Рекомендации по настройке программного продукта (ПП) АРМ КБР-Н

Установка и настройка ПП АРМ КБР-Н производится в соответствии с документом «Автоматизированное рабочее место клиента Банка России новое. Руководство администратора».

ЦЭПС обращает внимание участников обмена (далее – УО) о необходимости импортировать в локальный справочник сертификатов пользователя ПП АРМ КБР-Н, выполняющего функции шифрования, сертификаты оператора, контролера УО, сертификаты ЦОИ (для расшифрования и проверки ЗК/КА).

При переходе на использование ПП АРМ КБР-Н УО должен иметь следующий комплект ключей:

CN=PROCESSING
OID расширенная область применения ключа -1.3.6.1.4.1.3670.5.10.15
Область применения ключа: Электронная подпись.

CN=CONTROL
OID расширенная область применения ключа -1.3.6.1.4.1.3670.5.10.16
Область применения ключа: Электронная подпись.

CN=ARMKBRN
OID расширенная область применения ключа -1.3.6.1.4.1.3670.5.10.120
Область применения ключа: Шифрование ключа, Шифрование данных.

Настройка ПП АРМ КБР-Н

1. Режим «Настройки»

В настройках конфигурационных параметров ПП АРМ КБР-Н необходимо указать OID расширенной области применения ключа, загружаемого при старте ПП АРМ КБР-Н представителем эксплуатационного персонала с функциональной ролью «Оператор»:

OID ключа для загрузки - 1.3.6.1.4.1.3670.5.10.120

Степень распараллеливания (параллельная обработка ЭС реализована в ПП АРМ КБР-Н версии 2022.4.0)

Выбор из списка:
-1 – обработка, использующая все ресурсы процессора. В данном случае управление использования ресурсов процессора происходит средствами Framework,
1 – последовательная обработка,
2 и более – параллельная обработка, определяет количество логических процессоров, участвующих в обработке. Ручная настройка ограничена и максимальное значение равно половине лог. процессоров. Если выставить значение больше, чем процессор может выдержать, то ПП КБР-Н будет нестабильно работать.
При выборе значения «0» и сохранении конфигурации АРМ КБР-Н автоматически изменит значение на 1.

Обращаем внимание УО:

1. УО для каждой точки обмена может использовать отдельную прикладную учетную запись (далее - УЗ), предназначенную для приема/отправки ЭС для этой точки. Таким образом, для ЦК ПС будет своя прикладная УЗ, для ПС СБП– своя, ОД ОПЕРУ-1 - своя. Обращаем внимание УО, что все регламентные ЭС (ЦК ПС, ПС СБП) идут на регламентный номер АРМ (НА=00 промышленная эксплуатация, НА=11 –стенд тестирования). ЭС ОД ОПЕРУ – идут на номер АРМ – НА=70 – промышленная эксплуатация, НА=71 – стенд

тестирования. При этом в настройке «СКАД Сигнатура» для данной точки указать все OID сертификатов ЦОИ.

2. Если нет отдельной УЗ, то в одной из точек рекомендуем разрешить запуск для входящих для АС клиента, в остальных отключить данную возможность и настроить в данной точке возможность создавать подкаталоги по адресу From из СК или по EDReceiver. При этом в настройке «СКАД Сигнатура» для данной точки указать все OID сертификатов ЦОИ.

Сертификаты ЦОИ (ПС БР, ПС СБП, ОД ОПЕРУ-1) **НЕОБХОДИМО** добавить в справочник сертификатов, а также прописать их OID в данном настроечном блоке «СКАД Сигнатура»:

OID сертификатов ЦОИ –

ЗК 1.3.6.1.4.1.3670.5.10.7 – ПС БР

ЗК 1.3.6.1.4.1.3670.5.10.123 – ПС СБП

ЗК 1.3.6.1.4.1.3670.5.2.3 - ОД ОПЕРУ-1

КА 1.3.6.1.4.1.3670.5.10.8 – ПС БР

КА 1.3.6.1.4.1.3670.5.10.124 – ПС СБП

КА 1.3.6.1.4.1.3670.5.2.4 – ОД ОПЕРУ-1

2. Рекомендации по настройкам ПП АРМ КБР - Н при направлении ЭС в платежную систему Банка России (3 вариант защиты).

Настройки точки обмена. Режим «СКАД Сигнатура»

В этой группе параметров необходимо указать атрибуты сертификатов СКАД «Сигнатура», по которым проверяется правомочность использования ключей для конкретных операций, а также варианты защиты ЭС с помощью ЗК:

OID сертификатов клиента:

ЗК 1.3.6.1.4.1.3670.5.10.15

КА 1.3.6.1.4.1.3670.5.10.16

OID сертификатов ЦОИ –

ЗК 1.3.6.1.4.1.3670.5.10.7

КА 1.3.6.1.4.1.3670.5.10.8

«Вариант защиты ЭС с помощью ЗК»

Указать установленный Банком России способ защиты ЭС, используемый при проверке ЗК на ЭС:

Подписание –3 вариант – ЗК на каждое ЭС

Проверка - 2 вариант – ЗК на весь пакет

OID ключа получателя 1.3.6.1.4.1.3670.5.10.8

Режим «Служебный конверт» - реквизиты служебного конверта

«Адрес получателя (ЦОИ)» - uic:4583001999НА

«Адрес отправителя (АРМ)» – uic:XXXXXXXXXXНА, где XXXXXXXXXX – УИС Клиента БР должен соответствовать заполненному УИС на закладке «Настройки» «УИС клиента БР(EdAuthor)» (например, 4525505000, соответственно, в этом поле 452550500011, где 11 – номер АРМа).

НА=11 для тестирования на стенде тестирования, НА=00 для промышленной эксплуатации.

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». Данный признак определяет формирование реквизита «LegacyTransportFileName» в служебном конверте.

Остальные настройки выполняются пользователем штатно.

3. Рекомендации по настройкам ПП АРМ КБР - Н при направлении ЭС в ПС СБП (3 вариант защиты).

Настройки точки обмена. Режим «СКАД Сигнатура»

В этой группе параметров необходимо указать атрибуты сертификатов СКАД «Сигнатура», по которым проверяется правомочность использования ключей для конкретных операций, а также варианты защиты ЭС с помощью ЗК:

OID сертификатов клиента:

ЗК 1.3.6.1.4.1.3670.5.10.15

КА 1.3.6.1.4.1.3670.5.10.16

OID сертификатов ЦОИ –

ЗК 1.3.6.1.4.1.3670.5.10.123

КА 1.3.6.1.4.1.3670.5.10.124

«Вариант защиты ЭС с помощью ЗК»

Указать установленный Банком России способ защиты ЭС, используемый при проверке ЗК на ЭС:

Подписание –3 вариант – ЗК на каждое ЭС

Проверка - 2 вариант – ЗК на весь пакет

OID ключа получателя 1.3.6.1.4.1.3670.5.10.124

Режим «Служебный конверт» - реквизиты служебного конверта

«Адрес получателя (ЦОИ)» - uic: 4511111111НА

«Адрес отправителя (АРМ)» – uic:XXXXXXXXXXНА, где XXXXXXXXXX - УИС

Клиента БР должен соответствовать заполненному УИС на закладке «Настройки» «УИС клиента БР(EdAuthor)» (например, 4525505000, соответственно, в этом поле 452550500011, где 11 – номер АРМа).

НА=11 для тестирования на стенде тестирования, НА=00 для промышленной эксплуатации.

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». Данный признак определяет формирование реквизита «LegacyTransportFileName» в служебном конверте.

Остальные настройки выполняются пользователем штатно.

4. Рекомендации по настройкам ПП АРМ КБР - Н при направлении ЭС в ОД ОПЕРУ-1 (3 вариант защиты). Данные ЭС предназначены для совершения операция по счетам Федерального казначейства в иностранной валюте.

Настройка точки обмена. Режим «СКАД Сигнатура»

В этой группе параметров необходимо указать атрибуты сертификатов СКАД «Сигнатура», по которым проверяется правомочность использования ключей для конкретных операций, а также варианты защиты ЭС с помощью ЗК:

OID сертификатов клиента:

ЗК 1.3.6.1.4.1.3670.5.10.15

КА 1.3.6.1.4.1.3670.5.10.16

OID сертификатов ЦОИ

ЗК 1.3.6.1.4.1.3670.5.2.3

КА 1.3.6.1.4.1.3670.5.2.4

«Вариант защиты ЭС с помощью ЗК»

Подписание –3 вариант – ЗК на каждое ЭС

Проверка - 2 вариант – ЗК на весь пакет

OID ключа получателя 1.3.6.1.4.1.3670.5.2.4

Режим «Служебный конверт» - реквизиты служебного конверта

«Адрес получателя (ЦОИ)» - uic:4501002000НА.

«Адрес отправителя (АРМ)» – uic:4501002900НА – для Федерального Казначейства (ФК), uic:4501002901НА для Московского Областного Управления Федерального Казначейства (МОУ ФК). УИС Клиента БР должен соответствовать заполненному УИС на закладке «Настройки» «УИС клиента БР(EdAuthor)» (например, 4501002901, соответственно, в этом поле 450100290171, где 71 – номер АРМа).

НА=71 для тестирования на стенде тестирования, НА=70 для промышленной эксплуатации.

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).

Опция «Передавать имя файла» должна быть установлена. Данный признак определяет формирование реквизита «LegacyTransportFileName» в служебном конверте.

Рекомендации по настройкам точек обмена «ТШ КБР» и «Шлюз»

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

Параметры подключения

Протокол – «HTTP»

Маркер формата – XMLEPD

Таймаут операций (с) – 60 с

При использовании **ПО «Cisco AnyConnect»,** предназначенного для установки VPN-соединения, группа «HTTP» содержит параметры:

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

Адрес отправки – - http://172.16.19.211:7777/in

Адрес приема - http://172.16.19.211:7777/get

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

WMQ / Сервер: 172.16.19.221

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)

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

Для работы в промышленном контуре –

Адрес отправки - http://172.16.18.211:7777/in

Адрес приема - http://172.16.18.211:7777/get

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

WMQ / Сервер: 172.16.18.211

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)

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 должны соответствовать учетной записи для подключения к сервисам отправки и получения данных.

На сайте Банка России по адресу www.cbr.ru/development/mcirabis/Involve_EM/ размещены:

«Инструкция по работе ТШ КБР» (при использовании ПО «Cisco AnyConnect»);

«Порядок подключения участников обмена к автоматизированной системе «Транспортный шлюз Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России (ТШ КБР)» с использование средств криптографической защиты каналов DiSec-W» (при использовании СКЗИ DiSec-W).

Режим «Шлюз»

Для возможности работать с использованием протоколов HTTP/IBM MQ необходимо выбрать из списка «Интерфейс с ЦОИ» – «HTTP» или «IBM WebSphere MQ».

При выборе указанных протоколов значения в полях «Выходной ресурс» («Исходящие для АС клиента»/«Входящие для АС клиента») будут заполнены автоматически значением, указанными в точке обмена «ТШ КБР» – «HTTP»/ «IBM WebSphere MQ».

При выборе «Интерфейс с ЦОИ» – «Файловая система», УО может работать через каталоги обмена.

ЦЭПС рекомендует для возможности приема ответных, регламентных и многоадресных ЭС от разных ЦОИ в каждой точке обмена режима «Шлюз» для подгруппы «Входящие для АС клиента» настроить прием на общий каталог.

«Выходной ресурс» – указать путь к общему каталогу, который будет для всех точек обмена одинаковый.

Для возможности принимать и размещать ЭС в разные подкаталоги выбрать:

– «Создавать подкаталоги по адресу From из СК»;

– «Создавать подкаталоги по EDReceiver».

При этом в указанном выходном ресурсе будут сформированы подкаталоги по адресу From и в них будут подкаталоги, сформированные по EDReceiver.

Если УО не использует схему централизованного взаимодействия, то выбирать «Создавать подкаталоги по EDReceiver» не требуется.