Версия 1.3 от 24.07.2023

Инструкция по настройке и организации взаимодействия с использованием SFTP-сервера

Москва, 2023 г.

Оглавление

1. Общие положения 2
2. Подготовка к взаимодействию 2
2.1. Требования для взаимодействия 2
2.2. Порядок настройки взаимодействия через SFTP-сервер 2
2.2.1. Настройка криптографического шлюза «КриптоПро Ngate» для взаимодействия 3
2.2.2. Регистрация технического пользователя 3
2.2.3. Генерация рабочего ключа шифрования для Mac и Linux 3
2.2.4. Генерация рабочего ключа шифрования для Windows10 3
2.2.5. Генерация рабочего ключа шифрования для Windows версий до 10 3
2.2.6. Направление открытого ключа в Бюро 5
3. Взаимодействие с Бюро через SFTP-сервер 5
3.1. Адреса SFTP-серверов Бюро 5
3.2. Установление соединения с SFTP-сервером 5
3.2.1. Добавление закрытого ключа для Mac и Linux 5
3.2.2. Добавление закрытого ключа для Windows 5
3.2.3. Настройка соединения для Mac и Linux 6
3.2.4. Настройка соединения для Windows 6
3.2.5. Загрузка пакетов 6

1. Общие положения

1.1. Настоящая инструкция описывает порядок осуществления доступа Партнера к ПО SKB.CHD и использования его функциональности с помощью SFTP-сервера.

1.2. SFTP-сервер предназначен для автоматизированного обмена информацией в виде файлов между Партнером и Бюро с целью загрузки Партнером сведений о кредитной истории субъектов в базу данных Бюро или получения Партнером сведений о кредитных историях субъектов (кредитные отчеты).

1.3. Взаимодействие с сервисами Бюро осуществляется с использованием криптографического туннеля на базе «Крипто Про NGate», что гарантирует дополнительную защиту персональных данных, участвующих в обмене путем шифрования канала.

1.4. Для установления соединения с SFTP-сервером используется протокол SSH.

1.5. Для доступа к SFTP-серверу необходимо наличие служебной учетной записи.

1.6. На процессы обмена файлами между Партнером и Бюро через SFTP-сервер распространяется действие «Регламента электронного взаимодействия с Программой SKB.CHD».

1.7. Требования к организации взаимодействия при передаче сведений о кредитных историях субъектов в Бюро описан в «Порядке передачи кредитных историй в ООО СКБ», размещенных на сайте Бюро в разделе «Документация» (https://cbch.ru/documentation/).

1.8. Требования к организации взаимодействия при получении кредитных отчетов в Бюро описан в «Порядке направления запросов на получение КО», размещенных на сайте Бюро в разделе «Документация» (https://cbch.ru/documentation/).

2. Подготовка к взаимодействию

2.1. Требования для взаимодействия

Для взаимодействия с Бюро через SFTP-сервер Партнеру необходимо:

– наличие заключенного договора (на передачу КИ или получение КО) 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;

2.2. Порядок настройки взаимодействия через SFTP-сервер

– Партнер и Бюро производят настройку криптографического шлюза «КриптоПро NGate».
– Бюро регистрирует служебного пользователя Партнера на основании заявления от Партнера.
– Партнер генерирует ключ шифрования и направляет публичную часть в Бюро.

– Бюро настраивает соединение с SFTP для Партнера.

2.2.1. Настройка криптографического шлюза «КриптоПро Ngate» для взаимодействия

Для настройки защищенного канала Партнеру необходимо:

– Направить в адрес Бюро открытую часть сертификата электронной подписи;

– Получить от Бюро Корневой сертификат удостоверяющего центра КриптоПро.

Настройка защищенного канала связи с использованием технологии на базе СКЗИ «КриптоПро NGate» (настройка VPN-туннеля) осуществляется по Инструкции, размещенной на сайте Бюро в разделе «Документация» (https://cbch.ru/documentation/).

2.2.2. Регистрация технического пользователя

Для регистрации учетной записи служебного пользователя, Партнеру необходимо направить электронное сообщение на почту на supportb2b@cbch.ru в соответствии с документом «Регламента электронного взаимодействия с Программой SKB.CHD».

Бюро зарегистрирует технического пользователя и направляет реквизиты доступа ответным сообщением.

2.2.3. Генерация рабочего ключа шифрования для Mac и Linux

Для **Mac или Linux** необходимо выполнить команду:

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

где:

<имя пользователя> - имя технического пользователя, полученное от ТП Бюро.

<хранилище ключей> - путь до папки[1], где будут храниться ключи (требуется право на запись)

<password> - пароль ключа шифрования.

Пример:

```
$ ssh-keygen -t ecdsa -b 521 -C "username" -f ./directory -N password
Generating public/private ecdsa key pair.
Your identification has been saved in ./directory
Your public key has been saved in ./directory.pub
The key fingerprint is:
SHA256:nRgRsZ+PUwfxAFG4MENI5HfXmwo1FJnnGM3eVaIMUDE username
```

2.2.4. Генерация рабочего ключа шифрования для Windows10

Для **Windows 10** и выше можно выполнить вышеуказанную команду в терминале Powershell:

Пример:

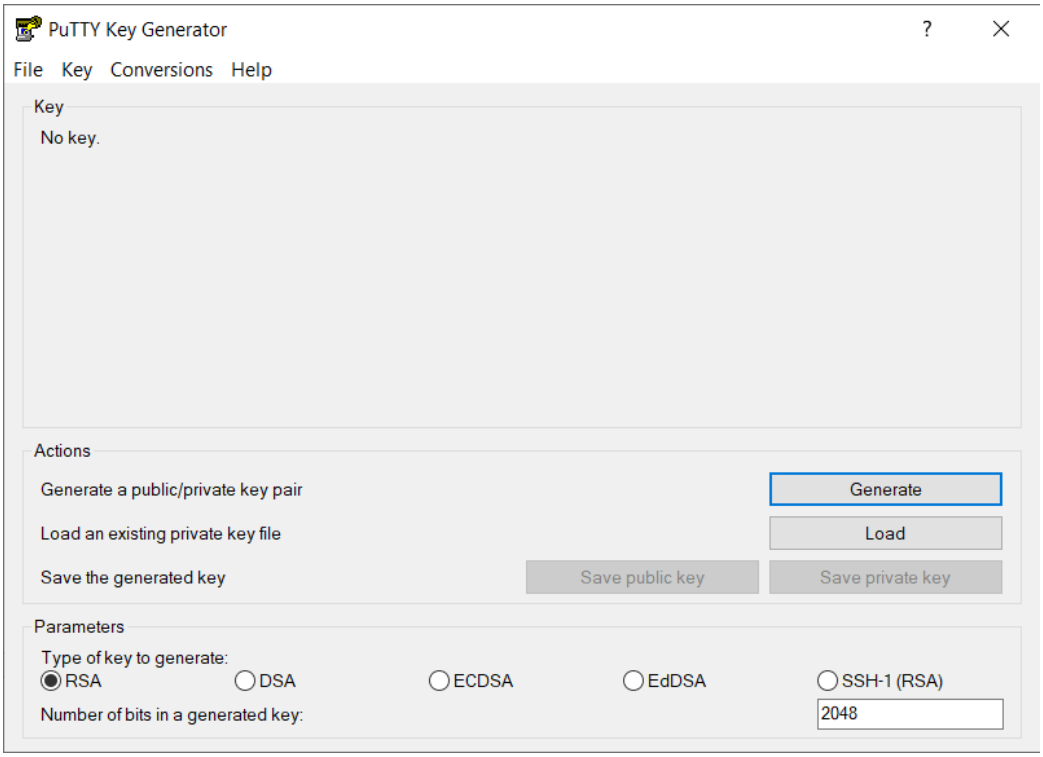
```
PS C:\Users\user.DOMAIN> ssh-keygen.exe -t ecdsa -b 521 -C "username" -f .\directory -N password
Generating public/private ecdsa key pair.
Your identification has been saved in .\ directory.
Your public key has been saved in .\ directory.pub.
The key fingerprint is:
SHA256:t44ZVTfgIat7U/9dZqcAhx6fqciPpnn53xcMdf7AwEE username
```

2.2.5. Генерация рабочего ключа шифрования для Windows версий до 10

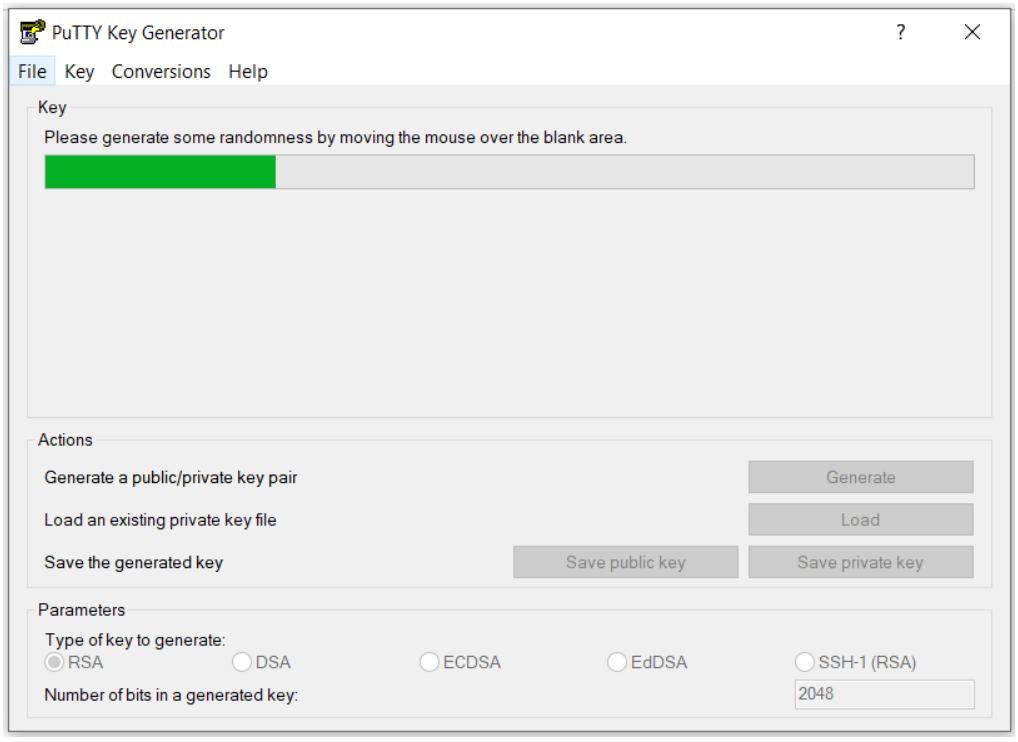
Для **Windows** ниже 10 требуется установить PuTTY и запустить PuTTYgen. Генерация ключевой информации с помощью PuTTYgen осуществляется в следующей последовательности.

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

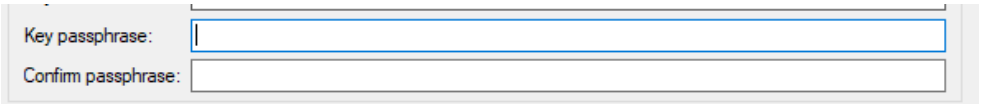
[1] Рекомендуется указывать имена каталогов, не содержащих знаков пробела (например, ./directory – рекомендуется, а ./new folder – не рекомендуется, при необходимости можно указать ./new_folder)



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.



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 mfo1234
```

   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**

2.2.6. Направление открытого ключа в Бюро

После успешной генерации ключей в папке <хранилище ключей> появится два ключа.
Ключ с расширением .pub требуется отправить на почтовый ящик admin@cbch.ru с темой письма <название компании / ИНН>.
Администратор SFTP-сервера настроит со своей стороны канал связи и ответным письмом вышлет адрес SFTP-сервера, с которым будет производиться взаимодействие

3. Взаимодействие с Бюро через SFTP-сервер

3.1. Адреса SFTP-серверов Бюро

Тестовая система: staging-exchange-storage.cbch.int
Промышленная система: exchange-storage.cbch.int
Порт: 39109

3.2. Установление соединения с SFTP-сервером

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

3.2.1. Добавление закрытого ключа для Mac и Linux

Для **Linux** или **Mac OS** в консоли Client SFTP:

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

3.2.2. Добавление закрытого ключа для Windows

Для **Windows** используется Pageant – агент аутентификации PuTTY SSH:

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.

3.2.3. Настройка соединения для Mac и Linux

Для **Linux** или **Mac OS** в консоли Client SFTP необходимо выполнить команды

sftp –I <your_private_key> –P 39109 username@staging-exchange-storage.cbch.int

Где:

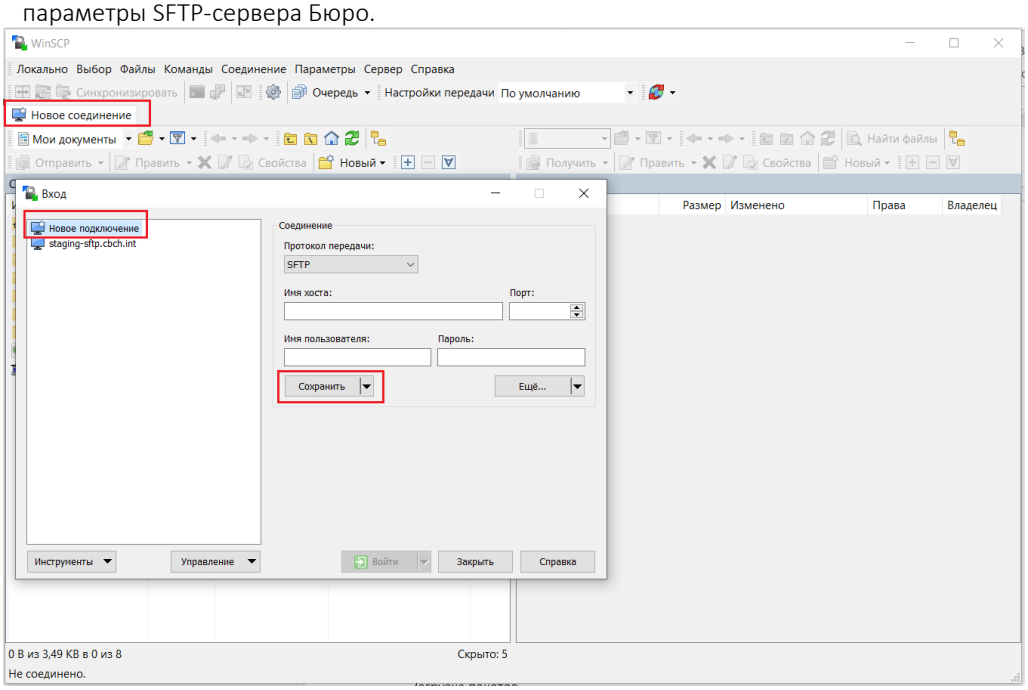
<your_private_key> - закрытый ключ шифрования Партнера

<username> - имя технического пользователя, полученное от ТП Бюро

3.2.4. Настройка соединения для Windows

Для Windows необходимо использовать WinSCP:

1) Запустить WinSCP: меню Пуск → WinSCP
2) В открывшемся окне создать новое подключение через кнопку «Новое подключение», ввести параметры SFTP-сервера Бюро.



a. Если работа будет производится через интеграционное решение Партнера, то соединение будет устанавливаться через sftp-клиента этого интеграционного сервиса Партнера.

3.2.5. Загрузка пакетов

1) Перейдите в каталог inbox
2) Загрузите подготовленный пакет в подкаталог inbox/draft
3) После окончания загрузки пакета переместите пакет в подкаталог inbox/ready

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.
При обнаружении ошибок в пакете, он будет перемещен в подкаталог error.

Описание состава квитанций приведены в «Порядке передачи кредитных историй в ООО СКБ», размещенном на сайте Бюро в разделе «Документация» (https://cbch.ru/documentation/).