Рекомендации по настройкам ПП АРМ КБР – СПФС-L

Установка и настройка программного продукта (далее – ПП) АРМ КБР-СПФС-L производится в соответствии с документами «Автоматизированное рабочее место клиента Банка России пользователя системы передачи финансовых сообщений–L. Регламент эксплуатации» и «Автоматизированное рабочее место клиента Банка России пользователя системы передачи финансовых сообщений-L. Руководство администратора».

ЦЭПС обращает внимание УО, что все входящие ЭС, направляемые клиентом в Центр обработки сообщений (далее - ЦОС) в рамках Системы передачи финансовых сообщений (далее - СПФС) должны быть снабжены кодом аутентификации для каждого ЭС/пакета ЭС (первый вариант защиты).

Для обеспечения обмена ЭС с ЦОС в рамках СПФС сообщений с использованием ПП АРМ КБР-СПФС должна использоваться отдельная прикладная учетная запись УО в промышленной транспортной системе Банка России с закрепленным за ней номером АРМ 53 для обмена ЭС с промышленным ЦОС и отдельная прикладная учетная запись УО в тестовой транспортной системе Банка России с закрепленным за ней номером АРМ 63 для обмена ЭС с тестовым ЦОС.

1. Общие параметры

Параметры программного комплекса

«Режим работы»: рекомендуем использовать комбинированный или автоматический «НСИ и контроль»:

Рекомендуем установить:

- «Автоматический импорт ED574»
- «Контроль на дубликаты»
- опцию Всемирное время «Выполнять преобразование».

УИС получателя (ЦОС) – 7777777000

Остальные параметры заполняются пользователем штатно.

Реквизиты служебного конверта:

- **для тестирования**

адрес получателя (ЦОС): uic:777777700011 - адрес отправителя АРМ – uic:XXXXXXXXXXHA, где XXXXXXXXXX - УИС клиента

БР должен соответствовать заполненному УИС на закладке «Реквизиты организации»

(например, 4525225000, соответственно в этом поле 4525225000НА*, где НА – номер АРМа 63*)

- для промышленной эксплуатации

адрес получателя (ЦОИ):

uic:777777700000

адрес отправителя АРМ – uic:XXXXXXXXXXНА, где XXXXXXXXX УИС клиента БР должен соответствовать заполненному УИС на закладке «Реквизиты организации»

(например, 4525225000, соответственно в этом поле 4525225000НА, *где НА – номер АРМа 53*).

Обращаем внимание, что адреса отправителя и получателя должны начинаться с «uic:»

- включенная опция «Запрашивать квитанции» актуальна для работы с транспортным адаптером (формируется квитанция об отправке).

Рекомендуем включить опцию «Передавать имя файла»

Настройки, связанные с использованием СКАД Сигнатура

Группа реквизитов **«Предупреждать об истечении срока действия»** сертификата и ключа – рекомендуем указать **15 дней**.

1. Комплект специальных криптографических ключей

Формирование КА

CN=<NAME>

Область применения ключа: Электронная подпись, Шифрование.

Списки OID используемых ключей:

Формирование КА 1.3.6.1.4.1.10244.7.20.1

Проверка ЗК

1.3.6.1.4.1.3670.5.10.27 – ЦОС

Проверка КА

1.3.6.1.4.1.3670.5.10.28 – ЦОС

Если списки OID используемых ключей не заполнены, то проверка на соответствие OID не производится.

OID ключа получателя 1.3.6.1.4.1.3670.5.10.28

При загрузке ключа и при проверке КА на ЭС, полученных от клиента, дополнительно к OID расширенной области применения ключей по спискам разрешенных

для формирования КА проверяется OID регламента использования сертификата (1.3.6.1.4.1.3670.4.20.20).

2. Комплект специальных криптографических ключей при использовании первого варианта защиты, если ПП АРМ КБР-СПФС-L используется только для шифрования/расшифрования:

Формирование ЗК*

CN=<*NAME*_ABS>

OID:1.3.6.1.4.1.10244.7.20.1

Область применения ключа: Электронная подпись.

*Используется в АБС клиента для формирования ЭС в формате конверта КА

Шифрование

CN=<NAME>

OID:1.3.6.1.4.1.10244.7.20.1

Область применения ключа: Шифрование ключа, Шифрование данных.

Списки OID используемых ключей:

Формирование КА 1.3.6.1.4.1.10244.7.20.1

Проверка ЗК

1.3.6.1.4.1.3670.5.10.27 – ЦОС

Проверка КА

1.3.6.1.4.1.3670.5.10.28 – ЦОС

OID ключа получателя 1.3.6.1.4.1.3670.5.10.28

Настройки, связанные с обработкой сообщений

Блоки настроек «Обработка УФЭБС», «Обработка SWIFT MT», «Обработка SWIFT MX», «Обработка собственных форматов» могут заполняться штатно.

Для блока «Обработка УФЭБС» в каталог для входа необходимо помещать файл в формате УФЭБС: Это могут быть неподписанные сообщения типа ED501-ED599 или сообщения с КА в формате SigEnvelope.

Для блока «Обработка SWIFT MT» в каталог для входа необходимо помещать файл в SWIFT формате, на его основе будет сформирован ed503.

Для блока «Обработка SWIFT MX» в каталог для входа необходимо помещать файл в SWIFT формате, на его основе будет сформирован ed514.

Если в качестве каталогов обмена ЭС указаны каталоги, отличные от стандартных, сформированных при инсталляции АРМ, то права доступа пользователя на эти каталоги следует установить по аналогии с правами доступа на стандартные каталоги обмена ЭС.

Обращаем внимание, что требования к структуре имён файлов определены в документе «Автоматизированное рабочее место клиента Банка России пользователя системы передачи финансовых сообщений-L. Руководство разработчика»

При проведении апробации АРМ СПФС для ОС Alt Linux до получения средства криптографической защиты (СКЗИ) «Клиент криптографического сервера доступа DiSec» для ОС Linux взаимодействие со стендом совмещённого тестирования (далее - ССТ) можно выполнить с помощью защищенного VPN-соединения, установленного с использованием СКЗИ DiSec-W на отдельной ПЭВМ под управлением ОС Windows. ЭС в формате служебного конверта, сформированное АРМ СПФС для ОС Linux, можно направить на ССТ через личный кабинет ТШ КБР (далее ЛК) с ПЭВМ под управлением ОС Windows или настроив прикладное проксирование на ПЭВМ под управлением ОС Windows.

Для возможности передавать ЭС через ЛК, необходимо в настройке «Транспорт» снять галку «Передача в транспорт. Протокол» и «Прием из транспорта. Протокол».

Режим «Настройка ТШ КБР» – «Настройка взаимодействия с ТШ КБР»

Параметры подключения

Протокол – «HTTP»

Маркер формата – XMLEPD

Попыток отправки – 1-2

Таймаут операций (с) – 60 с

При использовании средств криптографической защиты каналов DiSec-W группа «HTTP» содержит параметры:

Для работы в тестовом контуре по протоколу HTTP должны использоваться следующие настройки:

Адрес отправки: http://172.21.5.57:7777/in

Адрес получения: http://172.21.5.57:7777/get

Также необходимо указать резервные значения IP-адресов сервера:

172.21.5.58:7777

172.21.5.59:7777

172.21.5.60:7777

Резервные сервера– по кнопке открывается окно, в котором нужно задать список IP адресов ТШ КБР, на которые будет перенаправляться соединение в случае отсутствия подключения к основному серверу.

Для работы в тестовом контуре по протоколу IBM MQ должны использоваться следующие настройки:

WMQ / Сервер: 172.21.5.57

WMQ / Порт: 1414

WMQ / Канал: KBR.SVRCONN

WMQ / Менеджер: FRONTGATE

Отправка / Очередь: FROM.KBR

Отправка / Менеджер ответов: FRONTGATE

Отправка / Очередь ответов: INBOX.xxxxxx (уточняется через Единую службу поддержки пользователей при начале работы по MQ)

Опция Отправка / Запрашивать квитанции о доставке/получении устанавливается опционально при необходимости

Приём / Очередь: INBOX.xxxxxx (уточняется через Единую службу поддержки пользователей при начале работы по MQ)

Также необходимо указать резервные значения IP-адресов сервера:

172.21.5.58:7777

172.21.5.59:7777

172.21.5.60:7777

Для работы в промышленном контуре по протоколу HTTP должны использоваться следующие настройки:

Адрес отправки: http://172.21.1.57:7777/in

Адрес получения: http://172.21.1.57:7777/get

Также необходимо указать резервные IP-адреса сервера:

172.21.1.58:7777

172.21.1.59:7777

172.21.1.60:7777

Для работы в промышленном контуре по протоколу IBM MQ должны использоваться следующие настройки:

WMQ / Сервер: 172.21.1.57

WMQ / Порт: 1414

WMQ / Канал: KBR.SVRCONN

WMQ / Менеджер: FRONTGATE

Отправка / Очередь: FROM.KBR

Отправка / Менеджер ответов: FRONTGATE

Отправка / Очередь ответов: INBOX.xxxxxx (уточняется через Единую службу поддержки пользователей при начале работы по MQ)

Опция Отправка / Запрашивать квитанции о доставке/получении устанавливается опционально при необходимости

Приём / Очередь: INBOX.xxxxxx (уточняется через Единую службу поддержки пользователей при начале работы по MQ)

Также необходимо указать резервные IP-адреса сервера:
172.21.1.58:7777
172.21.1.59:7777
172.21.1.60:7777

«Аутентификация» - «Прикладная аутентификация»

Имя пользователя*

Пароль*

*Данные значения Администратор заполняет в соответствии с полученными учетными записями.

Режим «Транспорт»

Для возможности работать с использованием протоколов HTTP/MQ необходимо выбрать из списка – «HTTP» или «IBM MQ», предварительно установив галку «Передача в транспорт. Протокол» и «Прием из транспорта. Протокол».