

Часто задаваемые вопросы по DiSec-W и МГК-3

- 1. Вопрос: У участника обмена возникла необходимость в получении СКЗИ. Где можно получить?**

Ответ:

Все участники обмена кроме Московского региона могут получить СКЗИ в своём ТУ, сроки и порядок получения необходимо уточнить в обслуживающем ТУ. Для участников обмена Московского региона выдача СКЗИ осуществляется в соответствии с «Условиями передачи программного обеспечения Клиенту Банка России», опубликованными на сайте Банка России в разделе https://www.cbr.ru/development/mcirabis/involve_em/, по адресу: ул. Свободы, 57, корпус 1, строение 2 по рабочим пятницам с 12.00 до 15.00.

При необходимости можно связаться с ЦЭПС ДИТ по телефонам: 8 (495) 987-75-83, 8 (495) 987-75-87 и согласовать дату и время получения СКЗИ.

- 2. Вопрос: Где почитать информацию про DiSec-W? Как настраивать?**

Ответ:

Необходимая информация содержится в документе «Порядок подключения участников обмена к автоматизированной системе «Транспортный шлюз Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России (ТШ КБР)» с использованием средств криптографической защиты каналов «DiSecW», документ опубликован на сайте Банка России в разделе

https://www.cbr.ru/development/mcirabis/involve_em/.

- 3. Вопрос: Есть ли клиент DiSec-W под ОС линукс?**

Ответ:

Нет, только под ОС Windows.

- 4. Вопрос: Когда появится клиент DiSec-W под ОС линукс?**

Ответ:

Не ранее 4 квартала 2025 года.

- 5. Надо ли настраивать что-то ещё кроме DiSec-W?**

Ответ:

Да, надо изменить настройки ПП АРМ КБР-Н/ПП АРМ КБР-СПФС согласно «Порядку подключения участников обмена к автоматизированной системе «Транспортный шлюз Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России (ТШ КБР)» с использованием средств криптографической защиты каналов «DiSecW», опубликованному на сайте Банка России в разделе https://www.cbr.ru/development/mcirabis/involve_em/.

Обращаем внимание, что при нажатии кнопки «Проверить соединение» в ПП АРМ КБР-Н/ПП АРМ КБР-СПФС происходит проверка соединения только с основным сервером. Переключение на резервные серверы происходит только при штатной работе АРМа с ролью Оператор в случае недоступности основного сервера. В протоколе отображается только попытка подключения к основному серверу.

6. Минимальная версия ОС Windows? Можно ли использовать Windows 7/8/8.1/сервер?

Ответ:

В соответствии с формуляром на СКЗИ DiSec-W должна использоваться операционная система Windows 10, либо Windows Server 2016. Работа на других версиях операционных систем не гарантируется, консультации по работе СКЗИ на таких версиях операционных систем не оказываются. Поддерживаются только 64-разрядные версии ОС Windows10, либо Windows Server 2016.

7. Может ли участник обмена получить больше/меньше рекомендованного количества СКЗИ?

Ответ:

Участник обмена может запросить большее или меньшее число СКЗИ. Для этого необходимо направить письмо «О необходимом ПО и лицах, уполномоченных осуществлять получение ПО» в адрес Банка России по форме приложения 1 «Условий передачи программного обеспечения Клиенту Банка России», размещенных на сайте Банка России в разделе https://www.cbr.ru/development/mcirabis/involve_em/.

8. Возможна ли установка СКЗИ DiSec-W на одном ПЭВМ с ПП АРМ КБР-Н / ПП АРМ КБР-СПФС, либо необходимо разносить ПО на разные ПЭВМ?

Ответ:

Установка СКЗИ DiSec-W на одном ПЭВМ с ПП АРМ КБР-Н/ ПП АРМ КБР-СПФС возможна. СКЗИ DiSec-W не конфликтует со СКАД «Сигнатура».

9. Можно ли установить один экземпляр СКЗИ на несколько ПЭВМ?

Ответ:

Для каждой ПЭВМ используется свой собственный экземпляр СКЗИ DiSec-W, в том смысле, что для каждой установки должен использоваться свой собственный учётный номер СКЗИ. При этом для нескольких инсталляций можно использовать один и тот же дистрибутивный комплект (компакт-диск), затем, при запросе на активацию, для каждого установленного экземпляра СКЗИ нужно делать запрос на активацию с индивидуальным номером СКЗИ. Активация и использование одного экземпляра СКЗИ DiSec-W одновременно на нескольких ПЭВМ является нарушением правил пользования СКЗИ DiSec-W.

10. Должен ли токен с закрытым ключом всегда быть присоединён к ПЭВМ?

Ответ:

Да, извлечение токена с закрытым ключом приведёт к нарушению работы DiSec-W.

11. Можно ли в акте и письме «О необходимом ПО и лицах, уполномоченных осуществлять получение ПО» указывать сразу несколько комплектов DiSec-W или на каждый комплект должен составляться свой акт и письмо?

Ответ:

Да, в письме и акте можно указать сразу несколько комплектов СКЗИ для получения.

12. Участник обмен решил использовать аппаратное решение (например, Dionis-NX). Нужно ли в таком случае получать DiSec-W?

Ответ:

Программный продукт DiSec-W распространяется Банком России бесплатно для выполнения требований 747-П. Если клиент самостоятельно и за свой счёт приобрел ПАК Dionis-NX для организации защиты канала, то его можно использовать вместо DiSec-W, соответственно в таком случае участник обмена может отказаться от

использования DiSec-W и не получать его вовсе, либо получить в ограниченном количестве, например, для целей резервирования или тестирования. В данном случае решение принимается участником обмена.

13. При генерации запроса, появляется диалоговое окно «Инициализация выполнена», далее нажимается Ок, однако выбор ключевого носителя не запускается – приложение закрывается (п.4 Инструкции по изготовлению КИ КБР).

Ответ:

Необходимо выполнить следующие действия:

- a. Удалить МГК-3. Удалить драйвер токена. Перезагрузить АРМ.
- b. Установить МГК-3 с правами администратора.
- c. Остановить антивирус или добавить путь C:\Program Files (x86) \Factor-TS\Request3 в исключения.
- d. Выполнить первый запуск с правами администратора.
- e. По инструкции сформировать запрос/ключ на внешний flash-носитель.

14. При запуске DiSec-W, иконка не появляется в трее, или исчезает при попытке вызвать всплывающее меню.

Ответ:

Необходимо отключить (перевести в состояние Disable) следующие службы и перезагрузить АРМ:

- a. Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности (IKE and AuthIP IPsec keying Modules).
- b. Агент политики IPsec (IPsec Policy Agent).

15. В логе СКЗИ «DiSec-W» присутствует фраза «Обновление CRL выполнено с ошибками для сертификата пользователя?»

лог имеет вид:

04-10-2024 13:03:49,760: ++++++++ [[CD-TUZ01]]: УСТАНОВЛЕН ТУННЕЛЬ [8426A8C0 <=>

1B92D50B] ++++++++

04-10-2024 13:03:49,760: [[CD-TUZ01]]: ВСЕ ТУННЕЛИ для целевых объектов ДОБАВЛЕНЫ

04-10-2024 13:03:55,619: [[CD-TUZ01]]: Обновление CRL выполнено с ошибками для сертификата пользователя. См. Журнал

04-10-2024 13:03:55,650: [[CD-TUZ01]]: Начата процедура обновления CRL для сертификата оппонента

04-10-2024 13:04:05,618: [[CD-TUZ01]]: Обновление CRL выполнено с ошибками для сертификата оппонента. См. Журнал

Ответ:

В окне «Настройка РКИ пользователя» необходимо убрать галку «Выполнить до установки туннеля» и установить галку «Выполнить после установки туннеля».

16. Где взять данные для генерации закрытого ключа?

Ответ:

Клиенты Московского региона руководствуются «Регламентом взаимодействия Банка России и Клиента (косвенного участника Клиента), Пользователя при управлении криптографическими ключами», опубликованном на сайте Банка России в разделе https://www.cbr.ru/development/mcirabis/involve_em/.

Клиенты ТУ должны руководствоваться локальными регламентами, определяющими их взаимодействие с ТУ в части ключевой информации.

17. Что делать с канальными/прикладными учётными записями?

Ответ:

Канальные учётные записи использовались для работы ПО Cisco AnyConnect. После перехода на использование СКЗИ DiSec-W необходимость использования канальных учётных записей отпадает.

18. После установления туннеля недоступны прикладные порты 7777/1414/9697?

Ответ:

Средствами СКЗИ Disec-W устанавливается одновременно 4 VPN-туннеля до 4-х ЦОД ТШ КБР. Личный кабинет ТШ КБР должен быть доступен на TCP-порту 9697 по всем четырём прикладным ip-адресам. TCP-порты 7777(http) и 1414(mq) для прикладного взаимодействия ПП АРМ КБР-Н/ПП АРМ КБР-СПФС доступны **не менее, чем на одном** из четырёх прикладных ip-адресов. В ПП АРМ КБР-Н/ПП АРМ КБР-СПФС для этих целей настраивается основной и резервные прикладные ip-адреса, по которым АРМ осуществляет перебор. Таким образом по TCP портам 7777 и 1414 должен отвечать хотя бы один из четырёх адресов, но не обязательно все.

19. В логах ПП АРМ КБР-Н/ ПП АРМ КБР-СПФС присутствуют ошибки при подключении к узлам ТШ КБР (connection timeout)?

Ответ:

В конфигурации ПП АРМ КБР-Н/ ПП АРМ КБР-СПФС на вкладке «Настройки СВК/ТШ КБР» должны быть указаны как основной адрес подключения, так и резервные адреса. Резервные адреса должны быть указаны с номером порта! Например, 172.21.1.58:7777.

Сервис должен отвечать хотя бы по одному из четырёх адресов, но не обязательно все. Также необходимо установить тайм-аут соединения в размере 60 секунд или более.