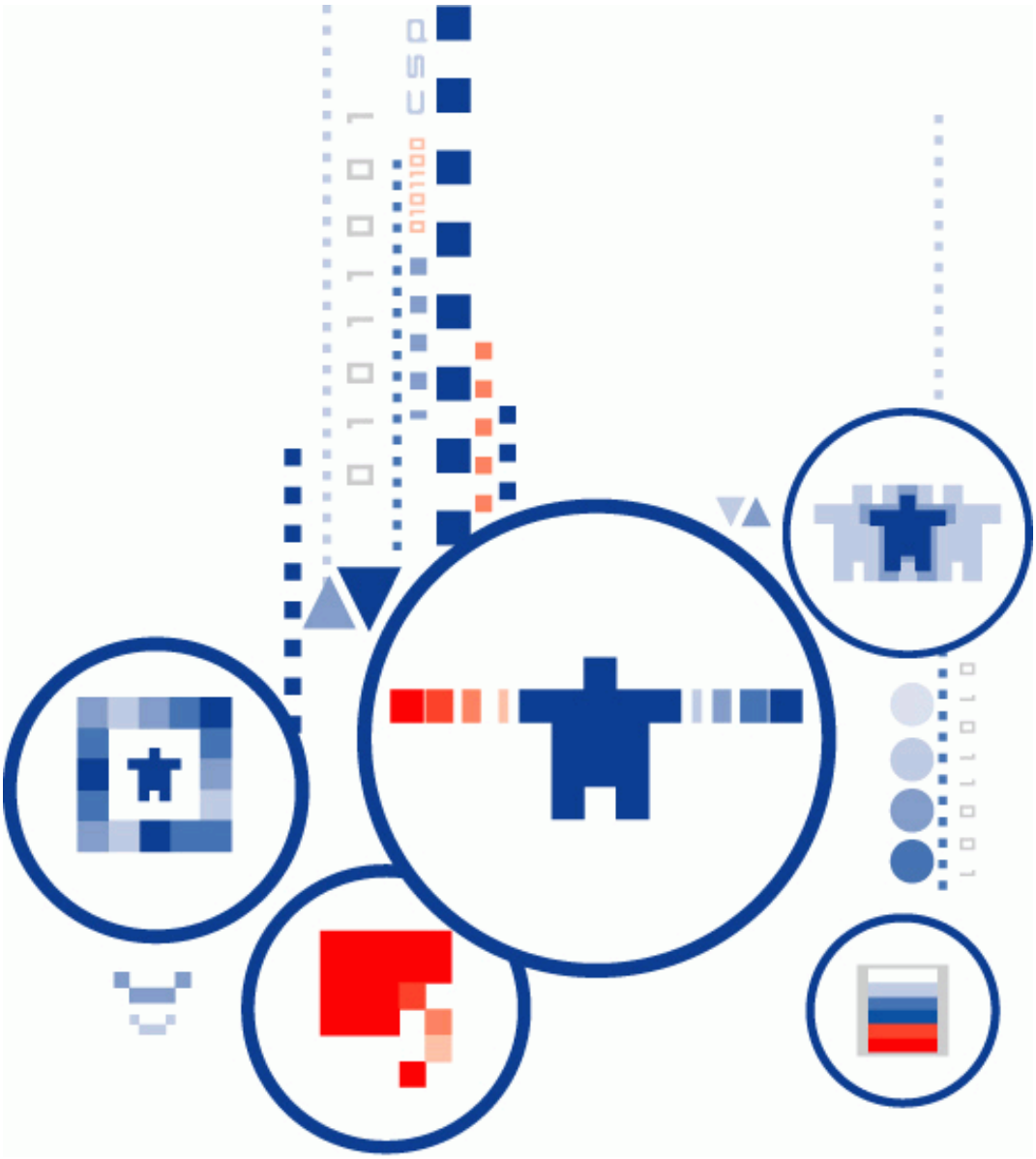

Сервер Электронной Подписи

«КриптоПро DSS»

Компонент ПАКМ «КриптоПро HSM»

Конкретизированные правила изготовления и использования векторов аутентификации и пользовательских ключей

СОДЕРЖАНИЕ

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

KID	—	Идентификатор ветора аутентификации (12-значный код)
АРМ	—	Автоматизированное рабочее место
АС	—	Автоматизированная система
БД	—	База данных
ВСП	—	Внутреннее структурное подразделение
ЕПК	—	
ЕСИА	—	Единая система идентификации и аутентификации
КСКП ЭП	—	Квалифицированный сертификат ключа проверки электронной подписи
МУ	—	Мобильное устройство
СМЭВ	—	Система межведомственного электронного взаимодействия
СОС	—	Список отозванных сертификатов
СЭП	—	Сервер электронной подписи
ПУЗ	—	Полная учетная запись
УЗ	—	Учетная запись
УЦ	—	Удостоверяющий Центр
ФГН	—	
ФЛ	—	Физическое лицо
ФЛК	—	
ЭП	—	Электронная подпись

1. Аннотация

Настоящий документ содержит конкретизированные правила изготовления и использования векторов аутентификации и пользовательских ключей при разработке систем с использованием исполнения «Сбербанк myDSS SDK» Комплектации 3 ПАКМ «КриптоПро HSM» версия 2.0 («КриптоПро DSS»).

2. Процесс очной идентификации и проверки данных ФЛ

Рисунок 1 — Схема процесса для очной идентификации и проверки данных ФЛ

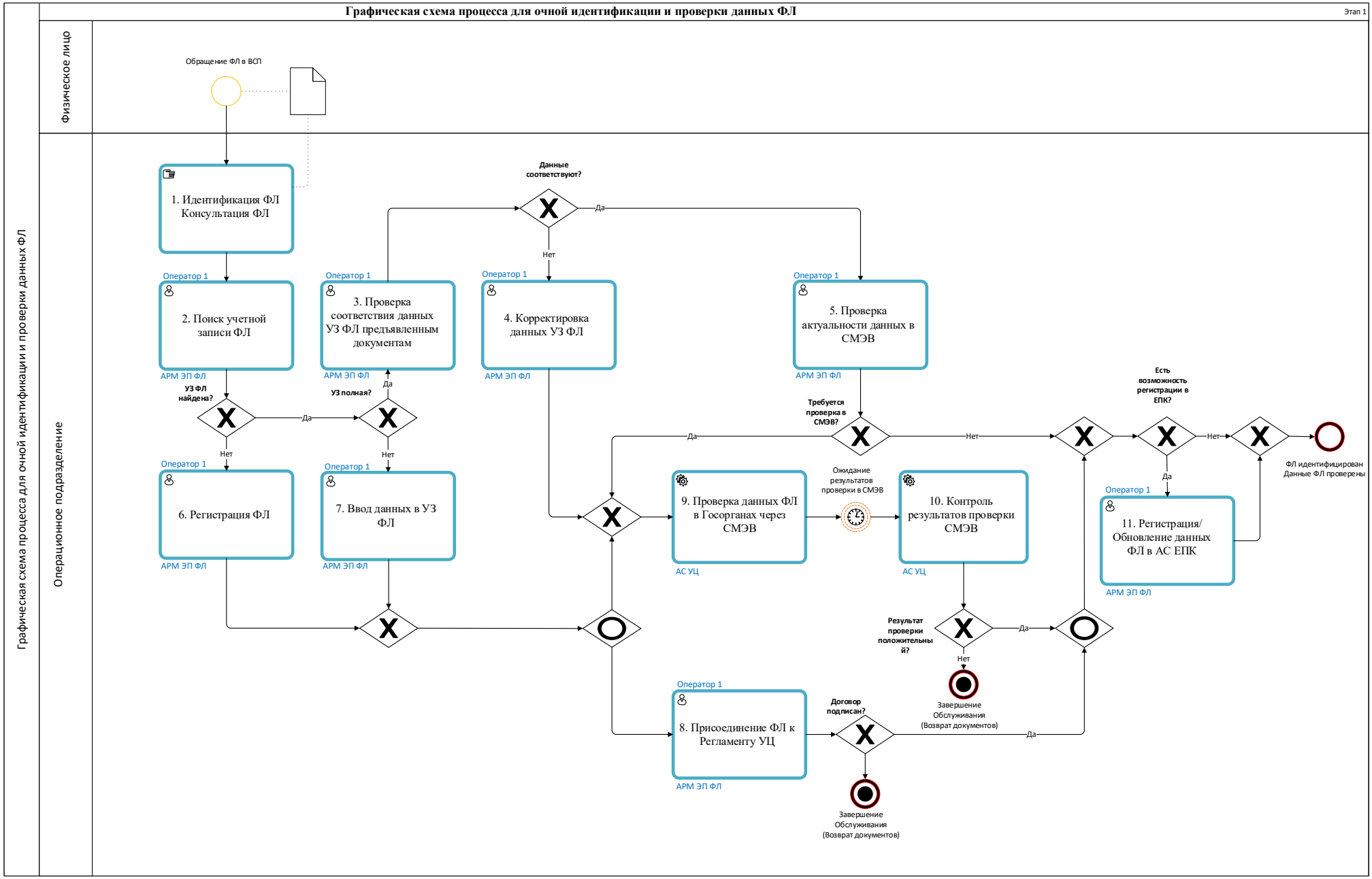

Таблица 1 — Описание процесса очной идентификации ФЛ и проверки данных

№ п/п	Операция	Входной документ/информация	Описание	Исполнитель	Продолжительность	Выходной документ	ИТ система	Переход к пункту и условие перехода
1.	Идентификация ФЛ. Проверка документов	Комплект документов: документ, удостоверяющий личность, СНИЛС, ИНН, доверенность, подтверждающая полномочия Представителя ФЛ	Сотрудник ВСП: 1. Осуществляет идентификацию Заявителя по документу, удостоверяющему личность. В случае, если лицо действует по поручению другого ФЛ, получение от лица, выступающего от имени ФЛ, нотариально заверенной доверенности с правом обращаться за получением ключа и сертификата ЭП. 2. Консультирует по вопросам применения средств ЭП, об этапах процесса сертификации, о необходимости подписи документов (Заявление в УЦ, Договор о присоединении к Регламенту УЦ, Расписка об ознакомлении с сертификатом). 3. Предлагает использовать шифровальные (криптографические) средства для последующего проведения идентификации без его личного присутствия и указывает страницу сайта в информационно-телекоммуникационной сети "Интернет", с которой безвозмездно предоставляются эти средства. 4. Осуществляет первичную проверку документов.	Сотрудник ВСП	-	Комплект документов	-	**2**
2.	Поиск учетной записи ФЛ	СНИЛС, ДУЛ, ДР	Сотрудник ВСП с ролью Оператор в АРМ ЭП ФЛ, средствами АРМ ЭП ФЛ, осуществляет поиск учетной записи ФЛ (УЗ ФЛ) в БД УЦ и в БД ЕПК: • поиск УЗ в БД УЦ осуществляется по СНИЛС; • поиск УЗ в БД ЕПК осуществляется по ФИО, ДУЛ, ДР; Сотрудник ВСП проверяет, является ли найденная учетная запись полной - ПУЗ[1]	Сотрудник ВСП	-	Результат поиска	АРМ ЭП ФЛ	**3** Найдена ПУЗ **7** Найдена неполная УЗ ФЛ **6** УЗ ФЛ не найдена

[1] ПУЗ содержит данные, необходимые для выпуска КСКП ЭП и признак присоединения ФЛ к Регламенту УЦ.

№ п/п	Операция	Входной документ/информация	Описание	Исполнитель	Продолжительность	Выходной документ	ИТ система	Переход к пункту и условие перехода
3.	Проверка соответствия данных УЗ ФЛ предъявленным документам	Результат поиска Комплект документов УЗ ФЛ	Сотрудник ВСП осуществляет сверку данных, найденной в результате поиска УЗ ФЛ, на соответствие предъявленным документам.	Сотрудник ВСП	-	УЗ ФЛ	АРМ ЭП ФЛ	**4** Данные не соответствуют **5** Данные соответствуют
4.	Корректировка данных УЗ ФЛ	УЗ ФЛ Комплект документов	Сотрудник ВСП производит корректировку данных в соответствии с предъявленными документами. Сохраняет внесенные изменения в УЗ ФЛ. Загрузка сканкопий первичных документов	Сотрудник ВСП	-	УЗ ФЛ	АРМ ЭП ФЛ	**9**
5.	Проверка актуальности данных в УЗ ФЛ	УЗ ФЛ Комплект документов	Сотрудник ВСП проверяет наличие указания АРМ на необходимость повторной проверки данных в Госорганах.	Сотрудник ВСП	-	Электронный запрос проверки данных УЗ ФЛ	АРМ ЭП ФЛ	**9** Проверка в СМЭВ требуется **11** Проверка в СМЭВ не требуется, есть возможность регистрации в АС ЕПК **Процесс завершен** Проверка в СМЭВ и регистрация в ЕПК не требуются

№ п/п	Операция	Входной документ/информация	Описание	Исполнитель	Продолжительность	Выходной документ	ИТ система	Переход к пункту и условие перехода
6.	Регистрация ФЛ	Результат поиска в БД УЦ и БД ЕПК Комплект документов	Сотрудник ВСП в АРМ ЭП ФЛ создает учетную запись ФЛ на основе данных, полученных из АС ЕПК либо вводит и сохраняет информацию о ФЛ в соответствии с предъявленными документами. Загружает сканкопии первичных документов. • Инициирует проверку данных в госорганах через СМЭВ; • Инициирует процесс присоединения ФЛ к Регламенту УЦ;	Сотрудник ВСП	-	УЗ ФЛ Электронный запрос проверки данных	АРМ ЭП ФЛ	**8 и 9**
7	Ввод данных в УЗ ФЛ	УЗ ФЛ Комплект документов	Сотрудник ВСП, согласно предъявленным документам, корректирует и сохраняет данные УЗ ФЛ (СНИЛС, ИНН, ДУЛ, ФИО) и проверяет наличие подписанного Договора о присоединении к Регламенту УЦ. Если ФЛ уже присоединен к Регламенту УЦ, инициирует только проверку данных ФЛ в госорганах через СМЭВ.	Сотрудник ВСП	-	УЗ ФЛ Электронные Запросы проверки данных	АРМ ЭП ФЛ	**9** Присоединен к регламенту УЦ **8** Требуется присоединение к регламенту УЦ **8 и 9** Требуется проверка в СМЭВ и присоединение к Регламенту УЦ

№ п/п	Операция	Входной документ/информация	Описание	Исполнитель	Продолжительность	Выходной документ	ИТ система	Переход к пункту и условие перехода
8.	Присоединение ФЛ к Регламенту УЦ	Электронное текстовое представление Договора о присоединении к Регламенту УЦ	Сотрудник ВСП распечатывает Договор о присоединении к Регламенту УЦ и передает его ФЛ на подпись. Если ФЛ/Представитель ФЛ отказывается подписывать договор, обслуживание прерывается, происходит возврат документов ФЛ.	Сотрудник ВСП И ФЛ/ Представитель ФЛ	-	Подписанный Договор присоединения к Регламенту УЦ	АРМ ЭП ФЛ	**11** Договор подписан, есть возможность регистрации в АС ЕПК **Процесс завершен** Договор подписан и регистрация в ЕПК не требуются **Обслуживание завершено** Договор не подписан
9.	Проверка данных ФЛ в Госорганах через СМЭВ	УЗ ФЛ	Проверка паспортных данных, СНИЛС, данных ИНН в государственных системах, формирование запросов с использованием СМЭВ[2].	-	-	Электронные Запросы проверки данных	АРМ ЭП ФЛ АС УЦ СМЭВ	**10**
10.	Контроль результатов проверки СМЭВ	Электронные Ответы проверки данных	Проверка паспортных данных, СНИЛС, данных ИНН в государственных системах, получение ответов на запросы с использованием СМЭВ. Если результат проверки данных СМЭВ отрицательный, обслуживание прерывается, происходит возврат документов ФЛ.	-	-	Результат проверки	АРМ ЭП ФЛ АС УЦ СМЭВ	Ожидание подписания Договора присоединения к регламенту УЦ и/или **Завершение процесса,** если результат проверки положительный

[2] Если ответ из СМЭВ не получен во время присутствия ФЛ в ВСП, то при формировании запроса на выпуск КСКП ЭП срок начала действия сертификата указывается + 24 часа.

№ п/п	Операция	Входной документ/информация	Описание	Исполнитель	Продолжительность	Выходной документ	ИТ система	Переход к пункту и условие перехода
11.	Регистрация/Обновление данных ФЛ в АС ЕПК	УЗ ФЛ	Если на момент идентификации ФЛ информация о ФЛ в АС ЕПК отсутствовала, то система предлагает зарегистрировать ФЛ в АС ЕПК. Сотрудник ВСП осуществляет регистрацию ФЛ в АС ЕПК. Если на момент идентификации ФЛ УЗ в АС ЕПК была найдена и были внесены изменения по данным ФЛ (ФИО, ДУЛ, ИНН и СНИЛС), при этом получены положительные результаты проверок в госорганах, система предлагает произвести обновление данных в АС ЕПК. Сотрудник ВСП инициирует процесс обновления данных в АС ЕПК.	Сотрудник ВСП	-	УЗ ФЛ	АРМ ЭП ФЛ АС ЕПК	-

3. Процесс выпуска КСКП ЭП при очной идентификации ФЛ с использованием «Облачного» сервиса ЭП

Рисунок 2 — Схема процесса выпуска КСКП ЭП при очной идентификации ФЛ с использованием «Облачного» сервиса ЭП

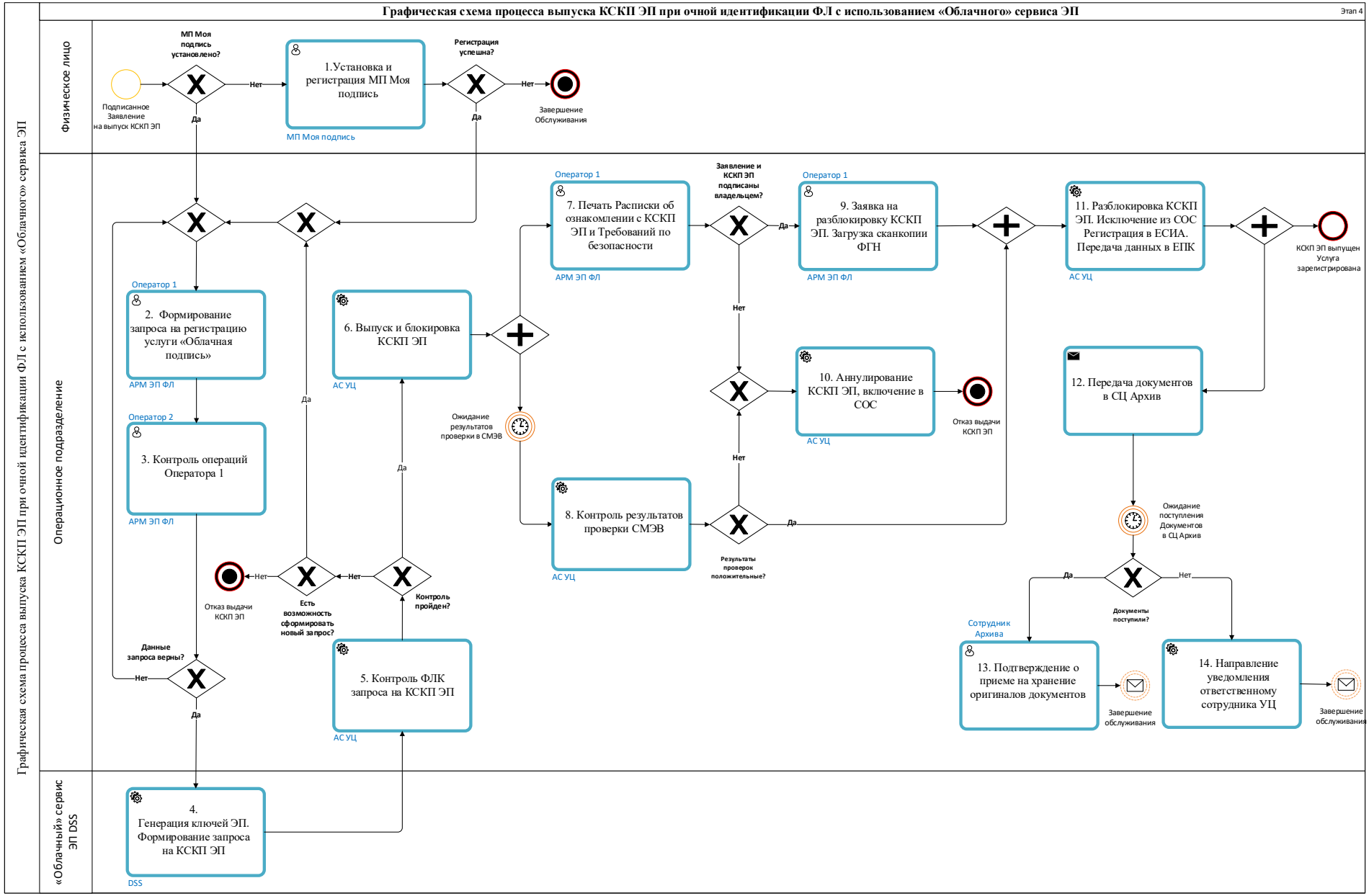

Таблица 2 — Описание процесса генерации ключей ЭП с использованием «Облачного» сервиса ЭП и выпуска КСКП ЭП при очной идентификации

№ п/п	Операция	Входной документ/информация	Описание	Исполнитель	Продолжительность	Выходной документ	ИТ система	Переход к пункту и условие перехода
1.	Установка и регистрация МП Моя подпись	МП Моя подпись в App Store Play Market	При выборе в качестве хранилища ЭП – «Облачный» сервис ЭП, ФЛ скачивает и устанавливает на своем личном мобильном устройстве МП «Моя подпись». При первом входе в МП «Моя подпись» происходит регистрация мобильного устройства в DSS, формируется KID[3], который необходимо сообщить/продемонстрировать на экране Сотруднику ВСП. **Примечание:** Срок действия вектора аутентификации ФЛ — 3 года. Ответственность за генерацию векторов аутентификации и их распространение/ использование несет ПАО «Сбербанк».	ФЛ	-	KID	МП Моя подпись	**2** МП Моя подпись установлено **Завершение обслуживание** МП Моя подпись не установлено
2.	Формирование запроса на регистрацию услуги «Облачная подпись»	Подписанное Заявление на выпуск КСКП ЭП KID	Сотрудник ВСП в УЗ ФЛ назначает Бизнес-услугу «МП Моя подпись». Формирует запрос на регистрацию услуги «Облачная подпись», в запросе проверяет наличие и корректность данных, необходимых для выпуска КСКП ЭП, включает в запрос дополнительные данные - KID и ID ЕПК.	Оператор 1	-	Запрос на регистрацию услуги	АРМ ЭП ФЛ	**3**
3.	Контроль операций Оператора 1	Запрос на регистрацию услуги	Руководитель Сотрудника ВСП, с ролью «Оператор 2» в АРМ ЭП ФЛ, сверяет данные в запросе, согласно предоставленным документам ФЛ и KID на мобильном устройстве ФЛ. Подтверждает запрос свой ЭП.	Оператор 2	-	Запрос на регистрацию услуги	АРМ ЭП ФЛ	**2** Ошибка данных в запросе **4** Данные запроса верны
4.	Генерация ключа ЭП. Формирование запроса на КСКП ЭП	Запрос на регистрацию услуги	Регистрация ФЛ в «Облачном» сервисе ЭП DSS: • создание УЗ пользователя DSS (логин УЗ пользователя DSS = ID ЕПК); • поиск по KID и привязка мобильного устройства к УЗ DSS; • генерация ключа ЭП; • формирование и передача запроса на выпуск КСКП ЭП в УЦ Банка	DSS	-	Файл Запроса на КСКП ЭП	DSS	**5**

[3] KID – Идентификатор вектора аутентификации (12-значный код)

№ п/п	Операция	Входной документ/информация	Описание	Исполнитель	Продолжительность	Выходной документ	ИТ система	Переход к пункту и условие перехода
5.	Контроль ФЛК запроса на КСКП ЭП	Файл Запроса на КСКП ЭП	Автоматическая функция АС УЦ по форматно-логическому контролю Запроса, его целостности, извлечению из него ключа проверки ЭП, и поиска его дубликата в реестре УЦ. В случае обнаружения дубликата ключа проверки ЭП, ФЛ потребуется повторная процедура генерации ключей ЭП, создания запроса на КСКП ЭП	АС УЦ	-	Файл Запроса на КСКП ЭП	АС УЦ	**6** ФЛК пройден **2** ФЛК не пройден и есть возможность сформировать новый запрос на выпуск КСКП ЭП **Отказ выдачи КСКП ЭП** ФЛК не пройден и нет возможности сформировать новый запрос на выпуск КСКП ЭП
6.	Выпуск и блокировка КСКП ЭП	Файл запроса на КСКП ЭП	Система УЦ в автоматическом режиме формирует квалифицированный сертификат ключа проверки ЭП с одновременной его блокировкой (включение в Список Отозванных Сертификатов) и передает КСКП ЭП в УЗ пользователя DSS.	АС УЦ	-	Электронный КСКП ЭП и файл его текстового представления СОС	АС УЦ	**6 и 8**
7.	Печать Расписки об ознакомлении с КСКП ЭП и Требований по безопасности	Файл текстового представления КСКП ЭП	Сотрудник ВСП: • через интерфейс АРМ ЭП ФЛ распечатывает проект Расписки об ознакомлении Владельца с информацией, содержащейся в его КСКП ЭП, расписывается в документе и передает на подпись владельцу (Представителю владельца) КСКП ЭП; • Распечатывает и передает ФЛ для ознакомления «Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи»	Оператор 1	-	Распечатка Расписки документа об ознакомлении Владельца с информацией, содержащейся в его КСКП ЭП.	АРМ ЭП ФЛ	**9** Расписка подписана **10** Отказ в подписании Расписки

№ п/п	Операция	Входной документ/информация	Описание	Исполнитель	Продолжительность	Выходной документ	ИТ система	Переход к пункту и условие перехода
8.	Контроль результатов проверки СМЭВ	Электронные Ответы проверки данных из СМЭВ	Производится сверка данных, содержащихся в ответах госорганов с данными, включенными в КСКП ЭП. В случае отрицательного результата сверки, КСКП ЭП аннулируется.	АС УЦ	-	Результат проверки	АС УЦ	**11** Результат проверки положительный **10** Результат проверки отрицательный
9.	Заявка на разблокировку КСКП ЭП. Загрузка сканкопии ФГН	Подписанные Владельцем Заявление на выпуск КСКП ЭП и Распечатка Расписки документа об ознакомлении Владельца с информацией, содержащейся в его КСКП ЭП	Сотрудник ВСП формирует в АРМ ЭП ФЛ электронную заявку на разблокировку КСКП ЭП, загружает сканкопии Расписки об ознакомлении Владельца с информацией, содержащейся в его КСКП ЭП и Заявки на выпуск КСКП ЭП. Подписывает Заявку своей ЭП.	Оператор 1	-	Заявка на разблокировку КСКП ЭП	АРМ ЭП ФЛ	**11** Заявка создана и Результат проверки положительный
10.	Аннулирование КСКП ЭП, включение в СОС	КСКП не признан его владельцем, отрицательный результат проверки данных владельца КСКП ЭП в госорганах	Аннулирование КСКП ЭП выполняется в автоматическом режиме при отрицательном результате проверки данных владельца КСКП ЭП в госорганах, при отказе ФЛ в подписании Расписки об ознакомлении с информацией, содержащейся в КСКП ЭП. В Список отозванных сертификатов включаются серийные номера блокированных КСКП ЭП.	АС УЦ	-	Реестр аннулированных сертификатов	АС УЦ	**-**
11.	Разблокировка КСКП ЭП. Исключение из СОС Регистрация в ЕСИА. Передача данных в ЕПК	Заявка на разблокировку КСКП ЭП Положительный результат проверки данных владельца КСКП ЭП в госорганах	Система УЦ в автоматическом режиме при условии положительной проверки данных владельца КСКП ЭП в госорганах и Заявки на разблокировку КСКП ЭП, подписанной ЭП Оператора 1, производит: • разблокировку КСКП ЭП; • исключение КСКП ЭП из СОС; • регистрацию данных КСКП ЭП и его владельца в ЕСИА; • передает в АС ЕПК признак предоставления ФЛ услуги «Облачная» подпись.	АС УЦ	-	СОС Запрос на регистрацию КСКП ЭП в ЕСИА Email сообщение ФЛ об изменении статуса КСКП ЭП Статус готовности КСКП к работе	АС УЦ	**Процесс завершен и 12**

№ п/п	Операция	Входной документ/информация	Описание	Исполнитель	Продолжительность	Выходной документ	ИТ система	Переход к пункту и условие перехода
12.	Передача документов в СЦ Архив	Заявление на КСКП ЭП, Расписка об ознакомлении с информацией содержащейся в КСКП ЭП, документы, подтверждающие полномочия Представителя ФЛ	Подготовка документов для передачи в СЦ Архив	Оператор 1	-	Оформленные в индивидуальной упаковке документы ФЛ для хранения в коробах	-	**13** Документы поступили в Архив **14** Документы не поступили в Архив
13.	Подтверждение о приеме на хранение оригиналов документов	Заявление на КСКП ЭП, Расписка об ознакомлении с информацией содержащейся в КСКП ЭП, документы, подтверждающие полномочия Представителя ФЛ	В АС Архив производится регистрация принимаемых на хранение документов. Подтверждение приема оригинала Заявления на выпуск КСКП ЭП и Расписки об ознакомлении с информацией, содержащейся в КСКП с подписью владельца (ФГН) может осуществляться с использованием сервиса АС Архив, взаимодействующего с АС УЦ.	Работник Архива	-	-	АС Архив/ АС УЦ	-
14.	Направление уведомления ответственному сотрудника УЦ	-	АС УЦ в автоматическом режиме по истечению установленного срока для регистрации документов (ФГН) осуществляет отправку уведомлений по e-mail ответственным сотрудникам для принятия дальнейших действий.	АС УЦ	-	E-mail уведомления	АС УЦ	-

4. Процесс отключения/подключения второго и последующего мобильного устройства к «Облачному» сервису ЭП

Рисунок 3 — Схема процесса отключения/подключения второго и последующего мобильного устройства к «Облачному» сервису ЭП

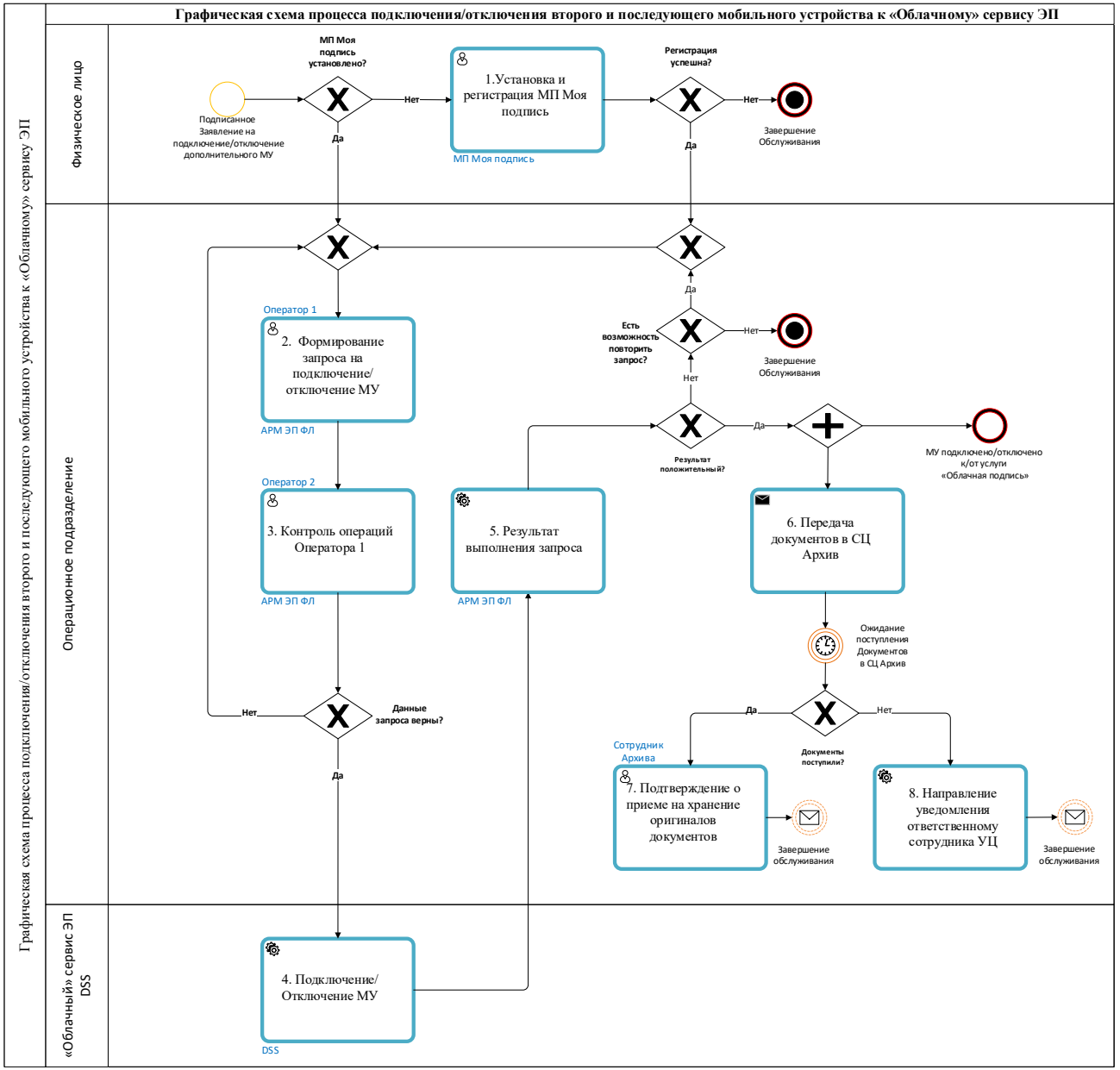

Таблица 3 — Описание процесса подключения/отключения второго и последующего мобильного устройства к «Облачному» сервису ЭП

№ п/п	Операция	Входной документ/информация	Описание	Исполнитель	Продолжительность	Выходной документ	ИТ система	Переход к пункту и условие перехода
1.	Установка и регистрация МП Моя подпись	МП Моя подпись в App Store Play Market	ФЛ скачивает и устанавливает на своем личном мобильном устройстве МП «Моя подпись». При первом входе в МП «Моя подпись» происходит регистрация мобильного устройства в DSS, формируется KID, который необходимо внести в заявление на подключение/ отключение мобильного устройства. ФЛ подписывает Заявление для предоставления Сотруднику ВСП. **Примечание:** Срок действия вектора аутентификации ФЛ — 3 года. Ответственность за генерацию векторов аутентификации и их распространение/ использование несет ПАО «Сбербанк».	ФЛ	-	KID	МП Моя подпись	**2** МП Моя подпись установлено **Завершение обслуживание** МП Моя подпись не установлено
2.	Формирование запроса на подключение/ отключение МУ	Подписанное Заявление на подключение/отключение мобильного устройства KID	Сотрудник ВСП с ролью Оператор в АРМ ЭП ФЛ, осуществляет поиск учетной записи ФЛ (УЗ ФЛ) в БД УЦ. В УЗ ФЛ проверяет наличие назначенной бизнес-услуги «МП Моя подпись». Формирует запрос на подключение/отключение МУ. В запрос вводит KID, указанный в подписанном Заявление. Загружает сканкопию Заявления	Оператор 1	-	Запрос на подключение /отключение МУ	АРМ ЭП ФЛ	**3**
3.	Контроль операций Оператора 1	Запрос на подключение/отключение МУ Заявление на подключение/отключение мобильного устройства	Руководитель Сотрудника ВСП, с ролью «Оператор 2» в АРМ ЭП ФЛ, сверяет данные в запросе, согласно предоставленным документам ФЛ. Подтверждает запрос свой ЭП	Оператор 2	-	Запрос на подключение /отключение МУ	АРМ ЭП ФЛ	**2** Ошибка данных в запросе **4** Данные запроса верны
4.	Подключение/ Отключение МУ	Запрос на подключение/отключение МУ	Автоматическая функция DSS: • поиск мобильного устройства по KID; • подключение (или отключение) мобильного устройства к (от) УЗ пользователя DSS; • отправка уведомления о результате выполнения запроса	DSS	-	Результат выполнения запроса	DSS	**5**

№ п/п	Операция	Входной документ/информация	Описание	Исполнитель	Продолжительность	Выходной документ	ИТ система	Переход к пункту и условие перехода
5.	Результат выполнения запроса	Результат выполнения запроса	Автоматическая функция АРМ ЭП ФЛ отображения уведомления о результате выполнения запроса. Если результат выполнения запроса отрицательный, на экране выводится сообщение с указанием причины отказа. Сотрудник ВСП принимает решение о необходимости повторного направления запроса. Если результат выполнения запроса положительный, Сотрудник ВСП устно уведомляет ФЛ о положительном исполнении Заявки	АРМ ЭП ФЛ Оператор 1	-	Результат выполнения запроса	АРМ ЭП ФЛ	**6 и Процесс завершен** Результат выполнения запроса положительный **2** Результат отрицательный и нет возможности сформировать новый запрос **Завершение обслуживание** Результат отрицательный и нет возможности сформировать новый запрос
6.	Передача документов в СЦ Архив	Подписанное Заявление на подключение/отключение мобильного устройства	Подготовка документов для передачи в СЦ Архив	Оператор 1	-	Оформленные в индивидуальной упаковке документы ФЛ для хранения в коробах		**7** Документы поступили в Архив **8** Документы не поступили в Архив
7.	Подтверждение о приеме на хранение оригиналов документов	Подписанное Заявление на подключение/отключение мобильного устройства	В АС Архив производится регистрация принимаемых на хранение документов. Подтверждение приема оригинала Заявления на подключение/отключение мобильного устройства осуществляется с использованием сервиса АС Архив, взаимодействующего с АС УЦ	Работник Архива	-	-	АС Архив/ АС УЦ	-
8.	Направление уведомления ответственному сотрудника УЦ	-	АС УЦ в автоматическом режиме по истечению установленного срока для регистрации документов осуществляет отправку уведомлений по e-mail ответственным сотрудникам для принятия дальнейших действий	АС УЦ	-	E-mail уведомления	АС УЦ	-