Руководителям организаций,
участвующих в электронном обмене с
Банком России
(по списку, кроме ДПУ, ПУ)

Об обновлении программного обеспечения СПФС

Информационное сообщение № ВН-16-4-6-1/4721 от 07.06.2019

Центр эксплуатации платежной системы Департамента информационных технологий (далее – ЦЭПС ДИТ) информирует участников обмена (далее – УО) о следующем:

1. До 28.06.2019 УО должны перейти на использование нового специального криптографического ключа для обмена с системой передачи финансовых сообщений (далее – СПФС).

2. С 07.08.2019 СПФС будет отбраковывать электронные сообщения, подписанные ключами, предназначенными для обмена с платежной системой Банка России (<BaseOID>.15 и <BaseOID>.16 соответственно).

3. В рамках перехода на новый режим обмена в СПФС УО необходимо заблаговременно зарегистрировать новый специальный криптографический ключ, предназначенный для обмена с СПФС, для чего необходимо одновременно с направлением в ГУ по ЦФО/Операционный департамент оформленного со стороны УО дополнительного соглашения к Договору об обмене электронными сообщениями при переводе денежных средств в рамках платежной системы Банка России (далее – Договор) направить в ЦЭПС ДИТ в соответствии с приложением 4 к Договору заявление на изготовление специального криптографического ключа, предназначенного для обмена с СПФС.

Работа по изготовлению ключей начинается только после поступления в ЦЭПС ДИТ информации от ГУ по ЦФО/Операционного департамента о подписании дополнительного соглашения к Договору.

Заявление направляется в ЦЭПС ДИТ через экспедицию Банка России по адресу: Сандуновский переулок, д.3 стр.1 (часы работы: пн-чт. 09:00-17:30. Пт.09:00-16:15, обед: с 12:00-13:00).

Обращаем внимание, что использование УО нового криптографического ключа, предназначенного для обмена в СПФС, допустимо в текущей версии программного обеспечения СПФС.

В приложениях к данному информационному сообщению представлены возможные комбинации комплектов ключей и рекомендации настроек ПК АРМ для различных вариантов защиты при взаимодействии с автоматизированными система Банка России.

4. О тиражировании новой версии ПК АРМ КБР-Н, в которой будет исключена возможность обмена с СПФС, будет сообщено дополнительно.

Данное информационное сообщение будет размещено на сайте Банка России по адресу www.cbr.ru/mcirabis/ в разделе «Информация о работе платежной системы Банка России».

Контактные данные Единой службы поддержки пользователей Департамента информационных технологий:

многоканальный телефон - 8 (495) 957-80-01;

адрес электронной почты - helpdeskmci@cbr.ru

Контактный телефон ЕСПП для консультаций: 8(495)957-80-01

Приложение: 21 лист

Заместитель директора Департамента
информационных технологий –
директор Центра эксплуатации
платежной системы М.Н. Шашлов

Приложение 1

Ключи, необходимые для взаимодействия с СПФС,
при использовании ПК КБР-Н и ПК КБР-СПФС

	АРМ КБР-СПФС	**АРМ КБР-Н**	**АРМ КБР-Н**
Вариант защиты / АС	**I вариант защиты**	**I вариант защиты**	**III вариант защиты**
СПФС	Состав Комплекта: **1 Ключ** **Специальный ключ СПФС** **Подпись+ Шифрование** CN=<*NAME*> OID:1.3.6.1.4.1.10244.7.20.1 *(подпись и шифрование)* **2 Ключа*** Специальный ключ СПФС **Подпись** CN=<*NAME*_ABS> OID:1.3.6.1.4.1.10244.7.20.1 *(только подпись)* Специальный ключ СПФС **Шифрование** CN=<*NAME*> OID:1.3.6.1.4.1.10244.7.20.1 *(только шифрование)* * если ПК АРМ КБР-СПФС используется только для шифрования/расшифрования	**Недопустимо**	**Недопустимо**

Приложение 2

Рекомендации по настройке ПК АРМ КБР-Н

Установка и настройка ПК 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 ПК АРМ КБР-Н, выполняющего функции шифрования, сертификаты оператора, контролера УО, сертификаты ЦОИ (для расшифрования и проверки ЗК/КА).

При переходе на использование ПК 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 ПК КБР-Н

1. Режим «Настройки»

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

OID ключа для загрузки - 1.3.6.1.4.1.3670.5.10.120

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 АС ДКО, ПС СБП, 701 формы – своя.
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.

Сертификаты ЦОИ (ПС БР, АС ДКО, ПС СБП, 701 форма) **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 1.3.6.1.4.1.3670.5.10.323 – АС ДКО

ЗК 1.3.6.1.4.1.3670.5.2.3 - 701 форма

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 1.3.6.1.4.1.3670.5.10.322 – АС ДКО

КА 1.3.6.1.4.1.3670.5.2.4 – 701 форма

2. Рекомендации по настройкам ПК АРМ КБР - Н при направлении электронных сообщений (далее – ЭС) в платежную систему Банка России (1 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:

КА 1.3.6.1.4.1.3670.5.10.15

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 –1 вариант – не формировать ЗК

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 ПК 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 настраиваются в соответствии с рекомендациями п. 2.

4. Рекомендации по настройкам ПК АРМ КБР - Н при направлении ЭС в АС ДКО (ДОФР) (3 вариант защиты).

Настройка точки обмена. Режим «Параметры контроля и мониторинга»

«Входящие для АС клиента»

Признак проверки ЗК/КА, признак проверки варианта защиты должен быть снят.

Остальные настройки выполняются пользователем штатно

Настройка точки обмена. Режим «СКАД Сигнатура»

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 1.3.6.1.4.1.3670.5.10.323

КА 1.3.6.1.4.1.3670.5.10.322

«Вариант защиты ЭС с помощью ЗК»

Подписание –3 вариант – ЗК на каждое ЭС

Проверка - 2 вариант – ЗК на весь пакет

OID ключа получателя 1.3.6.1.4.1.3670.5.10.322

Режим «Служебный конверт» - реквизиты служебного конверта

Режим «Служебный конверт» - реквизиты служебного конверта

«Адрес получателя (ЦОИ)» - uic:5555555888НА

«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=10 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.

5. Рекомендации по настройкам ПК АРМ КБР - Н при направлении ЭС в ПС СБП (В ПС СБП используется 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.

6. Рекомендации по настройкам ПК АРМ КБР - Н для передачи отчетности по форме 0409701 «Отчет об операциях на валютных и денежных рынках» (1 вариант защиты).

Настройка точки обмена.

Режим «Контроль» - параметры контроля и мониторинга

«Исходящие от АС Клиента»*

«Проверка ЗК\КА» установить «V». Для компонент «Валидация», «Проверка варианта защиты» значение «V» отсутствует.

«Входящие для АС Клиента» рекомендовано установить «V» на компонентах «Валидация», «Проверка ЗК\КА», «Проверять вариант защиты».

Режим «СКАД Сигнатура»

OID сертификатов клиента:

КА 1.3.6.1.4.1.3670.5.10.15 или 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 –1 вариант – Не формировать ЗК

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:f701

«Адрес отправителя (АРМ)» – uic:XXXXXXXXXXHA, 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).

HA=11 для тестирования на стенде тестирования, HA=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).

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

Остальные настройки выполняются пользователем штатно

*Требования к имени файла:
символы 1-5 имени файла – символы 5-9 БИК банка;

символы 6-8 имени файла – номер дня в году, за который посылается отчет;

символ 9 имени файла – «.»;

символ 10 имени файла – последняя цифра номера года, за который посылается отчет;

символы 11-12 имени файла – «f0»

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

Режим «СВК/ТШ КБР»

1. Параметры подключения:

– «Протокол» – «HTTP»

– «Маркер формата» – XMLEPD

– «Попыток отправки» – количество повторных попыток отправки ЭС при

возникновении ошибок передачи данных в СВК устанавливается пользователем штатно;

Параметры протокола HTTP:

– «Адрес отправки» – адрес сервера СВК/ТШ КБР для отправки ЭС;

– «Адрес приема» – адрес сервера СВК/ТШ КБР для приема ЭС.

2. Параметры аутентификации:

– «Прикладная аутентификация»:

– указывается «Имя пользователя» и «Пароль». Данные значения должны соответствовать учетной записи для подключения к сервисам отправки и получения данных.

Режим «Шлюз»

Для возможности работать с использованием протокола HTTP необходимо выбрать из списка «Интерфейс с ЦОИ» – «СВК.HTTP».

При выборе данного протокола значения в полях «Выходной ресурс»

«Исходящие для АС клиента»/«Входящие для АС клиента») будут заполнены автоматически значением, указанными в точке обмена «СВК/ТШ КБР» –«HTTP».

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

каталоги обмена с использованием СПО УТА.

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.

Приложение 3

Рекомендации по настройкам АРМ КБР

Установка и настройка ПК АРМ КБР производится в соответствии с разделом 4 и 5 документа "Автоматизированное рабочее место клиента Банка России. Руководство администратора".

Варианты конфигурационных настроек приведены в документе «Автоматизированное рабочее место клиента Банка России. Руководство администратора» – в разделе «Возможные варианты конфигурации».

ЦЭПС обращает внимание УО, что использование разных вариантов защиты ЭС на одном ПК АРМ КБР не предусмотрено.

Для использования разных вариантов защиты исходящих ЭС от УО при обмене с разными автоматизированными системами (платежная система, СПФС, АС ДКО, ПС СБП) ЦЭПС рекомендует устанавливать ПК АРМ КБР на разных ПЭВМ или на одной ПЭВМ, но в разные директории. При этом одновременная работа двух экземпляров ПК АРМ КБР под одним пользователем невозможна. УО может запускать ПК АРМ КБР, установленный в разные каталоги, попеременно под одним пользователем, либо запускать ПК АРМ КБР под разными пользователями.

1. Общие параметры программного комплекса

«Режим работы»: рекомендуем использовать комбинированный или автоматический

«НСИ и контроль» заполняются штатно для клиента

Параметры ручного ввода:

Рекомендуем включить опцию Всемирное время «Выполнять преобразование».

Реквизиты служебного конверта:

- **для тестирования**

адрес получателя (ЦОИ): *uic:458300199911;*

адрес отправителя АРМ – uic:XXXXXXXXXXHA, где XXXXXXXXXX - УИС клиента БР должен соответствовать заполненному УИС на закладке «Реквизиты

организации клиента БР» (например 4525505000, соответственно в этом поле 452550500***11, где 11 – номер АРМа***);.

- **для промышленной эксплуатации**
адрес получателя (ЦОИ): *uic: 458300199900;*

адрес отправителя АРМ – uic:XXXXXXXXXXHA, где XXXXXXXXXX - УИС клиента БР должен соответствовать заполненному УИС на закладке «Реквизиты организации клиента БР» (например 4525505000, соответственно в этом поле 452550500***00***, ***где 00 – номер АРМа***);.

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).

2. Настройки, связанные с использованием СКАД Сигнатура

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

а. Рекомендации по настройке ПК АРМ КБР при использовании криптографических ключей, которые выпускаются для третьего варианта защиты, и могут быть использованы в действующей схеме, при использовании первого варианта защиты при направлении ЭС в платежную систему Банка России и ЦОС (до 07.08.2019 - до использования специального криптографического ключа, предназначенного для взаимодействия с ЦОС) (1 вариант защиты).

Работа в ПК АРМ КБР осуществляется пользователями с функциональными ролями «Оператор» и «Контролёр» с соответствующими ключевыми документами **PROCESSING и CONTROL** соответственно. Необходимо импортировать в локальный справочник сертификатов контролера сертификаты оператора, сертификаты КОИ, ЦОС.

Комплект ключей:

Формирование ЗК

CN=PROCESSING

OID расширенная область применения ключа - 1.3.6.1.4.1.3670.5.10.15

Область применения ключа: Электронная подпись.

Формирование КА и шифрование

CN=CONTROL

OID расширенная область применения ключа 1.3.6.1.4.1.3670.5.10.16

Область применения ключа: Электронная подпись, Шифрование ключа, Шифрование данных.

Настройки, связанные с использованием СКАД Сигнатура:

Списки OID используемых ключей:

Формирование КА 1.3.6.1.4.1.3670.5.10.15

Проверка ЗК

1.3.6.1.4.1.3670.5.10.7 – КОИ

1.3.6.1.4.1.3670.5.10.27 – ЦОС

Проверка КА

1.3.6.1.4.1.3670.5.10.8 - КОИ

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.

«Вариант защиты ЭС с помощью ЗК»

Подписание –1 вариант – Не формировать ЗК

Проверка - 2 вариант – ЗК на весь пакет

OID ключа получателя 1.3.6.1.4.1.3670.5.10.8

Обращаем внимание, что в данном случае **настройка машинно-зависимых параметров ПК АРМ КБР должна быть выполнена следующим образом:**

Настройка группы параметров «Обработка ЭС»:

Для пользователя с функциональной ролью «Оператор» должен быть установлен признак запуска на следующих компонентах:

Запускать:

«Входной контроль ЭС, поступивших из АС клиента»;

«Формирование КА»;

«Проверка КА/ЗК».

Для пользователя с функциональной ролью «Контролер» должен быть установлен признак запуска на следующих компонентах:

Запускать:

«Отправка ЭС»;

«Прием ЭС».

«Валидация» – галочки должны стоять на каждой закладке,

Для «Строгой валидации» - галочки должны стоять везде, **кроме компоненты**

«Прием сообщений».

б. Рекомендации по настройке ПК АРМ КБР при использовании криптографических ключей, которые выпускаются для третьего варианта защиты, и могут быть использованы в действующей схеме, при использовании первого варианта защиты (с использованием ключа CN=ARMKBRN) при направлении в платежную систему Банка России и ЦОС (до 07.08.2019 - до использования специального криптографического ключа, предназначенного для взаимодействия с ЦОС) (1 вариант защиты).

Работа в ПК АРМ КБР осуществляется пользователями с функциональными ролями «Оператор» и «Контролёр» с соответствующими ключевыми документами **PROCESSING и ARMKBRN** соответственно. Необходимо импортировать в локальный справочник сертификатов контролера сертификаты оператора, сертификаты КОИ, ЦОС.

Комплект ключей:

Формирование ЗК
CN=PROCESSING

OID расширенная область применения ключа - 1.3.6.1.4.1.3670.5.10.15

Область применения ключа: Электронная подпись.

Шифрование

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

Настройки, связанные с использованием СКАД Сигнатура:

Списки OID используемых ключей:

Формирование КА 1.3.6.1.4.1.3670.5.10.15

Проверка ЗК

1.3.6.1.4.1.3670.5.10.7 – КОИ

1.3.6.1.4.1.3670.5.10.27 – ЦОС

Проверка КА

1.3.6.1.4.1.3670.5.10.8 - КОИ

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.

«Вариант защиты ЭС с помощью ЗК»

Подписание –1 вариант – Не формировать ЗК

Проверка - 2 вариант – ЗК на весь пакет

OID ключа получателя 1.3.6.1.4.1.3670.5.10.8

Обращаем внимание, что в данном случае **настройка машинно-зависимых параметров ПК АРМ КБР должна быть выполнена следующим образом:**

Настройка группы параметров «Обработка ЭС»:

Для пользователя с функциональной ролью «Оператор» должен быть установлен признак запуска на следующих компонентах:

Запускать:

«Входной контроль ЭС, поступивших из АС клиента»;

«Формирование КА»;

«Проверка КА/ЗК».

Для пользователя с функциональной ролью «Контролер» должен быть установлен признак запуска на следующих компонентах:

Запускать:

«Отправка ЭС»;

«Прием ЭС».

«Валидация» – галочки должны стоять на каждой закладке,

Для «Строгой валидации» - галочки должны стоять везде, **кроме компоненты**

«Прием сообщений».

в. Рекомендации по настройке ПК АРМ КБР на третий вариант защиты при использовании криптографических ключей, предназначенных для третьего варианта защиты при направлении ЭС в платежную систему Банка России, АС ДКО и ПС СБП (3 вариант).

Работа в ПК АРМ КБР осуществляется пользователями с функциональными ролями «Оператор» и «Контролер» с соответствующими ключевыми документами.

Необходимо импортировать в локальный справочник сертификатов контролера

сертификаты оператора, сертификаты ЦОИ, АС ДКО, СБП.

Комплект ключей:

Формирование ЗК

CN=PROCESSING

OID расширенная область применения ключа - 1.3.6.1.4.1.3670.5.10.15

Область применения ключа: Электронная подпись.

Формирование КА и шифрование

CN=CONTROL

OID расширенная область применения ключа 1.3.6.1.4.1.3670.5.10.16

Область применения ключа: Электронная подпись, Шифрование ключа, Шифрование данных.

Настройки, связанные с использованием СКАД Сигнатура.

Списки OID используемых ключей:

Формирование ЗК 1.3.6.1.4.1.3670.5.10.15

Формирование КА 1.3.6.1.4.1.3670.5.10.16

Проверка ЗК

1.3.6.1.4.1.3670.5.10.7 - КОИ

1.3.6.1.4.1.3670.5.10.123- ПС СБП

1.3.6.1.4.1.3670.5.10.323 – АС ДКО

Проверка КА

1.3.6.1.4.1.3670.5.10.8 - КОИ

1.3.6.1.4.1.3670.5.10.124- ПС СБП

1.3.6.1.4.1.3670.5.10.322 – АС ДКО

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

«Вариант защиты ЭС с помощью ЗК»

Подписание –3 вариант – ЗК на каждое ЭС

Проверка - 2 вариант – ЗК на весь пакет

OID ключа получателя 1.3.6.1.4.1.3670.5.10.8

Настройка машинно-зависимых параметров ПК АРМ КБР

Настройка группы параметров «Обработка ЭС»:

Для пользователя с функциональной ролью «Оператор» должен быть установлен признак запуска на следующих компонентах:

Запускать:

«Входной контроль ЭС, поступивших из АС клиента»;

«Формирование ЗК»;

«Проверка КА/ЗК».

Для пользователя с функциональной ролью «Контролер» должен быть установлен признак запуска на следующих компонентах

Запускать:

«Формирование КА»;

«Отправка ЭС»;

«Прием ЭС».

Все варианты конфигурационных настроек приведены в документе

«Автоматизированное рабочее место клиента Банка России. Руководство администратора» –

в разделе «Возможные варианты конфигурации» (см. варианты конфигурации с простановкой ЗК и КА).

3. Обмен с ДОФР

Если УО производит обмен ЭС с Департаментом операций на финансовых рынках (ДОФР) Банка России:

– ***Производить обмен с ДОФР Банка России*** – должен быть установлен признак, при установке которого становится доступен обмен ЭС со ДОФР Банка России.

– ***УИС ДОФР БР*** – уникальный идентификатор составителя для ДОФР БР. Равен значению «5555555888»

– ***Логический адрес ДОФР БР*** – логический адрес, используемый при формировании служебного конверта для отправки в ДОФР Банка России;

- **для тестирования**

логический адрес ДОФР: *uic:555555588811;*

- **для промышленной эксплуатации**

логический адрес ДОФР: *uic:555555588810;*

OID ключа ДОФР 1.3.6.1.4.1.3670.5.10.322

4. Обмен с ЦОС

Если УО производит обмен ЭС с ЦОС:

– ***Производить обмен с ЦОС*** – должен быть установлен признак, при установке которого становится доступен обмен ЭС с ЦОС;

Логический адрес ЦОС

- **для тестирования**

логический адрес ЦОС: *uic:777777700**11;***

- **для промышленной эксплуатации**

логический адрес ЦОС: *uic:777777700000;*

OID ключа ЦОС 1.3.6.1.4.1.3670.5.10.28

Настройки, связанные с использованием собственных форматов

Данная группа параметров определяет работу компонентов ПК «Шлюз»: «Формирование ED501» и «Приём ED501». Содержит следующие параметры:

Запускать – признак запуска данного компонента пользователем, имеющим функциональную роль «Оператор» или «Контролер», соответственно;

«***Формирование ed501***» В каталог для входа помещается файл в любом виде, он будет преобразован в base64 и на его основе будет сформирован ed501.

Имя файла сообщения в собственных форматах УЭО должно быть следующим:

<УИС получателя>[0-9]{10}<уникальный в течение операционного дня для УИС номер>[0-9]{9}.ED501,

где [0-9] – набор допустимых символов, в данном случае – цифры от 0 до 9,

{10}, {9} – длина поля.

Атрибуты ed501 ActualReceiver и Edno формируются следующим образом:

ActualReceiver берется из имени файла **<УИС получателя[10]>**. Поэтому имя файла должно содержать корректное значение УИС получателя, в противном случае сформированный ed501 будет забракован на этапе логического контроля.

EdNo берется из имени файла **<уникальный в течение ОД для УИС номер [0-9][9]>**.

«***Прием ed501***» ожидает на входе файл в формате SigEnvelope с выхода компоненты шлюза «Проверка КА/ЗК». Если включен флажок «Помещать принятые ЭС в подкаталоги», то после преобразования полученные файлы раскладываются по подкаталогам в соответствии со значением поля ActualReceiver.

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.

Настройки, связанные с использованием SWIFT форматов

На закладке «Обработка SWIFT»

Данная группа параметров определяет работу компонентов ПК «Шлюз»: «Формирование ED503» и «Приём ED503». Содержит следующие параметры:

«***Формирование ed503***» В каталог для входа помещается файл в SWIFT формате, на его основе будет сформирован ed503.

«***Прием ed503***» ожидает на входе файл в формате SigEnvelope с выхода компоненты шлюза «Проверка КА/ЗК». Если включен флажок «Помещать принятые ЭС в подкаталоги», то после преобразования полученные файлы раскладываются по подкаталогам в соответствии со значением поля ActualReceiver.

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.

Если в конфигурации установлен параметр «Добавлять в квитанции исходное сообщение», то при получении из ЦОС ЭСИС о состоянии конверта, формируется SWIFT-извещение для всех сообщений формата SWIFT прошедших контроль в составе конверта и дополняется блоками 1-5 исходного сообщения.

Если в конфигурации установлен параметр «Формировать уникальные идентификаторы», то будет осуществляться программное заполнение полей «номер сессии» и «номер последовательности» блока 1 сообщения формата SWIFT

Полученное SWIFT-сообщение (с разделами {3:}{4: -}{5:} либо {1:}{2:}{3:}{4: -}{5:}) передается в АС клиента Банка России.

УО может с помощью собственной АС формировать текстовые файлы, содержащие документы в формате SWIFT, и подавать их на дальнейшую обработку в ПК АРМ КБР. Текстовые файлы должны удовлетворять требованиям уникальности имени файла в ечение операционного дня и содержать информационные блоки {1:}{2:}{3:}{4: -}{5:}.

5. **Обмен с ПС СБП**

Если УО производит обмен ЭС с ПС СБП:

– ***Производить обмен с ПС СБП*** – должен быть установлен признак, при установке которого становится доступен обмен ЭС с ПС СБП;

Логический адрес ЦОС

- **для тестирования**

логический адрес ЦОиР СБП: uic:451111111111*;*

- **для промышленной эксплуатации**

логический адрес ЦОиР СБП uic:451111111100*;*

OID ключа ЦОС 1.3.6.1.4.1.3670.5.10.124

Приложение 4

Рекомендации по настройкам ПК АРМ КБР - СПФС

Установка и настройка ПК АРМ КБР-СПФС производится в соответствии с документами «Автоматизированное рабочее место клиента Банка России пользователя системы передачи финансовых сообщений. Руководство по установке и настройке» и «Автоматизированное рабочее место клиента Банка России пользователя системы передачи финансовых сообщений. Руководство администратора».

ЦЭПС обращает внимание УО, что все входящие ЭС, направляемые клиентом в Центр обработки сообщений 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 ПК 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 программного комплекса

«Режим работы»: рекомендуем использовать комбинированный или автоматический

«НСИ и контроль»:

Рекомендуем установить:

- «Автоматический импорт ED574»

- опцию Всемирное время «Выполнять преобразование».

УИС получателя (ЦОС) – 7777777000

Язык интерфейса (language) – русский.

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 4525505000, соответственно в этом поле 4525505000HA*, где HA – номер АРМа - 11 или 63*);.

- для промышленной эксплуатации

адрес получателя (ЦОИ): *uic:777777700000;*

адрес отправителя АРМ – uic:XXXXXXXXXXHA, где XXXXXXXXXX - УИС клиента БР должен соответствовать заполненному УИС на закладке «Реквизиты организации» (например 4525505000, соответственно в этом поле 4525505000HA, *где HA – номер АРМа -00 или 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»

2. 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 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

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 ПК АРМ КБР-СПФС 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.

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

3. Настройки, связанные с обработкой сообщений

Блоки настроек «обработка УФЭБС», «обработка SWIFT», «обработка собственных форматов» могут заполняться штатно.

Для блока «обработка собственных форматов» в каталог для входа необходимо помещать файл, имя которого должно быть следующим:

<УИС получателя>[0-9]{10}<уникальный в течение операционного дня для УИС номер>[0-9]{9}.ED501, где [0-9] – набор допустимых символов, в данном случае – цифры от 0 до 9, {10}, {9} – длина поля.

Атрибуты ed501 ActualReceiver и Edno формируются следующим образом:

ActualReceiver берется из имени файла <УИС получателя[10]>. Поэтому имя файла должно содержать корректное значение УИС получателя, в противном случае сформированный ed501 будет забракован на этапе логического контроля.
EdNo берется из имени файла <уникальный в течение ОД для УИС номер [0-9][9]>.

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

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.

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.

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

Режим «СВК/ТШ КБР»

1. Параметры подключения:

– «Протокол» – «HTTP»

– «Маркер формата» – XMLEPD

– «Попыток отправки» – количество повторных попыток отправки ЭС при возникновении ошибок передачи данных в СВК устанавливается пользователем штатно;

Параметры протокола HTTP:

– «Адрес отправки» – адрес сервера СВК/ТШ КБР для отправки ЭС;

– «Адрес приема» – адрес сервера СВК/ТШ КБР для приема ЭС.

2. Параметры аутентификации: – «Прикладная аутентификация»:

– указывается «Имя пользователя» и «Пароль». Данные значения должны соответствовать учетной записи для подключения к сервисам отправки и получения данных.

Режим «Транспорт»

Для возможности работать с использованием протокола HTTP необходимо выбрать из списка – «СВК.HTTP», предварительно установив галку «Передача в транспорт. Протокол» и «Прием из транспорта. Протокол».