Инструкция по настройке рабочего места при подключении к WEB сервисам НРД с использованием TLS соединения

Москва, 2022

Под термином «подключение к WEB сервисам НРД» имеется в виду подключение клиентов НРД для целей электронного взаимодействия (промышленный контур) или для целей тестирования (тестовый контур) с использованием локального рабочего места Системы электронного документооборота НРД (далее - ЛРМ СЭД НРД) ПО «Луч» в режиме «WEB канала» или ЛРМ СЭД НРД (WEB-кабинет депозитарно-клиринговых услуг, ДКУ), ЛРМ СЭД НРД (WEB-кабинет системы управления обеспечением, СУО), ЛРМ СЭД НРД (WEB-кабинет системы управления обеспечением, СУО), ЛРМ СЭД НРД (WEB-кабинет корпоративных действий, КД), ЛРМ СЭД НРД (WEB-кабинет ЦСУ ИП ПИФ, Платформа ПИФ), ЛРМ СЭД НРД (WEB-кабинет Единый кабинет администратора участника, ЕКА), к WEB-сервису НРД т.е. программному средству, развернутому на стороне НРД, имеющему адрес (URL) в сети Интернет через TLS соединение.

1. Для подключения к WEB-сервисам НРД через TLS соединение необходимо получить, установить и настроить средства криптографической защиты (далее - СКЗИ). Подробно процесс получения СКЗИ описан на сайте ПАО Московская Биржа в разделе «<u>Первичное подключение</u> к СЭД». Порядок настройки СКЗИ описан на сайте <u>Московской Биржи</u> в разделах <u>ГОСТ-криптография</u> и <u>RSA-криптография</u>.

Для работы с WEB-сервисом в тестовом и промышленном контурах НРД требуются следующие версии СКЗИ и их компоненты:

1.1 <u>При использовании сертифицированных СКЗИ, неквалифицированных сертификатов</u> ключей проверки электронной подписи (далее – СКПЭП ГОСТ или сертификаты ГОСТ):

• криптопровайдер "Валидата CSP" и программный комплекс «АПК Валидата Клиент Справочник сертификатов» для 32bit или 64bit в зависимости от операционной системы (далее – OC), установленной на компьютере (для 64bit OC устанавливаются ПК Справочник сертификатов 32bit и 64bit) версии не ниже расположенной на странице http://www.moex.com/s1292

СКЗИ "Валидата СЅР" версия 6 и АПК "Валидата Клиент" функционируют на ЭВМ с x86 и x64 архитектурами, а также на виртуальных машинах, находящихся под управлением гипервизоров Microsoft Hyper-V и VMware ESXi версий 6.0/6.5/6.7 из состава VMware vSphere, в следующих OC Windows:

- Windows 7 (х86 и х64) с пакетом обновлений 1 (SP1) и выше;
- Windows Server 2008 R2 (х64) с пакетом обновлений 1 (SP1) и выше;
- Windows 8.1 (x86 и x64);
- Windows Server 2012 R2 (x64);
- Windows 10 (x86 и x64);
- Windows Server 2016 (x64);
- Windows Server 2019 (x64).

Версии криптобиблиотеки Валидата-СЅР и «АПК Валидата Клиент Справочник сертификатов» можно посмотреть в меню «Панель управления – программы и компоненты» для ОС Microsoft Windows 7 и выше

| 🕏 СКЗИ Валидата СЅР | ООО Валидата | 18.10.2021 | 22,5 MB | 6.0.0451.0 |
|---|--------------|------------|---------|------------|
| 😻 АПК Валидата Клиент. Версия 4.0: Справочник сер | ООО Валидата | 18.10.2021 | 30,9 ME | 6.0.0453.0 |
| 😻 АПК Валидата Клиент. Версия 4.0: Справочник сер | ООО Валидата | 18.10.2021 | 20,6 MB | 6.0.0453.0 |

или «Пуск - Все программы - папка Валидата СЅР - Программа конфигурации СКЗИ - окно Программа конфигурации Валидата СЅР - верхний левый угол экрана (значок «Щит») – О программе..».

| 😻 Про | грамма конф | игураци | и СКЗИ | Валидата CSP | | | | _ | | × |
|-------------------------|---|---|---------------------------------|---|---------------------------|---------------|-------|-----|---------------------|------|
| ДСЧ | Считыватели | ключа | Ключи | Сертификаты | Сервис | | | | | |
| Для Бик Вла До | я всех пользов ологический да аделец: ООО В полнительные | ателей (атчик слу алидата свойств | по умолч ичайных а: Требу | анию) чисел. Версия 6 ет GUI. | .0.451. | | | | е Выбрать | |
| _ Ра | азрешить поль: я текущего пол | зователя ьзовате | ям измен | нять ДСЧ | | Инициали | зация | C | брос ДСЧ Выбрать | |
| | | | | | | ОК | Отм | ена | Приме | нить |
| | | О прог | рамме | | | | × | | | |
| | | Ø | Прог Верс | грамма конфигу сия 6.0.451.0 might © Validata | рации СКЗИ В 2008-2020 | Валидата CSP. | | | | |
| | | | 00099 | ngn - Yanadia. | 2000 2020 | ОК | | | | |

Вместе с криптобиблиотекой Валидата-CSP при начальной установке СКЗИ должна быть установлена программа монитора TLS. Устанавливается автоматически при установке по умолчанию.

В тестовом контуре необходимо использовать высылаемый по вашей заявке тестовый криптографический ключ и СКПЭП криптосервера НРД. Тестовый криптоключ получается клиентом только в НРД. Ключ криптосервера НРД (тестовая криптосессия) находится в высылаемом вам файле в папке SPR.

В тестовом контуре необходимо использовать высылаемый по вашей заявке тестовый криптографический ключ и СКПЭП криптосервера НРД. Тестовый криптоключ получается

клиентом только в НРД. Ключ криптосервера НРД (тестовая криптосессия) входит в комплект сертификатов, высылаемых с ключом. Собственный криптографический ключ генерируется клиентом самостоятельно в личном кабинете участника на сайте ПАО Московская Биржа. 1.2 При использовании несертифицированных СКЗИ, неквалифицированных сертификатов

(RSA) программный комплекс (ПК) «Справочник сертификатов» (RCS) v6.0.366.0; Программное обеспечение ПК "Справочник сертификатов" работает на ЭВМ, совместимых с IBM типа PC AT (процессор типа Pentium и выше) под управлением 32-х и 64-х разрядных версий операционных систем на платформе x86 или x64:

- Windows Vista SP1 или выше (начиная с версии Home Premium);
- Windows Server 2008 SP1 или выше;
- Windows 7 (начиная с версии Home Premium);
- Windows Server 2008 R2;
- Windows 8 / 8.1 (за исключением Windows RT);
- Windows Server 2012 / 2012 R2;
- Windows 10.

2. После установки СКЗИ необходимо обеспечить перенос криптографических ключей в системное хранилище WINDOWS для организации защищённого TLS соединения с WEB сервером НРД. Для корректного добавления криптоключа в системное хранилище необходимо, используя меню программы «АПК Валидата Клиент - Справочник сертификатов» или «ПКЗИ СЭД МБ», в зависимости от типа используемого ключа, выбрать меню «сервис-экспортировать сертификаты в системное хранилище» и согласиться со всеми задаваемыми программой вопросами.

| | | | | _ | | |
|--|---------------|--|------|----|---------|------------|
| 🗁 Справочник сертификатов | | | | _ | | × |
| Файл Справочник сертификатов Настройки | Ce | рвис Профили Вид ? | | | | |
| | 8 | Журнал работы | | | | |
| | - | Резервное копирование справочников | [| | | |
| 🖃 🚡 Справочник сертификатов | • | Восстановление справочников | | | Владеле | ц: Фамил |
| Персональный справочник сертификат | | Сформировать справочники из каталога | - | ит | Шляппо | Андрей А |
| Покальный справочник сертификатов | | Копирование справочников | | | | |
| Сетевые справочники сертификатов Jdap://simple/vcert.pki.moex.com;50001/ | | Экспортировать сертификаты в системное хранилище | | | | |
| ldap://simple/vcert.pki.moex.com:50005/ | | Экспортировать справочники в платформонезависимый формат | | | | |
| ldap://simple/vcert.pki.moex.com:50003/ | | Объекты с истекающим сроком действия | | | | |
| 🔚 🔤 ldap://simple/vcert.pki.moex.com:50007/ | (| Проверка ЭП | | | | |
| | | Установка ЭП | | | | |
| | <u></u> 28 | Tower (t | rl+F | | | |
| 1 | шu | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| < | > | | | | | > |
| Экспортировать сертификаты в системное хранили | ще И | /indows [0 из 1 | 1 | | 21 Map | r 2022 🛛 🦯 |

Необходимо убедится, что Ваши сертификаты перенесены в системное хранилище сертификатов WINDOWS. Правой кнопкой нажать «Пуск» - «Выполнить», набрать mmc

| 💷 Выполни | ГЬ | × |
|-----------|--|--------|
| | Введите имя программы, папки, документа или ресур Интернета, которые требуется открыть. | ca |
| Открыть: | mmc | \sim |
| | ОК Отмена Обзор | |

Выбрать из меню «Добавить или удалить оснастку...»

| | Консо | оль1 - [Корен | ь конс | оли] | | | |
|---|-------|---------------|--------|-------------|------|---------|--|
| - | Файл | Действие | Вид | Избранное | Окно | Справка | |
| | С | оздать | | | | Ctrl+N | |
| C | 0 | ткрыть | | | | Ctrl+O | |
| | C | охранить | | | | CTRL+S | |
| | C | охранить как | | | | | |
| | Д | обавить или | удали | гь оснастку | | CTRL+M | |
| | П | араметры | | | | | |
| | | | | | | | |

Выбрать сертификаты, нажать «Добавить» и «ОК».

| снастка | Поставщик | ^ | | Корень консоли | | Изменить расширени: |
|-------------------|-------------|---|------------|------------------------------------|--------------|---------------------|
| Монитор IP-безо | Microsoft C | | | Ц <mark>а</mark> Р Сертификаты - 1 | гекущий поль | Удалить |
| Общие папки | Microsoft C | | | | | |
| Папка | Microsoft C | | | | | |
| Планировщик за | (с) Корпора | | | | | Вверх |
| Просмотр событий | (с) Корпора | | | | | Вниз |
| Редактирование | Microsoft C | | Добавить > | | | DIND |
| ∫ Редактор GPO ин | Корпораци | | | | | |
| 🛿 Редактор объек | Microsoft C | | | | | |
| 🛿 Редактор управл | Корпораци | | | | | |
| 🛿 Результирующа | Microsoft C | | | | | |
| Сертификаты | Корпораци | | | | | |
| Осистемный мони | Корпораци | | | | | |
| Службы | Microsoft C | 5 | | < | | Дополнительно |
| N | | * | | | - | 4 |

Находим личный сертификат.



Кликаем по нему дважды, убеждаемся что сертификат не имеет предупреждающих отметок в поле «Сведения о сертификате» и есть закрытый ключ.

| 💼 Сер | тификат | | × |
|-------|---------------------------------|--|---|
| Общие | Состав | Путь сертификации | |
| | Свед | ения о сертификате | |
| Эт | от сертис | фикат предназначается для: | |
| | • Обеспе | ечивает получение идентификации от удаленного | |
| | • Подтве вашего н • Класс | еридает удаленному компьютеру идентификацию компьютера гредства ЭП КС1 | |
| Ко | му выда | н: Петухов Дмитрий Анатольевич | |
| Ke | м выдан | : Корневой УЦ | |
| | Действ | ителен с 07. 12. 2021 по 07. 12. 2031 | |
| 9 | Есть зак | рытый ключ для этого сертификата. | |

Если на значке сертификата есть крест в круге, то это означает что сертификат ключа добавлен некорректно. Тогда нужно удалить сертификат из системного хранилища и экспортировать его туда заново.

| бщие | Состав | Путь сертификации | |
|------|--------|--|--|
| | | Internet and the second s | |

3. Для обеспечения корректной работы ЛРМ СЭД НРД «WEB-кабинет Депозитария/Клиринговой организации», ПО «Луч» в режиме «WEB канала» необходимо выполнить настройки интернет-обозревателя (далее – IE):

• Сбросьте настройки IE в вариант «по умолчанию», убедитесь, что настройки SSL и TLS установлены как в окне:



- Очистите куки и кэш память IE;
- Проверьте отсутствие галочки «прокси-сервер» (в меню: «Свойства обозревателя-Подключения-Настройки сети»);

| Í | Настройка параметров локальной сети |
|---|--|
| | Автоматическая настройка Чтобы использовать установленные вручную параметры, отключите автоматическую настройку. |
| | Автоматическое определение параметров |
| | Использовать сценарий автоматической настройки |
| | Адрес |
| | Прокси-сервер |
| | Истодьзовать прокси-сервер для локальных подключений (не применяется для коммутируемых или VPN-подключений). |
| | Адрес: Порі: 80 Дополнительно |
| | Не использовать прокси-сервер для локальных адресов |
| | ОК Отмена |

• В форме «Надежные узлы» необходимо снять галку «Для всех узлов этой зоны требуется проверка серверов (https:)», если она включена;

| В эту зону можно добавлять веб-узл Заданные для зоны параметры безо использоваться для всех ее узлов. | ы и удалять их из нее. пасности будут |
|---|--|
| Доб <u>а</u> вить в зону следующий узел: | |
| http://localhost | <u>Доб</u> авить |
| 3еб-узлы: | |
| *.micex.com | 🔺 Удалить |
| *.micex.ru * microsoft.com | |
| file://garant.office.micex.com | |
| http://*.bilet.ru | + |
| | |
| Для всех узлов этой зоны требуется про | верка серверов (https:) |
| | |
| | 2 |

Если у вас MS Edge и нет возможности проверить в IE:

- Заходите в «Параметры»;
- Выбираете «Браузер по умолчанию»;
- Нажимаете «Разрешить» в меню «разрешить сайтам перезагружаться в режиме IE»;
- Добавляете необходимый URL в разрешения.

| Па | раметры | E | раузер по умолчанию | | | |
|--------------------------|--|---|---|---|----------------------------|---------|
| Q | Поиск настроек | | Назначить Microsoft Edge браузером по умолчанию | | Назначить по умол | чанию |
| 0 | Профили | | | | | |
| Ċ | Конфиденциальность, поиск и службы | 0 | Обеспечение совместимости с Internet | Explorer | | |
| 0 | Внешний вид | | | • | | |
| | Боковая панель | | Разрешение Internet Explorer открывать сайты в Micro | soft Edge 🕐 | Никог | la ∼ |
| | Пуск, главная и новые вкладки | | При просмотре в Internet Explorer вы можете автоматически отк | рывать сайты в Microsoft Edge | | |
| È | Общий доступ, копирование и вставка | | Разрешить сайтам перезагружаться в режиме Internet | : Explorer (Режим IE) 🕜 | Разреши | гь ∨ |
| □ | Файлы cookie и разрешения сайтов | | При просмотре веб-страниц в Microsoft Edge, если сайту требует перезагрузку в режиме Internet Explorer | rcя Internet Explorer для обеспечения совме | стимости, вы можете вы | толнить |
| 6 | Браузер по умолчанию | | CTD3HULL B DEWUME Internet Evolorer | | 10 | барить |
| $\underline{\downarrow}$ | Загрузки | | Эти страницы будут открываться в режиме Internet Explorer в теч | ение 30 дней с даты добавления страницы | . У вас есть 3 страницы, к | оторые |
| 썅 | Семейная безопасность | | будут автоматически открываться в режиме Internet Explorer | | | |
| Ał | Языки | | Страница | Дата добавления | Окончание срока | |
| Ø | Принтеры | | https://edog.nsd.ru/ | 29.05.2023 | 28.06.2023 | ť |
| | Система и производительность | | https://edog.nsd.ru/onyxpr | 29.05.2023 | 28.06.2023 | Tî |
| 0 | Сбросить настройки | | b https://adag.acd.su/anara/ | 20.05.2022 | 28.06.2022 | - 1 |
| _ | Телефон и другие устройства | | Intps://edog.nsd.ru/onyxpr/ | 23.05.2025 | 20.00.2025 | Ľ |
| Ŷ | Специальные возможности | | Параметры браузера | | | C |
| a | О программе Microsoft Edge | | | | | |

В адресную строку браузера нужно вставить URL https://edog.nsd.ru/onyxpr - для ключей ГОСТ или https://edor.nsd.ru/onyxpr - для RSA ключей. Для тестового контура https://gost.nsd.ru и https://rsa.nsd.ru соответственно. Если все настройки выполнены правильно, то вы увидите страницу:

| B Mps/1001144/0001 | | and the second se | and the second states | State of the local division of the local div |
|--|--|---|--|--|
| | | | L + B + X A Anno | R.1 |
| K Sept + 3 - Treses - Surrey State - Ditoria 4 - 2 | 0-0-0-0-0-0-0-0 | | | Pages Station + d |
| K BECCHE + #* Torste freme-Binder, E* & B. C.R. | tres Blaconstance #Hype #Horn Millions POwers | | (1 Mynester 8, 10.21 4, 45.17 - 444 | 10.000 +2°C #3 41 |
| 🙀 Halpanos 👔 🚽 Rowa pickas 🚻 Copensar - Taenes rop | n. 🔂 Capanetari - Transer capa // 2020 Web 🗰 Distances | Angolati 😫 Rading 🏠 settera- | | |
| Bit management and | | | A · D · 2 · cossa · learnesses · | Const + @+ |
| Акпозитична | | | | |
| | Web-ceps | инс НРД силх | | |
| | | - B-41- | | |
| | Adress: | | | |
| | Adress: Web Service Type: | JAX-WS 2.1 | | |
| | Adress: Web Service Type: Version; | JAX-W5 2.1 1.1.2.13 | | |
| | Adress: Web Service Type: Version; WBDL page VED seture: | JAX-W5 2.1 1.1.2.13 | | |
| | Adress: Web Service Type: Version: WSDL page XSD schema | JAK-WS 2.1 1.1.2.13 | | |
| | Adress: Web Service Type: Version: WSDLpage XSD schema | JAX-WIS 2.1 1.1.2.13 Inter Inter | E (M-Genteress, Vjahes, | |
| | Adress: Web Bervice Type: Version: W8DL.page X8D schema | 44X-WIS 2.1 1.1.2.13 117 117 117 117 | E 104 - Gartanessa Vannes, m. 20 E 104 - Gartanessa Vannes, m. 20 172 - 12 - 12 - 12 - 12 - 12 - 12 - 12 - | |

Если вместо отбражения таблицы вы получите сообщение о невозможности отображения страницы, нужно проверить доступность узла командами:

telnet edog.nsd.ru 443 и nslookup edog.nsd.ru, при отсутствии доступа попытаться настроить прокси и файервол для доступа к указанным узлам. Если не удается настроить доступ, нужно вывести машину из корпоративной сети или создать новую установив на неё предварительно СКЗИ и проверить доступ.

Известные проблемы:

Одной из проблем является высокий приоритет в параметрах управления учетными записями пользователей «движок» должен находиться в положении «Никогда не уведомлять», если это не так, то переведите его в это положение.



Часто возникают проблемы при установке на одной машине различных СКЗИ, причем даже удаление ранее установленных СКЗИ не позволяет восстановить работоспособность. Исправить можно только переустановкой ОС.

Если после всех манипуляций у вас все равно не работает WEB доступ необходимо включить протоколирование операций через реестр

• SYSTEM\CurrentControlSet\Control\Session Manager\Debug Print Filter

VD_LOGMASK_CSP,

VD_LOGMASK_SSP,

VD_LOGMASK_CNG,

VD_LOGMASK_HOOKS

все значения выставить в 496 десятичное;

• перезагрузка ПК (!!!);

• почистите все системные протоколы (Приложения и Система);

• попытайтесь подключиться ТОЛЬКО через IE к <u>https://gost.nsd.ru</u> - для тестового контура или <u>https://edog.nsd.ru</u> - для рабочего контура пару раз и пришлите системные протоколы (Приложения и Система).

После выполнения выше описанных процедур пришлите логи журналов Windows Приложения и Система, а также скриншоты, подтверждающие выполнение процедур настройки, на адрес <u>soed@nsd.ru</u>.

По всем возникшим вопросам необходимо обращаться к первой линии технической поддержки (адрес электронной почты <u>soed@nsd.ru</u>, телефон 8(495)956-09-34).