Подготовка к установке.

Перед началом установки убедитесь:

- 1. Вы подключены к ЭДО НРД через систему электронного документооборота. Подробнее о подключении к системе ЭДО, установке криптографического ПО и справочника сертификатов криптографического ПО можно прочесть здесь: https://www.nsd.ru/ru/workflow/system/member/
- Вы зарегистрированы в системе 'паспорт' биржи. Внимание! Для целей опытной эксплуатации необходимо регистрироваться на сайте <u>http://passport.beta.moex.com/</u>. Во время запуска сайта возникнет вопрос о доверии сертификату сервера паспорта, необходимо подтвердить доверие.
- 3. Полученный на паспорте при регистрации Логин необходимо передать в НРД, для привязки учётной записи на паспорте к вашей компании в вэб кабинете. Кроме Логина в НРД должны быть переданы следующие сведения о пользователе
 - а. Депозитарный код участника
 - b. СНИЛС
 - с. Мобильный номер
 - d. E-mail
- 4. На Вашем компьютере установлена версия Windows не ниже 7.0.
- 5. На Вашем компьютере установлен Net.Framework не ниже 4.5 (Подробнее можно прочитать здесь <u>http://www.microsoft.com/ru-RU/download/details.aspx?id=40779</u>)
- 6. У Вас на руках есть комплект специализированного броузера доступа в вэб кабинет (архив NSD.Web Room.exe).
- 7. Распаковать приложенный файл 'NSD.Web Room_reg_emitent.rar' в отдельную папку.
- 8. Распакованный архив содержит директорию 'NSD.Web Room\Redist', в которой находится файл NRD.DesktopShell.exe.
- 9. В распакованном архиве находится конфигурационный файл 'NRD.DesktopShell.exe.config'
- В случае, если Вы используете криптографию на основе RSA (неквалифицированную ЭП), необходимо исправить конфигурационный файл 'NRD.DesktopShell.exe.config', поменяв в строку '<add key="PkiType" value="GOST" />' на '<add key="PkiType" value="RSA" />'

Начало работы

- 1. Распакованный архив содержит директорию 'NSD.Web Room\Redist', в которой находится файл NRD.DesktopShell.exe. Запустите его.
- 2. Во время запуска сайта возникнет вопрос о доверии сертификату сервера паспорта, необходимо подтвердить доверие. Данный вопрос будет возникать при каждом запуске специализированного броузера. Вы можете настроить свой броузер на доверие серверу вэб кабинета, включив корневой сертификат биржи в число доверенных сертификатов. Наиболее простой способ сделать это описан в в последнем разделе инструкции.
- 3. Возникнет окно с логином и паролем. В этом окне необходимо ввести логин и пароль, полуцченный Вами в системе 'паспорт' биржи (см пункт Подготовка к установке).



Наиболее простой способ установки доверия вэб кабинету :

1. Открыть браузер chrome* и перейти по ссылке <u>https://edor.nsd.ru/WebRoom/</u> Отобразится следующее сообщение:

🕒 Ошибка нарушения кон (🗴 🦲	An analysis of an address of the observer of	transfer Hard
← → C		
	Ваше подключение не защищено Злоумышленники могут пытаться похитить ваши данные с с (например, пароли, сообщения или номера банковских кар NET::ERR_CERT_AUTHORITY_INVALID	айта edor.nsd.ru т).
	Дополнительно	Назад к безопасности
*Скачать последнюю версию Chrome можно с http:	s://www.google.com/chrome/brows	er/desktop/

2. Навести указатель мыши на «замок» и нажать правую кнопку мыши. Далее нажать на ссылку «Данные сертификата»

С Ошибка нарушения конс х			
← → C 隆 https://edor.nsd.ru/WebRoom/			
еdor.nsd.ru X Идентификационные данные не подтверждены Разрешения Соединение			
Идентификационные данные этого сайта не проверены. • Сертификат сервера не является доверенным. <u>Данные сертификата</u>			
Соединение с едоглясили зашифровано с помощью устаревших технологий.	Ваше подключение не защищено		
Информация о сайте Этот сайт не посещался до сегодняшнего дня.	Злоумышленники могут пытаться похитить ваши данные с сайта edor.nsd.ru (например, пароли, сообщения или номера банковских карт). Net::err_cert_authority_invalid		
Что это значит?	<u>Дополнительно</u> Назад к безопасности		

В открывшемся окне «Сертификат» перейти на вкладку «Путь сертификации».
 После необходимо выбрать «Центр сертификации» и нажать кнопку «Просмотр Сертификата»

Сертификат
Общие Состав Путь сертификации
Пут <u>ь</u> сертификации
ы Центр Сертификации
Просмотр сертификата
<u>С</u> остояние сертификата:
Нет доверия к этому корневому сертификату центра сертификации, поскольку он не найден в хранилище доверенных корневых сертификатов центров сертификации.
Подробнее о путях сертификации
ОК

4. В открывшемся дочернем окне «Сертификат» перейти на вкладку «Состав» и нажать кнопку «Копировать в файл...»

Сертификат	X
Общие Состав Путь сертифика	ции
Показать: <все>	-
Поле	Значение
Версия Серийный номер Алгоритм подписи Алгоритм хэширования по Издатель Действителен с Действителен по	V3 40 40 10 a8 d9 eb 39 2c 09 5d sha1RSA sha1 007702077840, 10277393874 20 ноября 2012 г. 11:04:00 21 ноября 2028 г. 2:59:00 0077702077840, 10277393874
, Св Подробнее о <u>составе сертификат</u> .	юйства Копировать в файл
	ОК

5. В открывшемся окне «Мастер экспорта сертификатов» нажать кнопку «Далее»

Мастер экспорта сертификато	ов
	Мастер экспорта сертификатов
	Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов из хранилища сертификатов на локальный диск. Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов - это область системы, предназначенная для хранения сертификатов. Для продолжения нажмите кнопку "Далее".
	< Назад Далее > Отмена

6. Выбрать формат файла сертификата «Файлы X.509 (.CER) в кодировке DER» и нажать кнопку «Далее»

Форм С	ат экспортируемого файла ертификаты могут быть экспортированы в различных форматах.	
B	ыберите формат файла сертификата:	
	Файлы Х. 509 (.CER) в кодировке DER	
	🔘 Файлы X.509 (.CER) в кодировке Base-64	
	🔘 <u>С</u> тандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)	
	Включить по возможности все сертификаты в путь сертификации	
	💿 файл обмена личной информацией - PKCS #12 (.PFX)	
	Включить по возможности все сертификаты в путь сертификации	
	<u>У</u> далить закрытый ключ после успешного экспорта	
Экспортировать все расширенные свойства		
	Хранилище сериализованных сертификатов (.SST)	
Подро	бнее о формате файлов сертификатов	
	< <u>Н</u> азад Далее > N Отмена	

 Нажать кнопку «Обзор» и указать любую папку для экспорта файла. После нажать «Сохранить» -> «Далее» -> «Готово».

Мастер экспорта сертификатов						
Имя экспортируемого файла Укажите имя экспортируемого файла						
Имя файла: Обзор.						
О Сохранить как						x
😋 🔍 🗣 🕨 ► Компьютер 🕨 Локальный диск (С:) 🕨 Test 🕨			• 4 ₇	Поиск: Test		٩
Упорядочить 🔻 Новая папка						0
№ Избранное	Дата изменения	Тип	Размер			
У Избранное Загрузки Недавние места Рабочий стол Библиотеки Видео Документы Узображения Музыка Компьютер Силонанный диск Generational Content of Content	21.04.2015 16:56	Папка с файлами				
🖙 depo (\\Argon.n: 🎽						
<u>И</u> мя файла: Сертификат_НРД <u>Т</u> ип файла: Двоичные файлы X.509 (*.cer) в кодировке DER						- -
🔿 Скрыть папки				Со <u>х</u> ранить	Отмена	1

В результате должно появиться финальное окно:



Необходимо нажать «ОК»

8. Открыть командную строку и выполнить команду: certmgr.msc

Программы (1)		
a certmgr		
0.0		
🎾 Ознакомиться с другими результатами		
certmgr.msc	×	Завершение работы 🕨

 В открывшемся окне переходим в «Доверенные корневые центры сертификации» -> «Сертификаты» (нажать правую кнопку мыши) -> «Все задачи» -> «Импорт»

🚡 certmgr - [Сертификаты - текущий пользователь\Доверенные корневые центры сертиф 💷 💷 🗾 🗮				
Файл Действие Вид Справка				
🗢 🔿 🖄 🖬 📋 🙆	🔒 🔽 🖬			
🙀 Сертификаты - текущий г	юльзователь	Кому выдан	Кем выдан 🔺	
 Доверенные корневые Список отзыва сер 	е центры сертификации тификатов	AddTrust External CA Root	AddTrust Ex Baltimore C	
Сертификаты р 🛗 Доверительные (Все задачи	→ Импорт t C	Class 2 Prim E Class 3 Publ	
 Промежуточные Объект пользова 	Вид	giCert Global Root CA	DigiCert Glo	
 Доверенные изда Сертификаты, к п Сторонние корн 	Обновить Экспортировать список	itrust Root Certification Auth trust.net Certification Author	Entrust Root Entrust.net (
 Доверенные лиц Другие пользователи 	Справка	uifax Secure Certificate Auth 	Equifax Secu GeoTrust Glo	
Доверенные корневые	е сертификаты смарт-карты	GlobalSign Root CA	GlobalSign F Go Daddy C	
		Go Daddy Root Certificate Auth	Go Daddy Ri	
			b Cyberli	
Добавить сертификат в хранил	лище			

10. В открывшемся окне «Мастер импорта сертификатов» нажать кнопку «Далее»

Мастер импорта сертификатов		x
	Мастер импорта сертификатов	
	Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов. Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов - это область системы, предназначенная для хранения сертификатов. Для продолжения нажмите кнопку "Далее".	
	< Назад Далее > От	ена

11. Нажать кнопку «Обзор» и открыть сохраненный ранее файл с типом Сертификат.



12. Нажать кнопку «Далее»

Mac	стер импорта сертификатов
	Импортируемый файл
	Укажите импортируемый файл.
-	
	Имя фа <u>й</u> ла:
	C:\Test\Cepтификат_HPД.cer
	Замечание: следующие форматы файлов могут содержать более одного сертификата в одном файле:
	Файл обмена личной информацией - PKCS #12 (.PFX,.P12)
	Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)
	Хранилище сериализованных сертификатов (.SST)
	Подробнее о формате файлов сертификатов
_	
	< <u>Н</u> азад Далее > Отмена

13. Выбрать «Поместить все сертификаты в следующее хранилище» -> Хранилище сертификатов: «Доверенные корневые центры сертификации» и нажать кнопку «Далее»

Мастер импорта сертификатов
Хранилище сертификатов
Хранилища сертификатов - это системные области, в которых хранятся сертификаты.
Выбор хранилища может быть произведен Windows автоматически, или же можно указать размещение сертификата вручную.
🔘 Автоматически выбрать хранилище на основе типа сертификата
Поместить все сертификаты в следующее хранилище
Хранилище сертификатов:
Доверенные корневые центры сертификации Обзор
Подробнее о <u>хранилищах сертификатов</u>
< Назад Далее > Отмена

14. Нажать кнопку «Готово»

macrep minopra ceprintpinaroi	a strand that have further. The there
	Завершение мастера импорта сертификатов
	Сертификат будет импортирован после нажатия кнопки "Готово". Были указаны следующие параметры:
	Хранилище сертификатов, выбранное пользователем Содержание Имя файла
	۲
	< Назад Готово Отмена

В результате появится финальное окно с подтверждением на добавление нового сертификата. Необходимо нажать кнопку «Да»

15. Подключить eToken

16. Запустить браузер \NSD.Web Room\Redist\ NRD.DesktopShell

Далее действовать в соответствии с Руководством пользователя.