса пользователя (файл web.xml) располагается в каталоге /WEB-INF приложения.

В дескрипторе развёртывания задаётся путь к файлу конфигурации ПАК Cloud DSS в параметре приложения с именем configFileName, например:

```
...  
<context-param>  
  <param-name>configFileName</param-name>  
  <param-value> ${catalina.base }/conf/dss-webserver.properties </param-value>  
</context-param>  
...
```

3.10.3. Параметры конфигурации

Веб-сервис пользователя использует следующие параметры файла конфигурации ПАК Cloud DSS:

- «ru.signalcom.dss.confirmed.actions» - задает список операций пользователя, которые требуют подтверждения с помощью двухфакторной аутентификации, по умолчанию значение не задано; данный параметр используется, если значение параметра «ru.signalcom.dss.allow.confirmation.policy.override» (см. ниже) равно false или в профиле пользователя и профиле группы пользователя не задан список этих операций;
- «ru.signalcom.dss.allow.confirmation.policy.override» - задает уровень использования параметра «ru.signalcom.dss.confirmed.actions» (см. выше), по умолчанию значение равно true; если значение параметра «ru.signalcom.dss.allow.confirmation.policy.override» равно false, то будет использоваться список операций, заданных параметром «ru.signalcom.dss.confirmed.actions»; если равно true, то может использоваться список операций, заданных в профиле пользователя и в профиле группы пользователя;
- «ru.signalcom.dss.confirmation.timeout» - задает период (в секундах), в течение которого пользователь должен подтвердить операцию, по умолчанию значение равно 30;
- «ru.signalcom.dss.transaction.timeout» - задает период (в секундах), в течение которого пользователь должен завершить операцию, по умолчанию значение равно 30;
- «ru.signalcom.dss.document.printed.bytes» - задает максимальное количество байт, записываемых в файл журнала веб-сервиса пользователя для каждого запроса, по умолчанию значение равно 1536;
- «ru.signalcom.dss.document.size» - задает максимальный размер подписываемого пользователем документа (в байтах), по умолчанию значение равно 5242880;
- «ru.signalcom.dss.document.name.length» - задает максимальный размер названия или краткого содержания подписываемого документа (в байтах), по умолчанию значение равно 256.

3.10.4. Требования по безопасности

Каналы взаимодействия веб-сервиса пользователя со смежными системами должны быть защищены от активного несанкционированного вторжения, включая атаку MITM.

Доступ к веб-сервису пользователя должен быть ограничен (средствами сервера приложений, использованием VPN и т. д.).

Защите от несанкционированного изменения подлежит файл дескриптора развёртывания веб-сервиса оператора (/WEB-INF/web.xml) и файл конфигурации ПАК Cloud DSS (\$CATALINA_BASE/conf/dss-webserver.properties).

3.11. Настройка клиентских веб-приложений

В состав дистрибутива Cloud DSS входят три клиентских веб-приложения:

- веб-приложение администратора DSS Administrator Web;
- веб-приложение оператора DSS Operator Web;
- веб-приложение пользователя DSS Customer Web;

Эти веб-приложения являются клиентами веб-сервисов администратора DSS Administrator API, оператора DSS Operator API и пользователя DSS Customer API, а также клиентами веб-приложения идентификации DSS Identity Web при аутентификации и подтверждении операций.

В дистрибутиве веб-приложения идентификации содержится эталонный файл конфигурации applicationContext.xml, содержащий настройки OAuth 2.0 клиентов для трех поставляемых клиентских веб-приложений администратора, оператора и пользователя.

Каждое клиентское приложение, использующее для аутентификации и подтверждения операций веб-приложение идентификации DSS Identity Web, включает одного или более OAuth 2.0 клиента, зарегистрированного в DSS Identity Web (см. п. 3.7.3.).

Процедура аутентификации и подтверждения операций внешнего приложения в веб-приложении идентификации описана в «Cloud DSS. Руководство программиста» (раздел. 6).

При настройке клиентских приложений необходимо задать в файлах конфигурации актуальные значения имен (ip-адресов) серверов размещения следующих приложений:

- веб-приложения администратора DSS Administrator Web;
- веб-приложения оператора DSS Operator Web;
- веб-приложения пользователя DSS Customer Web;
- веб-сервиса администратора DSS Administrator API;
- веб-сервиса оператора DSS Operator API;
- веб-сервиса пользователя DSS Customer API;
- веб-приложения идентификации DSS Identity Web;

Основные параметры, определяющие сетевые адреса приложений, задаются в файле \$CATALINA_BASE/conf/catalina.properties:

```
...
ru.signalcom.dss.administrator.logout_url=http:// idp_web_hostname:[port]/dss-identity-
sp/exit?client_id=<ID-ADMIN>
ru.signalcom.dss.operator.logout_url=http:// idp_web_hostname:[port]/dss-identity-
sp/exit?client_id=<ID-OPERATOR>r
ru.signalcom.dss.customer.logout_url=http:// idp_web_hostname:[port]/dss-identity-
sp/exit?client_id=<ID-CUSTOMER>

ru.signalcom.dss.administrator.api=http://admin_api_hostname:[port]
ru.signalcom.dss.operator.api=http://operator_api_hostname:[port]
ru.signalcom.dss.customer.api=http://customer_api_hostname:[port]
...
```

где

- ru.signalcom.dss.administrator.logout_url=http:// idp_web_hostname:[port]/dss-identity-sp/exit?client_id=<ID-ADMIN> - URL в приложении DSS Identity Web для редиректа браузера для завершения сессии веб-приложения администратора на DSS Identity Web (см. «Cloud DSS. Руководство программиста» (п. 6.6.));
- <ID-ADMIN> - идентификатор OAuth 2.0 клиента приложения администратора (см. п. 3.7.3.2.);
- ru.signalcom.dss.operator.logout_url=http:// idp_web_hostname:[port]/dss-identity-sp/exit?client_id=<ID-OPERATOR> - URL в приложении DSS Identity Web для редиректа браузера для завершения сессии веб-приложения оператора на DSS Identity Web (см. «Cloud DSS. Руководство программиста» (п. 6.6.));
- <ID-OPERATOR> - идентификатор OAuth 2.0 клиента приложения оператора (см. п. 3.7.3.2.);
- ru.signalcom.dss.customer.logout_url=http:// idp_web_hostname:[port]/dss-identity-sp/exit?client_id=<ID-CUSTOMER> - URL в приложении DSS Identity Web для редиректа браузера для завершения сессии веб-приложения пользователя на DSS Identity Web (см. «Cloud DSS. Руководство программиста» (п. 6.6.));
- <ID-CUSTOMER> - идентификатор OAuth 2.0 клиента приложения пользователя (см. п. 3.7.3.2.);
-
- ru.signalcom.dss.administrator.api=http:// admin_api_hostname:[port] - URL веб-сервиса администратора DSS Administrator API
- ru.signalcom.dss.operator.api=http:// operator_api_hostname:[port] - URL веб-сервиса оператора DSS Operator API
- ru.signalcom.dss.customer.api=http:// customer_api_hostname:[port] - URL веб-сервиса пользователя DSS Customer API

3.11.1. Настройка веб-приложения администратора

Настройка OAuth 2.0 клиента для аутентификации веб-приложения администратора выполняется с использованием механизма java spring security в xml-файле конфигурации \$CATALINA_BASE/webapps/dss-administrator-web/WEB-INF/classes/securityContext.xml

```
...
<bean id="oauthClient" class="org.pac4j.oauth.client.GenericOAuth20Client">
```

```

    <property name="configuration" ref="oauthConfig" />
    <property name="key" value="<ID>" />
    <property name="secret" value="<PASSWORD>" />
    <property name="authUrl" value="http://idp_web_hostname:[port]/dss-identity-
sp/idp/oauth/authorize" />
    <property name="tokenUrl" value="http:// idp_web_hostname:[port]/dss-identity-
sp/api/token" />
    <property name="profileUrl" value="http:// idp_web_hostname:[port]/dss-identity-
sp/verify/token" />
    <property name="callbackUrl" value="http:// admin_web_hostname:[port]/dss-
administrator-web/callback?client_name=GenericOAuth20Client" />
    <property name="authorizationGenerator" ref="roleAuthGeneratorOAuth" />
</bean>
...

```

где

- <ID> - идентификатор OAuth 2.0 клиента (см. п. 3.7.3.2.);
- <PASSWORD> - секрет OAuth 2.0 клиента (см. п. 3.7.3.2.);
- <property name="authUrl" value="http://idp_web_hostname:[port]/dss-identity-sp/idp/oauth/authorize" /> - URL в приложении DSS Identity Web для редиректа браузера при аутентификации OAuth 2.0 клиента (см. п. 3.7.3.2.);
- <property name="tokenUrl" value="http:// idp_web_hostname:[port]/dss-identity-sp/api/token" /> - URL в приложении DSS Identity Web для получения маркера доступа OAuth 2.0 клиентом (см. «Cloud DSS. Руководство программиста» (п. 6.1.2.));
- <property name="profileUrl" value="http:// idp_web_hostname:[port]/dss-identity-sp/verify/token" /> - URL в приложении DSS Identity Web для валидации маркера доступа OAuth 2.0 клиентом (см. «Cloud DSS. Руководство программиста» (п. 6.5.));
- <property name="callbackUrl" value="http:// admin_web_hostname:[port]/dss-administrator-web/callback?client_name=GenericOAuth20Client" /> - URL в приложении OAuth 2.0 клиента для редиректа браузера при аутентификации OAuth 2.0 клиента (см. п. 3.7.3.2.);

3.11.2. Настройка веб-приложения оператора

Настройка OAuth 2.0 клиента для аутентификации веб-приложения оператора выполняется с использованием механизма java spring security в xml-файле конфигурации \$CATALINA_BASE/webapps/dss-operator-web/WEB-INF/classes/securityContext.xml

```

...
<bean id="oauthClient" class="org.pac4j.oauth.client.GenericOAuth20Client">
    <property name="configuration" ref="oauthConfig" />
    <property name="key" value="<ID>" />
    <property name="secret" value="<PASSWORD>" />
    <property name="authUrl" value="http://idp_web_hostname:[port]/dss-identity-
sp/idp/oauth/authorize" />
    <property name="tokenUrl" value="http:// idp_web_hostname:[port]/dss-identity-
sp/api/token" />
    <property name="profileUrl" value="http:// idp_web_hostname:[port]/dss-identity-
sp/verify/token" />
    <property name="callbackUrl" value="http://operator_web_hostname:[port]/dss-operator-
web/callback?client_name=GenericOAuth20Client" />
    <property name="authorizationGenerator" ref="roleAuthGeneratorOAuth" />
</bean>
...

```

где

- <ID> - идентификатор OAuth 2.0 клиента (см. п. 3.7.3.2.);
- <PASSWORD> - секрет OAuth 2.0 клиента (см. п. 3.7.3.2.);
- <property name="authUrl" value="http://idp_web_hostname:[port]/dss-identity-sp/idp/oauth/authorize" /> - URL в приложении DSS Identity Web для редиректа браузера при аутентификации OAuth 2.0 клиента (см. п. 3.7.3.2.);

- `<property name="tokenUrl" value="http:// idp_web_hostname:[port]/dss-identity-sp/api/token" />` - URL в приложении DSS Identity Web для получения маркера доступа OAuth 2.0 клиентом (см. «Cloud DSS. Руководство программиста» (п. 6.1.2.));
- `<property name="profileUrl" value="http:// idp_web_hostname:[port]/dss-identity-sp/verify/token" />` - URL в приложении DSS Identity Web для валидации маркера доступа OAuth 2.0 клиентом (см. «Cloud DSS. Руководство программиста» (п. 6.5.));
- `<property name="callbackUrl" value="http://operator_web_hostname:[port]/dss-operator-web/callback?client_name=GenericOAuth20Client" />` - URL в приложении OAuth 2.0 клиента для редиректа браузера при аутентификации OAuth 2.0 клиента (см. п. 3.7.3.2.);

Для подтверждения операций в веб-приложении оператора реализован дополнительный OAuth 2.0 клиент, зарегистрированный в веб-приложении идентификации:

В веб-приложении оператора параметры OAuth 2.0 клиента для подтверждения операций задаются в файле \$CATALINA_BASE/conf/catalina.properties:

```
...
ru.signalcom.dss.operator.confirm.auth_url=http:// idp_web_hostname:[port]/dss-identity-sp/idp/oauth/authorize
ru.signalcom.dss.operator.confirm.token_url=http:// idp_web_hostname:[port]/dss-identity-sp/api/token
ru.signalcom.dss.operator.confirm.callback_url=http://operator_web_hostname:[port]/dss-operator-web/oauth2client/authorization_code
ru.signalcom.dss.operator.confirm.client_id=<ID>
ru.signalcom.dss.operator.confirm.client_passw=<PASSWORD>
...
```

где

- `ru.signalcom.dss.operator.confirm.auth_url=http:// idp_web_hostname:[port]/dss-identity-sp/idp/oauth/authorize` - URL в приложении DSS Identity Web для редиректа браузера при аутентификации OAuth 2.0 клиента (см. п. 3.7.3.2.);
- `ru.signalcom.dss.operator.confirm.token_url=http:// idp_web_hostname:[port]/dss-identity-sp/api/token` - URL в приложении DSS Identity Web для получения маркера доступа OAuth 2.0 клиентом (см. «Cloud DSS. Руководство программиста» (п. 6.1.2.));
- `ru.signalcom.dss.operator.confirm.callback_url=http://operator_web_hostname:[port]/dss-operator-web/oauth2client/authorization_code` - URL в приложении OAuth 2.0 клиента для редиректа браузера при аутентификации OAuth 2.0 клиента (см. п. 3.7.3.2.);
- `ru.signalcom.dss.operator.confirm.client_id=<ID>` - идентификатор OAuth 2.0 клиента (см. п. 3.7.3.2.);
- `ru.signalcom.dss.operator.confirm.client_passw=<PASSWORD>` - секрет OAuth 2.0 клиента (см. п. 3.7.3.2.);

3.11.3. Настройка веб-приложения пользователя

Настройка OAuth 2.0 клиента для аутентификации веб-приложения пользователя выполняется с использованием механизма java spring security в xml-файле конфигурации \$CATALINA_BASE/webapps/dss-customer-web/WEB-INF/classes/securityContext.xml

```
...
<bean id="oauthClient" class="org.pac4j.oauth.client.GenericOAuth20Client">
  <property name="configuration" ref="oauthConfig" />
  <property name="key" value="<ID>" />
  <property name="secret" value="<PASSWORD>" />
  <property name="authUrl" value="http://idp_web_hostname:[port]/dss-identity-sp/idp/oauth/authorize" />
  <property name="tokenUrl" value="http:// idp_web_hostname:[port]/dss-identity-sp/api/token" />
  <property name="profileUrl" value="http:// idp_web_hostname:[port]/dss-identity-sp/verify/token" />
</bean>
```

```
<property name="callbackUrl" value="http://customer_web_hostname:[port]/dss-
customer-web/callback?client_name=GenericOAuth20Client" />
<property name="authorizationGenerator" ref="roleAuthGeneratorOAuth" />
</bean>
...
```

где

- <ID> - идентификатор OAuth 2.0 клиента (см. п. 3.7.3.2.);
- <PASSWORD> - секрет OAuth 2.0 клиента (см. п. 3.7.3.2.);
- <property name="authUrl" value="http://idp_web_hostname:[port]/dss-identity-sp/idp/oauth/authorize" /> - URL в приложении DSS Identity Web для редиректа браузера при аутентификации OAuth 2.0 клиента (см. п. 3.7.3.2.);
- <property name="tokenUrl" value="http:// idp_web_hostname:[port]/dss-identity-sp/api/token" /> - URL в приложении DSS Identity Web для получения маркера доступа OAuth 2.0 клиентом (см. «Cloud DSS. Руководство программиста» (п. 6.1.2.));
- <property name="profileUrl" value="http:// idp_web_hostname:[port]/dss-identity-sp/verify/token" />- URL в приложении DSS Identity Web для валидации маркера доступа OAuth 2.0 клиентом (см. «Cloud DSS. Руководство программиста» (п. 6.5.));
- <property name="callbackUrl" value="http://customer_web_hostname:[port]/dss-customer-web/callback?client_name=GenericOAuth20Client" /> - URL в приложении OAuth 2.0 клиента для редиректа браузера при аутентификации OAuth 2.0 клиента (см. п. 3.7.3.2.);

Для подтверждения операций в веб приложении пользователя реализован дополнительный OAuth 2.0 клиент, зарегистрированный в веб-приложении идентификации:

В веб-приложении пользователя параметры OAuth 2.0 клиента для подтверждения операций задаются в файле \$CATALINA_BASE/conf/catalina.properties:

```
...
ru.signalcom.dss.customer.confirm.auth_url=http:// idp_web_hostname:[port]/dss-identity-
sp/idp/oauth/authorize
ru.signalcom.dss.customer.confirm.token_url=http:// idp_web_hostname:[port]/dss-identity-
sp/api/token
ru.signalcom.dss.customer.confirm.callback_url=http://customer_web_hostname:[port]/dss-
customer-web/oauth2client/authorization_code
ru.signalcom.dss.customer.confirm.client_id=<ID>
ru.signalcom.dss.customer.confirm.client_passw=<PASSWORD>
...
```

где

- ru.signalcom.dss.customer.confirm.auth_url=http:// idp_web_hostname:[port]/dss-identity-sp/idp/oauth/authorize - URL в приложении DSS Identity Web для редиректа браузера при аутентификации OAuth 2.0 клиента (см. п. 3.7.3.2.);
- ru.signalcom.dss.customer.confirm.token_url=http:// idp_web_hostname:[port]/dss-identity-sp/api/token - URL в приложении DSS Identity Web для получения маркера доступа OAuth 2.0 клиентом (см. «Cloud DSS. Руководство программиста» (п. 6.1.2.));
- ru.signalcom.dss.customer.confirm.callback_url=http://customer_web_hostname:[port]/dss-customer-web/oauth2client/authorization_code - URL в приложении OAuth 2.0 клиента для редиректа браузера при аутентификации OAuth 2.0 клиента (см. п. 3.7.3.2.);
- ru.signalcom.dss.customer.confirm.client_id=<ID> - идентификатор OAuth 2.0 клиента (см. п. 3.7.3.2.);
- ru.signalcom.dss.customer.confirm.client_passw=<PASSWORD> - секрет OAuth 2.0 клиента (см. п. 3.7.3.2.);

3.11.4. Требования по безопасности

Каналы взаимодействия клиентских веб-приложений администратора, оператора и пользователя со смежными системами должны быть защищены от активного несанкционированного вторжения, включая атаку MITM.

Доступ к клиентским веб-приложениям администратора, оператора и пользователя должен быть ограничен (средствами сервера приложений, использованием VPN и т. д.).

Защите от несанкционированного изменения подлежат следующие файлы клиентских веб-приложений администратора, оператора и пользователя:

- дескрипторы развёртывания /WEB-INF/web.xml;
- файлы конфигурации безопасности /WEB-INF/classes/securityContext.xml;
- файл конфигурации общих параметров ПАК Cloud DSS
\$CATALINA_BASE/conf/catalina.properties;

Меры обеспечения безопасности сервера приложений описаны в соответствующем разделе документации (для Apache Tomcat 8 – <http://tomcat.apache.org/tomcat-8.0-doc/security-howto.html>).

3.12. Настройка сервера оповещений

Конфигурирование сервера оповещений осуществляется путём редактирования файла дескриптора развёртывания сервера оповещений.

3.12.1. Быстрый старт

Для развёртывания и старта сервера оповещений необходимо выполнить следующие действия:

- убедиться, что сервер Apache Tomcat загружен;
- скопировать файл dss-notification-webapp.war в каталог \$CATALINA_BASE/webapps.

Сервер оповещений будет автоматически развёрнут и загружен на выполнение в контексте /dss-notification-webapp.

3.12.2. Дескриптор развёртывания

Дескриптор развёртывания сервера оповещений (файл web.xml) располагается в каталоге /WEB-INF приложения.

В дескрипторе развёртывания задаются следующие параметры сервера оповещений ПАК Cloud DSS:

- «activeMQ.url» - ip адрес и номер порта Apache ActiveMQ;
- «activeMQ.username» - имя пользователя Apache ActiveMQ;
- «activeMQ.password» - пароль Apache ActiveMQ;
- «activeMQ.topic» - название подписки Apache ActiveMQ;
- «activeMQ.useTransaction» - сеанс может быть указан как транзакционный;
- «activeMQ.alwaysSessionAsync» - флаг асинхронного соединения;
- «activeMQ.useAsyncSend» - настройка асинхронной отправки;
- «activeMQ.clientId» - Id клиента;
- «activeMQ.clientName» - имя клиента;
- «transportSet» - список используемых вариантов доставки сообщений;
- «sms.smpp.enquireLinkTimer» - интервал в миллисекундах между проверками достоверности;
- «sms.smpp.transactionTimer» - максимально допустимый период бездействия после транзакции ;
- «sms.smpp.host» - адрес SMPP сервера;
- «sms.smpp.port» - номер порта SMPP сервера;
- «sms.smpp.username» - имя пользователя;
- «sms.smpp.password» - пароль;
- «sms.smpp.systemType» - тип сервера SMPP;
- «sms.smpp.serviceType» - тип службы SMPP;
- «sms.smpp.signature» - подпись отправителя;
- «mail.smtp.host» - адрес SMTP сервера;

-
- «mail.smtp.port» - номер порта SMTP сервера;
 - «mail.smtp.username» - имя пользователя;
 - «mail.smtp.password» - пароль;
 - «mail.smtp.sender» - адрес отправителя;
 - «mail.smtp.auth» - флаг аутентификации SMTP;
 - «mail.smtp.starttls.enable» - использование STARTTLS;
 - «mail.smtp.socketFactory.port» - порт для подключения при использовании указанной фабрики сокетов;
 - «mail.smtp.socketFactory.class» - имя класса, который реализует интерфейс javax.net.SocketFactory;
 - «mail.smtp.signature» - подпись отправителя;
 - «mail.transport.protocol» - протокол передачи почты.

3.12.3. Требования по безопасности

Каналы взаимодействия сервера оповещений со смежными системами должны быть защищены от активного несанкционированного вторжения, включая атаку MITM.

Доступ к серверу оповещений должен быть ограничен (средствами сервера приложений, использованием VPN и т. д.).

Защите от несанкционированного изменения подлежат следующие файлы сервера оповещений:

- дескрипторы развёртывания /WEB-INF/web.xml;
- файл конфигурации общих параметров ПАК Cloud DSS
\$CATALINA_BASE/conf/catalina.properties;

Меры обеспечения безопасности сервера приложений описаны в соответствующем разделе документации (для Apache Tomcat 8 – <http://tomcat.apache.org/tomcat-8.0-doc/security-howto.html>).

3.13. Настройка сервера аудита событий

Конфигурирование сервера аудита событий осуществляется путём редактирования файла дескриптора развёртывания сервера аудита событий.

3.13.1. Быстрый старт

Для развёртывания и старта сервера аудита событий необходимо выполнить следующие действия:

- убедиться, что сервер Apache Tomcat загружен;
- скопировать файл dss-audit-webapp.war в каталог \$CATALINA_BASE/webapps.

Сервер аудита событий будет автоматически развёрнут и загружен на выполнение в контексте /dss-audit-webapp.

3.13.2. Дескриптор развёртывания

Дескриптор развёртывания сервера аудита событий (файл web.xml) располагается в каталоге /WEB-INF приложения.

В дескрипторе развёртывания задаются следующие параметры сервера аудита событий ПАК Cloud DSS:

- «activeMQ.url» - ip адрес и номер порта Apache ActiveMQ;
- «activeMQ.username» - имя пользователя Apache ActiveMQ;
- «activeMQ.password» - пароль Apache ActiveMQ;
- «activeMQ.topic» - название подписки Apache ActiveMQ;
- «activeMQ.useTransaction» - сеанс может быть указан как транзакционный;
- «activeMQ.alwaysSessionAsync» - флаг асинхронного соединения;

- «activeMQ.useAsyncSend» - настройка асинхронной отправки;
- «activeMQ.clientId» -Id клиента;
- «activeMQ.clientName» - имя клиента;
- «saveThreadNameFormat» - шаблон имени отправителя;
- «timerThreadNameFormat» - шаблон имени таймера;
- «nThreads» - количество потоков;
- «minDSSEventPerThread» - минимальное количество сообщений в потоке;
- «counterDelay» - начальная задержка;
- «counterTimer» - периодическая задержка;
- «dssEventCollectorSize» - размер сборщика событий;
- «dssEventCollectorFillFactor» - коэффициент заполнения;
- «hikari.jdbcUrl» - адрес БД;
- «hikari.user» - имя пользователя;
- «hikari.password» - пароль;
- «hikari.driverClassName» - имя класса драйвера;
- «hikari.cachePrepStmts» - флаг кеширования подготовленных операторов;
- «hikari.rewriteBatchedStatements» -флаг пакетной отправки операторов;
- «hikari.useServerPrepStmts» - использование хранимых процедур;
- «hikari.isAutoCommit» - автоматическое фиксирование транзакции.

3.13.3. Создание базы данных сервера аудита событий

В состав сервера аудита событий входит SQL-скрипт «dssaudit.sql» для создания базы данных сервера аудита событий.

3.13.4. Требования по безопасности

Каналы взаимодействия сервера аудита событий со смежными системами должны быть защищены от активного несанкционированного вторжения, включая атаку MITM.

Доступ к серверу аудита событий должен быть ограничен (средствами сервера приложений, использованием VPN и т. д.).

Защите от несанкционированного изменения подлежат следующие файлы сервера аудита событий:

- дескрипторы развёртывания /WEB-INF/web.xml;
- файл конфигурации общих параметров ПАК Cloud DSS
\$CATALINA_BASE/conf/catalina.properties;

Меры обеспечения безопасности сервера приложений описаны в соответствующем разделе документации (для Apache Tomcat 8 – <http://tomcat.apache.org/tomcat-8.0-doc/security-howto.html>).

3.14. Настройка базы данных

3.14.1. Создание базы данных

В состав дистрибутива ПАК Cloud DSS входит пример файла SQL-скрипта «hsmapp-schema.sql» для создания базы данных ПАК Cloud DSS.

Для создания базы данных ПАК Cloud DSS необходимо выполнить следующие действия:

- скопировать файл «hsmapp-schema.sql» в произвольный каталог на диске сервера;
- запустить командную оболочку ОС;
- с помощью команды cd установить каталог с файлом «hsmapp-schema.sql» текущим;
- выполнить следующую команду:

```
mysql -u user -ppassword < hsmapp-schema.sql
```

где:

user – имя администратора MariaDB;
password – пароль администратора MariaDB.

3.14.2. Настройка Hibernate

Компоненты ПАК Cloud DSS взаимодействуют с базой данных MariaDB с помощью ORM-библиотеки Hibernate.

Для настройки компонентов ПАК Cloud DSS на работу с Hibernate необходимо выполнить следующие действия:

- скопировать пример файла конфигурации Hibernate из состава дистрибутива hibernate.cfg.xml в каталог \$CATALINA_BASE/conf;
- в параметре «ru.signalcom.dss.webserver.dao.HibernateUtil.configurationFile» файла \$CATALINA_BASE/conf/catalina.properties задать полный путь к файлу конфигурации hibernate.cfg.xml;
- в элементе «hibernate.hikari.dataSource.url» файла hibernate.cfg.xml задать правильный IP-адрес и порт сервера базы данных MariaDB;
- в элементе «hibernate.hikari.dataSource.user» файла hibernate.cfg.xml задать имя пользователя базы данных ПАК Cloud DSS;
- в элементе «hibernate.hikari.dataSource.password» файла hibernate.cfg.xml задать пароль пользователя базы данных ПАК Cloud DSS.

3.15. Управление приложениями

Веб-приложения компонентов ПАК Cloud DSS могут быть развёрнуты любым из стандартных методов (см. <http://tomcat.apache.org/tomcat-8.0-doc/deployer-howto.html>):

- помещением war-файла в каталог appBase (по умолчанию \$CATALINA_HOME/webapps); этот способ работает только при значении атрибута autoDeploy=true в элементе <Host> (см. файл конфигурации \$CATALINA_HOME/conf/server.xml);
- помещением разархивированного приложения (т.е. каталогов META-INF и WEB-INF) в один из подкаталогов appBase; этот способ также работает только при значении атрибута autoDeploy=true;
- с помощью Tomcat Manager (см. <http://tomcat.apache.org/tomcat-8.0-doc/manager-howto.html>);
- с использованием Tomcat Client Deployer.

Запуск/останов и удаление веб-приложений компонентов ПАК Cloud DSS производятся также стандартными методами (см. <http://tomcat.apache.org/tomcat-8.0-doc/deployer-howto.html>).

Для использования административной оболочки Apache Tomcat 8 необходимо настроить в файле \$CATALINA_HOME/conf/tomcat-users.xml доступ для ролей manager-script и manager-gui, например:

```
...  
<role rolename="manager-script"/>  
<role rolename="manager-gui"/>  
<user username="tomcat" password="*****" roles="manager-gui,manager-script"/>  
...
```

В результате при загруженном приложении manager пользователю с идентификатором tomcat будет доступно приложение по адресу <http://localhost:8080/manager/html/> или <http://localhost:8080/manager/text/>, позволяющее осуществлять административные функции.

5. СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

Компоненты ПАК Cloud DSS направляют сообщения в журналы событий, для настройки которых используется общий файл log4j2.xml, который должен размещаться в каталоге \$CATALINA_BASE/conf.

Файл конфигурации журналирования должен настраиваться согласно руководству <http://logging.apache.org/log4j/2.x/manual/index.html>.

В состав дистрибутива ПАК Cloud DSS входит пример файла log4j2.xml.

ЛИТЕРАТУРА

1. Signal-COM DSS Server. Руководство системного программиста. ШКНР.00042-01 32 01. АО «СИГНАЛ-КОМ», 2021.
2. Signal-COM DSS Key Manager. Руководство системного программиста. ШКНР.00042-01 32 02. АО «СИГНАЛ-КОМ», 2021.
3. СКЗИ «Сигнал-КОМ HSM». Формуляр. ШКНР.00048-01 30 01. АО «СИГНАЛ-КОМ», 2021.
4. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
5. PKCS #10 v1.7: Certification Request Syntax Standard. RSA Laboratories, May 26, 2000.
6. J. Schaad, M. Myers, Certificate Management over CMS (CMC), RFC 5272, June 2008.
7. Housley, R., Cryptographic Message Syntax, RFC 5652, September 2009.
8. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS. Рекомендации по стандартизации. Федеральное агентство по техническому регулированию и метрологии (Росстандарт), Технический комитет 26 «Криптографическая защита информации», 2014.
9. XML Signature Syntax and Processing (Second Edition). W3C Recommendation, 10 June 2008.
10. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 в протоколах и форматах сообщений на основе XML (проект). Рекомендации по стандартизации. Федеральное агентство по техническому регулированию и метрологии (Росстандарт), Технический комитет 26 «Криптографическая защита информации», 2014.
11. D. Pinkas, N. Pope, J. Ross, CMS Advanced Electronic Signatures (CAAdES). RFC 5126, February 2008.
12. C. Adams, P. Cain, D. Pinkas, R. Zuccherato, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), RFC 3161, August 2001.
13. ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.
14. Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509. Рекомендации по стандартизации. Федеральное агентство по техническому регулированию и метрологии (Росстандарт), Технический комитет 26 «Криптографическая защита информации», 2014.
15. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.
16. ETSI EN 319 142-1 V1.1.1 (2016-04): Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures. European Telecommunications Standards Institute ETSI.
17. ECMA-376. Office Open XML file formats, 4th edition, December 2012. Ecma International.