**Инструкция по установке, настройке и работе в JMS Client**

**I Установка и настройка JMS Client**

**JMS (JaCarta Management System)** - система управления жизненным циклом ключевых носителей JaCarta, eToken и Рутокен

**JMS Client –** программное обеспечение,устанавливается на стороне пользователя, с помощью которого имеется возможность перевыпустить сертификат и ключи электронной подписи зарегистрированному Пользователю УЦ, при условии, что на ключевом носителе имеется действующий сертификат Пользователя УЦ.

1. **Обеспечение связи с сервером JMS**

- На рабочем месте должен быть установлен VipNet Client.

- В списке защищенной сети VipNet Client обязательно наличие узла «**HW ЦОД ПНО СБ**» (Проверить доступ к серверу JMS можно командой ping 10.101.53.22)
 - для подключения к серверу JMS КриптоПро, доступ проверить командой ping 10.101.53.21

- Должен быть установлен, VipNet CSP (КриптоПро CSP – при необходимости)

1. **Установка и первоначальная настройка компонента JMS Client**

Чтобы установить компонент JMS Client, выполните следующие действия:

- В зависимости от разрядности операционной системы запустите один из следующих файлов.

- 32 бит: **Aladdin.JMS.Client.STS-x86.msi**

- 64 бит: **Aladdin.JMS.Client.STS-x64.msi**

Отобразится следующее окно:



🡪далее🡪 Я принимаю условия лицензионного соглашения 🡪 Полная 🡪 Установить 🡪 Готово.

Меню быстрого запуска JMS Client будет отображаться в области уведомлений в виде значка  (Клиент JMS).

1. **Настройка соединения JMS Client с сервером JMS**

Для автоматической настройки соединения с сервером JMS необходимо запустить исполняемый файл: **jc-config\_vipNet.exe** с правами локального Администратора.

Для автоматической настройки соединения с сервером JMS КриптоПро, необходимо запустить исполняемый файл **jc-config\_criptoPro.exe** с правами локального Администратора.

В файле /Windows/System32/drivers/ec/hosts в самом конце добавить строку:

10.101.53.24 rz-uc-jms.nso.loc

1. **Установка сертификатов**

На рабочей станции, с установленным JMS Clientустановить сертификаты **jms.cer** и **nso.cer** (для подключения к серверу, JMS КриптоПро, дополнительно установить – **jms\_criptoPro.cer)** в доверенные корневые центры сертификации локального компьютера.

1. **В случае, если возникает ошибка при открытии сессии, рекомендуется:**

1) в редакторе Реестра Windows в ветке HKEY\_LOCAL\_MACHINE\ SOFTWARE\ Aladdin\ Enetrprise Application Platform Client\ Default\ TransportManager:

а) создать строковый параметр (типа REG\_SZ )

 - с именем ForceNonDomainAuthentication

 - значение установить true

б) изменить значения

 - ServerAdrress - на <http://rz-uc-jms-app02.nso.loc:9009/EAPEngine/Default/ClientManager>

 - StsAddress - на <http://rz-uc-jms-app02.nso.loc:9011/EAPEngine/Default/STS>

в) проследить, что там же есть параметры:

 - UseDNSSearch со значением false

 - DisableCrlValidation со значением true

2) в файле /Windows/System32/drivers/ec/hosts в самом конце добавить строку

10.101.53.22 rz-uc-jms-app02.nso.loc

3) перезагрузить компьютер

**II Запуск JMS Client и синхронизация ключевого носителя**

1. **Запуск JMS Client**

Меню быстрого запуска JMS Client доступно с помощью значка  (Клиент JMS) в области уведомлений и выглядит следующим образом (см. изображение ниже)



При успешной настройке и подключении к серверу JMS VipNet, окно JMS Client выглядит следующим образом:



При успешной настройке и подключении к серверу JMS КриптоПро, окно JMS Client выглядит следующим образом:



1. **Открытие сессии**

**Сессия –** сеанс подключения JMS Client к серверу JMS

- Для открытия сессии с помощью электронного ключа необходимо подключить ключевой носитель зарегистрированного Пользователя.

- Для открытия сеанса подключения к JMS, щелкните по ссылке «**Открыть сессию**»

Отобразится окно:



Войти 🡪 Ввести ПИН код от контейнера

При открытии сессии вкладка «Ключевые носители» будет иметь следующий вид:



1. **Синхронизация электронной подписи**.

**Синхронизация** – это процесс пересоздания сертификата и ключей электронной подписи на ключевом носителе зарегистрированного Пользователя УЦ, при условии, что на ключевом носителе имеется действующий сертификат Пользователя УЦ,

Чтобы синхронизировать электронный ключ, выполните следующие действия:

- Подсоедините электронный ключ, который вы хотите синхронизировать, к компьютеру.

- Щёлкните правой кнопкой на значке  (Клиент JMS) в области уведомлений и выберите Открыть.

- Откройте сессию на вкладке Статус

- В отобразившемся окне перейдите на вкладку Ключевые носители.

- В секции Действия под значком вашего электронного ключа щёлкните на ссылке Синхронизировать и дождитесь окончания процедуры синхронизации.

Подробно о работе JMS Client можно ознакомиться в руководстве пользователя.