Приложение № 8 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

УТВЕРЖДАЮ

Директор по информационным технологиям

АО «Гринатом»

М.П.

_____ / А.Н. Киселёв /

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ПО ИТ.
НАЧ. УПРАВЛ. И.П. ТАРАСОВ
ДОВЕРЕННОСТЬ ОТ 18.06.2021
22/306/2021-ДОВ

ПОРЯДОК

предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с использованием информационной системы Органа криптографической защиты»

Москва 2021 г.

Содержание

Назначение и область применения

Настоящий Порядок Корпоративного Удостоверяющего центра Госкорпорации «Росатом» (далее КУЦ), именуемый в дальнейшем «Порядок», разработан в соответствии с действующим законодательством Российской Федерации, регламентирующим деятельность удостоверяющих центров.

Общая информация о КУЦ:

Официальный сайт: https://crypto.rosatom.ru

Официальный E-mail: ca@rosatom.ru

Телефон: +7 (499) 949-49-19 доб. 54-54

Адрес нахождения: г. Москва, 1-й Нагатинский проезд, дом 10, стр. 1

Официальный адрес ИС ОКЗ: https://crypto.rosatom.local

Адрес публикации списков отозванных сертификатов:

http://crl1.rosatom.ru/ra/cdp/

http://crl2.rosatom.ru/ra/cdp/

http://crl1.rosatom.local/ra/cdp/

http://crl2.rosatom.local/ra/cdp/

Адрес публикации служб OCSP:

http://ocsp1.rosatom.ru/ocsp4/ocsp.srf

http://ocsp2.rosatom.ru/ocsp4/ocsp.srf

http://ocsp1.rosatom.local/ocsp4/ocsp.srf

http://ocsp2.rosatom.local/ocsp4/ocsp.srf

Адрес публикации служб TSP:

http://tsp1.rosatom.ru/tsp3/tsp.srf

http://tsp2.rosatom.ru/tsp3/tsp.srf

http://tsp1.rosatom.local/tsp3/tsp.srf

http://tsp2.rosatom.local/tsp3/tsp.srf

Требования настоящего Порядка распространяются на предприятия/ организации использующие автоматизированные и/или информационные системы, в которых применяются сертификаты ключей проверки электронных подписей, создаваемые КУЦ. Требования настоящего Порядка обязательны для выполнения сотрудниками, выполняющими следующие функциональные обязанности:

Руководитель предприятия/организации;

Пользователь КУЦ;

Администратор безопасности;

Сотрудник HR;

Оператор КУЦ;

Администратор КУЦ;

Порядок распространяется в форме электронного документа по адресу: URL= https://crypto.rosatom.ru/dokumentatsiya/reglamenty/reglament-kuts/

Порядок использует ссылки на следующие документы, необходимые для администрирования процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»:

Документ	Статус	Тип документа
Лицензия ФСБ России ЛСЗ №0014254 Рег.№15686 Н от 19.01.2017 на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)	Действует	Лицензия
Приказ ФАПСИ № 152 от 13 июня 2001г. «Об утверждении 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»	Действует	Приказ
Свидетельство об аккредитации удостоверяющего центра №758 от 21 августа 2017 г.	Действует	Свидетельство

Термины, определения и сокращения

Термин	Определение
Администратор безопасности	уполномоченный работник АО «Гринатом» (по договору) или уполномоченный сотрудник предприятия-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. N 63-ФЗ "Об электронной подписи"

Вручение сертификата ключа проверки электронной подписи	передача доверенным лицом удостоверяющего центра изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу
Информационная система органа криптографической защиты	Информационная система, предназначенная для автоматизации деятельности по управлению электронными ключами пользователей и средствами криптографической защиты
Квалифицированный сертификат ключа проверки электронной подписи (УКЭП)	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 аккредитованным 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
Неквалифицированный сертификат ключа проверки электронной подписи (УНЭП)	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, позволяющий формировать электронную подпись в соответствии со ст.5, часть 3 Федерального закона №63-ФЗ «Об электронной подписи»
Подписка	Заказ предприятия в ИС ОКЗ в соответствии с условиями договора присоединения на обеспечение сертификатами или средствами криптографической защиты и информации. Подписка подразумевает владение Пользователем КУЦ одним действующим сертификатом выбранного шаблона.
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;
Средства удостоверяющего центра	программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра
Средства электронной подписи	шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и 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	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	осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане
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

Сокращение	Расшифровка
ИАСУП	Информационная автоматизированная система управления персоналом Госкорпорации «Росатом»
ИС ОКЗ	Информационная система органа криптографической защиты
КУЦ	Корпоративный Удостоверяющий центр
Сертификат	Сертификат ключа проверки электронной подписи
СОС	Список отозванных сертификатов
УКЭП	Квалифицированный сертификат ключа проверки электронной подписи
УНЭП	Неквалифицированный сертификат ключа проверки электронной подписи
ЭД	Электронный документ
ЭП	Электронная подпись

Описание процесса

3.1 Цель процесса

Предоставление услуг КУЦ в соответствии с действующим законодательством Российской Федерации.

3.2 Задачи процесса

Данный процесс решает следующие задачи:

- создания сертификатов и выдачи таких сертификатов лицам, обратившимся за их получением;
- установления сроков действия сертификатов;
- аннулирования сертификатов, выданных КУЦ;
- выдачи по обращению заявителя средств ЭП, содержащих ключи ЭП и ключи проверки ЭП, созданные КУЦ;
- ведения реестра выданных и аннулированных сертификатов (далее - реестр сертификатов), в том числе включающего в себя информацию,

содержащуюся в сертификатах, и информацию о датах прекращения действия или аннулирования сертификатов и об основаниях таких прекращения или аннулирования;

- создания по обращениям заявителей ключей ЭП и ключей проверки ЭП;
- проверки уникальности ключей проверки ЭП в реестре сертификатов;
- осуществления по обращениям участников электронного взаимодействия проверки ЭП;
- информирования в письменной форме заявителей об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки;
- обеспечения актуальности информации, содержащейся в реестре сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- предоставления безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информации, содержащейся в реестре сертификатов, в том числе информации об аннулировании сертификатов ключей проверки ЭП;
- обеспечения конфиденциальности созданных КУЦ ключей ЭП;
- осуществления иной, связанной с использованием ЭП деятельности.

3.3. Участники группы процессов и их роли

№	Участники	Основные роли
1	Пользователь КУЦ	• Обладает учётной записью в домене GK • Создаёт обращение • Получает сертификаты
2	Уполномоченное лицо предприятия	• Согласовывает и подписывает электронные заявки в ИС ОКЗ на создание и сокращение подписок предприятия;
3	Сотрудник HR	• Согласование создания подписки на обеспечение сертификатом в части кадровых данных пользователя КУЦ • Корректировка подписки на обеспечение сертификатом в части кадровых данных пользователя КУЦ

4	Администратор безопасности ОКЗ	• Обработка и формализация обращения • Создание подписки на обеспечение сертификатом • Корректировка подписки на обеспечение сертификатом; • Сокращение подписки на обеспечение сертификатом • Согласование Перевыпуска сертификата • Вручение сертификата УКЭП и УНЭП • Контроль действия сертификата
5	Оператор КУЦ	• Создание сертификата УКЭП • Создание сертификата УНЭП
6	Администратор КУЦ	• Аннулирование сертификата

3.4 Описание подпроцессов

3.4.1. Подпроцесс «Обработка обращения»

Администратор безопасности получает обращение от следующих возможных инициаторов:

Пользователь КУЦ;

АБ;

уполномоченное лицо предприятия;

контактное лицо;

одним из следующих способов:

заявка в ИС ОКЗ;

заявка через порталы АО «Гринатом» или «Страна Росатом»;

заявка через СУ ИТ;

электронное письмо на п/я 1111@greenatom.ru;

электронное письмо на п/я ca@rosatom.ru;

звонок в центр поддержки пользователей АО «Гринатом»;

Администратор безопасности определяет наличие подписки и учётной записи в домене GK у пользователей КУЦ, указанных в обращении;

Администратор безопасности формализует обращение в соответствии с правилами формализации, изложенными на официальном сайте КУЦ в зависимости от следующих условий:

В случае если подписка на пользователя КУЦ, указанного в обращении, отсутствует и обращение на создание подписки, то исходящая информация

поступает в подпроцесс «Создание подписки на обеспечение сертификатом» в соответствии с выбранным шаблоном.

Администратор безопасности должен определить шаблон для выпуска сертификата на основании неформализованного обращения Пользователя КУЦ.

В случае если подписка на обеспечение сертификатом на пользователя КУЦ, указанного в обращении, есть и обращение связано с изменением данных пользователя КУЦ, то исходящая информация поступает в подпроцесс «Корректировка подписки»

В случае если подписка на обеспечение сертификатом на пользователя КУЦ, указанного в обращении, есть и обращение на сокращение подписки, то исходящая информация поступает в подпроцесс «Сокращение подписки на обеспечение сертификатом» в соответствии с указанным в обращении сертификатом.

В случае если подписка на обеспечение сертификатом на пользователя КУЦ, указанного в обращении, есть и обращение связано с компрометацией или подозрением на компрометацию, то исходящая информация поступает в подпроцесс «Перевыпуск сертификата».

Если обращение содержит иные данные, процесс оканчивается.

Исходящая информация поступает в подпроцесс «Создание сертификата», либо в подпроцесс «Сокращение подписки на обеспечение сертификатом», либо в подпроцесс «Корректировка подписки», либо в подпроцесс «Перевыпуск сертификата».

3.4.2. Подпроцесс «Создание подписки на обеспечение сертификатом»

Входящая информация поступает из подпроцесса «Обработка обращений»

Администратор безопасности получает электронное уведомление и визирует заявку. Если заявка отклонена – процесс завершается. Если заявка не отклонена – Администратор безопасности выбирает шаблон для выпуска сертификата и одобряет заявку.

В случае, если выбран шаблон Сертификат УНЭП, то сотрудник HR получает электронное уведомление, проверяет корректность информации о Сотруднике в объеме, необходимом для выпуска сертификата УНЭП и одобряет заявку. Данный шаг может быть произведён автоматически, при наличии данных о Пользователе КУЦ в Информационной автоматизированной системе управления персоналом Госкорпорации «Росатом» (далее - ИАСУП)

В случае если выбран шаблон Сертификат УКЭП, то сотрудник HR получает электронное уведомление, проверяет корректность информации о Сотруднике, вносит в информацию пользователе КУЦ, в объеме, необходимом для выпуска сертификата УКЭП и регистрации его в ЕСИА и

одобряет заявку. Данный шаг может быть произведён автоматически, при наличии данных о Пользователе КУЦ в ИАСУП.

Для выпуска Сертификата УКЭП ИС ОКЗ с использованием инфраструктуры осуществляет проверку достоверности документов и сведений: производится проверка СНИЛС в сервисе ПФР, получение выписки из ЕГРЮЛ в сервисе ФНС, проверка паспортных данных в сервисе МВД. В случае не получения ответа от любого сервиса СМЭВ процесс возвращается на предыдущий шаг.

Уполномоченному лицу формируется и отправляется электронное уведомление. Уполномоченное лицо подписывает PDF-документ, печатный аналог электронной заявки, с использованием сервиса электронной подписи КриптоПро DSS. Если заявка отклонена – процесс завершается, если заявка одобрена – Оператору УЦ формируется и отправляется электронное уведомление. Оператор УЦ вычисляется автоматически в соответствии с настройками ИС ОКЗ согласно принадлежности заявителя к той или иной организации.

Исходящая информация поступает в подпроцесс «Создание сертификата УКЭП» или подпроцесс «Создание сертификата УНЭП» в зависимости от выбранного шаблона.

3.4.3. Подпроцесс «Корректировка подписки на обеспечение сертификатом»

Входящая информация поступает из подпроцесса «Обработка обращений»

Корректировка подписки на обеспечение сертификатом УКЭП/УНЭП производится самостоятельно Пользователем КУЦ при помощи веб-интерфейса сервиса «Управление инфраструктурой открытых ключей».

Корректировка подписки на обеспечение сертификатом УНЭП может производиться в автоматическом режиме получении данных из ИАСУП, входящих в перечень полей «Имя субъекта» в сертификате УНЭП.

После подтверждения необходимости корректировки подписки Администратор безопасности одобряет заявку.

В случае корректировки подписки на обеспечение сертификатом УКЭП, Сотруднику HR формируется и отправляется электронное уведомление. Сотрудник HR получает электронное уведомление, вносит в информацию пользователе КУЦ, в объеме, необходимом для выпуска сертификата УКЭП и регистрации его в ЕСИА. Данный шаг может быть произведён автоматически, при наличии данных о Пользователе КУЦ в ИАСУП.

Для выпуска Сертификата УКЭП ИС ОКЗ с использованием инфраструктуры осуществляет проверку достоверности документов и сведений: производится проверка СНИЛС в сервисе ПФР, получение выписки из ЕГРЮЛ в сервисе ФНС, проверка паспортных данных в сервисе

МВД. В случае не получения ответа от любого сервиса СМЭВ процесс возвращается на предыдущий шаг.

Исходящая информация поступает в подпроцесс «Создание сертификата УКЭП»

3.4.4. Подпроцесс «Сокращение подписки на обеспечение сертификатом».

Входящая информация поступает из подпроцесса «Обработка обращений»

Сокращение подписки на обеспечение сертификатом УКЭП производится самостоятельно при помощи личного кабинета Пользователя ИС ОКЗ.

Сокращение подписки на обеспечение сертификатом УНЭП может производиться в автоматическом режиме при выборе соответствующего шаблона.

Инициирование сокращения подписки на обеспечение сертификатом УКЭП/УНЭП пользователю КУЦ (инициирование должно быть доступно пользователю КУЦ и Администратору безопасности).

Администратору безопасности формируется и отправляется электронное уведомление.

Администратор безопасности получает электронное уведомление и визирует заявку. Если заявка отклонена – процесс завершается, если заявка одобрена – Уполномоченному лицу формируется и отправляется электронное уведомление.

Уполномоченному лицу формируется и отправляется электронное уведомление.

Уполномоченное лицо получает электронное уведомление и визирует заявку. Если заявка отклонена – процесс завершается, если заявка одобрена – ИС ОКЗ автоматически отзывает сертификат на УЦ.

Исходящая информация поступает в подпроцесс «Аннулирование сертификата»

3.4.5. Подпроцесс «Перевыпуск сертификата».

Входящая информация поступает из подпроцесса «Обработка обращений»

Инициатором перевыпуска сертификата может быть Пользователь КУЦ, имеющий действующую подписку на сертификат с совпадающим шаблоном.

Перевыпуск сертификата производится при компрометации или подозрении на компрометацию сертификата ключа проверки электронной подписи.

Исходящая информация поступает в подпроцесс «Аннулирование сертификата»

3.4.6. Подпроцесс «Аннулирование сертификата».

Входящая информация поступает из подпроцессов «Корректировка подписки на обеспечение сертификатом», «Сокращение подписки на обеспечение сертификатом» и «Перевыпуск сертификата УКЭП»

Подпроцесс «Аннулирование сертификата» регламентирует аннулирование сертификатов КУЦ.

КУЦ уведомляет Пользователя КУЦ и всех лиц, зарегистрированных в КУЦ, об аннулировании сертификата не позднее 12 часов с момента наступления описанного события.

КУЦ аннулирует сертификат Пользователя КУЦ в следующих случаях:

- При сокращении Руководителем предприятия подписки на обеспечение сертификатом ключа проверки электронной подписи;
- по заявке Пользователя КУЦ в ИС ОКЗ;
- в случае прекращения действия Договора;
- в случае, если не подтверждено, что владелец сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- в случае, если установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате;
- в случае, если вступило в силу решение суда, которым, в частности, установлено, что сертификат содержит недостоверную информацию.
- при компрометации ключа ЭП Уполномоченного лица КУЦ. Временем аннулирования сертификата Пользователя КУЦ признается время компрометации ключа Уполномоченного лица КУЦ, фиксирующееся в реестре КУЦ.

Администратор УЦ получает электронное уведомление, проверяет отзыв сертификата на УЦ и визирует заявку. Администратор УЦ осуществляет обработку электронного заявления на аннулирование сертификата и вносит информацию об аннулировании в ИС ОКЗ.

Если заявка отклонена – процесс завершается, если заявка одобрена – сертификат принимает статус отозванного в ИС ОКЗ.

При наличии действующей подписки на обеспечение сертификатом, исходящая информация поступает в подпроцесс «Создание сертификата УКЭП»

При отсутствии действующей подписки на обеспечение сертификатом процесс заканчивается.

3.4.7. Подпроцесс «Создание сертификата УКЭП»

Входящая информация поступает из подпроцессов «Создание подписки на обеспечение сертификатом» и «Аннулирование сертификата»

Оператор КУЦ получает электронное уведомление, подключает ключевой носитель (при необходимости использования ключевого носителя) к рабочему месту Оператора КУЦ.

Оператор КУЦ выбирает параметры ключевого контейнера, создает ключевой контейнер и запрос на сертификат. Выполняется выпуск сертификата на УЦ, соответствующему шаблону сертификата в УЦ.

Оператор КУЦ устанавливает выпущенный сертификат на ключевой носитель (при необходимости использования ключевого носителя).

При выдаче квалифицированного ИС ОКЗ направляет в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра).

Оператор КУЦ создаёт пакет для передачи выпущенного сертификата Администратору безопасности лично или Службой специальной связи.

Исходящая информация поступает в подпроцесс «Вручение сертификата УКЭП»

3.4.8. Подпроцесс «Вручение сертификата УКЭП»

Входящая информация поступает из подпроцесса «Создание сертификата УКЭП»

Администратору безопасности формируется и отправляется электронное уведомление о необходимости получения ключевого носителя.

В случае использования ключевого носителя, Оператор УЦ передает ключевой носитель Администратору безопасности.

Администратор безопасности подтверждает получение в ИС ОКЗ.

Пользователю КУЦ формируется и отправляется электронное уведомление о выпуске сертификата.

Администратор безопасности верифицирует пользователя КУЦ и одобряет заявку. При вручении сертификата Администратор безопасности обязан установить личность Пользователя КУЦ и получить подтверждение правомочия обращаться за получением квалифицированного сертификата.

Пользователь КУЦ получает ключевой носитель с выпущенным сертификатом (при наличии).

В присутствии Администратора безопасности Пользователь КУЦ аутентифицируется в личном кабинете ИС ОКЗ, где ознакамливается с

информацией, содержащейся в квалифицированном сертификате и нажимает кнопку «Сертификат получен». Нажатие Пользователем КУЦ на кнопку «Сертификат получен» является равнозначным применению простой электронной подписи в Сертификате УКЭП.

Исходящая информация поступает в подпроцесс «Контроль действия сертификата»

3.4.9. Подпроцесс «Создание сертификата УНЭП»

Входящая информация поступает из подпроцессов «Создание подписки на обеспечение сертификатом УНЭП» и «Перевыпуск сертификата УНЭП»

При выборе шаблона для выпуска Сертификата УНЭП в автоматическом режиме, выпуск сертификата УНЭП производится без участия Оператора КУЦ.

В случае, если сертификат УНЭП выпускается на ключевом носителе, Оператор КУЦ получает электронное уведомление, подключает ключевой носитель к рабочему месту Оператора КУЦ.

Оператор КУЦ выбирает параметры ключевого контейнера, создает ключевой контейнер и запрос на сертификат. Выполняется выпуск сертификата на УЦ, соответствующему шаблону сертификата в УЦ.

Оператор КУЦ устанавливает выпущенный сертификат на ключевой носитель (при необходимости использования ключевого носителя).

Оператор КУЦ устанавливает выпущенный сертификат на ключевой носитель пользователя КУЦ (при необходимости использования ключевого носителя).

Создаёт пакет для передачи выпущенного сертификата Администратору безопасности лично или Службой специальной связи.

Исходящая информация поступает в подпроцесс «Вручение сертификата УНЭП»

3.4.10. Подпроцесс «Вручение сертификата УНЭП»

Входящая информация поступает из подпроцесса «Создание сертификата УНЭП»

При выдаче сертификата УНЭП на ключевом носителе Администратору безопасности формируется и отправляется электронное уведомление. Оператор УЦ передает ключевой носитель Администратору безопасности.

Администратор безопасности получает электронное уведомление и визирует заявку.

Пользователю КУЦ формируется и отправляется электронное уведомление о выпуске сертификата.

Администратор безопасности верифицирует пользователя КУЦ и одобряет заявку. При вручении сертификата Администратор безопасности обязан установить личность Пользователя КУЦ.

В присутствии Администратора безопасности Пользователь КУЦ аутентифицируется в личном кабинете ИС ОКЗ, где ознакамливается с информацией, содержащейся в квалифицированном сертификате, руководством по обеспечению безопасности Средства электронной подписи, ПИН-кодом и нажимает кнопку «Сертификат получен».

Исходящая информация поступает в подпроцесс «Контроль действия сертификата»

3.4.11. Подпроцесс «Контроль действия сертификата»

Контроль действия сертификата УКЭП инициируется автоматически за 90 дней до окончания действия сертификата.

Администратору безопасности формируется и отправляется электронное уведомление.

Администратор безопасности получает электронное уведомление и визирует заявку. Если заявка отклонена – процесс завершается. Если заявка не отклонена – Администратор безопасности выбирает шаблон для выпуска сертификата и одобряет заявку.

Сотруднику HR формируется и отправляется электронное уведомление.

Сотрудник HR получает электронное уведомление и визирует заявку. Сотрудник HR проверяет корректность информации о Сотруднике, заполняет недостающую информацию и одобряет заявку.

При выпуске сертификата УКЭП производится проверка СНИЛС в сервисе ПФР, получение выписки из ЕГРЮЛ в сервисе ФНС, проверка паспортных данных в сервисе МВД.

В случае не получения ответа от любого сервиса СМЭВ процесс возвращается на предыдущий шаг.

Исходящая информация поступает в подпроцесс «Создание сертификата УКЭП»

Нормативные ссылки

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

Приказ ФСБ РФ от 27 декабря 2011 г. N 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи".

Приказ ФСБ РФ от 27 декабря 2011 г. N 796 "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра".

Приказ Министерства связи и массовых коммуникаций РФ от 23 ноября 2011 г. № 320 “Об аккредитации удостоверяющих центров”.

Порядок внесения изменений

КУЦ в одностороннем порядке вносит изменения в Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с использованием Информационной системы органа криптографической защиты.

Внесение изменений (дополнений) в Порядок, а также в Приложения к нему, производится посредством утверждения новой редакции Порядка. Новая версия Порядка вступает в силу через 30 (тридцать) дней после публикации на сайте КУЦ.

Все Приложения, изменения и дополнения к настоящему Порядку являются его составной и неотъемлемой частью.

Контроль и ответственность

6.1 Контроль выполнения требований Порядка

За несоблюдение Порядка ответственные лица несут административную и дисциплинарную ответственность в соответствии с действующим законодательством.

Пользователь КУЦ несёт ответственность за:

- обеспечение конфиденциальности ключей ЭП, в частности не допущение использования принадлежащих ему ключей ЭП без его согласия;
- уведомление КУЦ и иных участников электронного взаимодействия о нарушении конфиденциальности ключа ЭП в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- не использование ключа ЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

Администратор безопасности несёт ответственность за:

- точность и своевременность формализации обращений пользователей КУЦ;
- идентификацию и аутентификацию Пользователя КУЦ и проверку представленных документов;
- выдачу Пользователю КУЦ ключевых документов;

Оператор КУЦ несёт ответственность за:

- формирование комплекта ключевых документов, выдаваемых КУЦ;
- передачу (отправку) комплекта документов, выдаваемых КУЦ;
- за правильность выполнения подпроцессов в соответствии с инструкцией Оператора;
- за конфиденциальность ключей ЭП.

Администратор КУЦ несёт ответственность за:

- правильность настройки и работоспособности ПАК и сервисов CRL;
- за конфиденциальность ключей ЭП КУЦ;

Администратор КУЦ контролирует действия Оператора КУЦ в рамках своих функциональных обязанностей.

Руководитель предприятия/организации несёт ответственность за достоверность предоставляемых документов в КУЦ.

6.2 Ответственность работников за несоблюдение требований Порядка

За несоблюдение Порядка ответственные лица несут административную и дисциплинарную ответственность в соответствии с действующим законодательством и в соответствии со следующей матрицей ответственности:

Подпроцессы в составе процесса	Участники процесса					
	Руководитель организации	Пользователь КУЦ	Администратор безопасности	HR	Оператор КУЦ	Администратор КУЦ
Подпроцесс «Обработка обращения»			О			К
Подпроцесс «Создание подписки на обеспечение сертификатом»	Инф		О	О		К
Подпроцесс «Корректировка подписки на обеспечение сертификатом»			О	О		К
Подпроцесс «Сокращение подписки на обеспечение сертификатом»	Инф		О			К
Подпроцесс «Перевыпуск сертификата»		Инф	О			К
Подпроцесс «Аннулирование сертификата»		Инф				О
Подпроцесс «Создание сертификата УКЭП»		Инф			О	К
Подпроцесс «Вручение сертификата УКЭП»		Инф	О			К
Подпроцесс «Создание сертификата УНЭП»		Инф			О	К
Подпроцесс «Вручение сертификата УНЭП»		Инф	О			К
Подпроцесс «Контроль действия сертификата»			О			К

Название (включая сокращение названия) и определение ролей в матрице распределения ответственности и полномочий справочно приведено в таблице ниже:

Сокращение	Название роли	Определение
	Контролер	Осуществляет контроль выполнения и достижения результатов подпроцесса/процедуры
О	Ответственный	Несет ответственность за достижение результата по подпроцессу/процедуре в совей предметной области

Сокращение	Название роли	Определение
Инф	Информируемый	Получает информацию о ходе/результате подпроцесса /процедуры

Перечень приложений

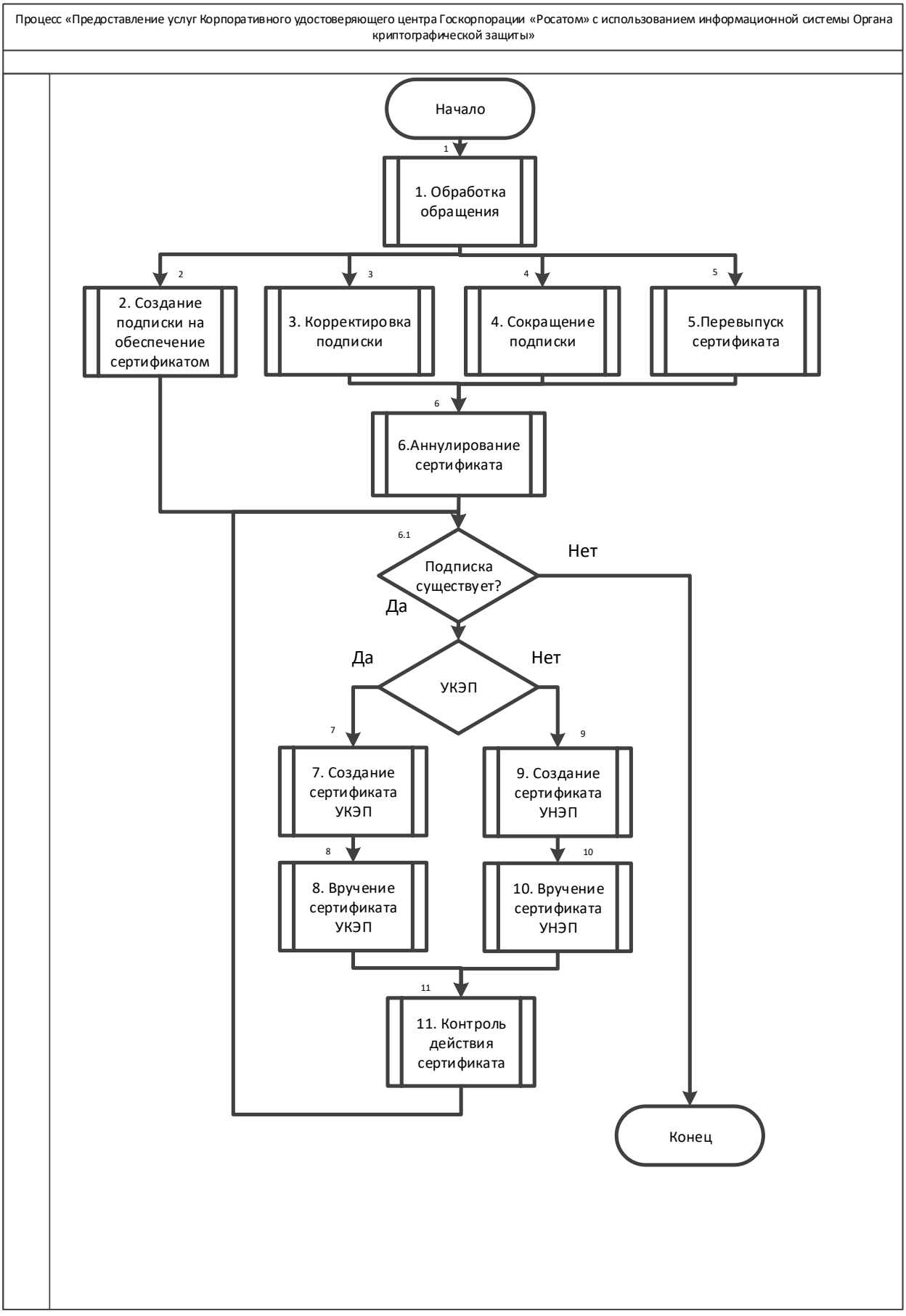
Приложение №1. Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»

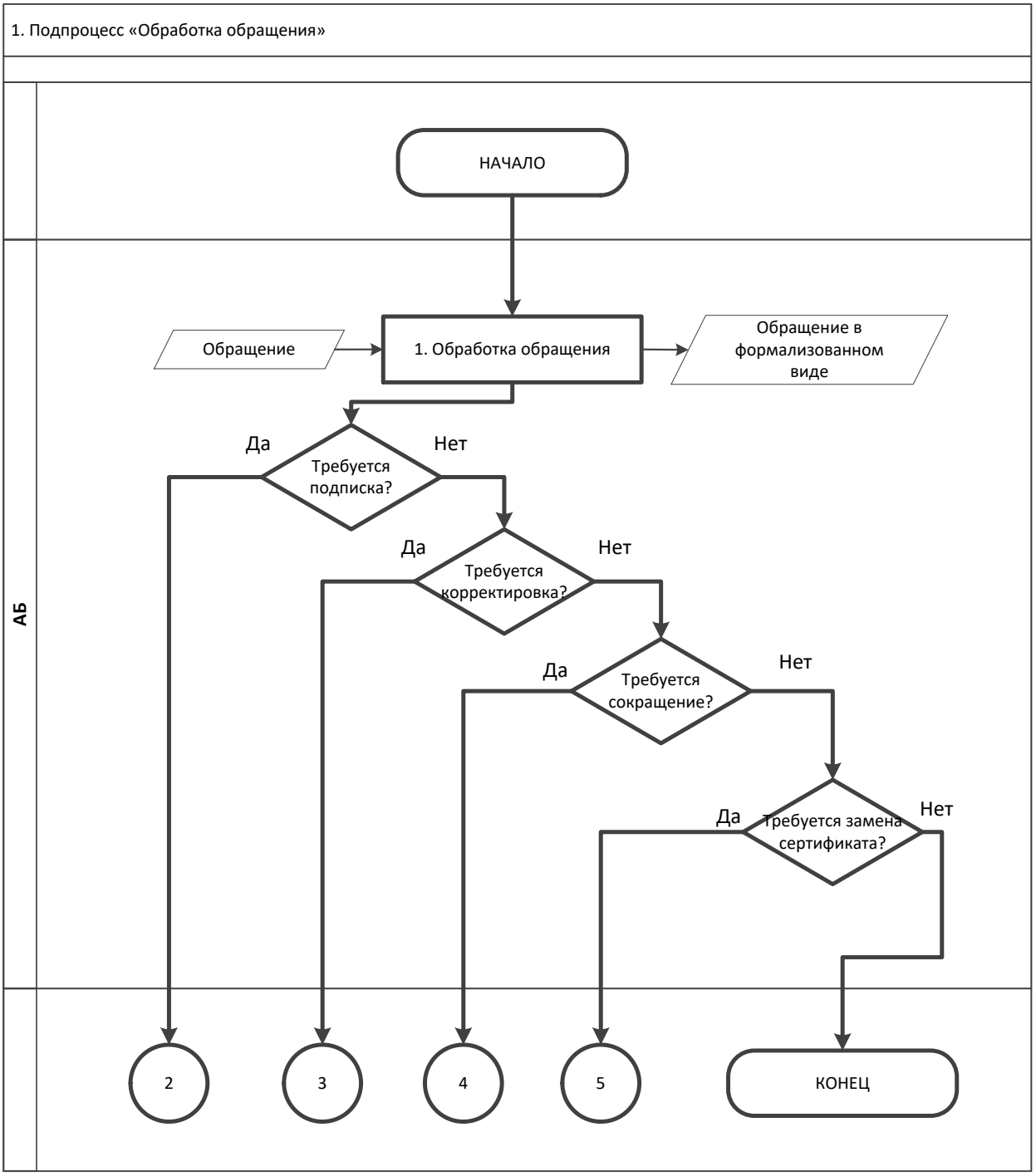
Приложение №2. Формат сертификатов ключа проверки электронной подписи

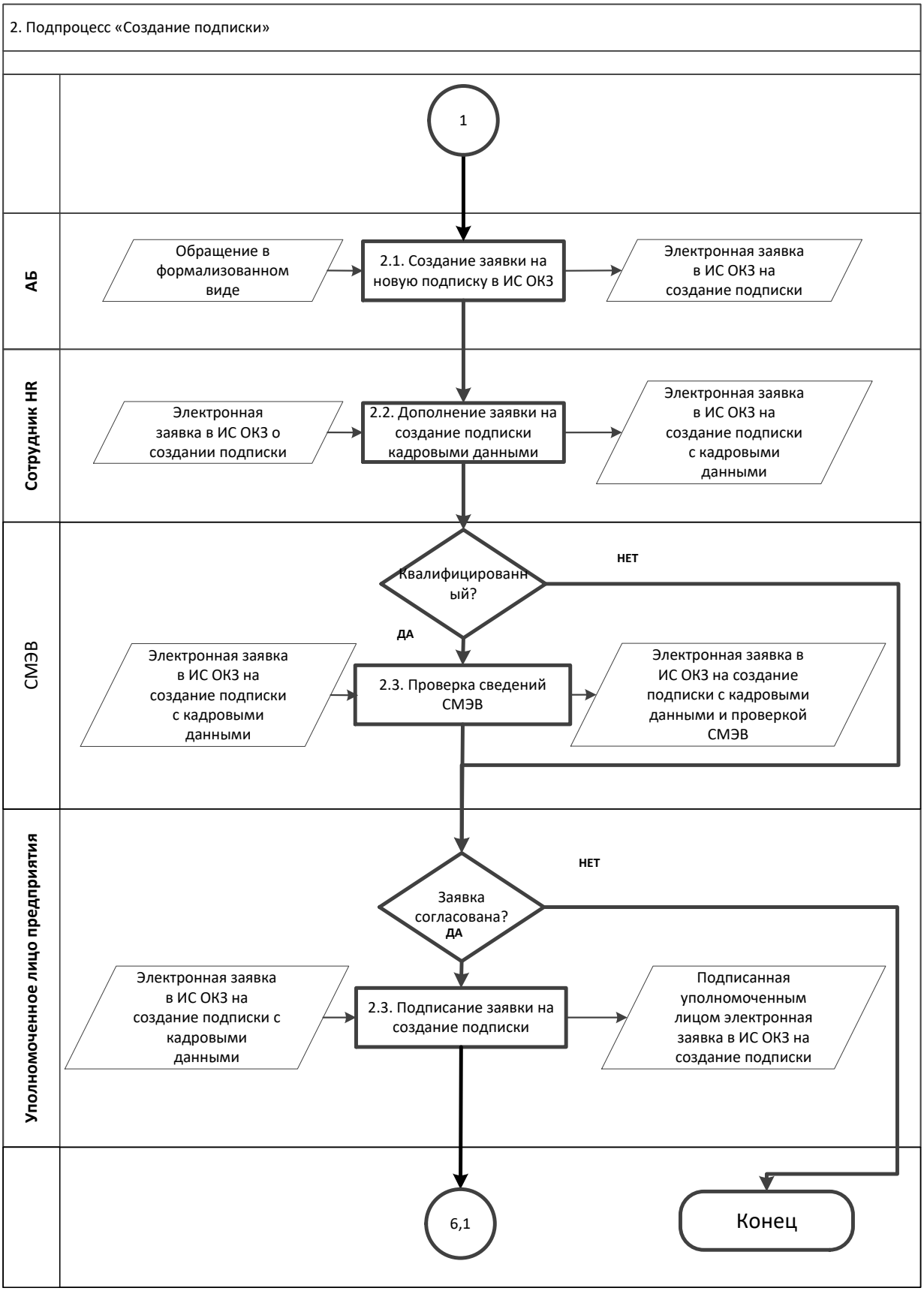
Приложение №3. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

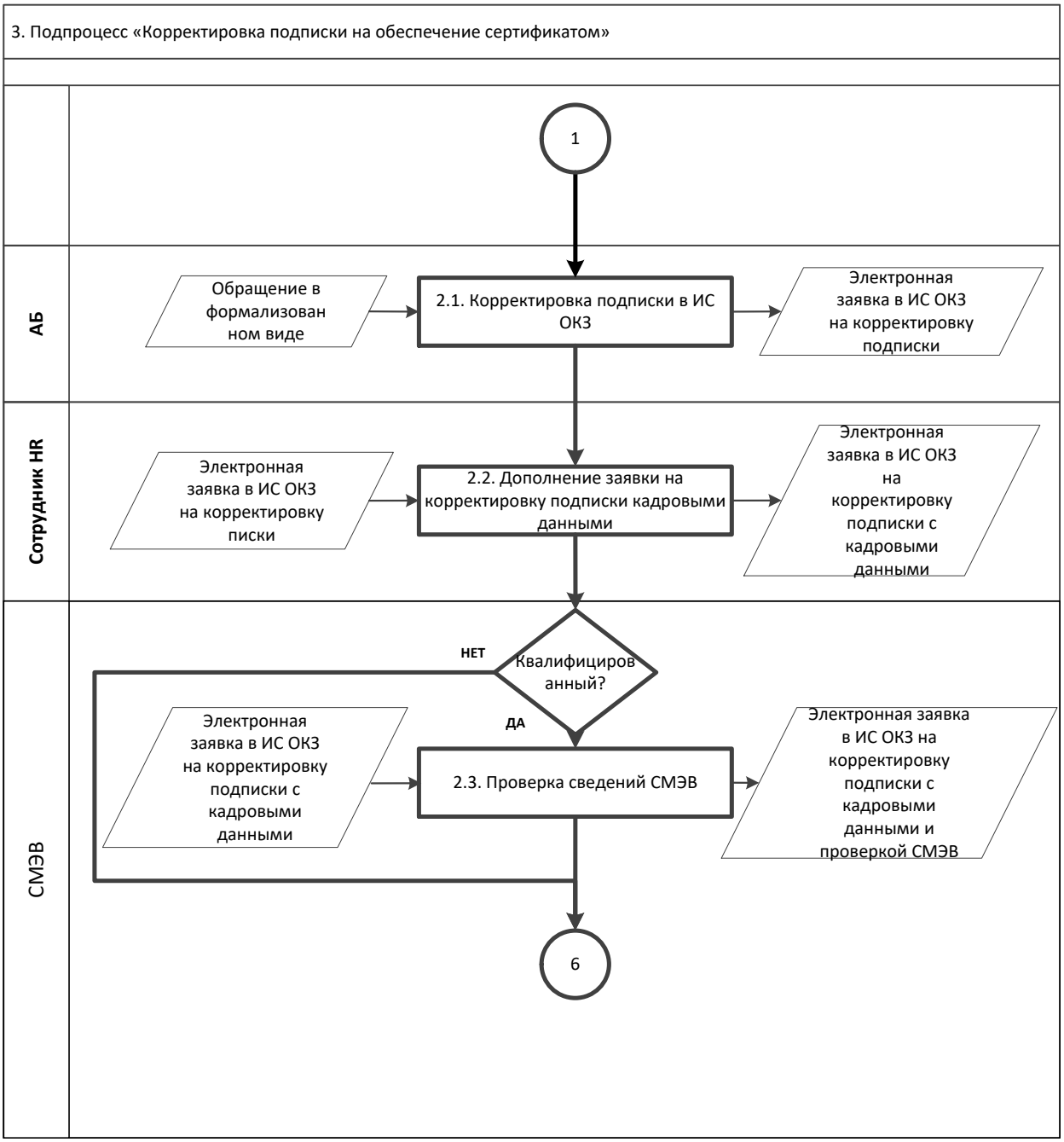
Приложение №4. Шаблоны сертификатов ключей проверки электронной подписи

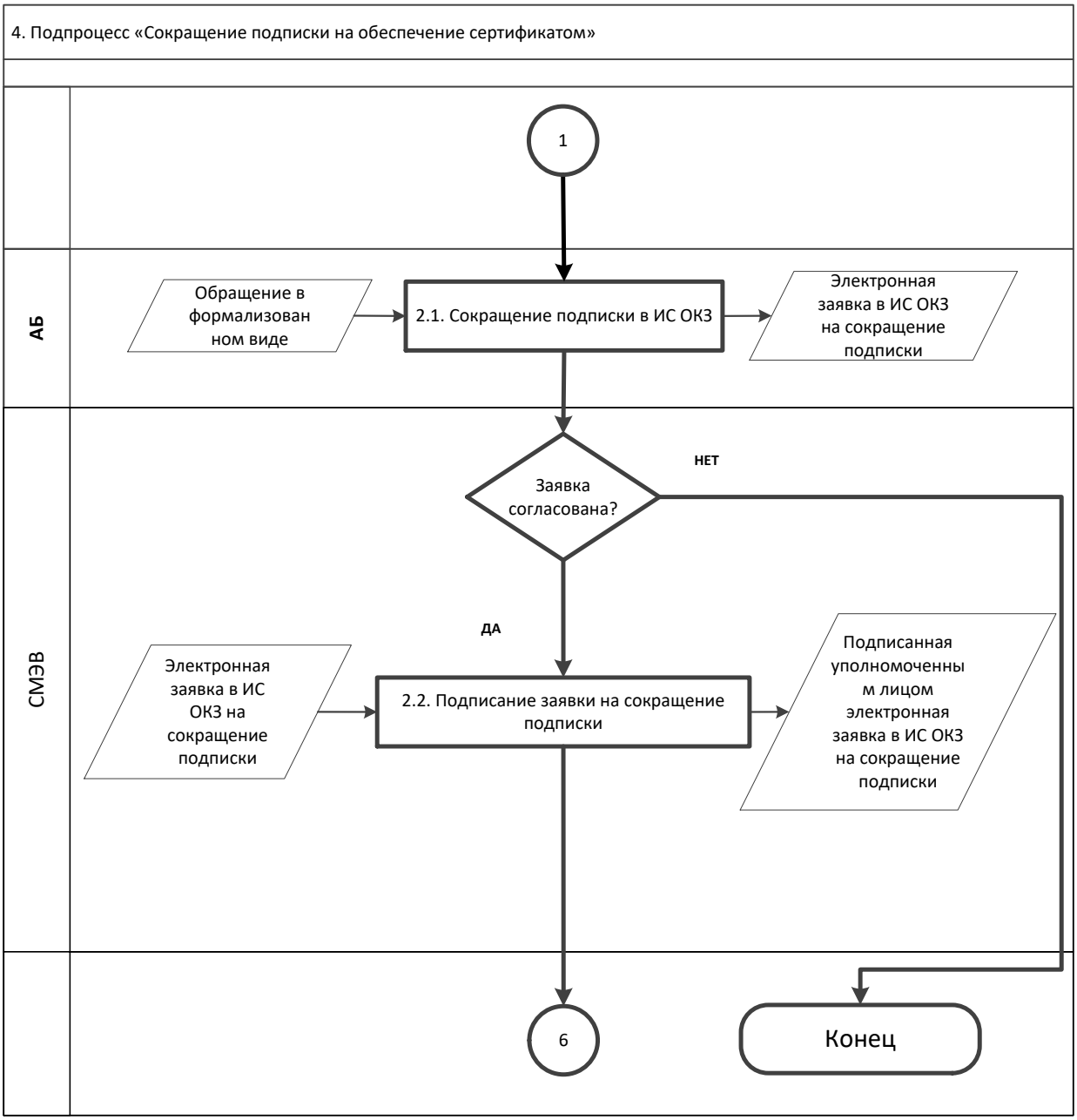
Приложение №1. Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»

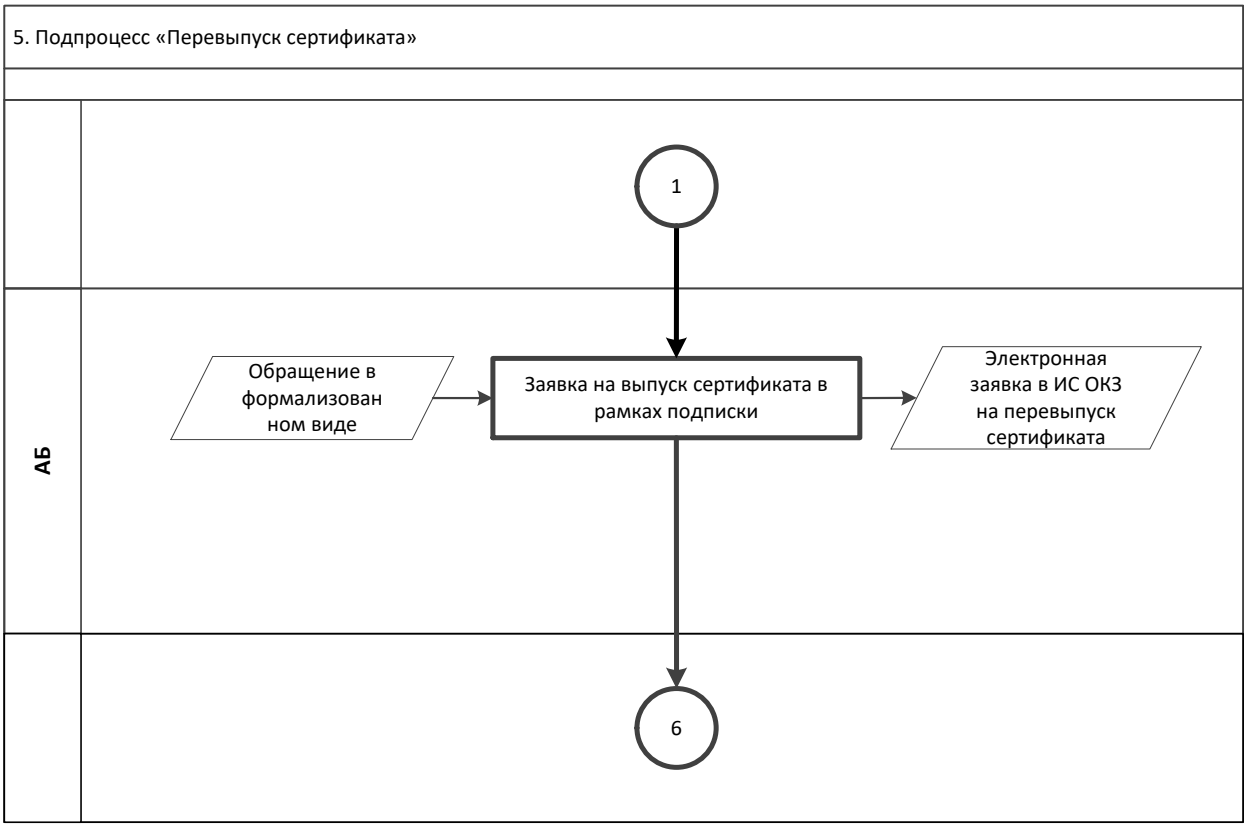


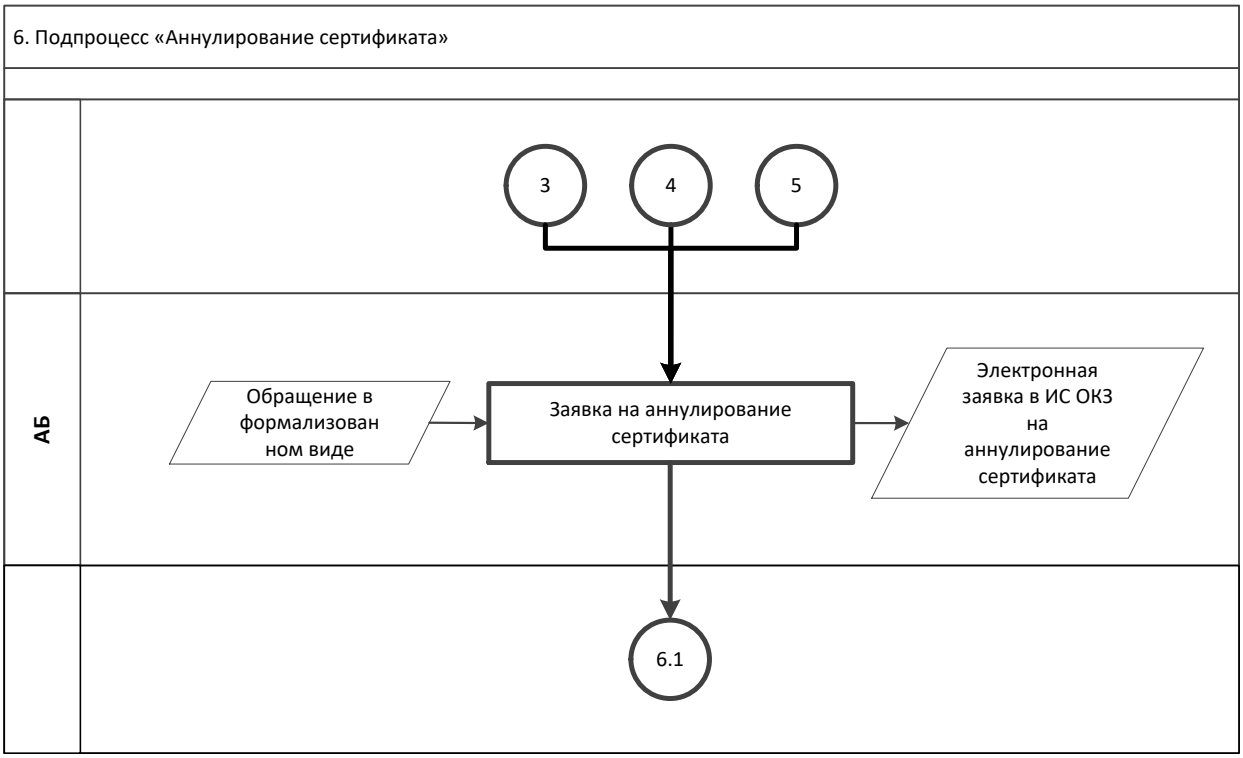

1. Подпроцесс «Обработка обращения»
АБ
НАЧАЛО
Обращение
1. Обработка обращения
Обращение в формализованном виде
Да
Требуется подписка?
Нет
Да
Требуется корректировка?
Нет
Да
Требуется сокращение?
Нет
Да
Требуется замена сертификата?
Нет
2
3
4
5
КОНЕЦ

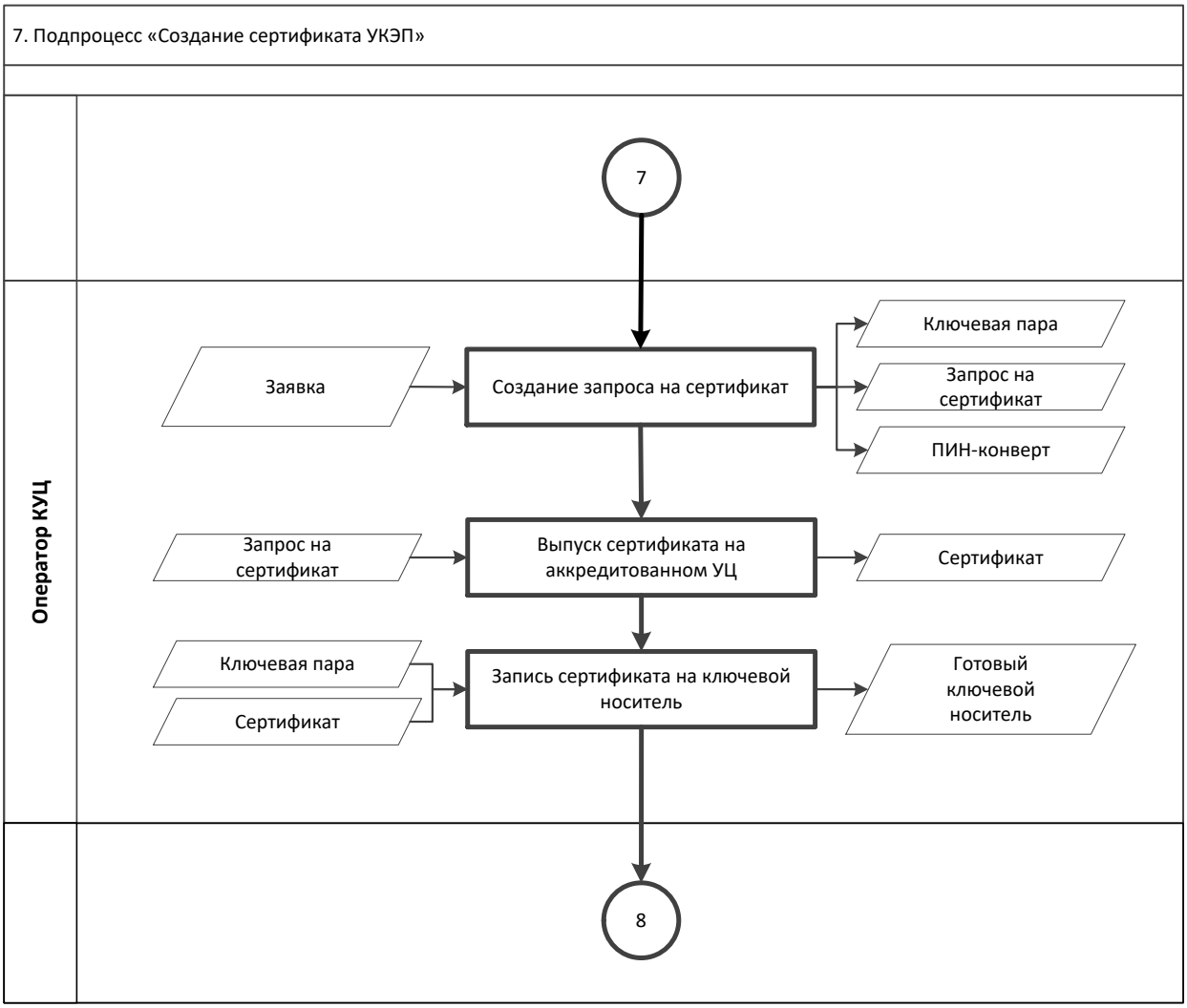

2. Подпроцесс «Создание подписки»
1
АБ
Обращение в формализованном виде
2.1. Создание заявки на новую подписку в ИС ОКЗ
Электронная заявка в ИС ОКЗ на создание подписки
Сотрудник HR
Электронная заявка в ИС ОКЗ о создании подписки
2.2. Дополнение заявки на создание подписки кадровыми данными
Электронная заявка в ИС ОКЗ на создание подписки с кадровыми данными
СМЭВ
Квалифицированный?
НЕТ
ДА
Электронная заявка в ИС ОКЗ на создание подписки с кадровыми данными
2.3. Проверка сведений СМЭВ
Электронная заявка в ИС ОКЗ на создание подписки с кадровыми данными и проверкой СМЭВ
Уполномоченное лицо предприятия
Заявка согласована?
НЕТ
ДА
Электронная заявка в ИС ОКЗ на создание подписки с кадровыми данными
2.3. Подписание заявки на создание подписки
Подписанная уполномоченным лицом электронная заявка в ИС ОКЗ на создание подписки
6,1
Конец


3. Подпроцесс «Корректировка подписки на обеспечение сертификатом»
1
АБ
Обращение в формализован ном виде
2.1. Корректировка подписки в ИС ОКЗ
Электронная заявка в ИС ОКЗ на корректировку подписки
Сотрудник HR
Электронная заявка в ИС ОКЗ на корректировку писки
2.2. Дополнение заявки на корректировку подписки кадровыми данными
Электронная заявка в ИС ОКЗ на корректировку подписки с кадровыми данными
СМЭВ
НЕТ
Квалифициров анный?
ДА
Электронная заявка в ИС ОКЗ на корректировку подписки с кадровыми данными
2.3. Проверка сведений СМЭВ
Электронная заявка в ИС ОКЗ на корректировку подписки с кадровыми данными и проверкой СМЭВ
6

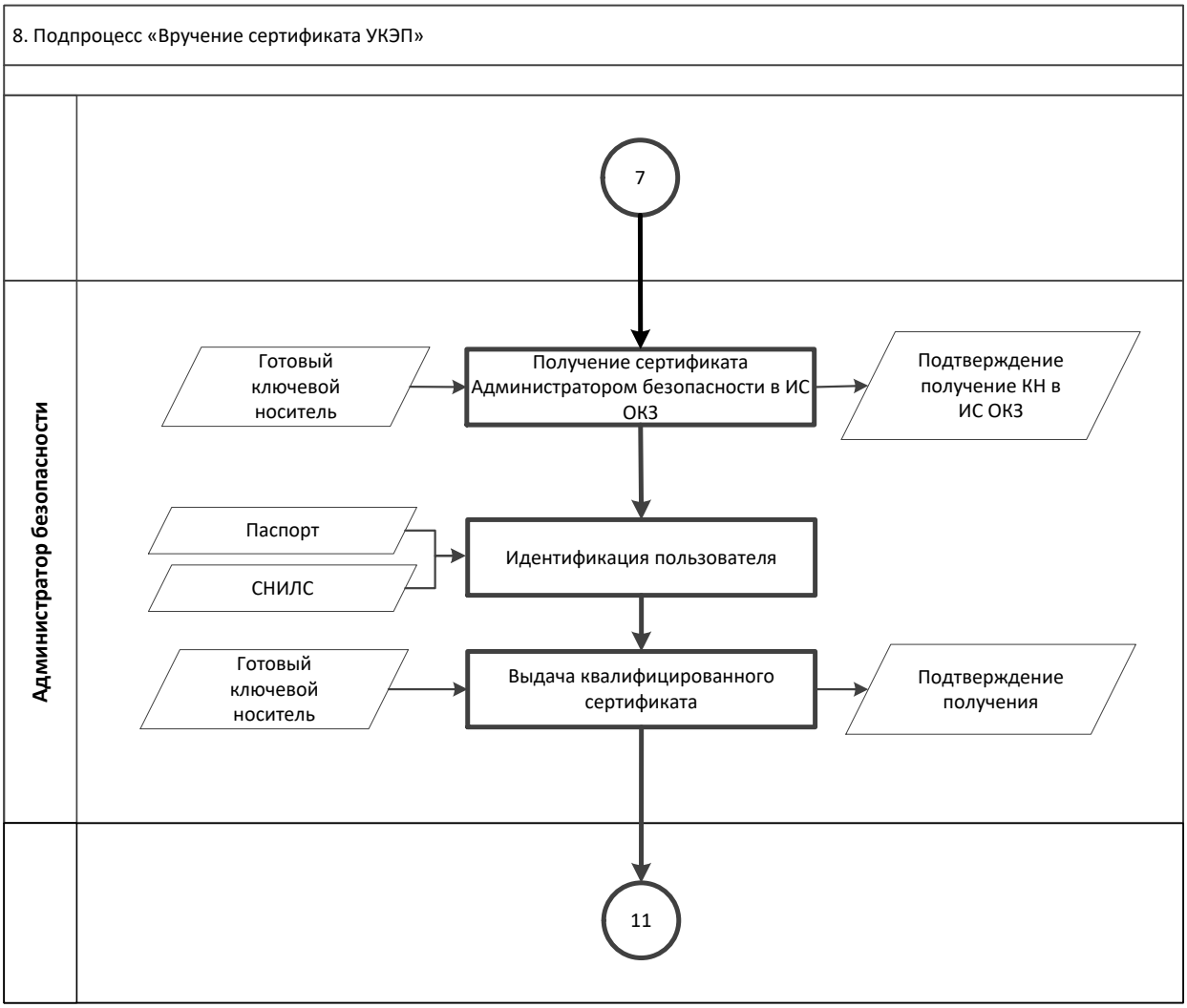

4. Подпроцесс «Сокращение подписки на обеспечение сертификатом»
АБ
СМЭВ
1
Обращение в формализованном виде
2.1. Сокращение подписки в ИС ОКЗ
Электронная заявка в ИС ОКЗ на сокращение подписки
Заявка согласована?
НЕТ
ДА
Электронная заявка в ИС ОКЗ на сокращение подписки
2.2. Подписание заявки на сокращение подписки
Подписанная уполномоченным лицом электронная заявка в ИС ОКЗ на сокращение подписки
6
Конец

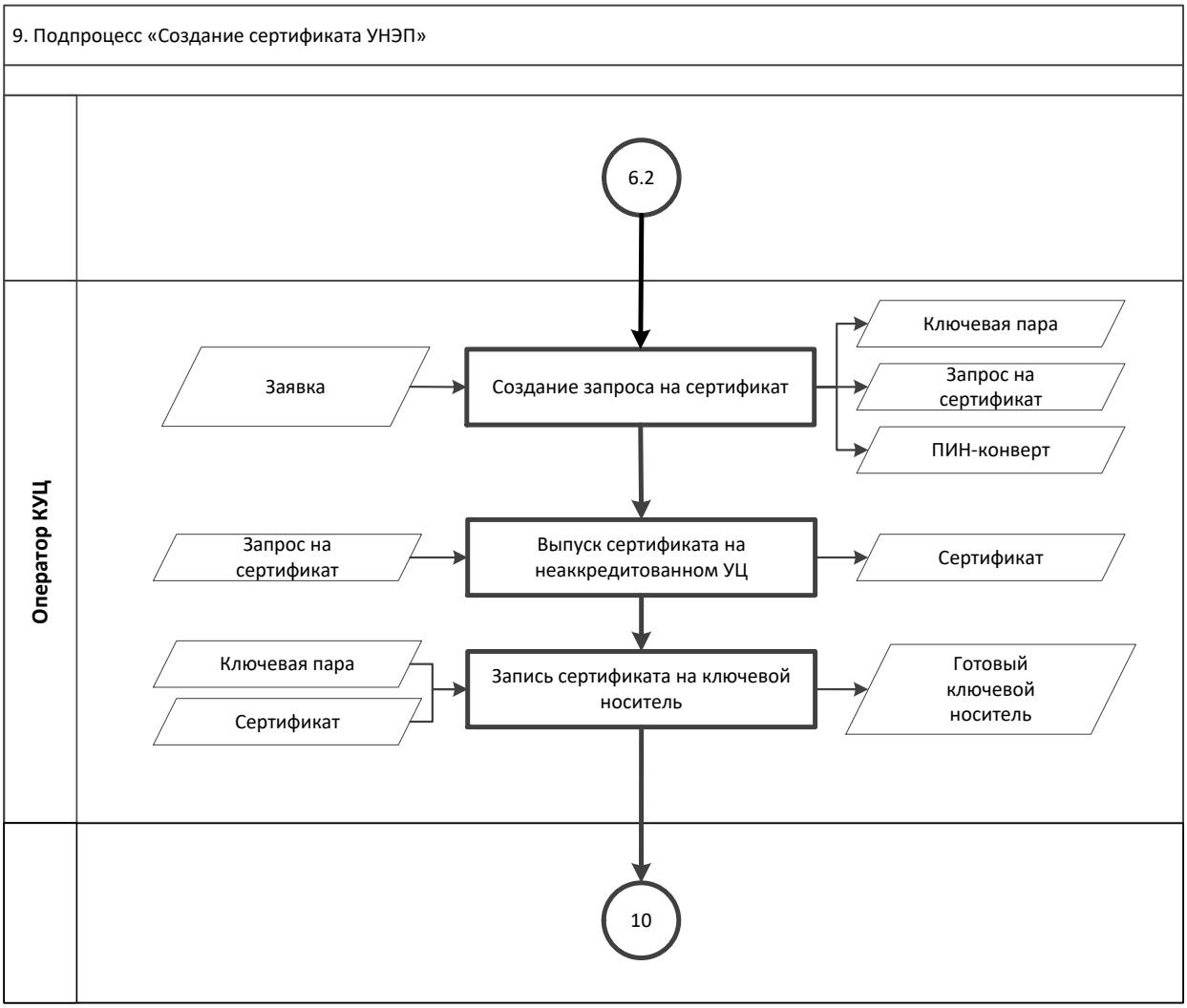

5. Подпроцесс «Перевыпуск сертификата»
АБ
1
Обращение в формализованном виде
Заявка на выпуск сертификата в рамках подписки
Электронная заявка в ИС ОКЗ на перевыпуск сертификата
6

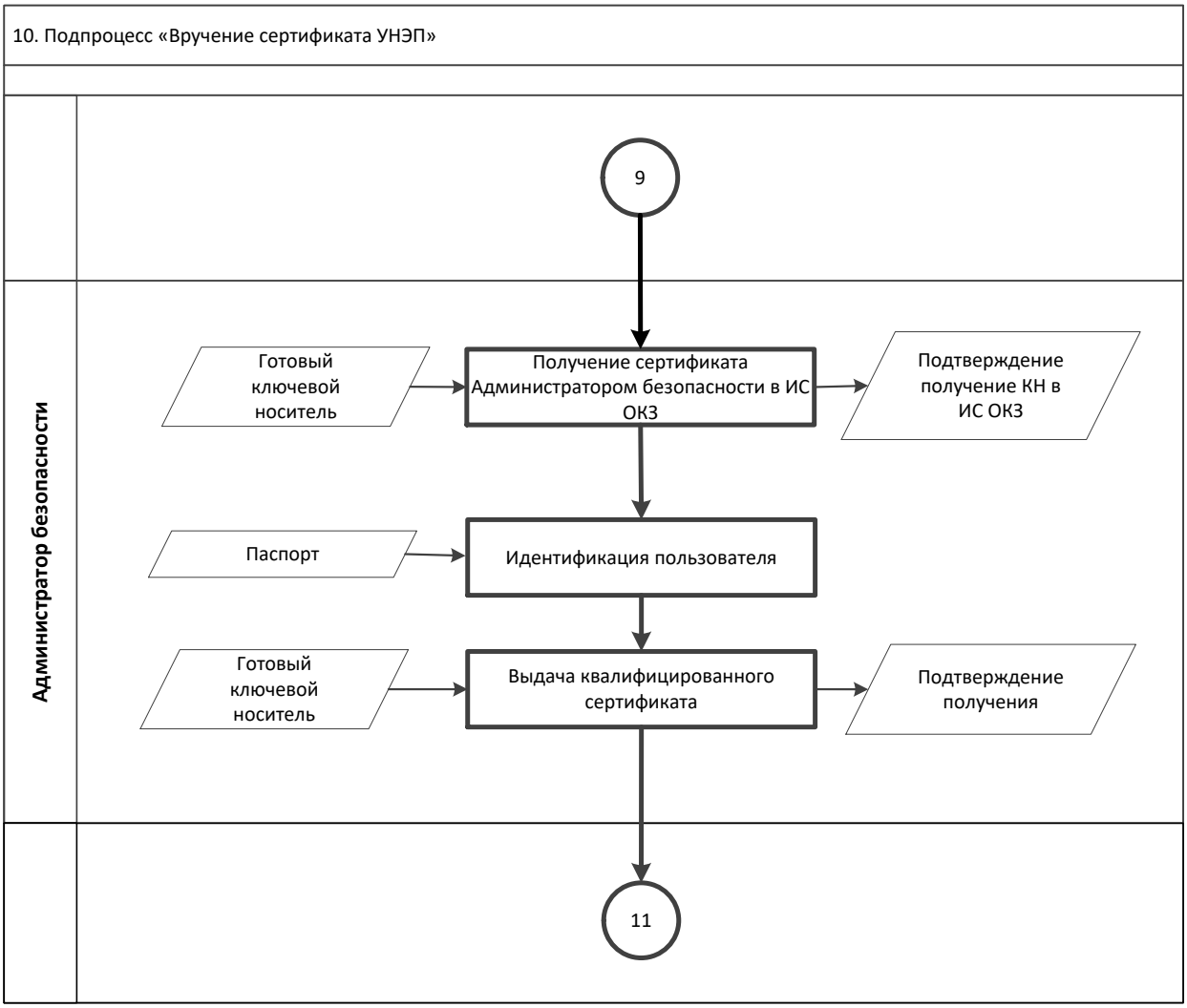

6. Подпроцесс «Аннулирование сертификата»
АБ
3
4
5
Обращение в формализован ном виде
Заявка на аннулирование сертификата
Электронная заявка в ИС ОКЗ на аннулирование сертификата
6.1

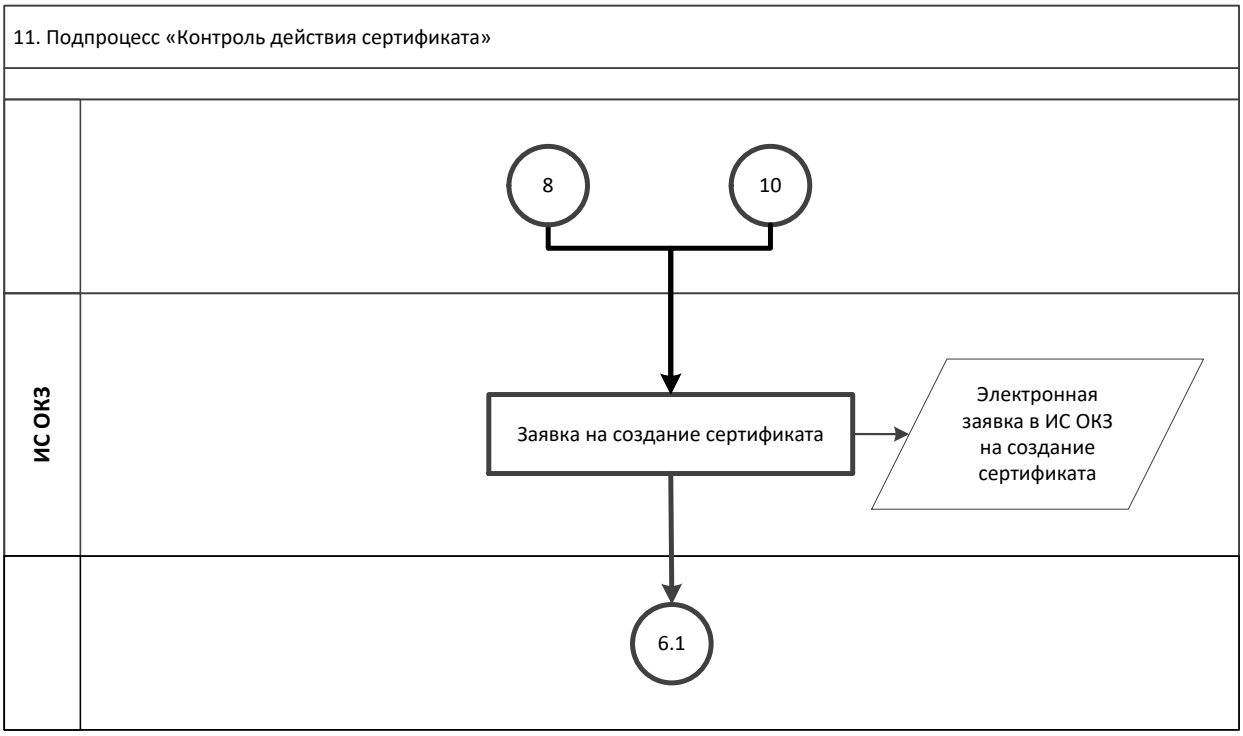

7. Подпроцесс «Создание сертификата УКЭП»
Оператор КУЦ
7
Заявка
Создание запроса на сертификат
Ключевая пара
Запрос на сертификат
ПИН-конверт
Запрос на сертификат
Выпуск сертификата на аккредитованном УЦ
Сертификат
Ключевая пара
Сертификат
Запись сертификата на ключевой носитель
Готовый ключевой носитель
8

8. Подпроцесс «Вручение сертификата УКЭП»




9. Подпроцесс «Создание сертификата УНЭП»
Оператор КУЦ
6.2
Заявка
Создание запроса на сертификат
Ключевая пара
Запрос на сертификат
ПИН-конверт
Запрос на сертификат
Выпуск сертификата на неаккредитованном УЦ
Сертификат
Ключевая пара
Сертификат
Запись сертификата на ключевой носитель
Готовый ключевой носитель
10


10. Подпроцесс «Вручение сертификата УНЭП»
Администратор безопасности
9
Готовый ключевой носитель
Получение сертификата Администратором безопасности в ИС ОКЗ
Подтверждение получение КН в ИС ОКЗ
Паспорт
Идентификация пользователя
Готовый ключевой носитель
Выдача квалифицированного сертификата
Подтверждение получения
11


11. Подпроцесс «Контроль действия сертификата»
ИС ОКЗ
8
10
Заявка на создание сертификата
Электронная заявка в ИС ОКЗ на создание сертификата
6.1

Приложение №2. Формат сертификатов ключа проверки электронной подписи

1. Формат квалифицированного сертификата ключа проверки электронной подписи

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	1) commonName (общее имя). 2) countryName (наименование страны). 3) stateOrProvinceName (наименование штата или области). 4) localityName (наименование населенного пункта). 5) streetAddress (название улицы, номер дома). 6) organizationName (наименование организации). 7) organizationUnitName (подразделение организации). 8) title (должность). 9) OGRN (ОГРН). 10) INN (ИНН).
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	1) commonName (общее имя). 2) surname (фамилия). 3) givenName (приобретенное имя). 4) countryName (наименование страны). 5) stateOrProvinceName (наименование штата или области). 6) localityName (наименование населенного пункта). 7) streetAddress (название улицы, номер дома). 8) organizationName (наименование организации). 9) organizationUnitName (подразделение организации). 10) title (должность). 11) E = электронная почта 12) UnsructuredName (UN) 13) OGRN (ОГРН). 14) SNILS (СНИЛС). 15) INN (ИНН).
Public Key	Открытый ключ	Уникальный ключ проверки электронной подписи (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения сертификата		
Private Key Validity Period	Срок действия закрытого ключа, соответствующего сертификату	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Key Usage	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшеный ключ	Могут быть внесены дополнительные области использования
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида:
certificatePolicies	Политики сертификата	Обозначение класса средств ЭП владельца квалифицированного сертификата
subjectSignTool		Наименование используемого владельцем квалифицированного сертификата средства ЭП
IssuerSignTool		Полное наименование средства ЭП, которое было использовано для создания ключа ЭП, ключа проверки ЭП и квалифицированного сертификата.
		Конкретный перечень используемых расширений устанавливается удостоверяющим центром
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280 и RFC 5280

2. Формат неквалифицированного сертификата ключа проверки электронной подписи

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	1) commonName (общее имя). 2) countryName (наименование страны). 3) stateOrProvinceName (наименование штата или области). 4) localityName (наименование населенного пункта). 5) streetAddress (название улицы, номер дома). 6) organizationName (наименование организации). 7) organizationUnitName (подразделение организации). 8) title (должность). 9) OGRN (ОГРН). 10) INN (ИНН).
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	1) commonName (общее имя). 2) surname (фамилия). 3) givenName (приобретенное имя). 4) countryName (наименование страны). 5) organizationName (наименование организации). 6) organizationUnitName (подразделение организации). 7) title (должность). 8) E = электронная почта
Public Key	Открытый ключ	Уникальный ключ проверки электронной подписи (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения сертификата		
Private Key Validity Period	Срок действия закрытого ключа, соответствующего сертификату	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Key Usage	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшеный ключ	Могут быть внесены дополнительные области использования
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида:
certificatePolicies	Политики сертификата	Обозначение класса средств ЭП владельца квалифицированного сертификата
subjectSignTool		Наименование используемого владельцем квалифицированного сертификата средства ЭП
IssuerSignTool		Полное наименование средства ЭП, которое было использовано для создания ключа ЭП, ключа проверки ЭП и квалифицированного сертификата.
		Конкретный перечень используемых расширений устанавливается удостоверяющим центром
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280 и RFC 5280

Приложение №3. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

Пользователь КУЦ обязан:

– соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием средств квалифицированной электронной подписи;

– сдать средства квалифицированной электронной подписи и ключи электронной подписи, эксплуатационную и техническую документацию к ним в соответствии с порядком, установленным при увольнении или отстранении от исполнения обязанностей, связанных с использованием средств квалифицированной электронной подписи;

– немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи средств квалифицированной электронной подписи, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений

– обеспечивать конфиденциальность ключей электронной подписи, в частности не допускать использование принадлежащих ему ключей электронной подписи без его согласия;

– уведомлять КУЦ, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

– использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированной электронной подписи и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с действующим Федеральным законодательством.

– не использовать ключ электронной подписи и немедленно обратиться в КУЦ для прекращения действия сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;

– использовать квалифицированную электронную подпись в соответствии с ограничениями, содержащимися в квалифицированном сертификате (если такие ограничения установлены).

– обновлять сертификат ключа проверки электронной подписи в соответствии с установленным регламентом.

– принять меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным средством квалифицированной электронной подписи, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на средства квалифицированной электронной подписи, технические средства, на которых эксплуатируется средства квалифицированной электронной подписи и защищаемую информацию.

Пользователю КУЦ запрещается:

– оставлять без контроля вычислительные средства, на которых эксплуатируется средства квалифицированной электронной подписи, после ввода ключевой информации либо иной конфиденциальной информации;

– вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;

– осуществлять несанкционированное администратором безопасности копирование ключевых носителей;

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;

– использовать ключевые носители в режимах, не предусмотренных функционированием средств квалифицированной электронной подписи;

– записывать на ключевые носители постороннюю информацию;

– использовать нестандартные, изменённые или отладочные версии операционных систем (ОС).

– использовать ОС, отличную от предусмотренной штатной работой.

– использовать возможность удалённого управления, администрирования и модификации ОС и её настроек.

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации.

– использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ

– подключать к компьютеру с установленным средством квалифицированной электронной подписи дополнительные устройства и соединители, не предусмотренные штатной комплектацией.

– изменять настройки, установленные программой установки средства квалифицированной электронной подписи или администратором.

– обрабатывать на ПЭВМ, оснащённой средством квалифицированной электронной подписи, информацию, содержащую государственную тайну.

– осуществлять несанкционированное вскрытие системных блоков ПЭВМ.

Пользователь КУЦ несёт ответственность за:

– полноту и своевременность предоставления документов (в соответствии с Приложениями) в КУЦ;

– обеспечение конфиденциальности ключей ЭП, в частности не допущение использования принадлежащих ему ключей ЭП без его согласия;

– уведомление КУЦ, выдавшего сертификат ключа проверки ЭП, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа ЭП в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

– не использование ключа ЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

Приложение №4. Шаблоны сертификатов ключей проверки электронной подписи

Шаблоны сертификатов ключей проверки электронной подписи

1. Квалифицированный сертификат Госкорпорации «Росатом»

Данные сертификаты ключа проверки электронной подписи предназначены для использования при участии в качестве заказчика на электронных торговых площадках, для использования в защищенной корпоративной почтовой системе Госкорпорации «Росатом», для аутентификации пользователей при доступе к корпоративным информационным системам ЦОД из сети Интернет.

В поле Дополнительное имя субъекта:

UPN = имя доменной учётной записи домена GK

В сертификате указываются следующие объектные идентификаторы:

- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
- Шифрующая файловая система (EFS) (1.3.6.1.4.1.311.10.3.4)
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
- Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1

2. Облачная подпись Госкорпорации «Росатом»

Данные сертификаты ключа проверки электронной подписи предназначены для Формирования квалифицированной электронной в Системе электронной подписи Госкорпорации «Росатом». В качестве ключевого контейнера используется Система электронной подписи Госкорпорации «Росатом»

В сертификате указываются следующие объектные идентификаторы:

В поле Дополнительное имя субъекта (UPN) = имя доменной учётной записи домена GK

В поле улучшенный ключ:

- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
- Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1

3. Квалифицированный сертификат для Росреестра (требуется доп. доверенность)

Данные сертификаты ключа проверки электронной подписи предназначены для формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости, для использования при участии в качестве заказчика на электронных торговых площадках, для использования в защищенной корпоративной почтовой системе Госкорпорации «Росатом», для аутентификации пользователей при доступе к корпоративным информационным системам ЦОД из сети Интернет.

В поле Дополнительное имя субъекта:

UPN = имя доменной учётной записи домена GK

В поле улучшенный ключ:

- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

- Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
- Шифрующая файловая система (EFS) (1.3.6.1.4.1.311.10.3.4)
- Вход со смарт-картой (1.3.6.1.4.1.311.20.2.2)
- Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости (1.2.643.5.1.24.2.30)

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1

4. Аутентификация сервера

Данные сертификаты ключа проверки электронной подписи предназначены для применения в следующих автоматизированных системах:

- Аутентификация веб-сервера.

В сертификате указываются следующие дополнительные поля:

В поле улучшенный ключ:

- Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1

5. Клиент S-Terra (КСПД)

Данные сертификаты предназначены для применения в АРМ Корпоративной сети передачи данных.

Создание данных сертификатов осуществляется при совместном формировании дистрибутива Клиента КСПД в Органе криптографической защиты ЗАО «Гринатом»

В поле Дополнительное имя субъекта:

UPN = имя доменной учётной записи домена GK

В сертификате указываются следующие дополнительные поля:

В поле улучшенный ключ:

- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
- Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1

6. Шлюз КСПД

Данные сертификаты ключа проверки электронной подписи предназначены для применения в следующих автоматизированных системах:

Узел Корпоративной системы передачи данных;

В сертификате указываются следующие дополнительные поля:

В поле улучшенный ключ:

- Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1
- 1.2.643.100.113.2 - класс средства ЭП КС 2

7. Неквалифицированный сертификат Госкорпорации «Росатом»

Данные сертификаты ключа проверки электронной подписи выпускаются самоподписанным сертификатом Центра сертификации «Росатом» и предназначены для:

- использования в во всех отраслевых системах, где законодательно не требуется квалифицированная подпись

- аутентификации пользователей при доступе к корпоративным информационным системам ЦОД из сети Интернет;
- использования в защищённой корпоративной почтовой системе Госкорпорации «Росатом»;

В сертификате указываются следующие объектные идентификаторы:

В поле Дополнительное имя субъекта (UPN) = имя доменной учётной записи домена GK

В поле улучшенный ключ:

- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
- Шифрующая файловая система (EFS) (1.3.6.1.4.1.311.10.3.4)
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
- Вход со смарт-картой (1.3.6.1.4.1.311.20.2.2)
- Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)

Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости (1.2.643.5.1.24.2.30)

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1