«Личный кабинет Участника / Личный кабинет Эмитента»

Раздел "Услуги УЦ"

Инструкция пользователя

Введение

Настоящий документ описывает порядок действий Участника СЭД при взаимодействии с удостоверяющим центром, функции которого выполняет ПАО Московская Биржа в рамках Системы электронного документооборота (далее - УЦ СЭД).

Взаимодействие Участника СЭД с УЦ СЭД осуществляется через раздел "Услуги УЦ" Личного кабинета Участника (далее - ЛКУ) или Личного кабинета Эмитента (далее - ЛКЭ).

Участник СЭД имеет возможность управлять всеми основными этапами жизненного цикла сертификатов ключей проверки электронных подписей (далее - СКПЭП), используемыми в СЭД:

- первичное создание СКПЭП;
- плановая/внеплановая замена СКПЭП;
- создание нового СКПЭП в связи с внесением изменений в действующий СКПЭП.

Функционал раздела "Услуги УЦ" обеспечивает Участнику СЭД возможность получения информации о ключах установки для СКЗИ "Валидата CSP", о созданных для Участника СЭД СКПЭП, а также возможность оплаты услуг УЦ СЭД и обновления СКПЭП контрагентов и УЦ СЭД на рабочем месте Участника СЭД.

Получение доступа к разделу "Услуги УЦ" в ЛКУ / ЛКЭ

Порядок получения доступа к ЛКУ описан в документе "Руководство Пользователя "Личный кабинет Участника" (http://moex.com/a1676).

Порядок получения доступа к ЛКЭ описан в документе "Инструкция о порядке использования информационного обеспечения "Личный кабинет Эмитента" (http://www.moex.com/s20).

Требования к рабочему месту Участника СЭД

Для взаимодействия с УЦ СЭД через ЛКУ / ЛКЭ Участнику СЭД необходимы:

- ПК, совместимый с IBM типа PC AT (процессор типа Pentium и выше) под управлением 32-х и 64-х разрядных версий операционных систем
  - Microsoft Windows (не ниже версии 7) на платформе x86 или x64;
  - Linux на платформе x64 (список поддерживаемых версий указан на странице https://www.moex.com/s1292);
- Браузер: Yandex Browser, Atom Browser, Microsoft Edge, Mozilla Firefox или Google Chrome (для Google Chrome требуется наличие доступа к магазину Chrome);
- Браузерный плагин MoexBrowserPlugin (инструкция по установке плагина находится по адресу: http://moex.com/a1676).

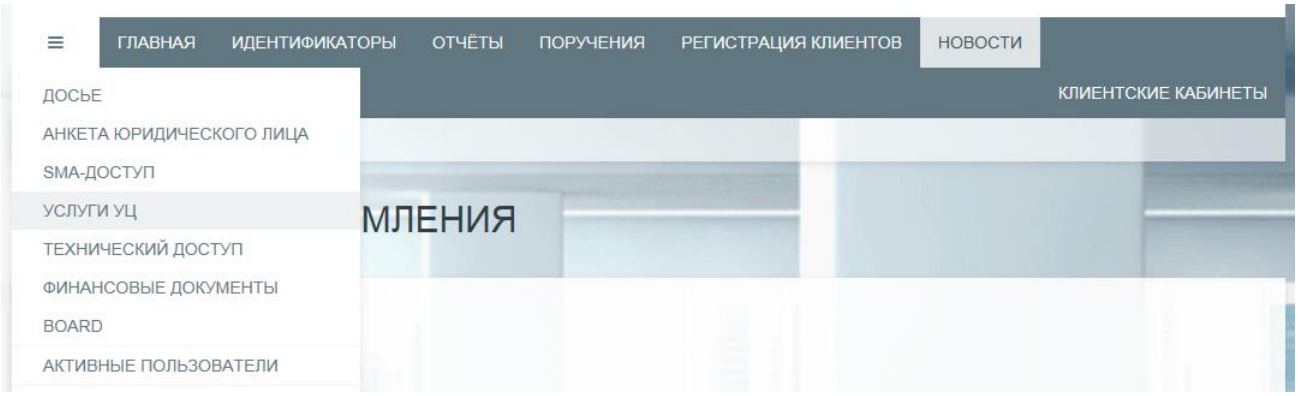
Если Участник СЭД планирует осуществлять управление криптографическими ключами на том же ПК, с которого осуществляет доступ в ЛКУ / ЛКЭ, на этом ПК должны быть дополнительно установлены:

- для работы со СКПЭП с использованием сертифицированных СКЗИ (ГОСТ-криптография) – программный комплекс АПК «Валидата Клиент» и СКЗИ "Валидата CSP" (http://moex.com/s1292);
- для работы со СКПЭП с использованием несертифицированных СКЗИ (RSA-криптография) - программный комплекс "ПКЗИ СЭД МБ" (https://www.moex.com/s1293).

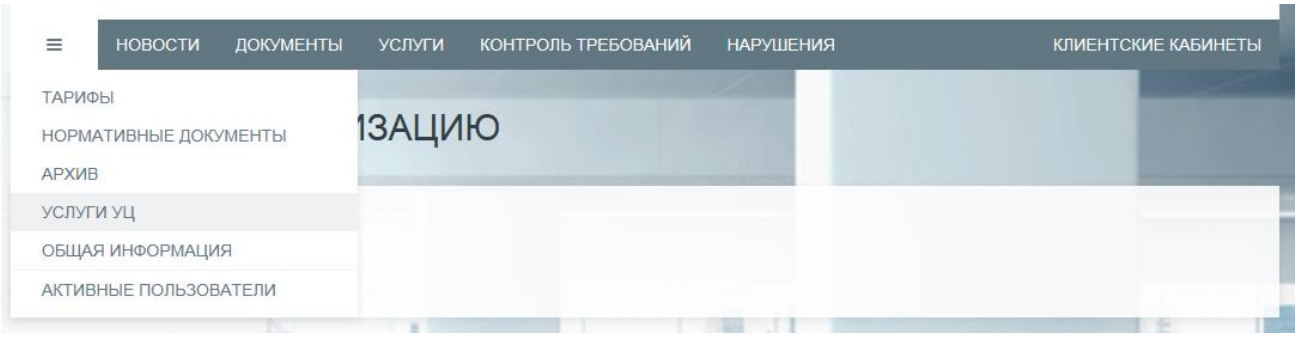
В противном случае управление криптографическими ключами должно осуществляться на отдельном ПК администратором безопасности Участника СЭД. На таком ПК должны быть установлены программные средства, указанные выше.

Начало работы с разделом "Услуги УЦ"

Вход в раздел "Услуги УЦ" в ЛКУ: Личный Кабинет Участника →  «Три полоски» → «Услуги УЦ»



Вход в раздел "Услуги УЦ" в ЛКЭ: Личный Кабинет Эмитента →  «Три полоски» → «Услуги УЦ»



Если часть кнопок в разделе «Услуги УЦ» неактивна, это означает, что плагин MoexBrowserPlugin на данном ПК не настроен.

Пункт меню "Акт на ПО"

Акт о предоставлении права использования программного обеспечения представляет собой документ, на основании которого Участнику СЭД предоставляются права использования программного обеспечения СКЗИ «Валидата CSP», АПК «Валидата Клиент» и "АПК Клиент ПКЗИ СЭД МБ".

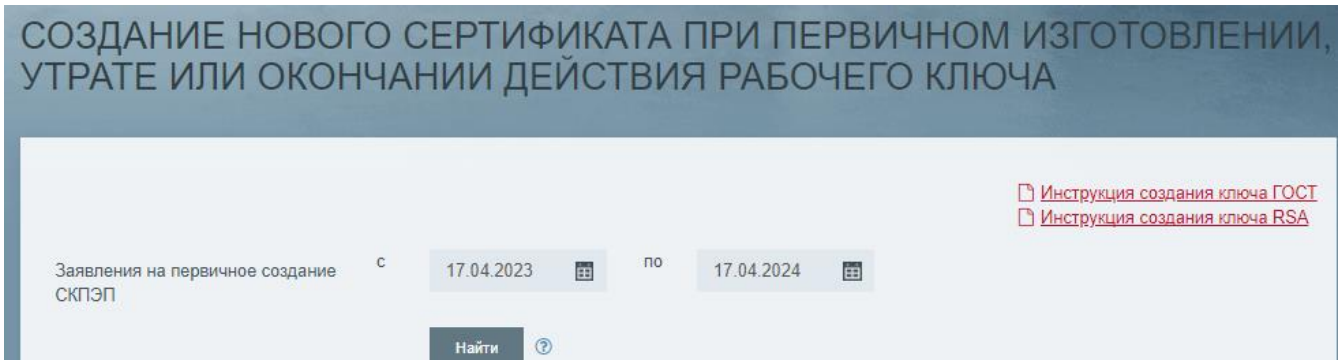
Акт содержит информацию о регистрационных номерах для предоставляемого ПО (если имеются) и ключе установки для СКЗИ "Валидата CSP".

Данный пункт меню позволяет Участнику СЭД, в первую очередь, оперативно получить информацию о ключе установки для СКЗИ «Валидата CSP».

Пункт меню "Первичное создание сертификата"

Создание нового СКПЭП при первичном изготовлении, утрате или окончании действия рабочего ключа возможно после предоставления Участником СЭД в ПАО Московская Биржа документов, оформленных в соответствии с требованиями Правил электронного документооборота (Заявление на создание СКПЭП (далее - Заявление) и Доверенность на владельца СКПЭП (http://moex.com/s1288).

Раздел содержит ссылки на инструкции по созданию ключей.



Для каждого Заявления отображается отдельная информационная строка, содержащая ФИО заявителя тип ключа и текущий статус обработки Заявления.

ВЛАДЕЛЕЦ СЕРТИФИКАТА	ДАТА ПОСТУПЛЕНИЯ ЗАЯВЛЕНИЯ В УЦ	ТИП КЛЮЧА	СТАТУС ОБРАБОТКИ ЗАЯВЛЕНИЯ	
Кузнецов Иван Иванович	16.05.2017	ГОСТ	Заявление получено. Ожидается запрос на создание СКПЭП.	
ТестОрг	19.04.2017	RSA	Сертификат выпущен.	
ТестОрг	19.04.2017	ГОСТ	Сертификат выпущен.	

В зависимости от типа ключа необходимо выполнить последовательность действий, указанных в следующих инструкциях:

ГОСТ: Инструкция создания ключа ГОСТ раздел «Первичное создание сертификата»

RSA: Инструкция создания ключа RSA раздел «Первичное создание сертификата»

ВАЖНО:

Если вы используете программу АПК «Валидата Клиент» - это **ГОСТ**.

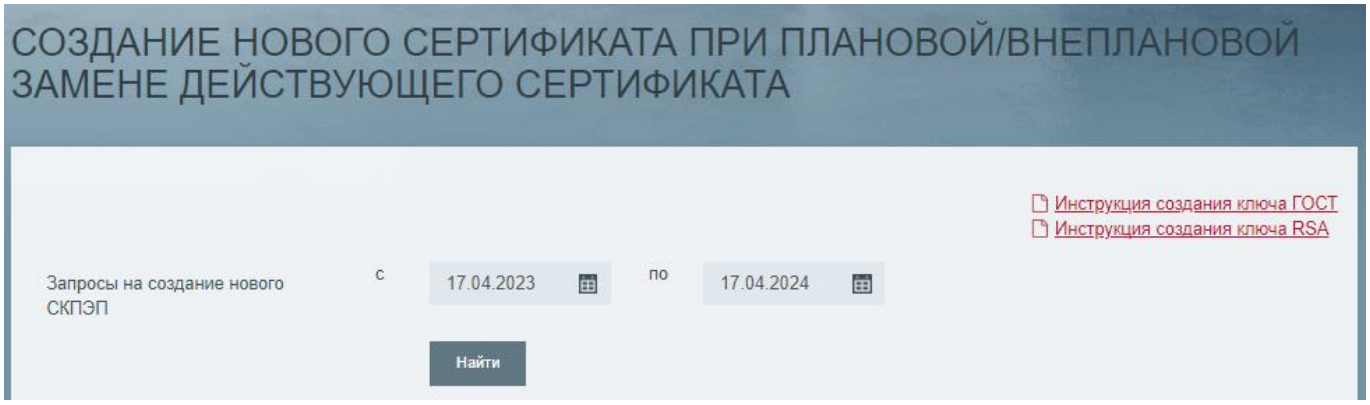
Если вы используете программу ПКЗИ СЭД МБ или MOEX EDI CryptoPS – это **RSA**.

Пункт меню "Плановая замена сертификата"

Используя данный пункт меню, Вы можете создать новый СКПЭП при плановой/внеплановой замене действующего сертификата.

На странице, соответствующей данному пункту меню, отображается список ранее сделанных запросов на создание СКПЭП (далее - Запросы).

Раздел содержит ссылки на инструкции по созданию ключей.



Для каждого Запроса отображается отдельная информационная строка, содержащая информацию о владельце создаваемого СКПЭП и статус его обработки.

В зависимости от типа используемого вами ключа вам необходимо выполнить последовательность действий, указанных в следующих инструкциях:

ГОСТ: Инструкция создания ключа ГОСТ раздел «Плановая замена сертификата»

RSA: Инструкция создания ключа RSA раздел «Плановая замена сертификата»

ВАЖНО:

Если вы используете программу АПК «Валидата Клиент» - это **ГОСТ**.

Если вы используете программу ПКЗИ СЭД МБ или MOEX EDI CryptoPS – это **RSA**.

Пункт меню "Изменение данных сертификата"

Стоимость услуги за создание такого сертификата ниже, чем в случае плановой/внеплановой замены, но дата окончания срока действия ключа электронной подписи, в этом случае, устанавливается равной дате окончания срока действия предыдущего ключа.

Для создания нового СКПЭП с измененными данными Вам необходимо:

1. Скачать на странице https://www.moex.com/s1288 форму Заявления на создание СКПЭП, внести все актуальные данные, с учетом предполагаемых изменений, сохранить файл на жестком диске. При помощи программы «Справочник сертификатов» необходимо подписать сформированный файл на текущем рабочем ключе пользователя (пункт меню «Сервис» - «Установка ЭП», далее «Присоединенная подпись») выбрать сохраненный файл с заявлением, нажать «Далее», в качестве имени файла указать «*Название организации*, изменение данных сертификата», затем установить галочку в чек-боксе «Добавлять сертификат в ЭП», нажать «Далее» и «Готово».
2. Подписанный файл с расширением «.p7s» отправьте через ЛКУ(ЛКЭ) своему персональному менеджеру. Более подробно, о способе отправки документа, можно узнать у персонального менеджера.
3. В настоящее время данный пункт меню находится на реконструкции, все операции по генерации запроса и получению сертификата проводятся в меню «Первичное создание сертификата». После получения персональным менеджером заявления на создание СКПЭП, в разделе «Первичное создание сертификата» появится запись для создания ключа и запроса на выпуск для него сертификата с измененными данными.

В зависимости от типа используемого вами ключа вам необходимо выполнить последовательность действий, указанных в следующих инструкциях:

ГОСТ: Инструкция создания ключа ГОСТ раздел «Первичное создание сертификата»

RSA: Инструкция создания ключа RSA раздел «Первичное создание сертификата»

После выполнения операции «Отправка запроса в УЦ» файл запроса на создание СКПЭП необходимо скачать, подписать действующим ключом пользователя, подписанный файл с расширением «.p7s» отправить на почтовый адрес pki@moex.com.

ВАЖНО:

Если вы используете программу АПК «Валидата Клиент» - это **ГОСТ**.

Если вы используете программу ПКЗИ СЭД МБ или MOEX EDI CryptoPS – это **RSA**.

Пункт меню "Обновление сертификатов"

Используя данный пункт меню, Вы можете обновить в своём локальном справочнике сертификатов сертификаты сотрудников Группы «Московская Биржа» и других Участников СЭД.

На странице, соответствующей данному пункту меню, отображается информация о профилях Справочника сертификатов для данного ПК.

Для каждого профиля отображается его наименование и информация о рабочем сертификате. Доступные для обновления профили имеют иконку  «Обновить сертификаты профиля».

ТестОрг_Кузнецов Иван Иванович_170516_104078	INN=005751032333,OGRN=1075742000531,SNILS=11111111111,T=Начальник отдела,CN=Кузнецов Иван Иванович,OU=Бухгалтерия,O=ТестОрг,L=г.Москва,ST=77 г.Москва,C=RU	ГОСТ	16.05.2018	12.05.2020	

Если целостность профиля нарушена и/или срок действия секретного ключа электронной подписи истек, то неисправныйпрофиль будет отображаться красным цветом.

ТестОрг_Кузнецов Иван Иванович_170516_104078	Ошибка профиля: Ошибка доступа к ПСП Для получения точной диагностики, запустите сп равочник сертификатов.	ГОСТ	нет данных	нет данных	

Нажмите на иконку  , выберите вариант обновления «Обновить сертификаты контрагентов сейчас».

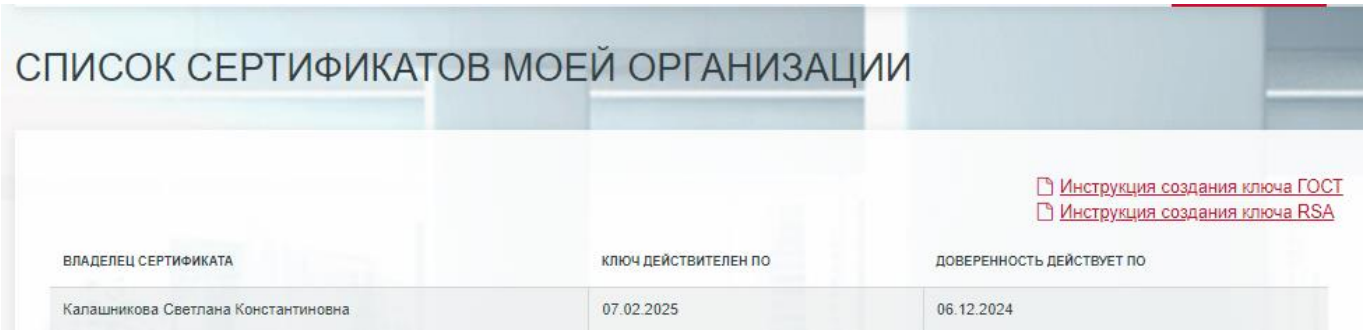
Обновление будет выполнено для выбранного профиля Вашего ПК.

Кнопка «Загрузить сертификаты контрагентов» предназначена для загрузки архива с сертификатами контрагентов для импортирования их вручную в Справочник сертификатов на своём или на другом ПК

Пункт меню "Список сертификатов"

В этом пункте меню представлена информация о сроках окончания действующих ключей владельцев сертификатов организации и их доверенностей.

Для каждого СКПЭП отображается следующая информация: владелец СКПЭП, дата окончания срока действия секретного ключа, дата окончания срока действия доверенности для владельца СКЭП.



Вниманию Администратора безопасности Участника СЭД

В организации Участника СЭД может быть реализовано централизованное управление криптографическими ключами, когда создание криптографических ключей осуществляется администратором безопасности на выделенном компьютере.

При централизованном управлении криптографическими ключами, на компьютере администратора безопасности могут не устанавливаться программные комплексы АПК «Валидата Клиент. Версия 4.0» или "ПКЗИ СЭД МБ". В таком случае, для первичной генерации секретных криптографических ключей администратор безопасности может использовать утилиту **xpki1tst.exe** для ГОСТ-криптографии или утилиту **rpki1tst.exe** для RSA-криптографии, которые находятся по ссылке «Утилита командной строки для использования в СЭД», размещенной по адресу https://www.moex.com/a7978, в ZIP-архиве в папке xml_req.

Данные утилиты позволяют создавать ключи электронной подписи и шифрования пользователя, а также запрос на первичное создание СКПЭП в виде XML-файла. Сформированный при помощи утилиты запрос должен быть загружен в ЛКУ / ЛКЭ.

Примеры запуска утилиты:

Для ГОСТ-криптографии:

32bit:

xpki1tst.exe -manage -xmlreq -minimal -2012 >Request.xml

или

64bit:

xpki1tstx64.exe -manage -xmlreq -minimal -2012 >Request.xml

В результате работы утилиты ключи электронной подписи и шифрования будут записаны на ключевой носитель, указанный в "Программе конфигурации СКЗИ" (флэшка, ruToken, eToken и т.п.), а запрос на первичное создание СКПЭП в виде XML-файла (Request.xml) - в текущий каталог.

Для RSA-криптографии:

32bit:

rpki1tst.exe -manage -xmlreq -minimal >Request.xml

или

64bit:

rpki1tstx64.exe -manage -xmlreq -minimal >Request.xml

В результате работы утилиты ключи электронной подписи и шифрования будут записаны в каталог C:\Users\.....\AppData\Roaming\Microsoft\Crypto\RSA, а запрос на первичное создание СКПЭП в виде XML-файла (Request.xml) - в текущий каталог.

В случае плановой/внеплановой замены сертификатов, администратор безопасности для генерации новых криптографических ключей должен использовать программу "Справочник сертификатов".

После создания в УЦ СЭД нового сертификата, администратор безопасности может выгрузить из ЛКУ необходимые для формирования локального справочника сертификатов файлы (рабочий сертификат пользователя, сертификаты контрагентов пользователя, корневые сертификаты и списки отозванных сертификатов УЦ СЭД) и сформировать для пользователя средствами "Справочника сертификатов" рабочий профиль на нужном ПК.