Приложение №13 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

УТВЕРЖДАЮ
Заместитель директора по
информационным технологиям
АО «Гринатом»

_____ И.П. Тарасов

М.П.

П О Р Я Д О К

предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском неквалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов

Москва
2023

Содержание

1. Назначение и область применения

Настоящий Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском неквалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов (далее - Порядок) разработан для установления последовательности действий по процессу группы процессов управления информационными технологиями с целями установления правил и условий предоставления и пользования услугами Корпоративного удостоверяющего центра Госкорпорации «Росатом» по созданию, выдаче и управлению неквалифицированными сертификатами ключей проверки электронной подписи с использованием Платформы доверенных сервисов.

Информация о Корпоративном удостоверяющем центре Госкорпорации «Росатом» размещена на официальном сайте https://crypto.rosatom.ru.

Соблюдение Порядка является обязательным для предприятий/ организаций, использующих автоматизированные информационные системы, в которых применяются сертификаты ключей проверки электронных подписей, создаваемые Корпоративным удостоверяющим центром Госкорпорации «Росатом».

Требования Порядка обязательны для сотрудников, выполняющих следующие функциональные роли:

подписчик;

куратор от организации;

уполномоченное лицо от организации;

администратор безопасности;

куратор ПДС;

оператор УЦ от ПУСК ПДС.

Ответственным за актуализацию Порядка и контроль его исполнения в соответствии с требованиями Положения о системе регламентирующих документов Госкорпорации «Росатом» является директор Департамента по информационным технологиям Блока по ИТ АО «Гринатом».

Актуальная версия Порядка размещена по адресу: https://crypto.rosatom.ru.

2. Термины, сокращения и аббревиатуры

2.1. Термины и определения

Термин	Определение
Администратор безопасности	Уполномоченный работник АО «Гринатом» (по договору) или уполномоченный работник организации-заказчика, наделенный полномочиями по вручению сертификатов ключей проверки электронных подписей от имени удостоверяющего центра
Аккредитация удостоверяющего центра	Признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»
Владелец сертификата ключа проверки электронной подписи	Лицо, которому в соответствии настоящим Порядком, с учетом Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной

	подписи», создан неквалифицированный сертификат ключа проверки электронной подписи
Вручение сертификата ключа проверки электронной подписи	Передача доверенным лицом удостоверяющего центра изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу
Неквалифицированный сертификат ключа проверки электронной подписи	Сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом №63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный неаккредитованным центром сертификации
Ключ проверки электронной подписи	Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи)
Ключ электронной подписи	Уникальная последовательность символов, предназначенная для создания электронной подписи
Ключевой носитель	Отчуждаемый носитель информации, предназначенный для хранения ключа электронной подписи и ключа проверки электронной подписи
Корпоративный удостоверяющий центр Госкорпорации «Росатом»	Удостоверяющий центр АО «Гринатом»
Куратор от организации	Сотрудник организации-заказчика, который дополняет заявки на создание Подписки, на перевыпуск Сертификата кадровыми данными Подписчика
Оператор Удостоверяющего центра от подсистемы управления сервисами и коннекторами Платформы доверенных сервисов	Сотрудник Корпоративного удостоверяющего центра Госкорпорации «Росатом», который создает Сертификаты
Подписка	Заказ предприятия в ПДС в соответствии с условиями договора присоединения на обеспечение сертификатами или средствами криптографической защиты и информации. Подписка подразумевает владение Подписчиком одним действующим сертификатом выбранного шаблона
Подписчик	Физическое лицо, для которого оформлена подписка на обеспечение сертификатом и (или) лицензией на средство криптографической защиты информации (обладает учётной записью в домене GK/inter, создаёт обращения, получает Сертификаты)
Подтверждение владения ключом электронной подписи	Получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата
Сертификат ключа проверки электронной подписи	Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность

	ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи
Удостоверяющий центр	Юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом
Уполномоченное лицо от организации	Работник юридического лица, указанный в ЕГРЮЛ и имеющий возможность обращаться в Удостоверяющий центр от имени юридического лица, либо работник имеющий право действовать от имени юридического лица на основании доверенности
Участники электронного взаимодействия	Государственные органы, органы местного самоуправления, организации, а также граждане, осуществляющие обмен информацией в электронной форме
Электронная подпись	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

В Порядке используются термины, установленные Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

2.2. Сокращения, используемые в целях данного документа, и расшифровки

Термин	Определение
ИАСУП	Информационная автоматизированная система управления персоналом Госкорпорации «Росатом»
КИС	Корпоративная информационная система
КУЦ	Корпоративный удостоверяющий центр Госкорпорации «Росатом»
ЛИС	Локальная информационная система
ПДС	Платформа доверенных сервисов
ПУСК ПДС	Подсистема управления сервисами и коннекторами Платформы доверенных сервисов
Сертификат	Неквалифицированный сертификат ключа проверки электронной подписи
СУ ИТ	Система управления информационными технологиями
УНЭП	Усиленная неквалифицированная электронная подпись
УЦ	Удостоверяющий центр
ЭП	Электронная подпись

3. Описание процесса

Описание процесса предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском неквалифицированного сертификата ключа проверки ЭП с использованием Платформы доверенных сервисов.

До начала процесса организация-заказчик должна направить в орган криптографической защиты АО «Гринатом» оригинал заявления

на предоставление услуги по форме Приложения №2, подписанное Уполномоченным лицом от организации.

3.1. Описание подпроцессов

3.1.1. Подпроцесс «Заведение информации в ПДС об объеме Подписки»

Администратор безопасности ПДС:

заводит информацию в ПДС об объеме Подписки организации-заказчика, согласно полученному заявлению на предоставление услуги (Приложение №2).

3.1.2. Подпроцесс «Обработка обращения»

Инициаторами обращения могут быть:

Подписчик, либо от него контактное лицо;

Администратор безопасности.

одним из следующих способов:

информация из ИАСУП о том, что Подписчик согласился/отказался использовать УНЭП (облачный Сертификат). В этом случае Сертификат Подписчику создается/аннулируется автоматически;

заявка в ПДС или заявка через автоматизированную информационную систему, подключенную к ПДС (далее – заявка в ПДС);

заявка через СУ ИТ;

электронное письмо на п/я 1111@greenatom.ru (Центр поддержки пользователей);

электронное письмо на п/я pds@rosatom.ru (Техническая поддержка ПДС);

звонок в центр поддержки пользователей АО «Гринатом» (+7 499 949 49 19, доб. 1111).

В случае если поступает неформализованное обращение, то Администратор безопасности:

определяет наличие Подписки и учётной записи в домене GK/inter у Подписчиков, указанных в обращении;

формализует обращение в соответствии с правилами формализации, изложенными на официальном сайте КУЦ https://crypto.rosatom.ru в зависимости от следующих условий:

в случае если Подписка отсутствует и обращение является обращением на создание Подписки, то информация поступает в подпроцесс «Создание подписки» в соответствии с выбранным шаблоном. Администратор безопасности должен определить шаблон для выпуска Сертификата на основании неформализованного обращения Подписчика;

в случае если Подписка на Подписчика, указанного в обращении, есть и обращение связано с компрометацией ключевой информации, подозрением на компрометацию или изменением кадровых данных о подписчике, то исходящая информация поступает в подпроцесс «Перевыпуск сертификата»;

в случае если Подписка на сотрудника организации, указанного в обращении, есть и обращение является обращением на сокращение Подписки, то исходящая информация поступает в подпроцесс «Сокращение подписки и аннулирование Сертификата»;

Исходящая информация поступает в подпроцесс «Создание подписки», «Сокращение подписки и аннулирование Сертификата», либо «Перевыпуск Сертификата».

Если обращение содержит иные данные, процесс завершается.

Если заявка была создана в ПДС, то процесс начинается с подпроцессов «Создание подписки», «Перевыпуск сертификата» или «Сокращение подписки и аннулирование Сертификата», в зависимости от типа заявки.

3.1.3. Подпроцесс «Создание Подписки»

Входящая информация поступает из подпроцесса «Обработка обращения».

Если заявка на создание Подписки создана автоматически в ПДС по причине согласия Подписчика в ИАСУП на использование облачного Сертификата, то исходящая информация поступает в подпроцесс «Создание Сертификата».

Если заявку на создание Подписки в ПДС создал Подписчик или Администратор безопасности (если заявка создана Администратором безопасности, то Подписчику отправляется уведомление о создании заявки), то Куратор от организации:

получает в ПДС заявку на создание Подписки, проверяет корректность информации о Подписчике, вносит информацию о Подписчике, в объеме, необходимом для выпуска Сертификата.

Если заявка на создание Подписки на Сертификат на ключевом носителе, то она переходит на рассмотрение Уполномоченному лицу от организации.

Если заявка на создание Подписки на облачный Сертификат, то исходящая информация сразу поступает в подпроцесс «Создание Сертификата».

Уполномоченное лицо от организации:

получает электронное уведомление о поступившей заявке на создание Подписки на Сертификат на ключевом носителе на подписание.

Если заявка отклонена, то процесс завершается и Подписчику отправляется уведомление об отклонении заявки.

Если заявка согласована, то:

подписывает PDF-документ (печатный аналог электронной заявки) с использованием сервиса усиленной квалифицированной/неквалифицированной электронной подписи.

Исходящая информация поступает в подпроцесс «Создание сертификата».

3.1.4. Подпроцесс «Перевыпуск Сертификата»

Входящая информация поступает из подпроцесса «Обработка обращения».

Если информация о Подписчике в ИАСУП изменилась, и она не связана с увольнением Подписчика или кадровые данные о Подписчике в ПДС изменил Куратор от организации, то ПДС автоматически создает заявку на перевыпуск Сертификата, при этом Подписчику отправляется уведомление о создании заявки на перевыпуск Сертификата.

Исходящая информация сразу поступает в подпроцесс «Сокращение подписки и аннулирование Сертификата» и «Создание Сертификата».

Если заявку на перевыпуск создал Подписчик, то Куратор от организации:

получает в ПДС заявку на перевыпуск Сертификата, проверяет корректность информации о Подписчике, вносит информацию о Подписчике, в объеме, необходимом для выпуска Сертификата (данный шаг может быть произведён автоматически, при наличии данных о Подписчике в ИАСУП).

Исходящая информация поступает в подпроцесс «Сокращение подписки и аннулирование сертификата» и «Создание Сертификата».

Если заявка на перевыпуск получена через обращение, то Администратор безопасности:

создает заявку в ПДС на перевыпуск Сертификата.

Куратор от организации*:*

получает в ПДС заявку на перевыпуск Сертификата, проверяет корректность информации о Подписчике, вносит информацию о Подписчике, в объеме, необходимом для выпуска Сертификата (данный шаг может быть произведён автоматически, при наличии данных о Подписчике в ИАСУП).

Если перевыпуск Сертификата связан с изменением кадровых данных о Подписчике, то сначала создается новый Сертификат, а потом аннулируется ранее выпущенный.

Если перевыпуск Сертификата связан с компрометацией, то сначала аннулируется действующий Сертификат и только потом выпускается новый.

Исходящая информация поступает в подпроцесс «Сокращение подписки и аннулирование Сертификата» и «Создание Сертификата».

3.1.5. Подпроцесс «Сокращение подписки и аннулирование Сертификата»

Входящая информация поступает из подпроцессов «Обработка обращения», «Перевыпуск Сертификата», «Вручение Сертификата».

Если в ИАСУП (внутреннему пользователю) или Куратором от организации в карточке пользователя ПДС (внешнему пользователю) была внесена информация об увольнении Подписчика, то процесс аннулирования Сертификата происходит в автоматическом режиме и процесс завершается. Подписчику отправляется уведомление о сокращении Подписки и аннулировании Сертификата. При этом если Сертификат на ключевом носителе, то Администратору безопасности также отправляется уведомление о сокращении Подписки и аннулировании Сертификата Подписчика, и он изымает ключевой носитель у Подписчика, уничтожает его и ставит отметку в ПДС об уничтожении.

Если входящая информация поступает из подпроцесса «Обработка обращения»:

Если заявку на сокращение Подписки на облачный Сертификат в ПДС создал Подписчик или Администратор безопасности, то ПДС отправляет запрос в УЦ на аннулирование Сертификата и процесс завершается. В случае если заявку на сокращение Подписки создал Администратор безопасности, то Подписчику отправляется уведомление о создании заявки на сокращение Подписки.

Если заявку на сокращение Подписки на Сертификат на ключевом носителе в ПДС создал Подписчик или Администратор безопасности, подпроцесс переходит к Уполномоченному лицу организации. В случае если заявку на сокращение Подписки создал Администратор безопасности, то Подписчику отправляется уведомление о создании заявки на сокращение Подписки.

Уполномоченное лицо от организации:

получает электронное уведомление о поступившей заявке на сокращение Подписки на подписание.

Если заявка отклонена, то процесс завершается (при этом Подписчику и Администратору безопасности отправляется уведомление об отклонении заявки).

Если заявка согласована, то:

подписывает PDF-документ (печатный аналог электронной заявки) с использованием сервиса усиленной квалифицированной/неквалифицированной электронной подписи.

ПДС отправляет запрос в УЦ на аннулирование Сертификата.

От ПУСК ПДС приходит уведомление Подписчику и Администратору безопасности об аннулировании Сертификата и процесс завершается.

Если входящая информация поступает из подпроцесса «Перевыпуск Сертификата»:

Сертификат аннулируется автоматически, при этом Подписчику и Администратору безопасности приходит уведомление об аннулировании Сертификата и о создании заявки на новый Сертификат, и процесс завершается.

Если входящая информация поступает из подпроцесса «Вручение Сертификата»:

Сертификат аннулируется автоматически, при этом Подписчику и Администратору безопасности приходит уведомление об аннулировании Сертификата, Подписка не начинает действовать.

3.1.6. Подпроцесс «Создание Сертификата»

Входящая информация поступает из подпроцессов «Создание Подписки», «Перевыпуск Сертификата» и «Контроль срока действия Сертификата».

Если получена заявка на выпуск облачного Сертификата, то создание Сертификата происходит автоматически в ПДС и исходящая информация поступает в подпроцесс «Контроль срока действия Сертификата». При этом Подписчик не получает ПИН-код в личном кабинете ПУСК ПДС. В качестве второго фактора для подтверждения операций используется одноразовый пароль (one time password).

Если получена заявка на выпуск Сертификата на ключевом носителе, то Оператор УЦ от ПУСК ПДС:

подключает ключевой носитель к своему рабочему месту;

форматирует ключевой носитель, запускает генерацию ключевой пары;

ПДС автоматически создаёт запрос на Сертификат и выпускает Сертификат на неаккредитованном УЦ;

устанавливает выпущенный Сертификат на ключевой носитель;

создаёт пакет для передачи выпущенного Сертификата Администратору безопасности лично или Службой специальной связи. Пакет содержит готовый ключевой носитель с содержащейся на нем ключевой информацией и Сертификатом. При этом ПИН-код от ключевого контейнера Подписчик получит в личном кабинете ПУСК ПДС после того, как подтвердит получение ключевого носителя.

Исходящая информация поступает в подпроцесс «Вручение Сертификата».

3.1.7. Подпроцесс «Вручение Сертификата»

Входящая информация поступает из подпроцесса «Создание Сертификата».

Администратору безопасности формируется и отправляется электронное уведомление о необходимости получения пакета с Сертификатом.

Оператор УЦ от ПУСК ПДС:

передает пакет с Сертификатом Администратору безопасности.

Администратор безопасности:

подтверждает получение Сертификата в ПДС. Подписчику формируется и отправляется электронное уведомление о получении Сертификата Администратором безопасности;

верифицирует Подписчика. Вручает Подписчику пакет с Сертификатом. При вручении Сертификата Администратор безопасности обязан установить личность Подписчика (если верификация не пройдена, то вносит данные в заявку на создание Подписки о причинах отказа в верификации, заявка закрывается с ошибкой выдачи Сертификата. Исходящая информация поступает в подпроцесс «Сокращение Подписки и аннулирование Сертификата», Подписка в этом случае не начинает действовать).

Подписчик:

получает пакет с Сертификатом;

аутентифицируется в личном кабинете ПДС (в присутствии Администратора безопасности), где ознакамливается с информацией, содержащейся в Сертификате и нажимает кнопку «Сертификат получен» (если информация, содержащаяся в Сертификате в ПДС не верна, то вносит в заявку на создание Подписки данные о причине отказа в получении Сертификата. При этом исходящая информация поступает в подпроцесс «Сокращение Подписки и аннулирование Сертификата»).

Исходящая информация поступает в подпроцесс «Контроль действия Сертификата».

3.1.8. Подпроцесс «Контроль срока действия Сертификата»

Входящая информация поступает из подпроцессов «Создание Сертификата» и «Вручение Сертификата».

ПДС в автоматическом режиме контролирует сроки действия Сертификатов и инициирует процесс выпуска нового Сертификата для Подписчика за 90 дней до окончания срока действия старого Сертификата.

Исходящая информация поступает в подпроцесс «Создание Сертификата».

4. Проверка электронной подписи в электронном документе

Проверка электронной подписи в электронном документе – процедура столь же ответственная, как и подписание электронного документа и может быть произведена только с использованием доверенных средств электронной подписи. Проверка усиленной неквалифицированной электронной подписи, как и подписание электронных документов осуществляется с использованием средств ПДС.

Услуга по подтверждению подлинности электронной подписи УНЭП в электронном документе предоставляется всем пользователям Корпоративного Удостоверяющего центра по запросу по одному из двух сценариев:

через интерфейс Корпоративных информационных систем по интеграционному взаимодействию с ПДС в автоматическом режиме согласно техническим условиям ПДС.

через обращение пользователя непосредственно в Корпоративный Удостоверяющий центр в ручном режиме Приложение № 3.

Для подтверждения подлинности УНЭП в электронных документах через интерфейс КИС пользователь КИС нажимает соответствующую кнопку. Корпоративная информационная система, интегрированная с ПДС, направляет запрос в ПДС на проверку подлинности УНЭП согласно техническим условиям на подключение № 22-2.4/10701-ВК от 27.04.2022. Результат проверки подлинности УНЭП будет содержаться в ответе ПДС корпоративной информационной системе и будет представлен КИС пользователю в виде информационного окна с информацией о действительности или недействительности УНЭП.

Для подтверждения подлинности УНЭП в электронных документах через обращение в Корпоративный Удостоверяющий центр необходимо подать заявление на подтверждение подлинности электронной подписи в электронном документе, оформляемого по форме Приложения № 3 к настоящему Порядку.

Заявление на подтверждение подлинности УНЭП в электронном документе должно содержать следующую информацию:

дата и время подачи заявления на подтверждение подлинности электронной подписи в электронном документе;

идентификационные данные Пользователя Корпоративного удостоверяющего центра, подлинность УНЭП которого необходимо подтвердить в электронном документе;

время и дата формирования УНЭП электронного документа;

время и дата, на момент наступления которых требуется установить подлинность УНЭП.

Обязательным приложением к заявлению на подтверждение подлинности УНЭП в электронном документе является электронный носитель, содержащий:

сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности УНЭП в электронном документе;

электронный документ – в виде одного файла, содержащего данные и значение УНЭП этих данных, либо двух файлов: один из которых содержит данные, а другой значение подписи этих данных (файл подписи .SIG или CMC).

Если формирование подписи осуществлялось на рабочем месте работника, в Корпоративный Удостоверяющий центр необходимо предоставить заключение соответствующего Органа криптографической защиты, подтверждающего выполнение на рабочем месте подписанта требований Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной Приказом ФАПСИ от 13 июня 2001 г. N 152.

Оказание услуг по подтверждению подлинности УНЭП в электронном документе осуществляется комиссионно сотрудниками Корпоративного Удостоверяющего центра.

Результатом оказания услуги по подтверждению подлинности УНЭП в электронном документе является заключение Корпоративного Удостоверяющего центра.

Заключение Корпоративного Удостоверяющего центра содержит:

состав комиссии, осуществлявшей проверку УНЭП в электронном документе;

основание для проведения проверки УНЭП в электронном документе;

результат проверки УНЭП в электронном документе;

данные, представленные комиссии для проведения проверки УНЭП в электронном документе;

отчет по выполненной проверке УНЭП в электронном документе.

Отчет по выполненной проверке УНЭП в электронном документе содержит:

время и место проведения проверки УНЭП в электронном документе;

содержание и результаты проверки УНЭП в электронном документе;

обоснование результатов проверки УНЭП в электронном документе.

Заключение Корпоративного Удостоверяющего центра по выполненной проверке УНЭП в электронном документе составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью Корпоративного Удостоверяющего центра. Один экземпляр заключения Корпоративного Удостоверяющего центра по выполненной проверке УНЭП в электронном документе предоставляется заявителю.

Срок оказания услуг по подтверждению подлинности УНЭП в одном электронном документе и предоставлению заявителю заключения Корпоративного Удостоверяющего центра по выполненной проверке УНЭП в электронном документе составляет 5 (пять) рабочих дней с момента поступления заявления на подтверждение подлинности электронной подписи в электронном документе в Корпоративный Удостоверяющий центр.

5. Нормативные ссылки

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи».

Приказ ФСБ РФ от 13 апреля 2021 г. N 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 29.10.2020 № 559 «Об утверждении Административного регламента предоставления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственной услуги по аккредитации удостоверяющих центров и Административного регламента осуществления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственного контроля (надзора) за соблюдением аккредитованными удостоверяющими центрами требований, которые установлены Федеральным законом «Об электронной подписи» и на соответствие которым эти удостоверяющие центры были аккредитованы».

Приказ Госкорпорации «Росатом» от 04.12.2015 № 1/1176-П (с учётом изменений, внесённых приказом Госкорпорации «Росатом» от 26.07.2019 № 1/764-П).

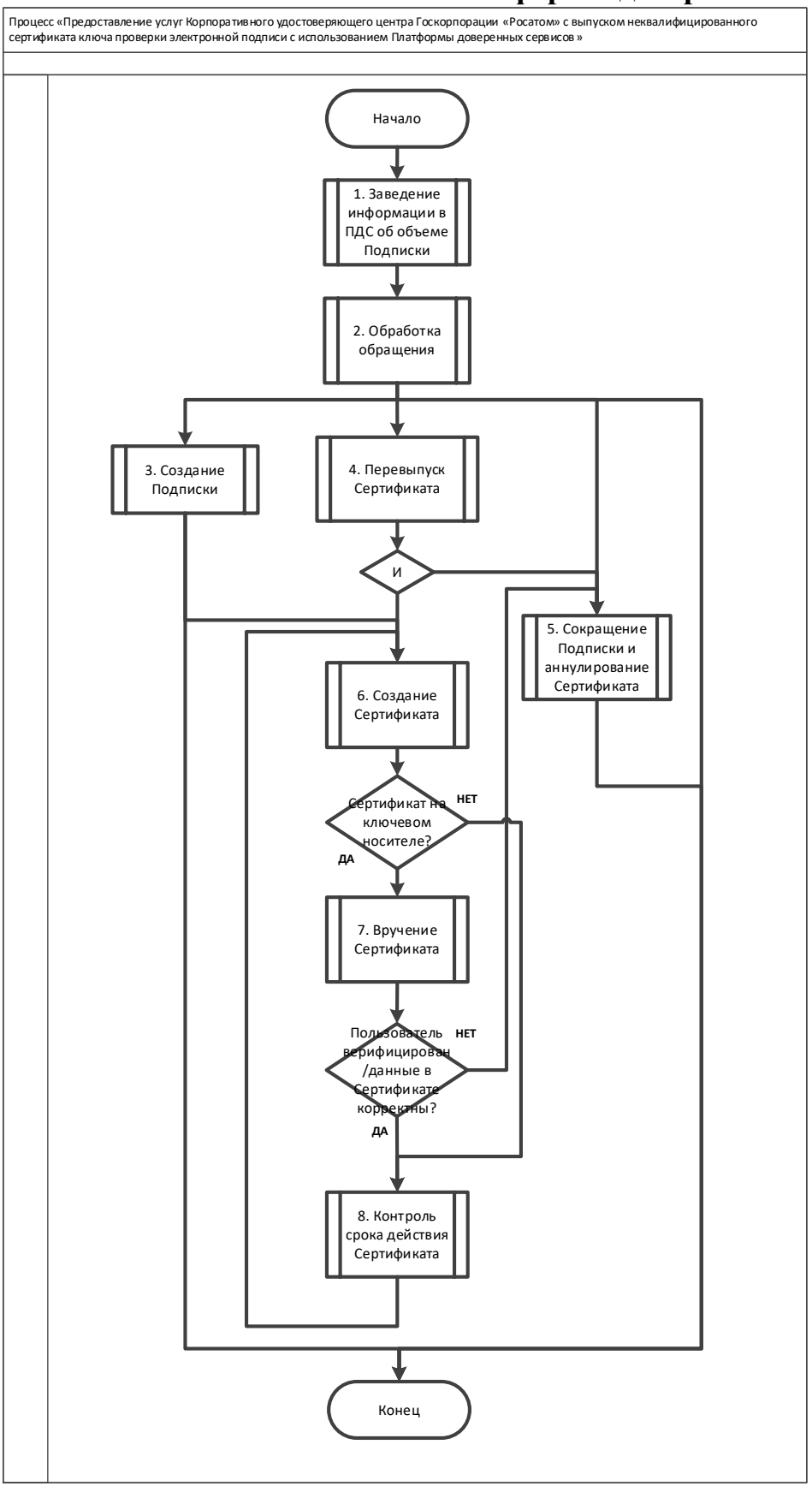
6. Перечень приложений

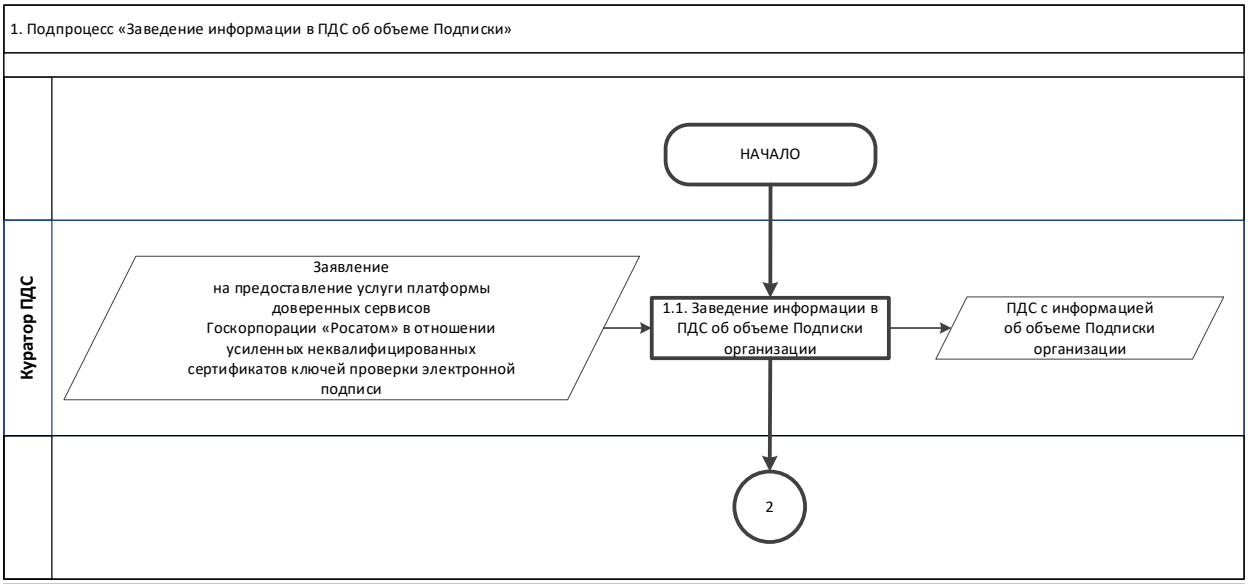
Приложение 1. Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском неквалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов;

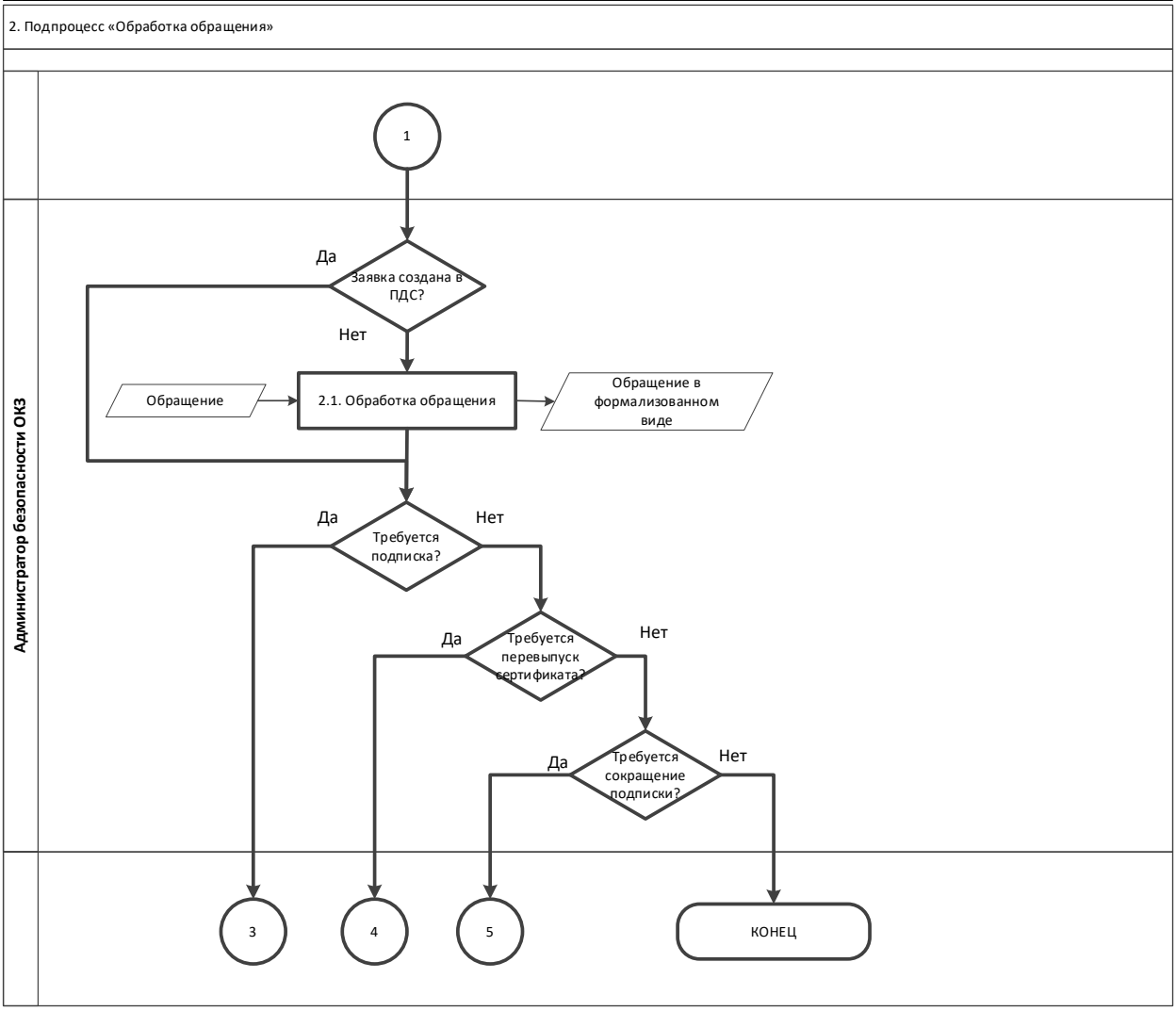
Приложение 2. Заявление на предоставление услуги платформы доверенных сервисов в отношении усиленных неквалифицированных сертификатов электронной подписи;

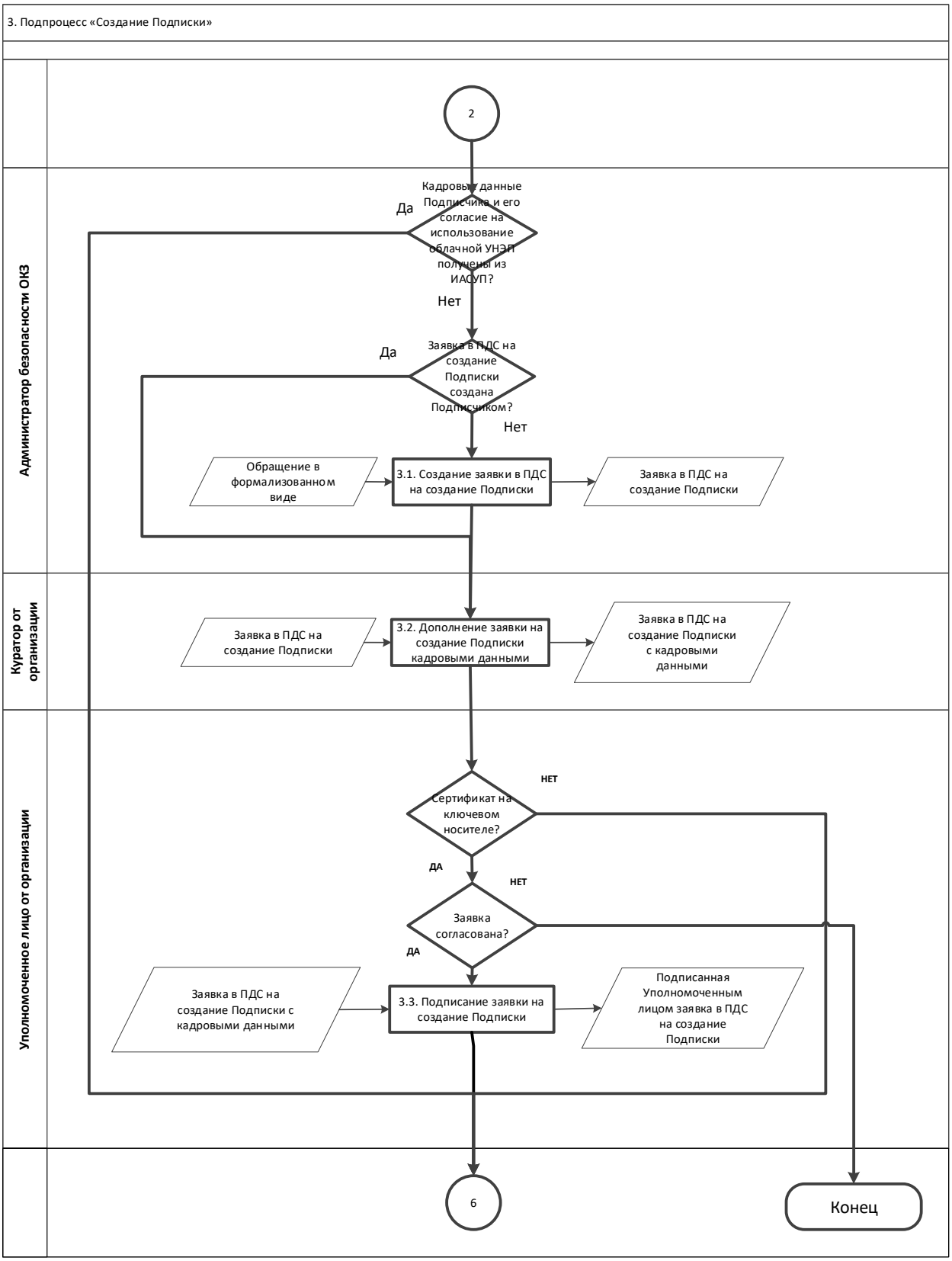
Приложение 3. Заявление на подтверждение электронной подписи в электронном документе.

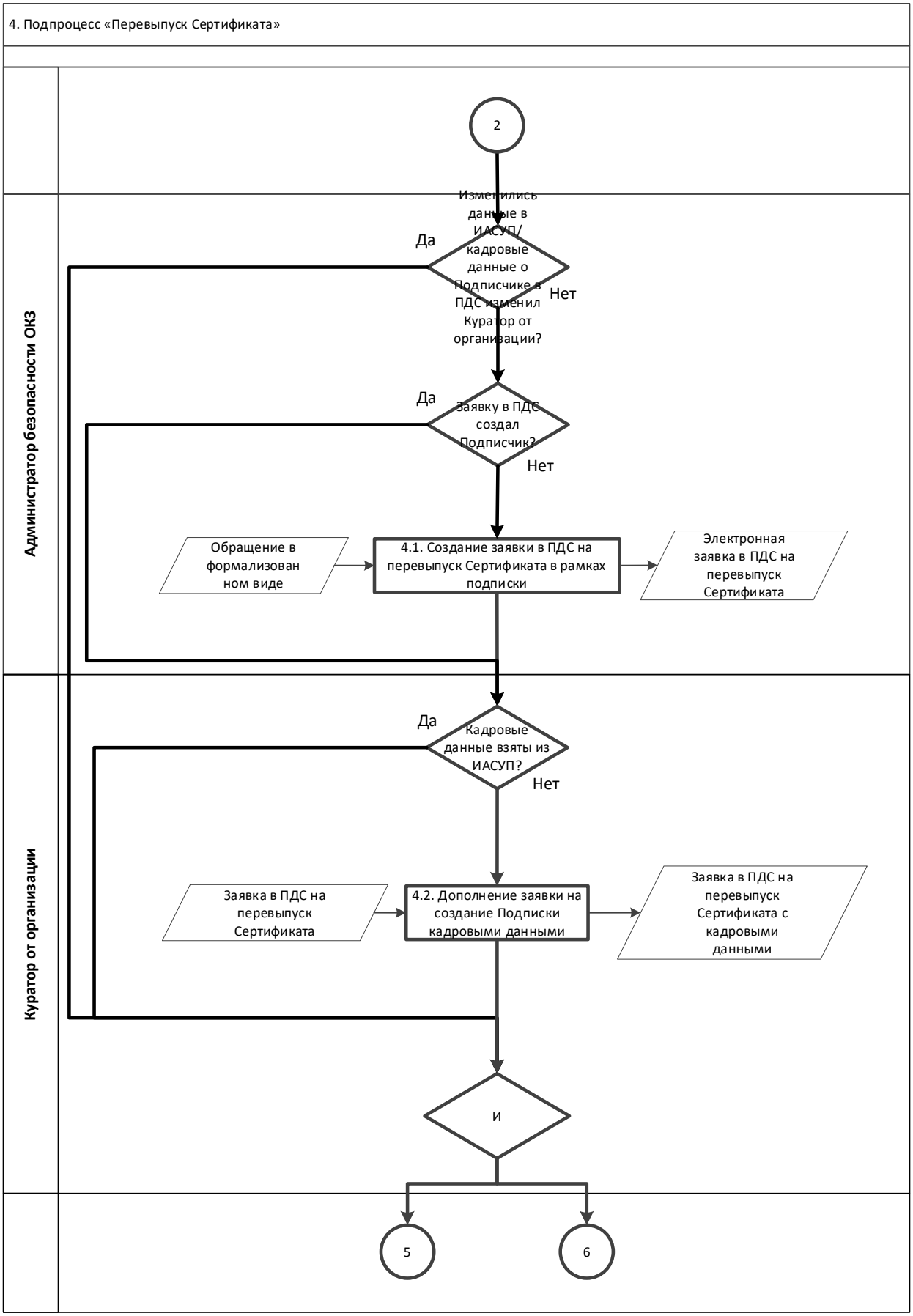
Приложение №1. Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском неквалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов

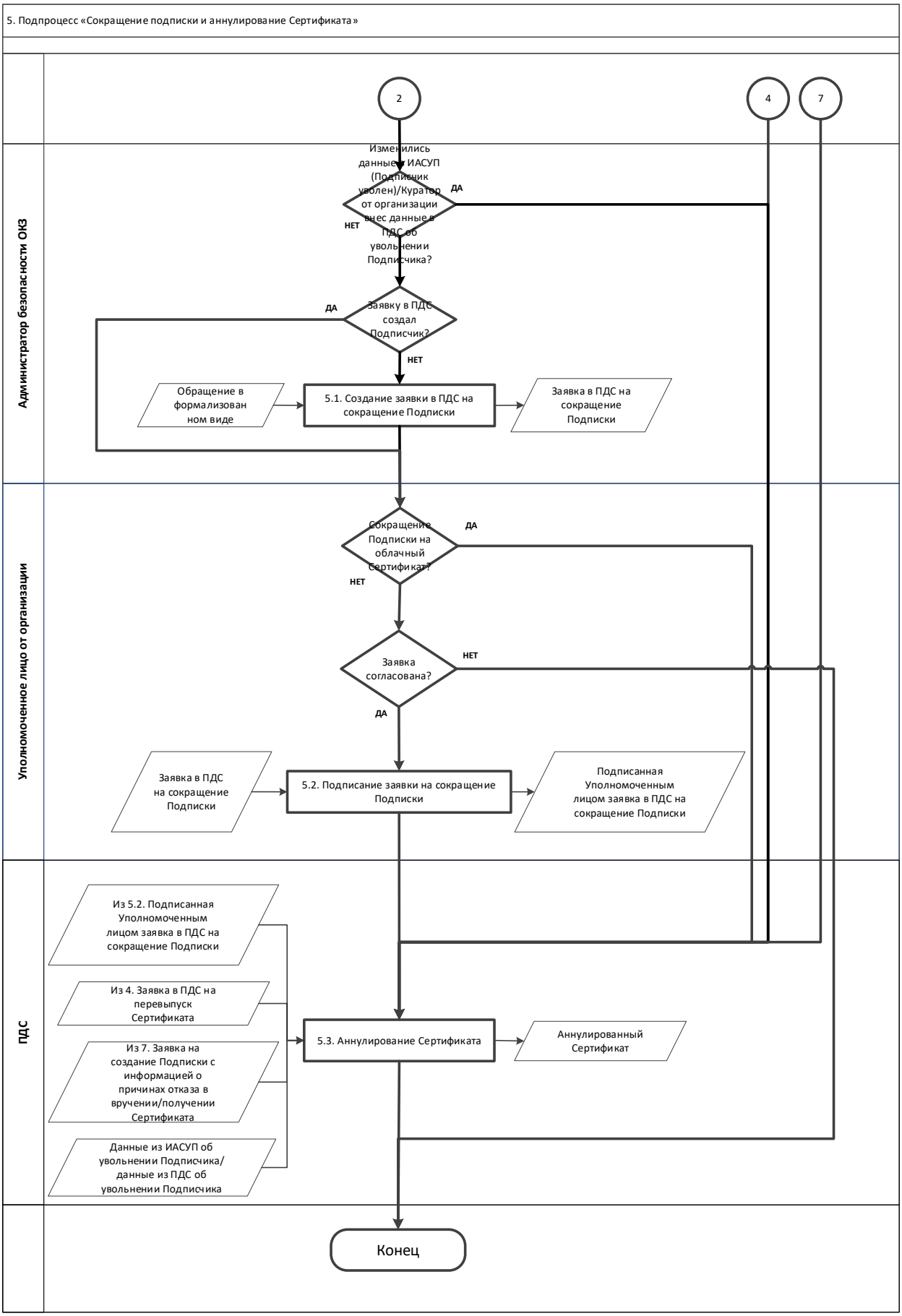


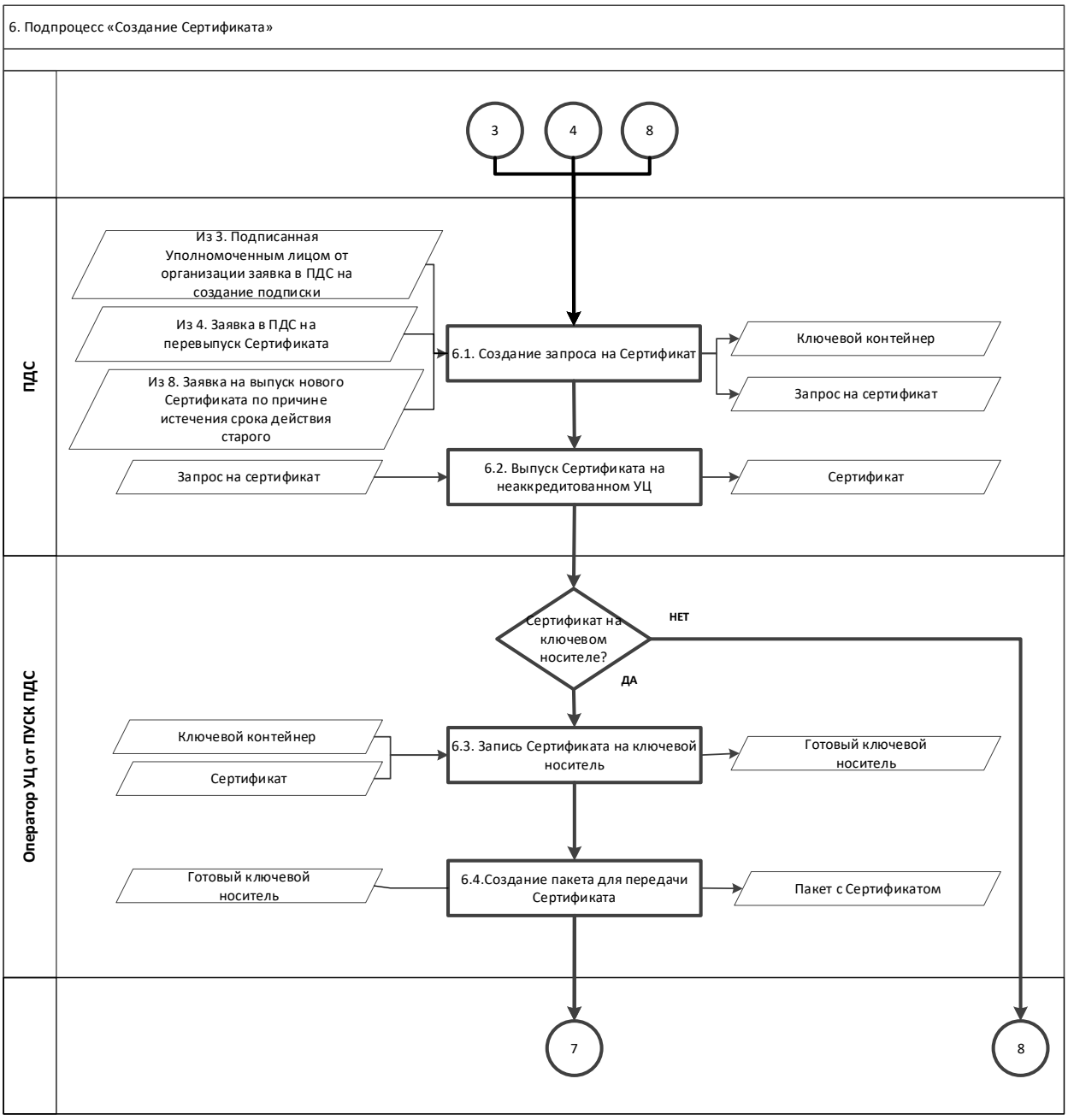

1. Подпроцесс «Заведение информации в ПДС об объеме Подписки»
Куратор ПДС
НАЧАЛО
Заявление на предоставление услуги платформы доверенных сервисов Госкорпорации «Росатом» в отношении усиленных неквалифицированных сертификатов ключей проверки электронной подписи
1.1. Заведение информации в ПДС об объеме Подписки организации
ПДС с информацией об объеме Подписки организации
2

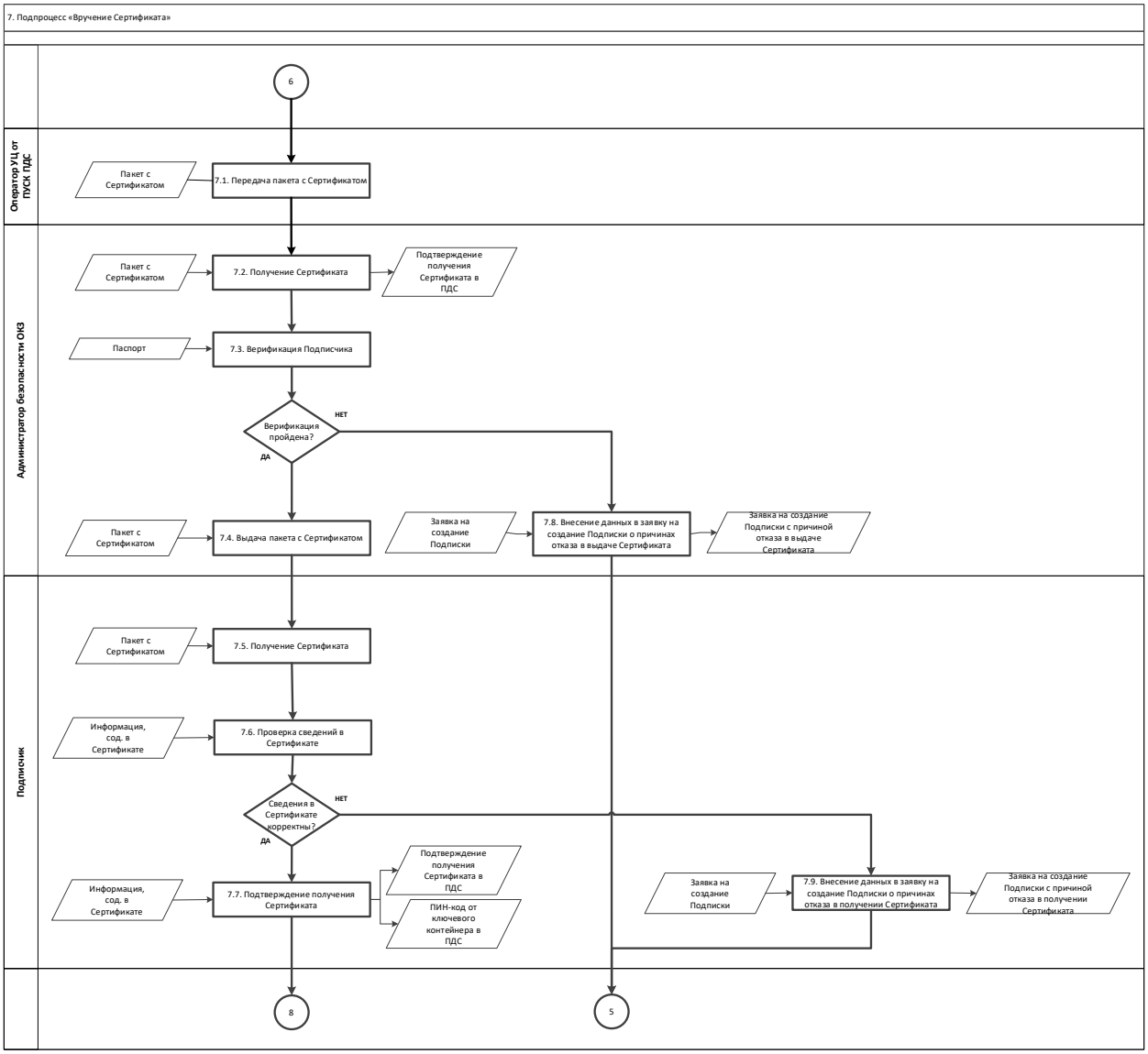

2. Подпроцесс «Обработка обращения»
Администратор безопасности ОКЗ
1
Да
Заявка создана в ПДС?
Нет
Обращение
2.1. Обработка обращения
Обращение в формализованном виде
Да
Требуется подписка?
Нет
Да
Требуется перевыпуск сертификата?
Нет
Да
Требуется сокращение подписки?
Нет
3
4
5
КОНЕЦ

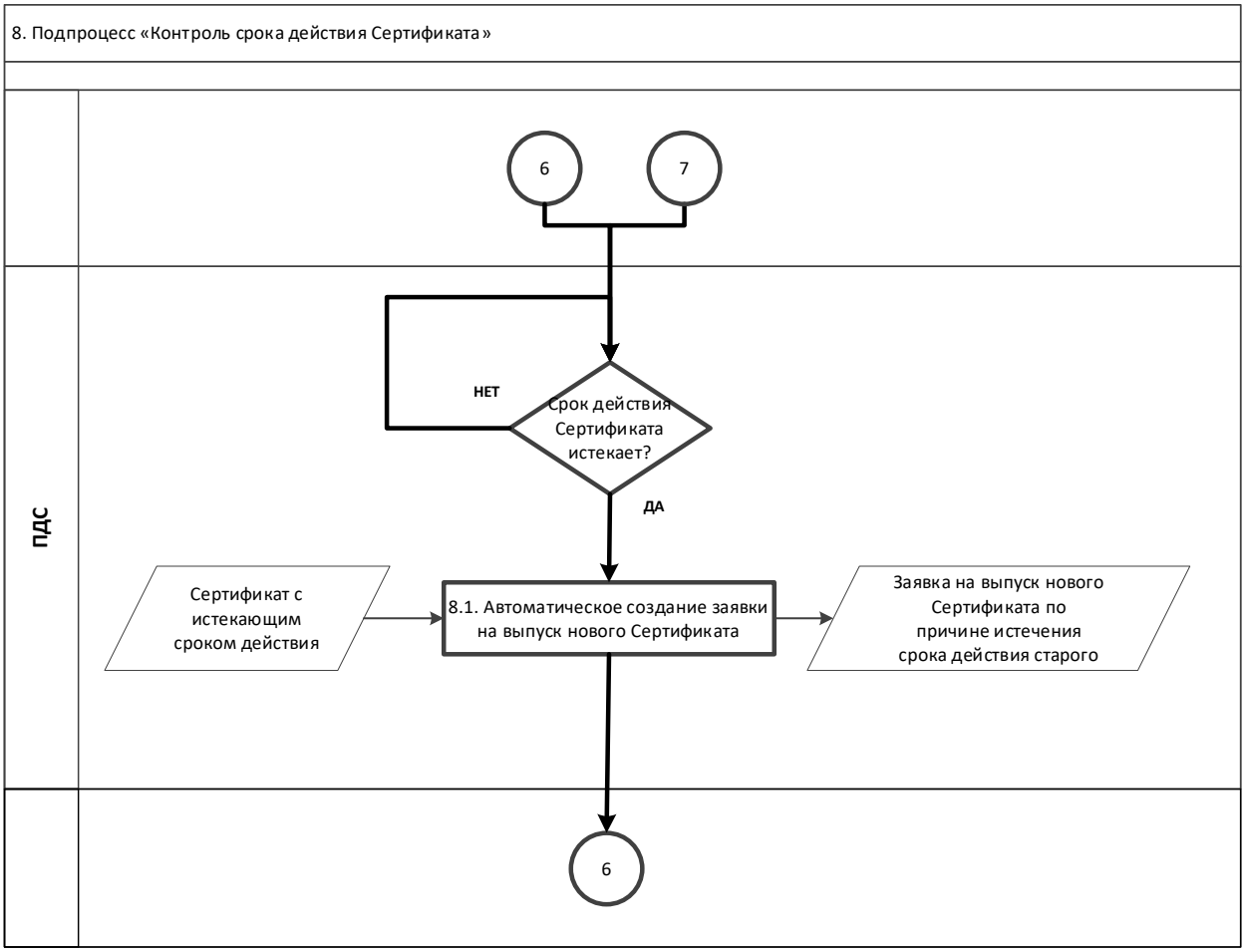

3. Подпроцесс «Создание Подписки»
Администратор безопасности ОКЗ
Куратор от организации
Уполномоченное лицо от организации
2
Кадровые данные Подписчика и его согласие на использование облачной УНЭП получены из ИАСУП?
Да
Нет
Заявка в ПДС на создание Подписки создана Подписчиком?
Да
Нет
Обращение в формализованном виде
3.1. Создание заявки в ПДС на создание Подписки
Заявка в ПДС на создание Подписки
Заявка в ПДС на создание Подписки
3.2. Дополнение заявки на создание Подписки кадровыми данными
Заявка в ПДС на создание Подписки с кадровыми данными
НЕТ
Сертификат на ключевом носителе?
ДА
НЕТ
Заявка согласована?
ДА
Заявка в ПДС на создание Подписки с кадровыми данными
3.3. Подписание заявки на создание Подписки
Подписанная Уполномоченным лицом заявка в ПДС на создание Подписки
6
Конец


4. Подпроцесс «Перевыпуск Сертификата»
Администратор безопасности ОКЗ
Куратор от организации
2
Изменились данные в ИАСУП/ кадровые данные о Подписчике в ПДС изменил Куратор от организации?
Да
Нет
Заявку в ПДС создал Подписчик?
Да
Нет
Обращение в формализован ном виде
4.1. Создание заявки в ПДС на перевыпуск Сертификата в рамках подписки
Электронная заявка в ПДС на перевыпуск Сертификата
Кадровые данные взяты из ИАСУП?
Да
Нет
Заявка в ПДС на перевыпуск Сертификата
4.2. Дополнение заявки на создание Подписки кадровыми данными
Заявка в ПДС на перевыпуск Сертификата с кадровыми данными
И
5
6


5. Подпроцесс «Сокращение подписки и аннулирование Сертификата»
Администратор безопасности ОКЗ
Уполномоченное лицо от организации
ПДС
2
4
7
Изменились данные в ИАСУП (Подписчик уволен)/Куратор от организации внес данные в ПДС об увольнении Подписчика?
ДА
НЕТ
Заявку в ПДС создал Подписчик?
ДА
НЕТ
Обращение в формализованном виде
5.1. Создание заявки в ПДС на сокращение Подписки
Заявка в ПДС на сокращение Подписки
Сокращение Подписки на облачный Сертификат?
ДА
НЕТ
Заявка согласована?
НЕТ
ДА
Заявка в ПДС на сокращение Подписки
5.2. Подписание заявки на сокращение Подписки
Подписанная Уполномоченным лицом заявка в ПДС на сокращение Подписки
Из 5.2. Подписанная Уполномоченным лицом заявка в ПДС на сокращение Подписки
Из 4. Заявка в ПДС на перевыпуск Сертификата
Из 7. Заявка на создание Подписки с информацией о причинах отказа в вручении/получении Сертификата
Данные из ИАСУП об увольнении Подписчика/ данные из ПДС об увольнении Подписчика
5.3. Аннулирование Сертификата
Аннулированный Сертификат
Конец


6. Подпроцесс «Создание Сертификата»
3
4
8
ПДС
Из 3. Подписанная Уполномоченным лицом от организации заявка в ПДС на создание подписки
Из 4. Заявка в ПДС на перевыпуск Сертификата
Из 8. Заявка на выпуск нового Сертификата по причине истечения срока действия старого
6.1. Создание запроса на Сертификат
Ключевой контейнер
Запрос на сертификат
Запрос на сертификат
6.2. Выпуск Сертификата на неаккредитованном УЦ
Сертификат
Оператор УЦ от ПУСК ПДС
Сертификат на ключевом носителе?
НЕТ
ДА
Ключевой контейнер
Сертификат
6.3. Запись Сертификата на ключевой носитель
Готовый ключевой носитель
Готовый ключевой носитель
6.4.Создание пакета для передачи Сертификата
Пакет с Сертификатом
7
8


7. Подпроцесс «Вручение Сертификата»
Оператор УЦ от ПУСК ПДС
Администратор безопасности ОКЗ
Подписчик
6
Пакет с Сертификатом
7.1. Передача пакета с Сертификатом
Пакет с Сертификатом
7.2. Получение Сертификата
Подтверждение получения Сертификата в ПДС
Паспорт
7.3. Верификация Подписчика
Верификация пройдена?
НЕТ
ДА
Пакет с Сертификатом
7.4. Выдача пакета с Сертификатом
Заявка на создание Подписки
7.8. Внесение данных в заявку на создание Подписки о причинах отказа в выдаче Сертификата
Заявка на создание Подписки с причиной отказа в выдаче Сертификата
Пакет с Сертификатом
7.5. Получение Сертификата
Информация, сод. в Сертификате
7.6. Проверка сведений в Сертификате
Сведения в Сертификате корректны?
НЕТ
ДА
Информация, сод. в Сертификате
7.7. Подтверждение получения Сертификата
Подтверждение получения Сертификата в ПДС
ПИН-код от ключевого контейнера в ПДС
Заявка на создание Подписки
7.9. Внесение данных в заявку на создание Подписки о причинах отказа в получении Сертификата
Заявка на создание Подписки с причиной отказа в получении Сертификата
8
5


8. Подпроцесс «Контроль срока действия Сертификата»
ПДС
6
7
НЕТ
Срок действия Сертификата истекает?
ДА
Сертификат с истекающим сроком действия
8.1. Автоматическое создание заявки на выпуск нового Сертификата
Заявка на выпуск нового Сертификата по причине истечения срока действия старого
6

Приложение №2. Заявление на предоставление услуги

Заявление
на предоставление услуги платформы доверенных сервисов в отношении усиленных неквалифицированных сертификатов электронной подписи

« _____ » _____ 202 __ г.

_____
наименование организации, включая организационно-правовую форму

в лице _____
должность

_____
фамилия, имя, отчество

действующего на основании _____

в рамках оказания услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств запрашивает услугу по предоставлению пользователям информационных систем, подключенных к «Платформе доверенных сервисов» (далее – ПДС), сервисы, обеспечивающие функционал усиленной неквалифицированной электронной подписи (код услуги CLB.23), просит УВЕЛИЧИТЬ/УМЕНЬШИТЬ

(нужное подчеркнуть)

объемный показатель согласно перечню:

Тип сертификата	**Количество УНЭП**
УНЭП облачный (дистанционный)	

Уполномоченное должностное лицо

_____ _____ _____
(должность) (подпись) (ФИО)

М.П.

Приложение №3. Заявление на подтверждение электронной подписи в электронном документе

Заявление на подтверждение электронной подписи в электронном документе

« _____ » _____ 202 __ г.

_____
(наименование организации, включая организационно-правовую форму)

в лице_____
(должность руководителя)

_____
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит подтвердить подлинность УНЭП в электронном документе на основании следующихданных:

1. Подпись формата .sig или СМС, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № МД–XXX;

2. Файл, созданный с использованием Платформы доверенных сервисов, содержащий подписанные электронной подписью данные и значение УНЭП, либо файл, содержащий исходные данные и файл, содержащий значение УНЭП с подписью формата .SIG или СМС, на прилагаемом к заявлению носителе – рег. № XXXX.

3. Время на момент наступления которых требуется подтвердить подлинность УНЭП:

«_____:_____» «_____/_____/_____»;
Час минута день месяц год

Уполномоченное должностное лицо

_____ _____ _____
(должность) (подпись) (ФИО)

м.п.