

Инструкция по настройке и
организации взаимодействия с
использованием SFTP-сервера

Оглавление

1. Термины и определения.....	3
2. Общие положения.....	4
3. Подготовка к взаимодействию	4
4. Настройка подключения через SFTP-сервер.....	6
5. Порядок работы на SFTP-сервере.....	7

1. Термины и определения

База данных – электронная база данных кредитных историй, хранящихся в Бюро структурированная в соответствии с правилами, установленным нормативно-правовыми актами Российской Федерации.

Бюро – общество с ограниченной ответственностью «Спектрум кредитное бюро» (Сокращенное наименование – ООО «СКБ») ИНН 7701720592, ОГРН 5077746740121, КПП 712501001, юридический адрес: 115533, г. Москва, Проспект Андропова, д. 22, офис 51.

Клиент – источник формирования кредитной истории и/или пользователь кредитной истории, как они описаны в Законе №218-ФЗ.

Кредитная история – информация, состав которой определен Законом №218-ФЗ.

Кредитный отчет – документ, который содержит информацию, входящую в состав кредитной истории, и который бюро кредитных историй предоставляет по запросу пользователя кредитной истории и иных лиц, имеющих право на получение указанной информации в соответствии с Законом №218-ФЗ.

Пакет – архив, состоящий из набора файлов, которые могут содержать:

- данные для формирования кредитной истории Субъекта;
- запрос кредитного отчёта по Субъекту;
- кредитный отчет по Субъекту.

SFTP-сервер – это информационный ресурс в составе Программы SKB.CHD, доступ к которому предоставляется по протоколу Secure File Transfer Protocol (протокол прикладного уровня передачи файлов, работающий поверх безопасного канала).

2. Общие положения

- 2.1. Настоящая инструкция описывает порядок осуществления доступа Клиента к ПО SKB.CHD и использования его функциональности с помощью SFTP-сервера.
- 2.2. SFTP-сервер предназначен для автоматизированного обмена информацией в виде файлов между Клиентом и Бюро с целью загрузки сведений о кредитной истории субъектов в базу данных Бюро или получения сведений о кредитных историях субъектов (кредитные отчеты).
- 2.3. Взаимодействие с сервисами Бюро осуществляется с использованием криптографического туннеля на базе «Крипто Про NGate», который обеспечивает дополнительную защиту персональных данных путем шифрования канала. Настройка защищенного канала связи описана в отдельной инструкции.
- 2.4. Соединение с SFTP-сервером происходит по протоколу SSH.
- 2.5. Для доступа к SFTP-серверу необходимо наличие служебной учетной записи.

3. Подготовка к взаимодействию

3.1. Для взаимодействия с Бюро через SFTP-сервер Клиенту необходимо:

- наличие заключенного договора с Бюро;
- наличие ПО СКЗИ КриптоПро CSP 4.0 или 5.0;
- наличие ПО для создания архивных файлов;
- наличие собственных закрытых ключей для формирования УЭП;
- направить в Бюро открытый ключ собственного сертификата.

3.2. Генерация рабочего ключа шифрования

Аутентификация Пользователя на SFTP-сервере происходит с помощью логина Учетной записи Личного кабинета и рабочего ключа шифрования. Рабочий ключ Клиент генерирует на своей стороне.

3.2.1. Генерация рабочего ключа шифрования для Mac и Linux

Для Mac или Linux выполнить команду:

```
$ ssh-keygen -t ecdsa -b 521 -C "<имя пользователя>" -f <хранилище ключей>/-N  
<password>
```

где:

<имя пользователя> - логин учетной записи пользователя, полученный от Бюро.

<хранилище ключей> - путь до папки, где будут храниться ключи (требуется право на запись)

<password> - пароль ключа шифрования.

Полученный ответ:

```
Generating public/private ecdsa key pair.  
Your identification has been saved in <хранилище ключей>  
Your public key has been saved in <хранилище ключей>/-pub  
The key fingerprint is:  
SHA256:nRgRsZ+PUwfxAFG4MENI5HfXmwo1FJnnGM3eValMUDE <имя пользователя>
```

3.2.2. Генерация рабочего ключа шифрования для Windows10

Для Windows 10 и выше выполнить команду в терминале Powershell:

```
PS C:\Users\user.DOMAIN> ssh-keygen.exe -t ecdsa -b 521 -C "<имя пользователя>" -f <хранилище ключей>/-N  
<password>
```

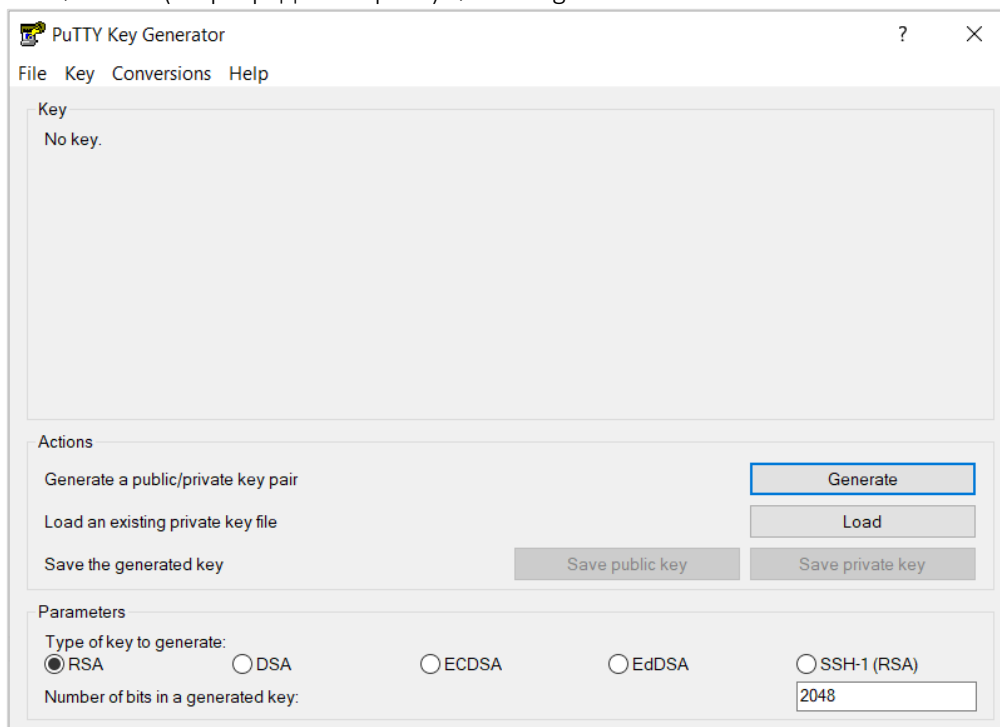
Полученный ответ:

```
Generating public/private ecdsa key pair.  
Your identification has been saved in <хранилище ключей>  
Your public key has been saved in <хранилище ключей>/-pub  
The key fingerprint is:  
SHA256:t44ZVTfglat7U/9dZqcAhx6fqciPpnn53xcMdf7AwEE <имя пользователя>
```

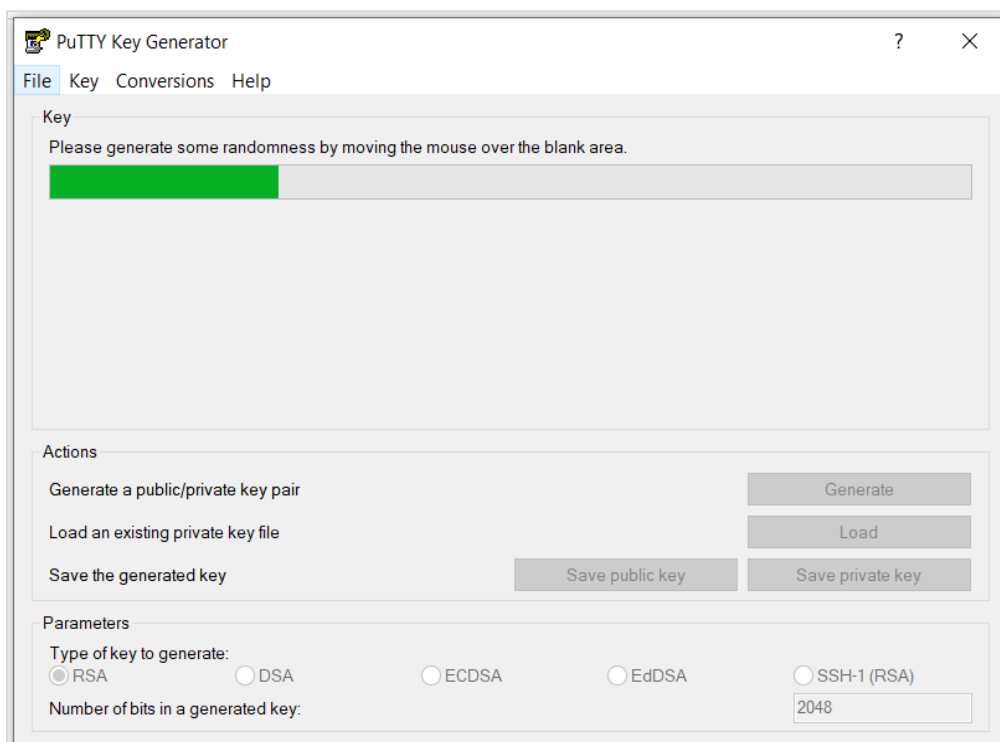
3.2.3. Генерация рабочего ключа шифрования для Windows версий до 10

Для Windows ниже 10 требуется установить PuTTY и запустить PuTTYgen. Генерация ключевой информации с помощью PuTTYgen осуществляется в следующей последовательности:

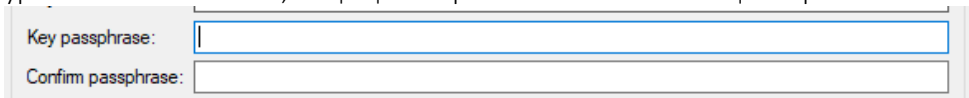
- 1) Запустите PuTTYgen, дважды щелкнув его файл «.exe» или выбрав в Windows меню «Пуск» → PuTTY (64-разрядная версия) → PuTTYgen.



В блоке «Тип ключа для генерации» оставьте RSA по умолчанию. В поле «Число бит в сгенерированном ключе» оставьте значение по умолчанию 2048, которого достаточно для большинства случаев использования. При желании вы можете изменить его на 4096. Вам будет предложено навести указатель мыши на пустую область в разделе «Ключ» («Key»), чтобы создать некоторую случайность. Когда вы перемещаете указатель, зеленый индикатор выполнения будет двигаться вперед. Процесс должен занять несколько секунд.



- 2) После генерации открытого ключа он будет отображаться в блоке «Ключ» («Key»). Для установки пароля, введите ее в поле «Ключевая фраза-пароль» («Key passphrase») и подтвердите его в поле подтверждения. Наличие пароля добавляет дополнительный уровень безопасности, защищая закрытый ключ от несанкционированного использования.



Key passphrase:

Confirm passphrase:

- 3) Сохраните закрытый ключ, нажав кнопку «Сохранить закрытый ключ» («Save private key»). Вы можете сохранить файл в любом каталоге как файл «.ppk» (закрытый ключ PuTTY), но желательно сохранить его в месте, где вы можете легко его найти. Обычно для файла закрытого ключа используется описательное имя, например <имя пользователя>.ppk.
- 4) Для сохранения открытого ключа, щелкните правой кнопкой мыши текстовое поле с надписью «Открытый ключ для вставки в файл авторизованных_ключей OpenSSH» («Public key for pasting into OpenSSH authorized_keys file») и выберите все символы, нажав «Выбрать все». Откройте текстовый редактор, вставьте символы и сохраните. Убедитесь, что вы вставляете весь ключ. В конце ключа укажите <имя пользователя>.

Ключ будет иметь вид:

```
sh-rsa AAAAB3NzaC1yc2EAAA.....gapVOK8uP6hQn0YOXACFN1nUvP7nDE8g9FV username
```

Рекомендуется сохранить файл в том же каталоге, в котором вы сохранили закрытый ключ, используя то же имя закрытого ключа и «.pub» в качестве расширения файла: <имя пользователя>.pub

- 3.2.4. Ключ с расширением .pub требуется отправить на почтовый ящик технической поддержки supportb2b@cbch.ru с темой письма <название компании / ИНН Открытый ключ для взаимодействия>, чтобы Бюро настроило со своей стороны канал связи.

4. Настройка подключения через SFTP-сервер

4.1. Адреса SFTP-серверов Бюро

Тестовая система: ekat-dth-staging-ext-sftp-vmc.cbch.cloud

Промышленная система: ekat-dth-prod-ext-sftp-vmc.cbch.cloud

Порт: 39109

- 4.2. Перед установкой соединения с SFTP необходимо добавить закрытый ключ, используя соответствующий агент аутентификации (например, ssh-agent для Linux и Pageant Для Windows). Это позволит заходить на SFTP-сервер без запроса пароля.

4.2.1. Добавление закрытого ключа для Mac и Linux:

- 1) Проверить запущен ли ssh-agent (нужен для добавления ключа, чтобы каждый раз его не прописывать в запросе соединения с SFTP-сервером)
eval \$(ssh-agent -s)
- 2) Добавить закрытый ключ в ssh-agent (при добавлении вводится пароль от закрытого ключа) ssh-add <хранилище ключей>
- 3) Проверить, что ключ добавлен ssh-add -L

4.2.2. Добавление закрытого ключа для Windows:

- 1) Запустить Pageant: меню Пуск → PuTTY (64-разрядная версия) → Pageant.
- 2) Когда вы запускаете Pageant, он помещает значок в системный трей. Дважды щелкните значок, и откроется окно Pageant.
- 3) Чтобы загрузить ключ, нажмите кнопку «Добавить ключ» («Add key»), при этом откроется диалоговое окно нового файла. Найдите файл закрытого ключа и нажмите «Открыть». Если вы не установили

пароль при генерации, ключ будет загружен немедленно. В противном случае вам будет предложено ввести пароль. После ввода пароля, Pageant загрузит закрытый ключ. После выполнения описанных выше действий вы сможете войти на удаленный сервер без запроса пароля.

4.2.3. Настройка соединения для Mac и Linux. В консоли Client SFTP необходимо выполнить команды:

```
sftp -I <your_private_key> -P 39109 <имя пользователя>@<адрес сервера>
```

Где:

<your_private_key> - закрытый ключ шифрования Клиента

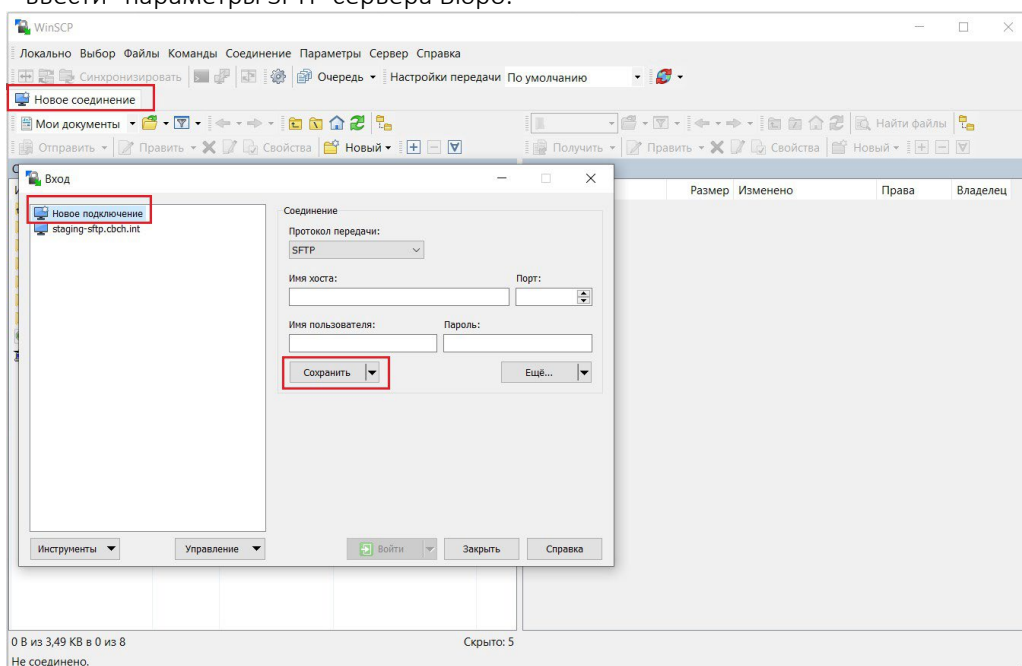
<имя пользователя> - логин учетной записи пользователя, полученный от Бюро

<адрес сервера> - адрес SFTP-сервера Бюро

4.2.4. Настройка соединения для Windows через WinSCP:

1) Запустить WinSCP: меню Пуск → WinSCP

2) В открывшемся окне создать новое подключение через кнопку «Новое подключение», ввести параметры SFTP-сервера Бюро.



4.2.5. Если работа будет производиться через интеграционное решение Клиента, то соединение будет устанавливаться через SFTP-клиента этого интеграционного сервиса Клиента.

5. Порядок работы на SFTP-сервере

5.1. На SFTP-сервере будет создан каталог Клиента, названием каталога будет выступать ИНН Клиента.

5.2. Каталог Клиента включает в себя следующую структуру:

- Inbox (каталог для направления Пакетов в Бюро)
- Draft (подкаталог для подготовки Пакетов)
- Ready (подкаталог для готовых Пакетов – система забирает пакеты из данного каталога автоматически)
- Processing (каталог для отображения Пакетов, находящихся в обработке)
- Outbox (каталог с квитанциями от Бюро о регистрации и обработке Пакетов)
- Error (каталог с ошибками, возникшими при обработке Пакетов)

5.3. Клиент загружает подготовленный и подписанный Пакет со сведениями кредитных историй или с запросом кредитного отчета в подкаталог draft каталога inbox.

5.4. После окончания загрузки Пакета Клиент перемещает его в подкаталог inbox/ready

5.5. Для направления запросов на кредитный отчет в наименовании пакета необходимо добавить в начало report_.

5.6. Система Бюро проверяет подкаталог inbox/ready и принимает Пакеты в обработку. Если Пакет принят в обработку, система перемещает его в подкаталог processing, где он недоступен для

редактирования.

- 5.7. После загрузки Пакета система Бюро проверяет корректность подписанного и заархивированного файла:
- Проверку факта отсутствия в Бюро документа от Клиента с теми же исходящими регистрационным номером и датой, что и у ранее поступившего от данного Клиента Пакета;
 - Проверку электронной подписи;
 - Проверку корректности наименования документа (в соответствии с Порядком передачи сведений о кредитных историях в Бюро);
 - Проверку корректности архивации файла Клиентом;
 - Проверку доступа Клиента к системе загрузки документов Бюро;
 - Проверку соответствия файла действующей xsd-схеме;
 - Проверка размера Пакета.
- 5.8. Если Пакет не прошел хотя бы одну из проверок, Бюро направляет извещение об отклонении Пакета Клиенту с указанием причины отклонения, если Пакет прошел проверки, Бюро направляет Клиенту извещение о получении Пакета.
- 5.9. Далее система Бюро начинает проверять содержимое файлов, проводится форматно-логический контроль сведений, по результатам формируется Квитанция об обработке, которая говорит об успешной/не успешной загрузке переданных сведений в Бюро.
- 5.10. После обработки Пакета Система Бюро размещает результаты обработки (квитанции) в каталоге outbox.
- 5.11. Если система Бюро не смогла корректно обработать файл, то Пакет будет перемещен в подкаталог error с описанием ошибки.
- 5.11.1.