Инструкция по
удаленной процедуре продления электронной подписи
для ОИВ Ленинградской области и им подведомственных учреждений
(версия 0.5 от 15.10.2021)

Санкт-Петербург
2020

Обращаем внимание!

Начиная с 11.01.2021 по данной процедуре обрабатываются запросы на продление сертификатов только пользователей ранее получавших сертификат ключа проверки электронной подписи в УЦ ГКУ ЛО «ОЭП».

Обязательно вводится необходимость подписания заполненного pdf-заявления (с проставленными датами) действующей электронной подписью дальнейшего владельца сертификата.

Шифрование и подписание пакета документов перед отправкой в УЦ ГКУ ЛО «ОЭП» остается возможным как личной электронной подписью будущего владельца сертификата, так и электронной подписью руководителя организации (Например, для отправки одним пакетом документов на продление сертификатов нескольких сотрудников возможно использовать ЭП руководителя организации при том что каждое заявление подписано действующей электронной подписью будущего владельца сертификата).

При соблюдении вышеизложенных изменений и предоставлении корректного пакета документов для продления сертификата, предоставление оригиналов документов в УЦ ГКУ ЛО «ОЭП» не требуется.

Для организации процедуры удаленного продления пользователям электронной подписи (далее ЭП) требуется установить и настроить следующее программное обеспечение:

1. КриптоПро CSP 4.0 https://cryptopro.ru/ (как правило, если вы до этого работали с электронной подписью, то данный продукт уже установлен и настроен на вашем рабочем месте)
2. КриптоАРМ Стандарт 5.0 https://cryptoarm.ru (данный продукт можно скачать и установить для работы бесплатно в рамках тестового периода в две недели)
3. КриптоПро PDF 2.0 https://www.cryptopro.ru/products/other/pdf/downloads (данный продукт можно скачать и установить для работы бесплатно в рамках тестового периода в 90 дней)

Установку и настройку производить согласно инструкциям к данным программным средствам.

1. Этика деловой переписки по электронной почте

В связи с дополнительной нагрузкой на Удостоверяющий центр (далее- УЦ) и необходимостью обрабатывать большой объем входящей корреспонденции. Мы составили несколько правил, которые помогут сэкономить время себе и работнику УЦ и быстрее решить рабочие вопросы.

- **Тема письма**

Тема — как заголовок, помогает быстро найти нужную переписку в почтовом ящике. Обязательно указывайте ее, чтобы проще работать с письмами. Формулировка темы должна быть информативной. В теме письма необходимо указывать название организации либо имена сотрудников на кого поступает тот или иной запрос, например: Администрация Всеволожского р-на, Пакет документов на Иванова И.И., досылаем паспорт на Петрова П.П., так сотрудник УЦ сможет оперативней обработать и осуществить поиск требуемого письма.

- **Указывайте точный срок**

Не пишите в теме или теле письма «срочно». Это понятие растяжимое: для одного — час, для другого — неделя. Лучше укажите точное время и дату, когда вы ждете ответа или результата.

- **Сохраняйте историю переписки**

Оставляйте всю предыдущую цепочку сообщений в письме. В большом потоке информации легко забыть, о чем вы общались с сотрудником УЦ — история переписки поможет вспомнить.

- **Подписывайте письма**

В подписи укажите имя, фамилию, должность и название организации. Добавьте способы связи: телефон, мессенджеры. Ограничьтесь нейтральным «с уважением» или «с наилучшими пожеланиями». Не стоит расписывать в автоматической подписи слова благодарности на полстраницы, размещать рекламу, ставить ссылки на сбор подписей и подобные проекты.

- **Добавляйте сразу все ссылки и файлы**

Бывает, что только после отправки обнаруживается, что важный файл не прикреплен или не указана нужная ссылка. Многие высылают вложения и дополнения отдельным письмом — «вот документ, который я забыл». И переписка раздваивается: в одной истории — обсуждение, в другой — нужные документы. На какое письмо ответит получатель, неизвестно — возможно, на то, в котором нет истории переписки. Поэтому лучше продублировать предыдущее и добавить к нему файл. В сообщении стоит попросить получателя удалить письмо без файла, чтобы избежать путаницы.

Еще есть люди, которые высылают пять файлов пятью отдельными письмами это засоряет почтовый ящик и отвлекает работника УЦ. Пожалуйста, отправляйте все вложения вместе. Если их слишком много, присылайте ссылку на файлообменник.

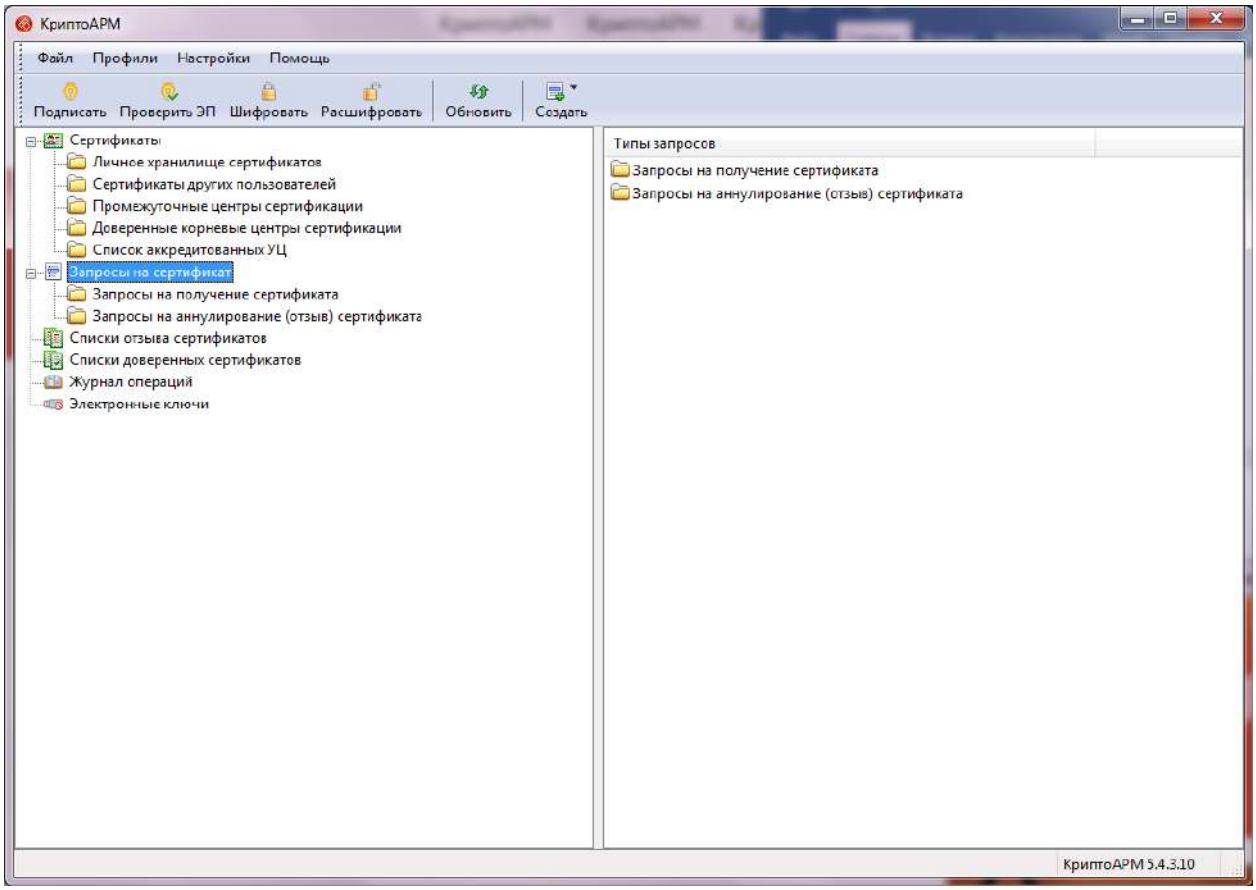
- **Называйте понятно файлы и документы**

Называйте файл так, чтобы сразу было понятно, о чем он и к чему относится. Тяжело отличить в перечне изображений один IMG568909865 от другого IMG6789988901. Гораздо лучше, если это будут паспорт Ивановой и заявление Петрова.

2. Формирование Запроса на сертификат

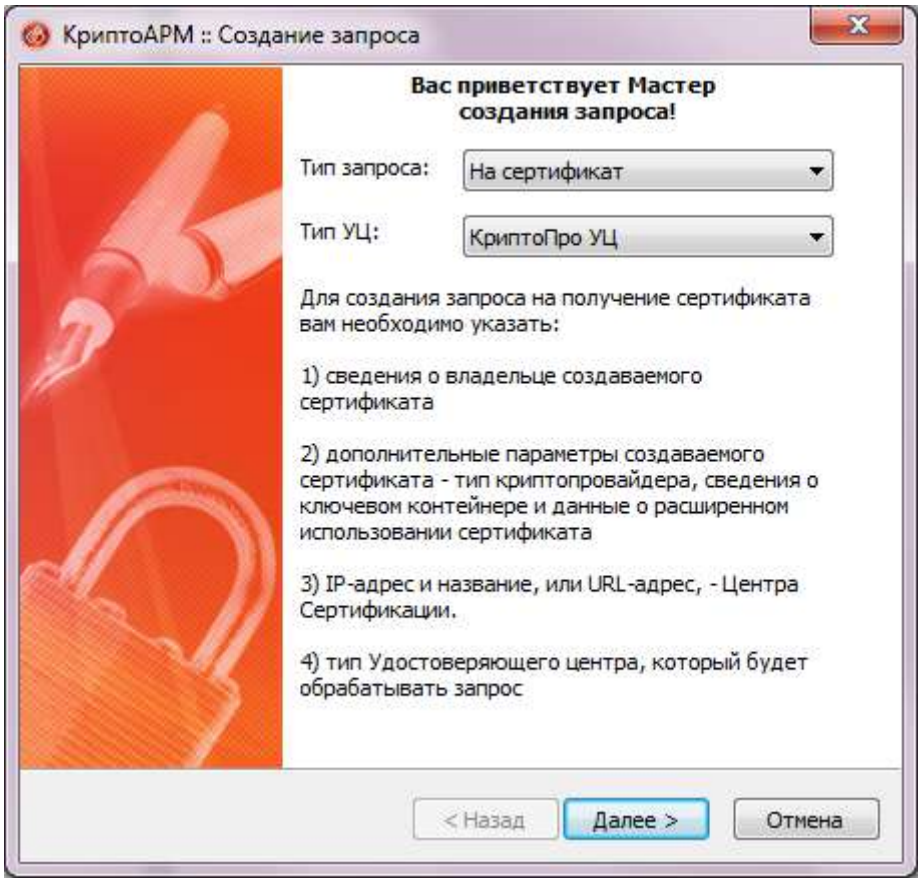
Для работы программы КриптоАРМ версии 5 необходимо запустить приложение КриптоАРМ (рисунок 1)

Рисунок 1



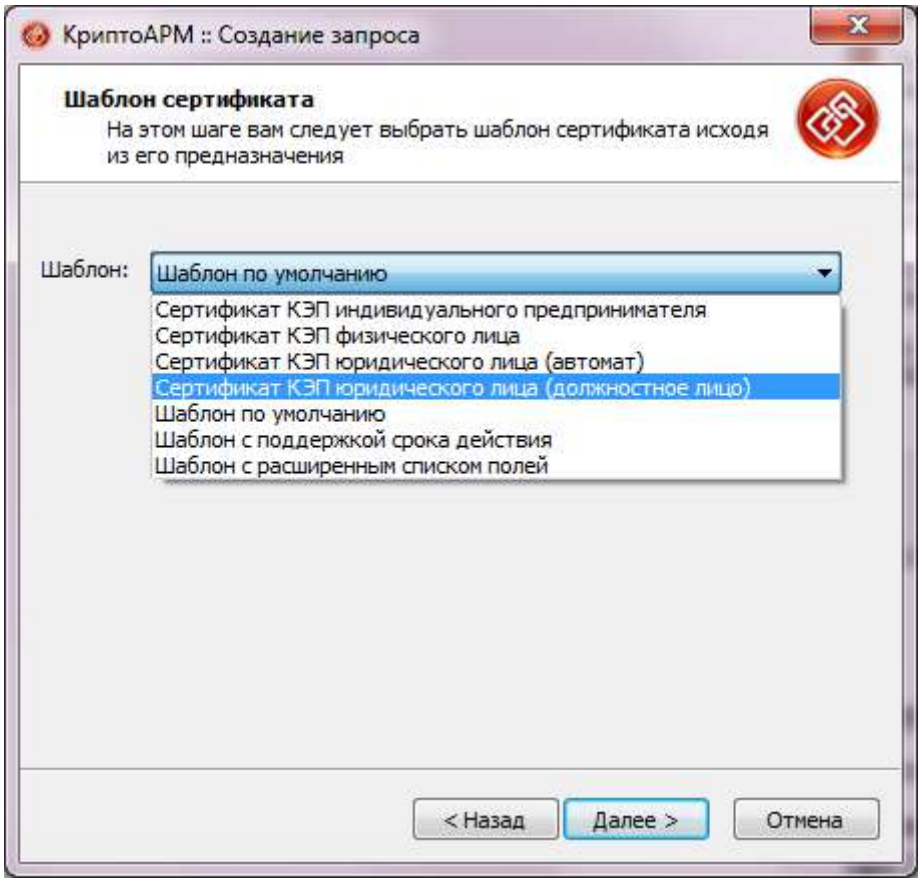
Далее выбираем в боковом меню «Запросы на сертификат», правой кнопкой мыши (далее ПКМ) выбираем – создать-запрос на сертификат. В первом окне (рисунок 2) оставляем все по умолчанию.

Рисунок 2



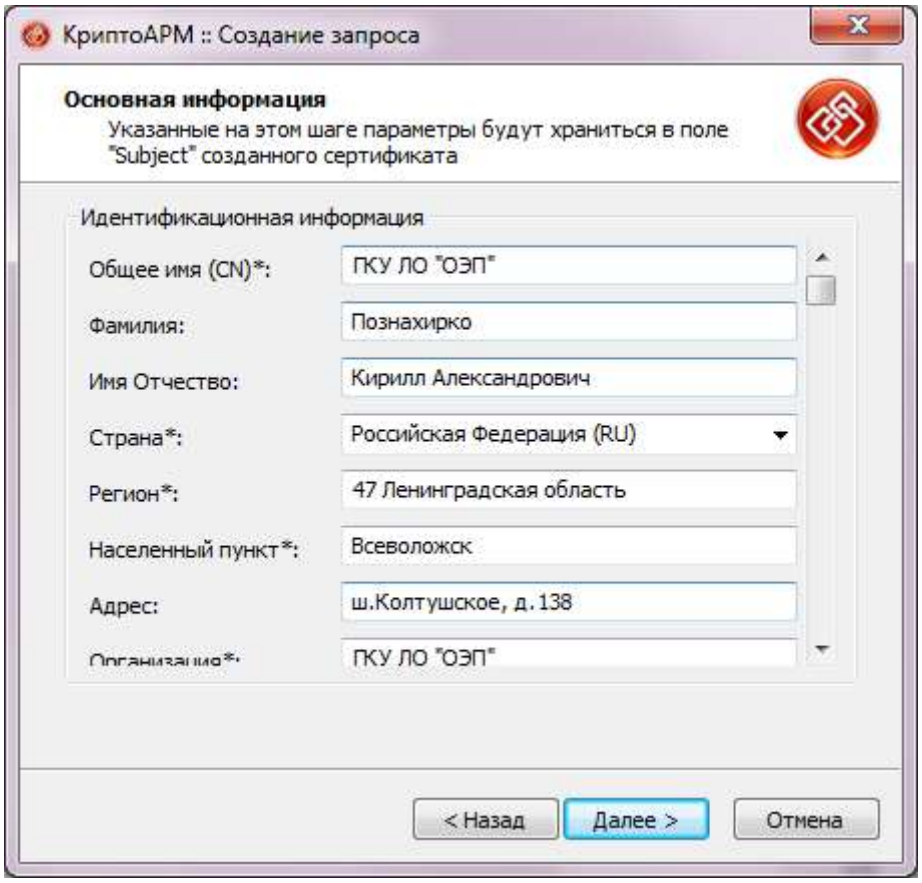
В следующем окне (рисунок 3) выбираем шаблон сертификат КЭП юридического лица (должностное лицо)

Рисунок 3



Далее заполняем данные согласно заявлению на изготовление сертификата (рисунок 4). Обращаем внимание поле подразделение, если вы его не заполняете в заявлении, то в графе ставьте цифру «1». Поле «Общее имя (CN)» имеет ограничение на количество знаков, если название не помещается, то специалист УЦ исправит это, в данном поле указывается наименование Вашей организации.

Рисунок 4

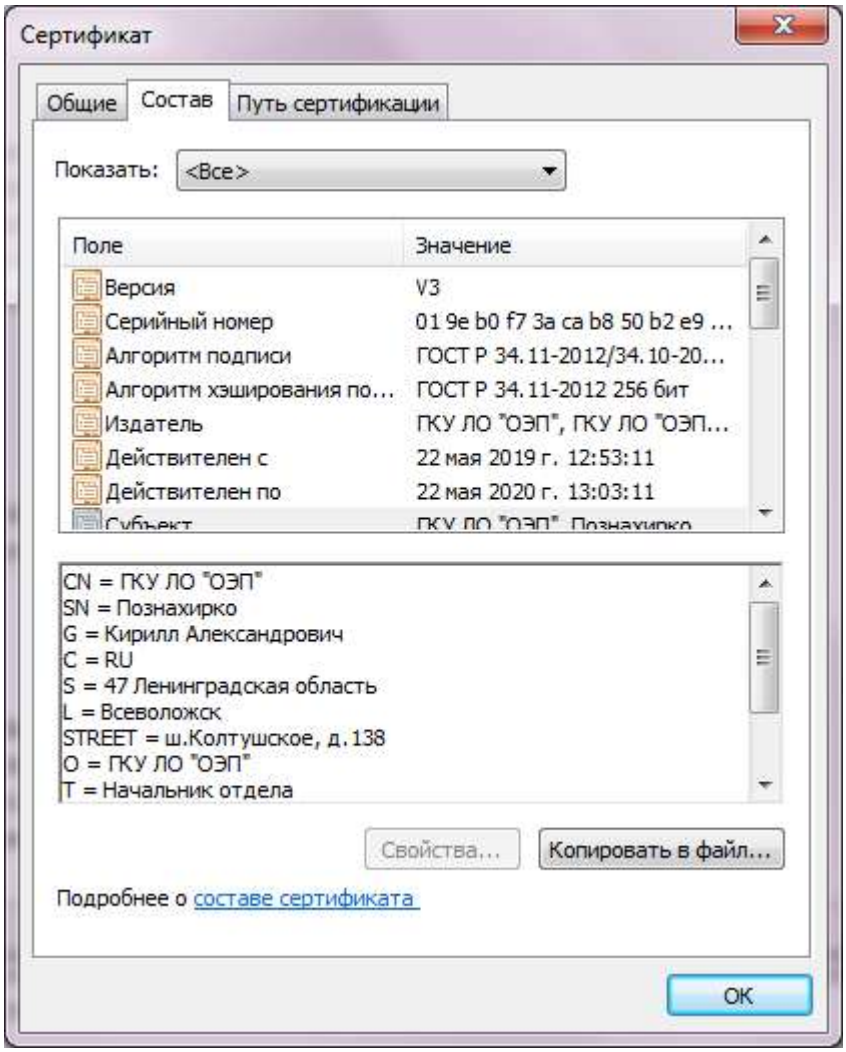


Данные также можно взять в ранее выданном сертификате, для этого запустите двойным нажатием на файл сертификата, перейдите на вкладку «Состав», поле «Субъект» (рисунок 5).

ВНИМАЕНИЕ!

Если данные изменились, то не надо бездумно их копировать из предыдущего сертификата. Данные должны в точности соответствовать данным в заявлении.

Рисунок 5

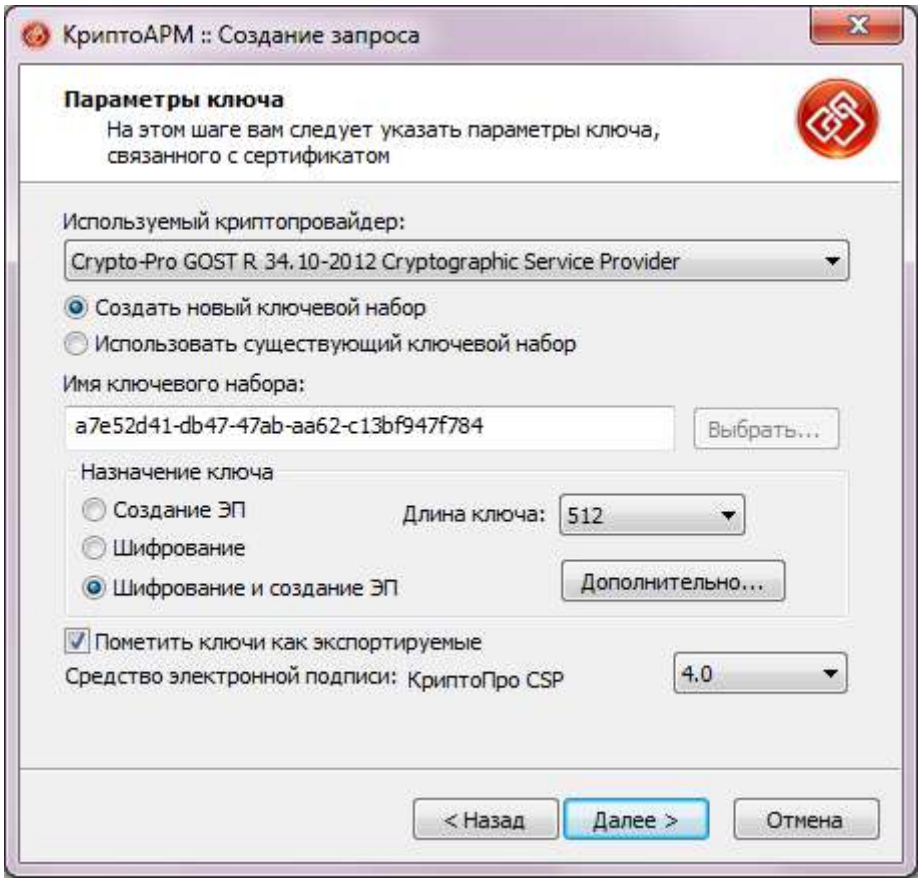


В окне выбора крипто провайдера (рисунок 6) обязательно выбрать Crypto-Pro GOST R 34/10-2012 Cryptographic Service Provider

ВНИМАНИЕ! Если в перечне крипто провайдеров он будет отсутствовать, то:

1. У вас не установлен КриптоПро CSP 4.0
2. У вас установлена не та версия КриптоАРМ, либо истекла лицензия на продукт.

Рисунок 6



Обязательно помечаем галочкой ключи как экспортируемые, далее необходимо выбрать место для сохранения файл запроса (для удобства файл запроса называть по шаблону фамилия лат. буквами и через черточку дату создания).

ВНИМАНИЕ!

Будьте внимательны куда сохраняете файл запроса, его необходимо переслать в УЦ вместе с комплектом документов.

В следующем окне (рисунок 8) еще раз все проверяем и нажимаем кнопку «Готово».

Рисунок 7

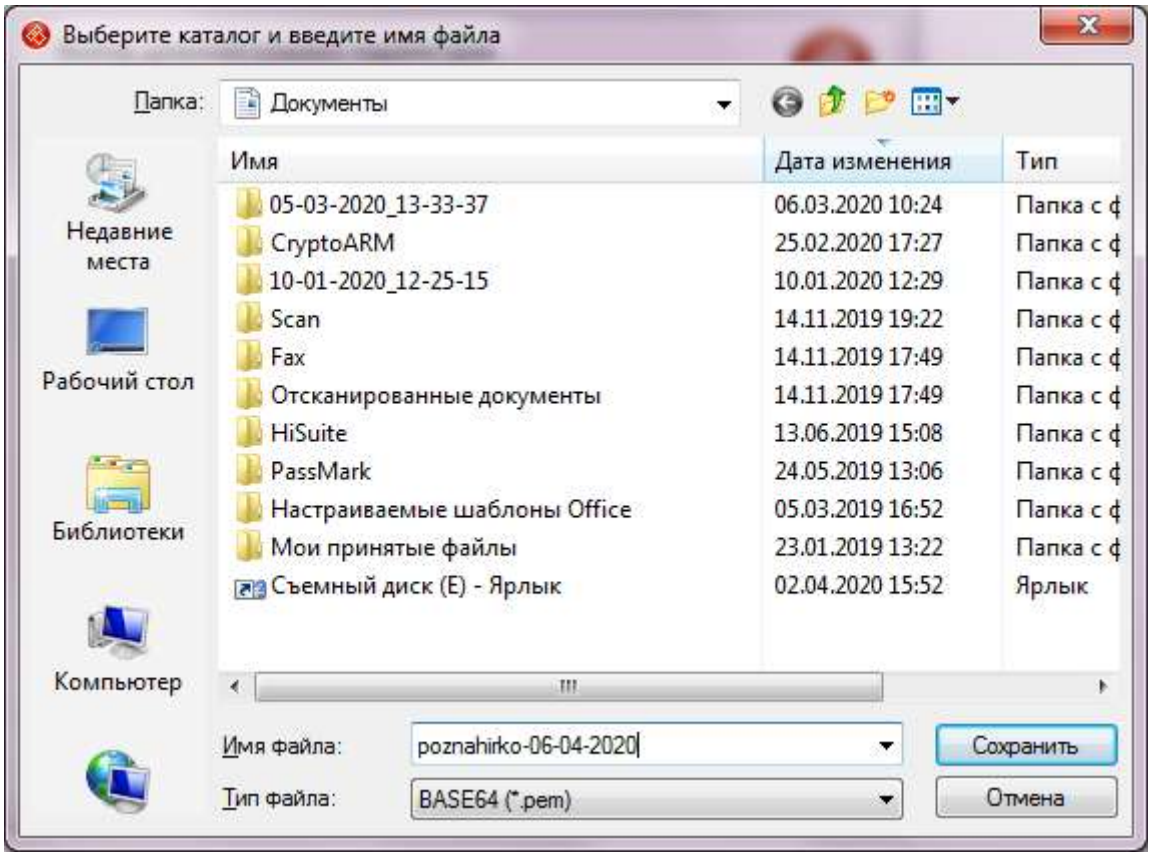
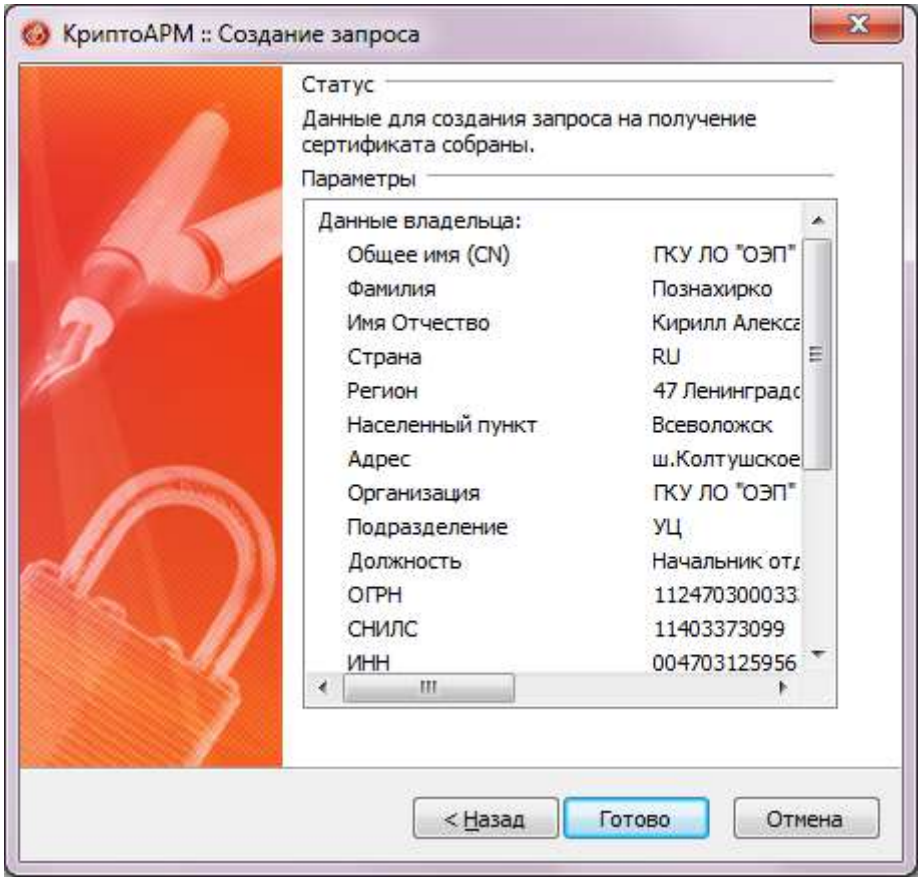
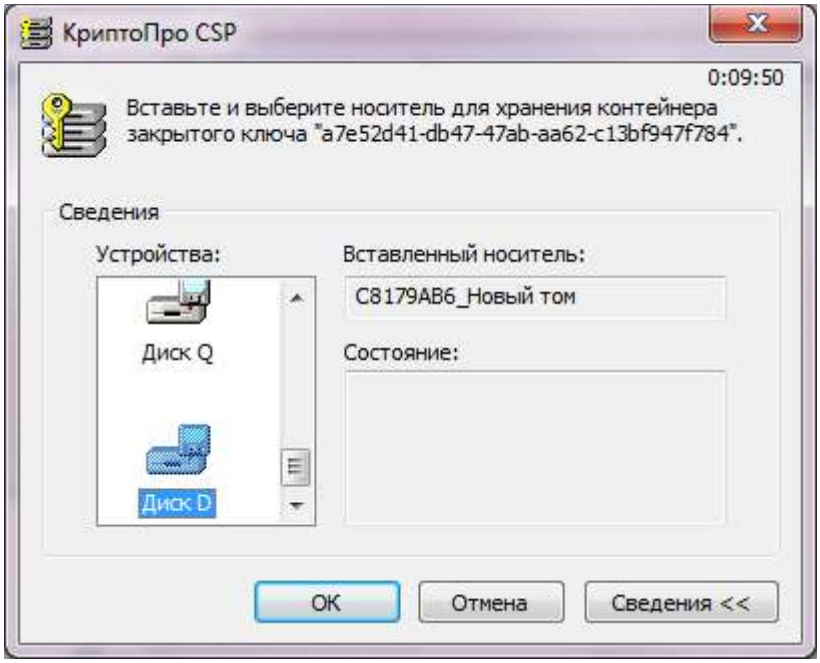


Рисунок 8



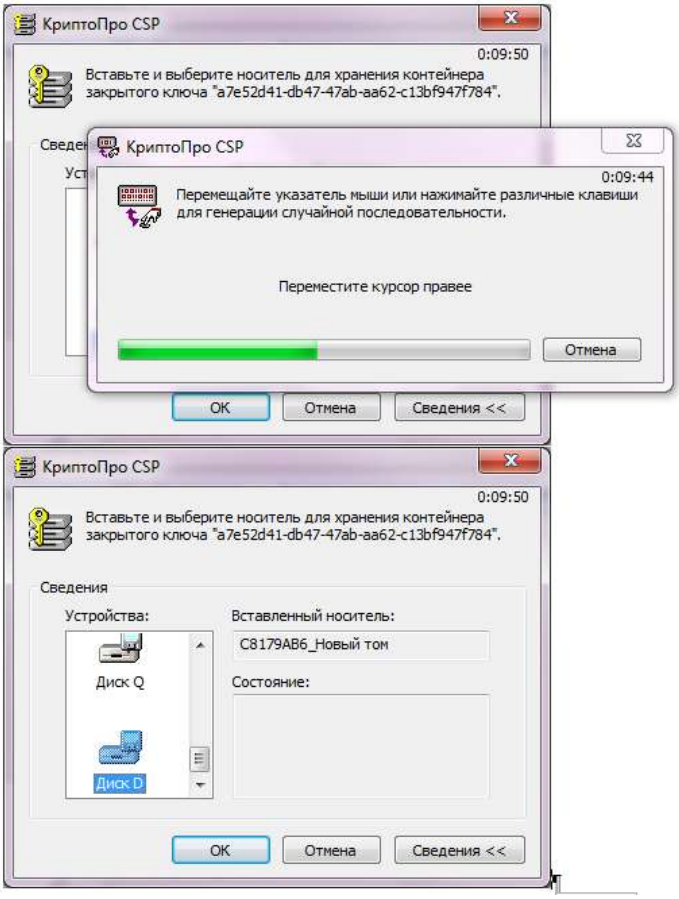
При нажатии кнопки «Готово» начнется формирование ключа электронной подписи, вставьте носитель, на котором у вас будут храниться ключи КЭП и выберете его.

Рисунок 9



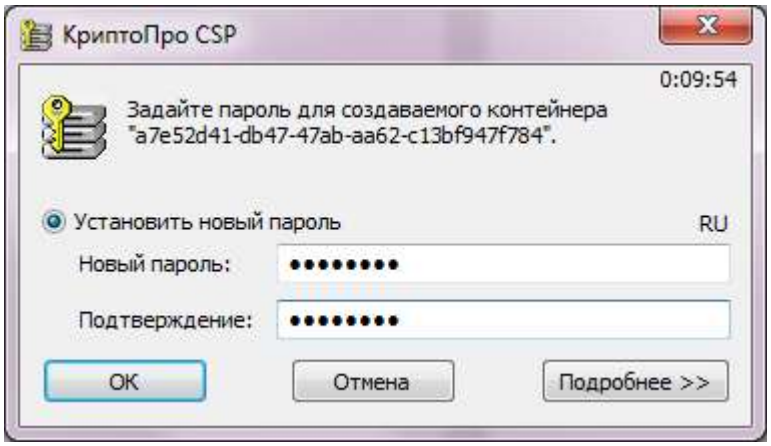
При генерации ключа сработает программный датчик случайных чисел, надо просто водить мышкой и нажимать случайные клавиши.

Рисунок 10



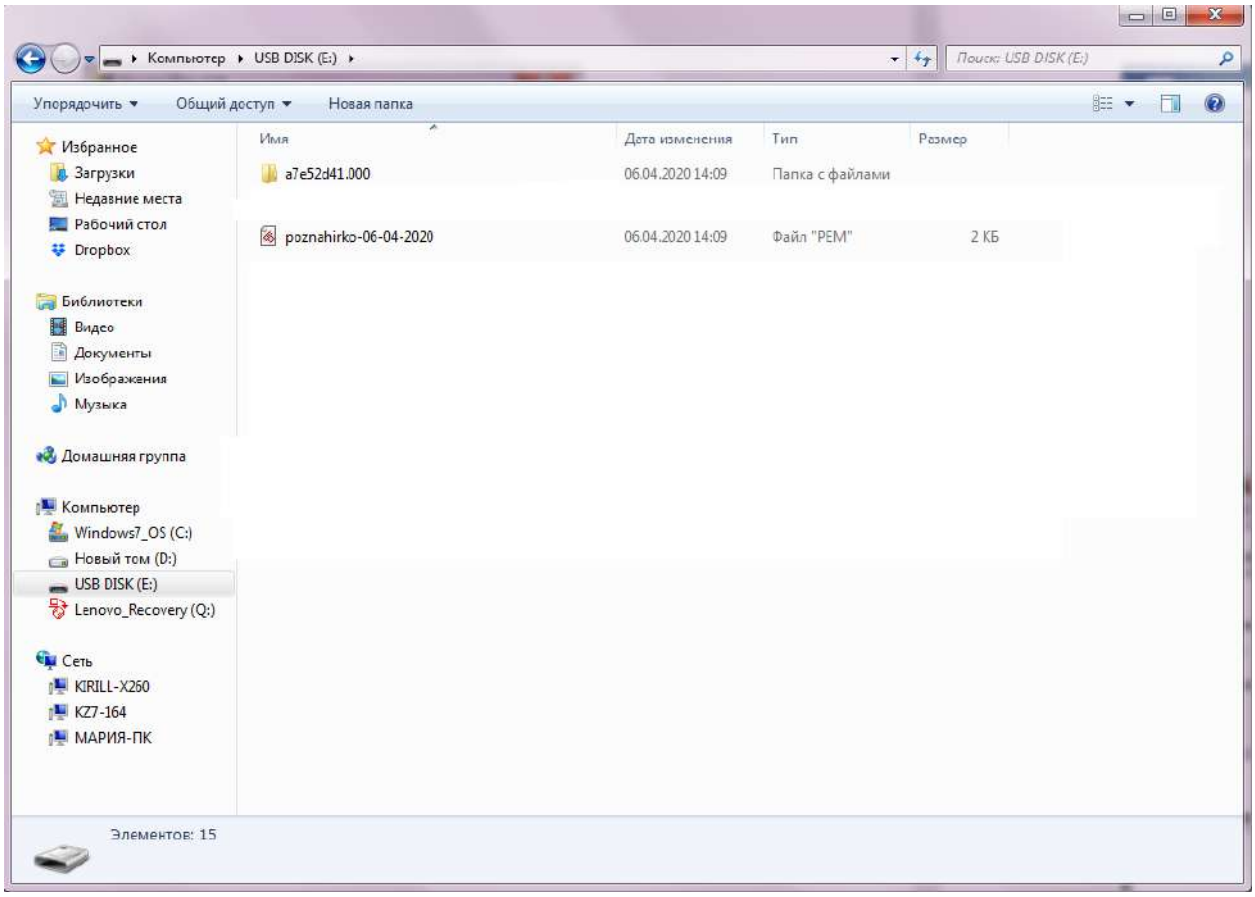
В следующем окне просят ввести пароль, вводим в обязательном порядке

Рисунок 11



После завершения процедуры генерации у вас появится папка с ключами и файл запроса.

Рисунок 12

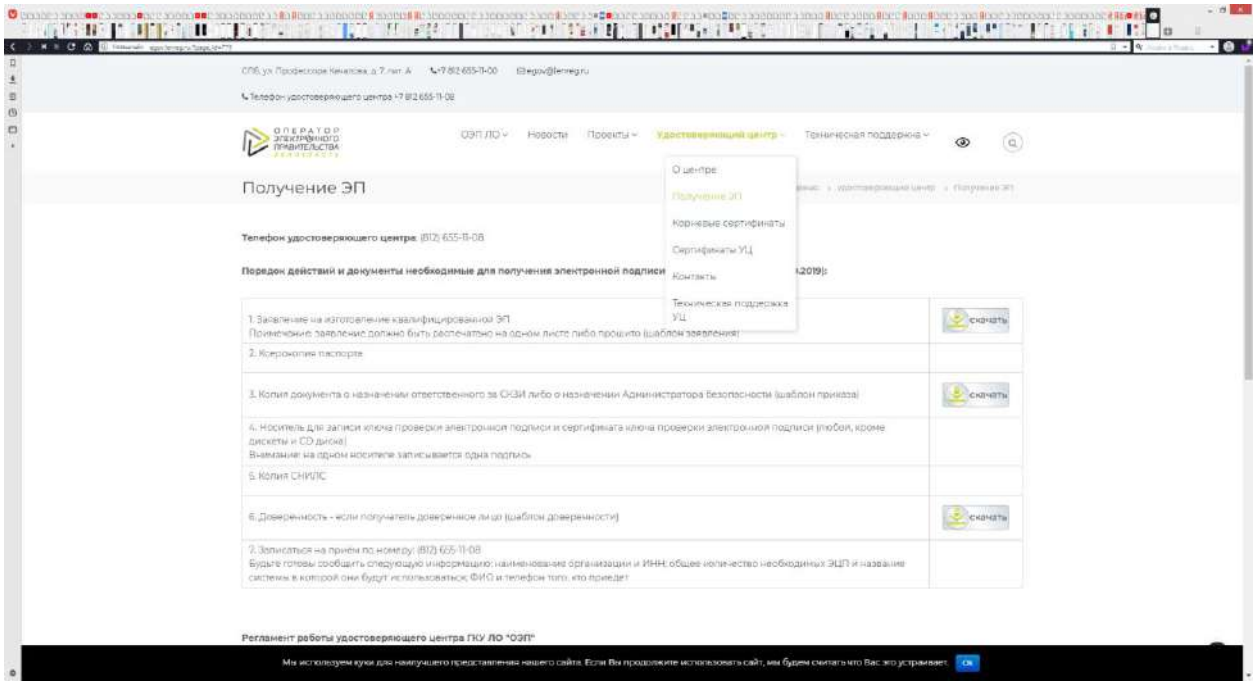


ВНИМАНИЕ

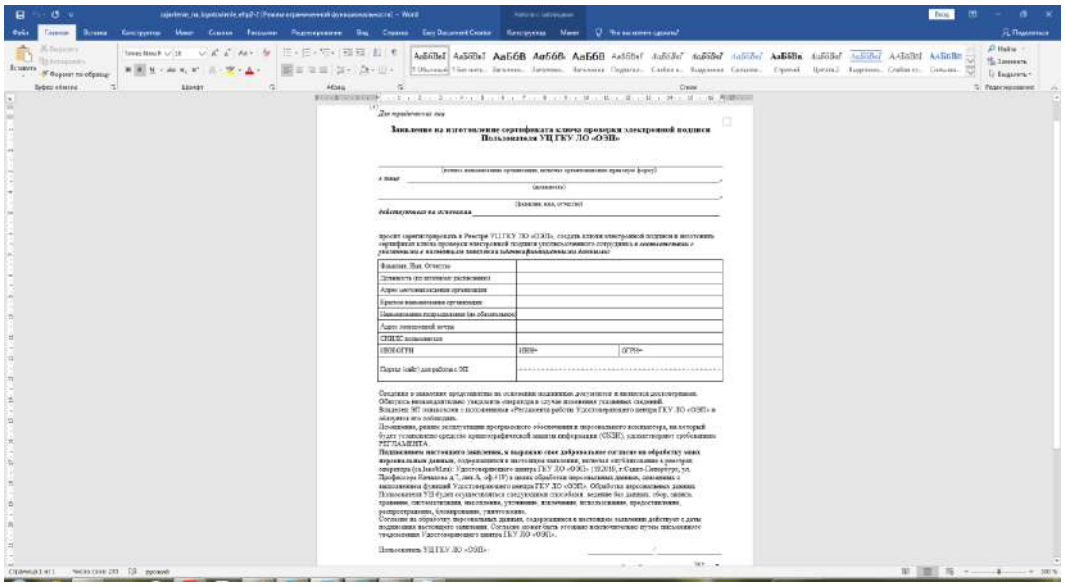
Папку вида xxxxxx.000 высылать не надо, в данной папке находится Ваш ключ, который никому нельзя передавать и тем более отправлять. Запросы с отправленным ключом будут считаться скомпрометированными и не будут приниматься.

3. Подготовка документов

Для подготовки документов надо зайти на сайт ГКУ ЛО «ОЭП» http://egov.lenreg.ru/, перейти на страничку Удостоверяющего центра и в разделе Получение ЭП скачать шаблон заявления, а также по перечню подготовить весь пакет документов.

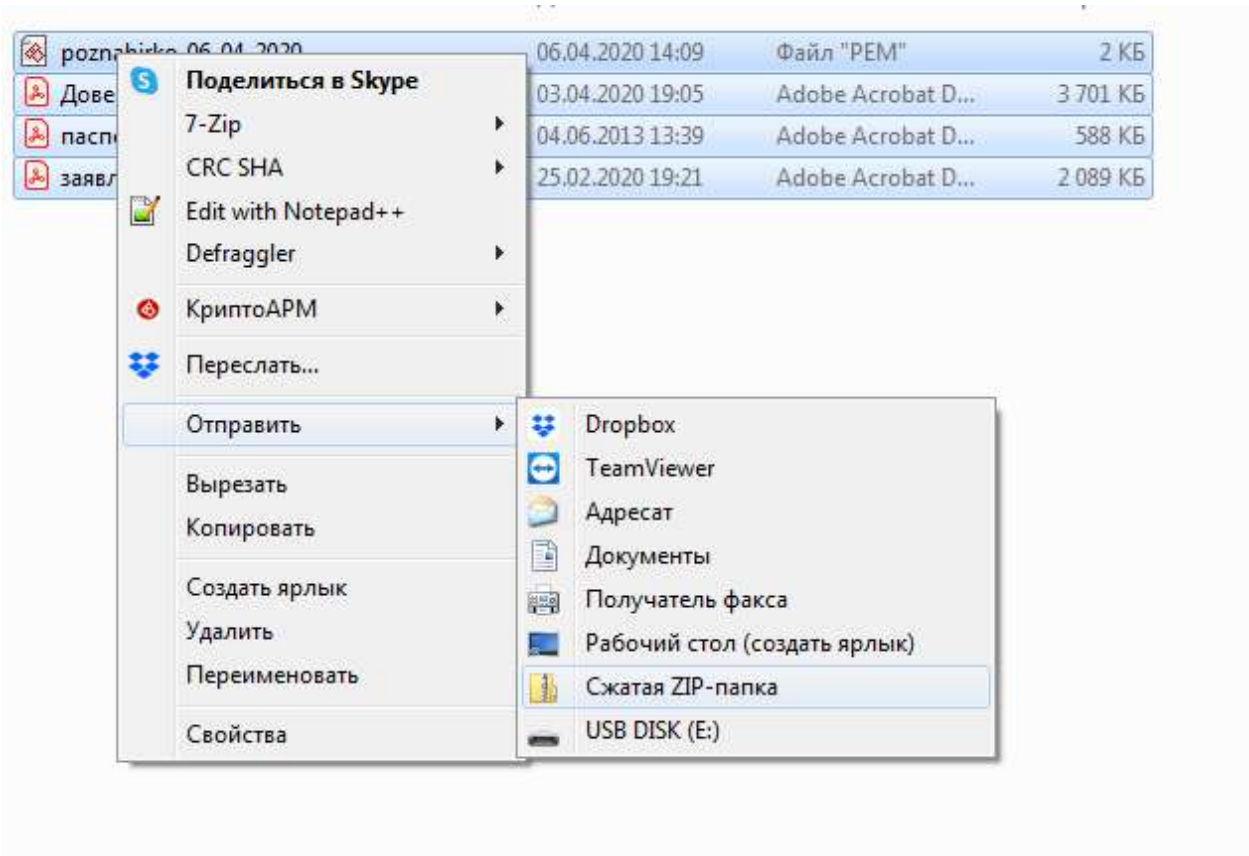


Заполнить заявление, отсканировать в формате PDF, подписать действующей электронной подписью будущего владельца сертификата (Навести на Ваше заявление.pdf – ПКМ – КриптоАрм – Подписать, в последующих окнах нет необходимости менять заданные значения, необходимо запомнить куда сохранится подписанный файл и выбрать подпись которой подписываете заявление (текущая подпись будущего владельца сертификата). Допускается подписание электронной подписью заявления через другие сервисы.



Также необходимо приложить первую страницу паспорта, СНИЛС и ИНН физического лица (Всегда проверяйте актуальный перечень и шаблоны документов на нашем сайте).

И весь комплект документов с файлом запроса (.pem) поместить в архив.

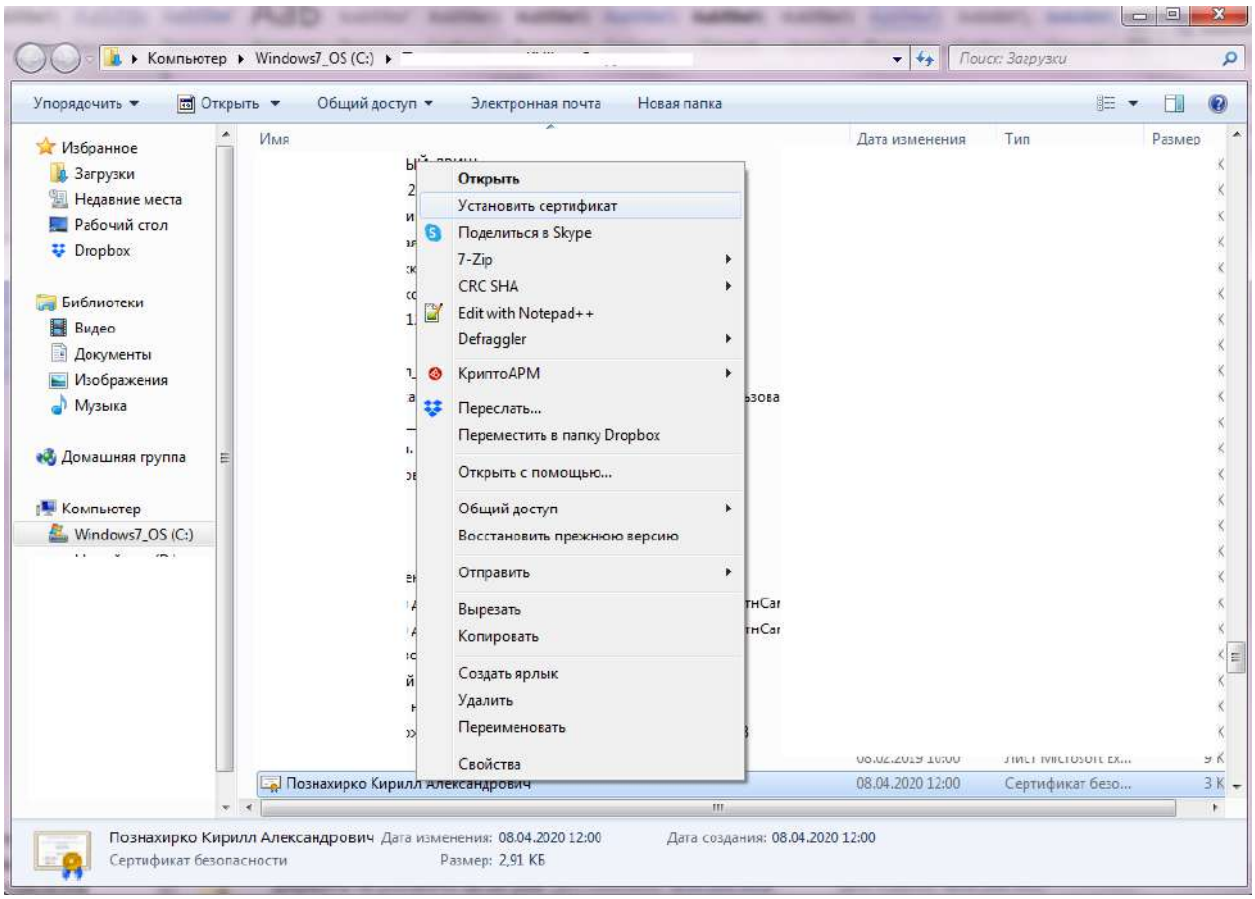


4. Подписание и шифрование архива для отправки в УЦ

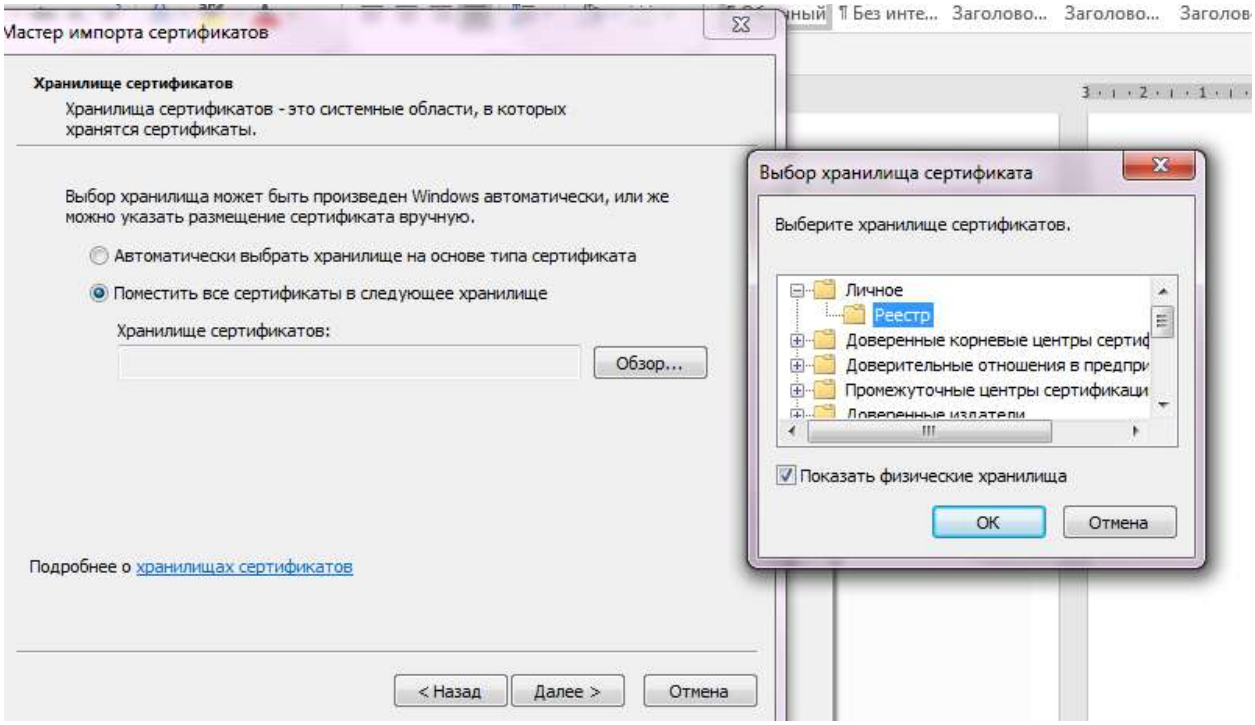
Для выполнения процедуры подписания и шифрования требуется чтобы на вашем компьютере был установлен ваш личный сертификат, которым вы будете подписывать и на котором будет шифровать, а также должен быть установлен сертификат лица, в адрес которого вы будете шифровать.

Сертификат уполномоченных лиц УЦ ГКУ ЛО «ОЭП» в адрес которых можно производить шифрование размещен на официально ресурсе http://egov.lenreg.ru/?page_id=783 в разделе «Удостоверяющий центр» в подразделе «Корневые сертификаты».

Для установки сертификата уполномоченного лица УЦ, требуется скачать его на компьютер. Выделить его ПКМ и из контекстного меню выбрать «Установить сертификат»

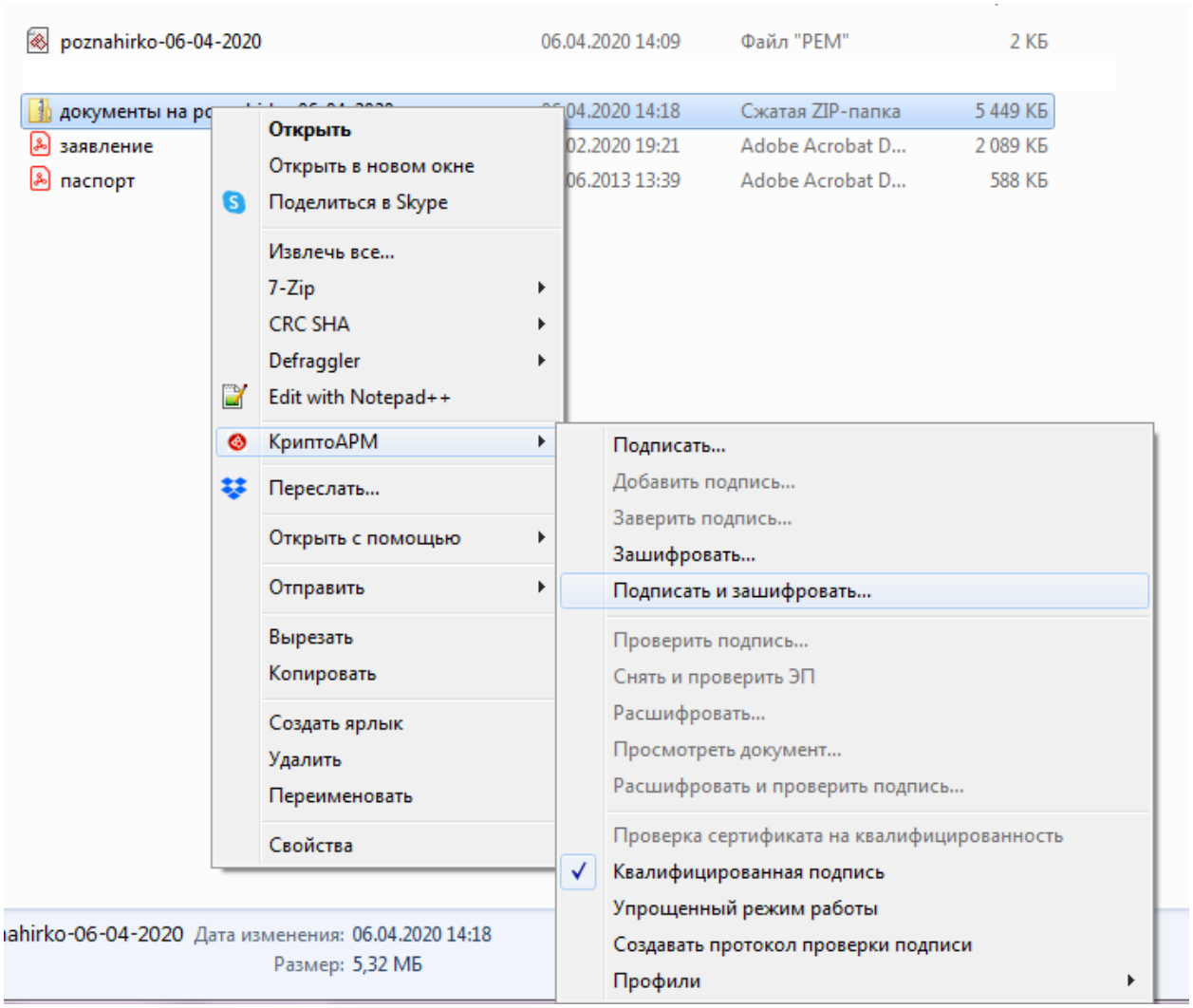


В следующем окне наживаем кнопку «Далее», и выбираем пункт «Поместить все сертификаты в следующие хранилище». В окне выбора хранилища устанавливаем галочку в «Показать физические хранилища» и выбираем хранилище Личное-Реестр

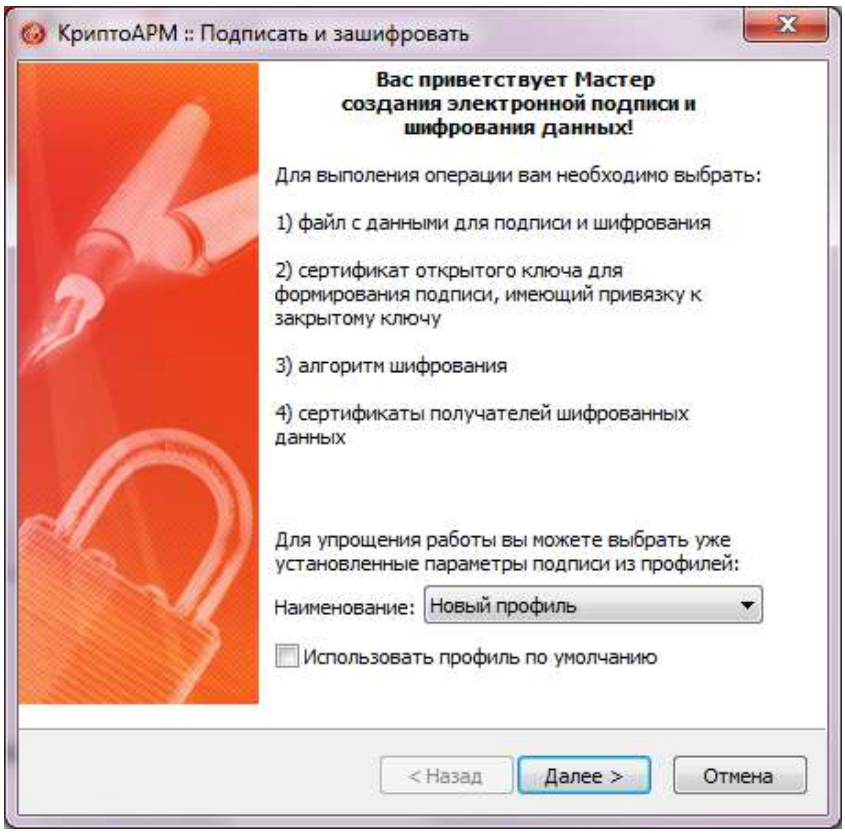


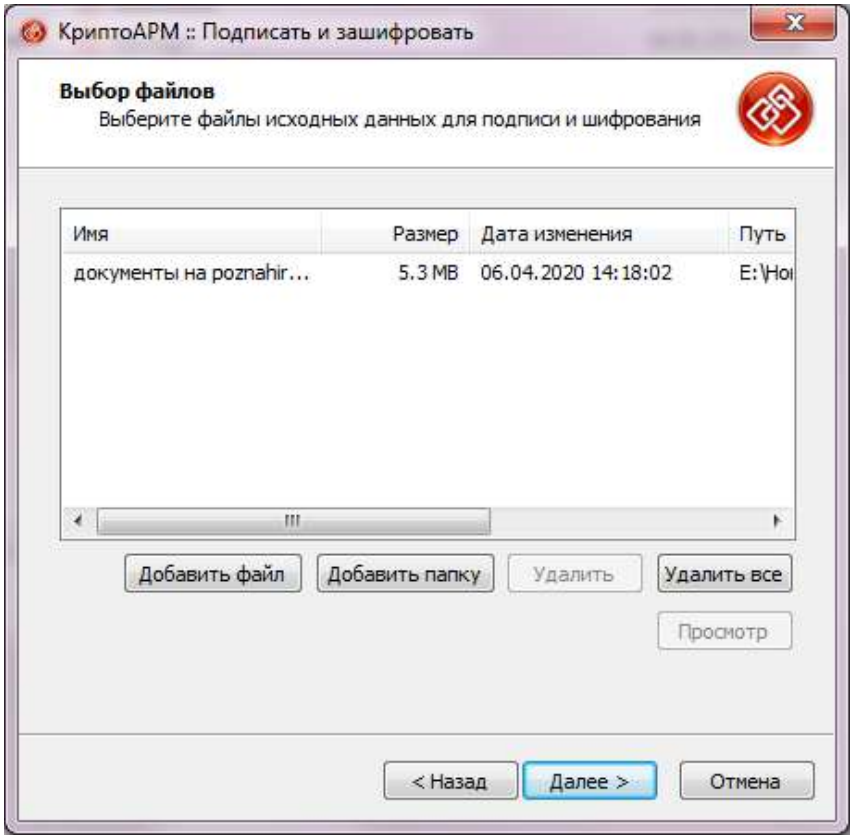
Нажимаем кнопку «ОК», кнопку «Далее» и «Готово», после чего переходим к подписанию и шифрованию.

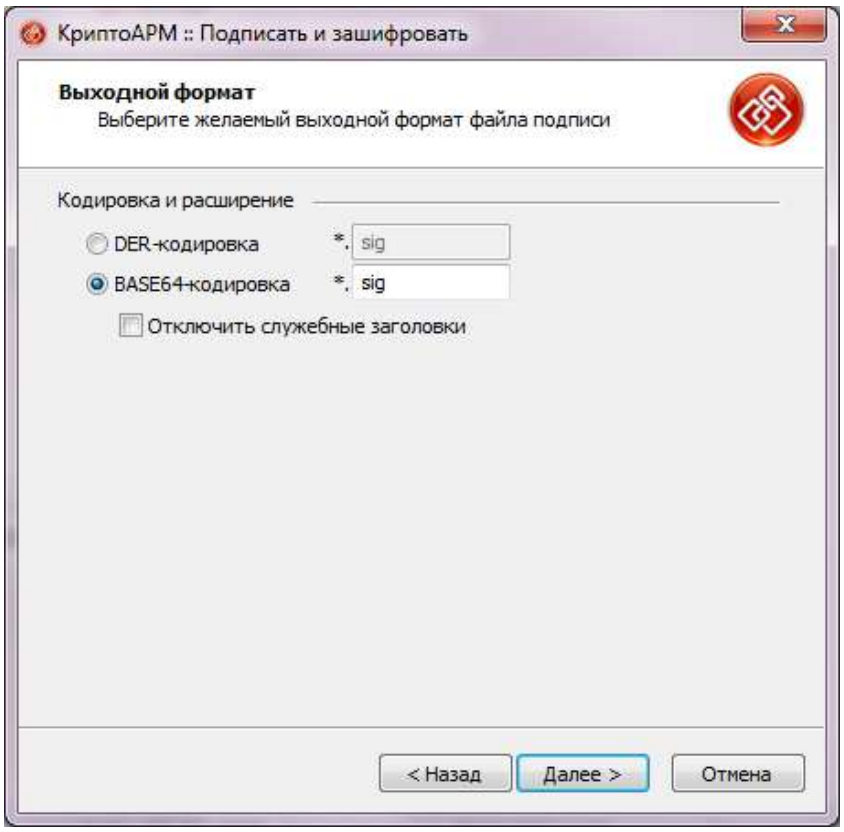
Для подписания и шифрования файлов перемещаем указатель на созданный архив, ПКМ и выбираем КриптоАрм-Подписать и зашифровать.

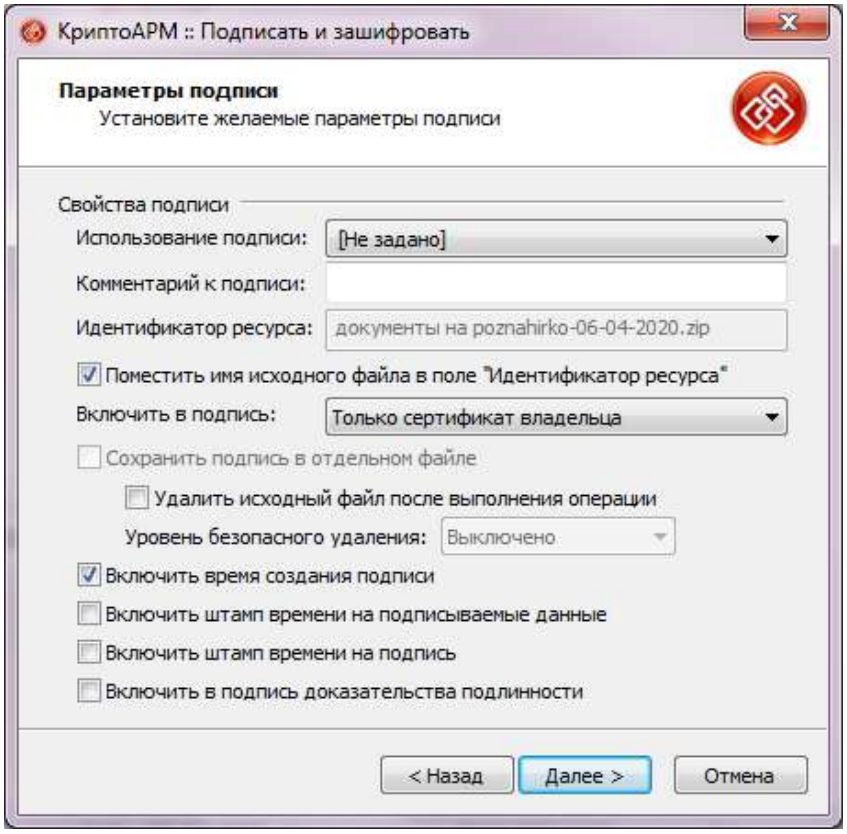


Проходим процедуру подписания, в первых 4-х окнах все оставляем по умолчанию.


КриптоАРМ :: Подписать и зашифровать
Вас приветствует Мастер создания электронной подписи и шифрования данных!
Для выполения операции вам необходимо выбрать:
1) файл с данными для подписи и шифрования
2) сертификат открытого ключа для формирования подписи, имеющий привязку к закрытому ключу
3) алгоритм шифрования
4) сертификаты получателей шифрованных данных
Для упрощения работы вы можете выбрать уже установленные параметры подписи из профилей:
Наименование:
Новый профиль
Использовать профиль по умолчанию
< Назад
Далее >
Отмена


КриптоАРМ :: Подписать и зашифровать
Выбор файлов
Выберите файлы исходных данных для подписи и шифрования
Имя
Размер
Дата изменения
Путь
документы на poznahir...
5.3 MB
06.04.2020 14:18:02
Добавить файл
Добавить папку
Удалить
Удалить все
Просмотр
< Назад
Далее >
Отмена





Далее необходимо выбрать личный сертификат для подписания и шифрования.

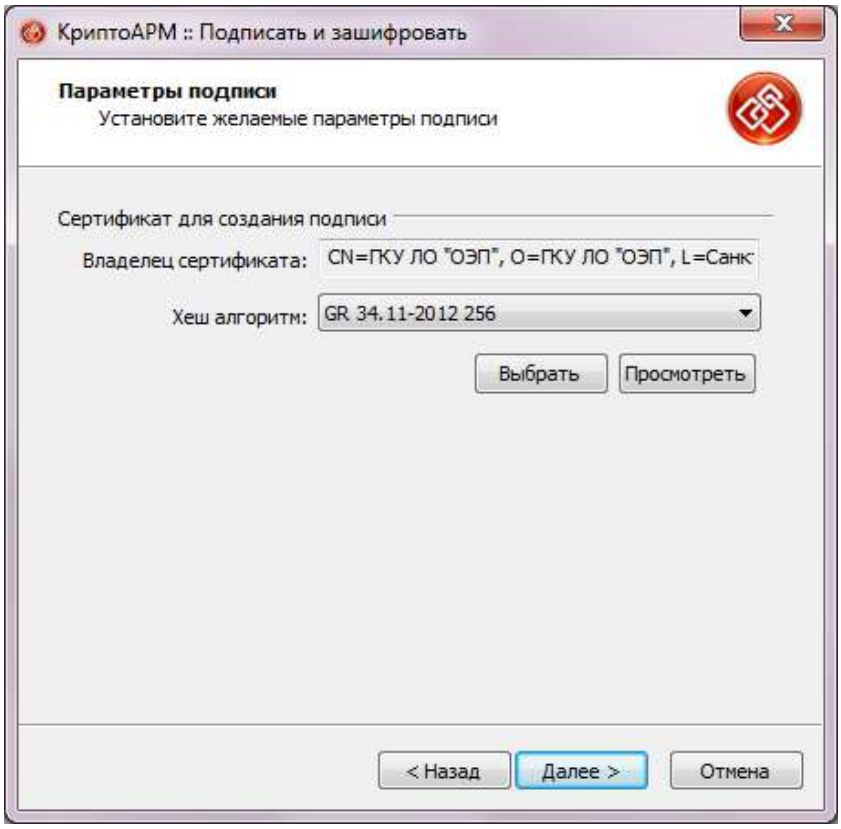
ВНИМАНИЕ!

Согласно процедуре удаленного продления сертификата вы можете выбрать один из способов подписания:

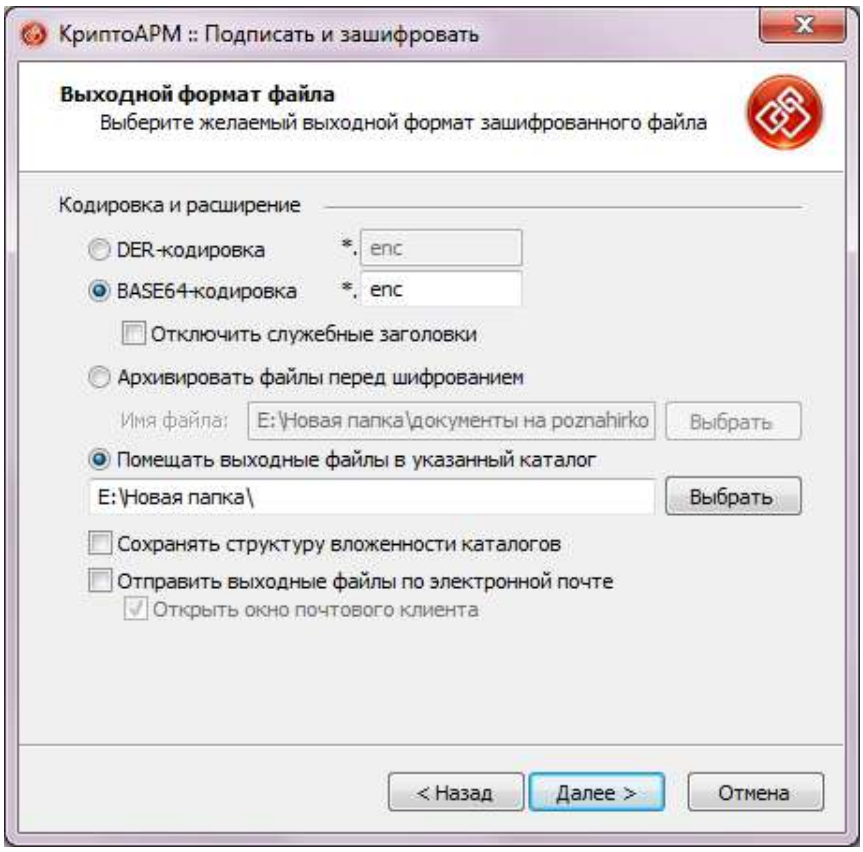
a. на своем личном действительном ключе электронной подписи;

b. на действительном ключе руководителя организации;

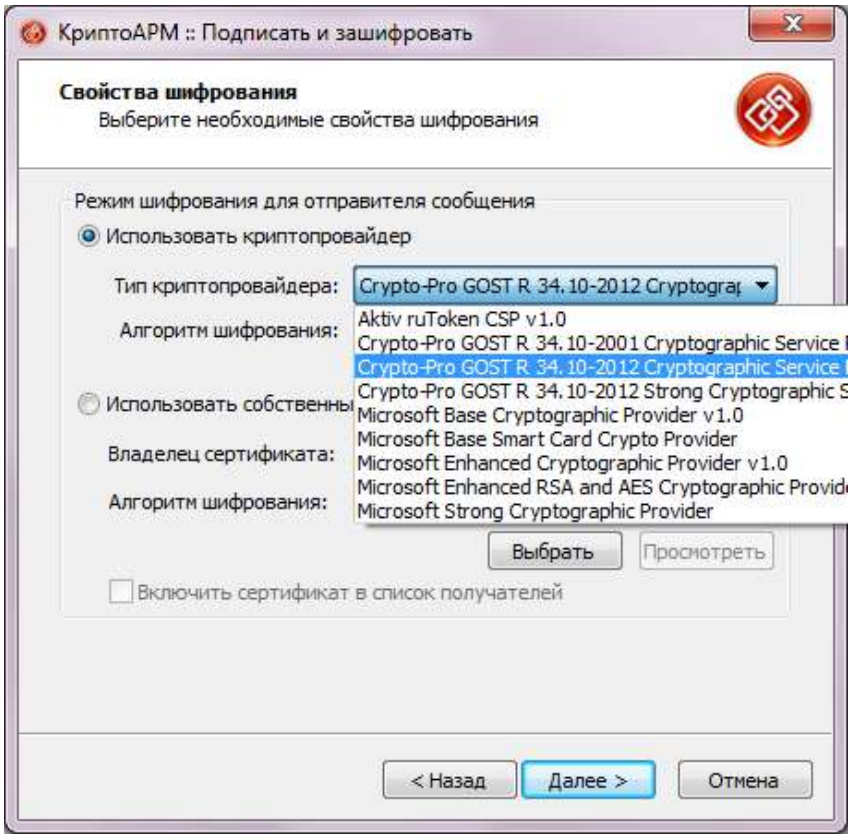
Также обращаем внимания сертификат может быть выдан любым аккредитованным удостоверяющим центром (например: сертификат выданный Федеральным Казначейством)



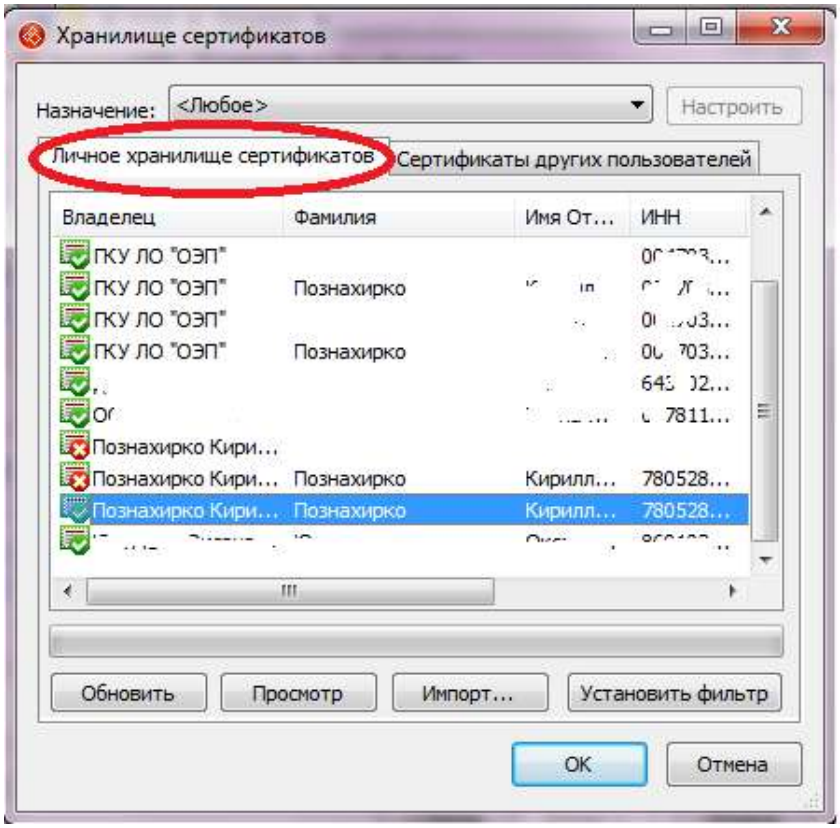
В последующем окне можно все оставить по умолчанию или выбрать путь куда сохранить подписанный и шифрованный файл.



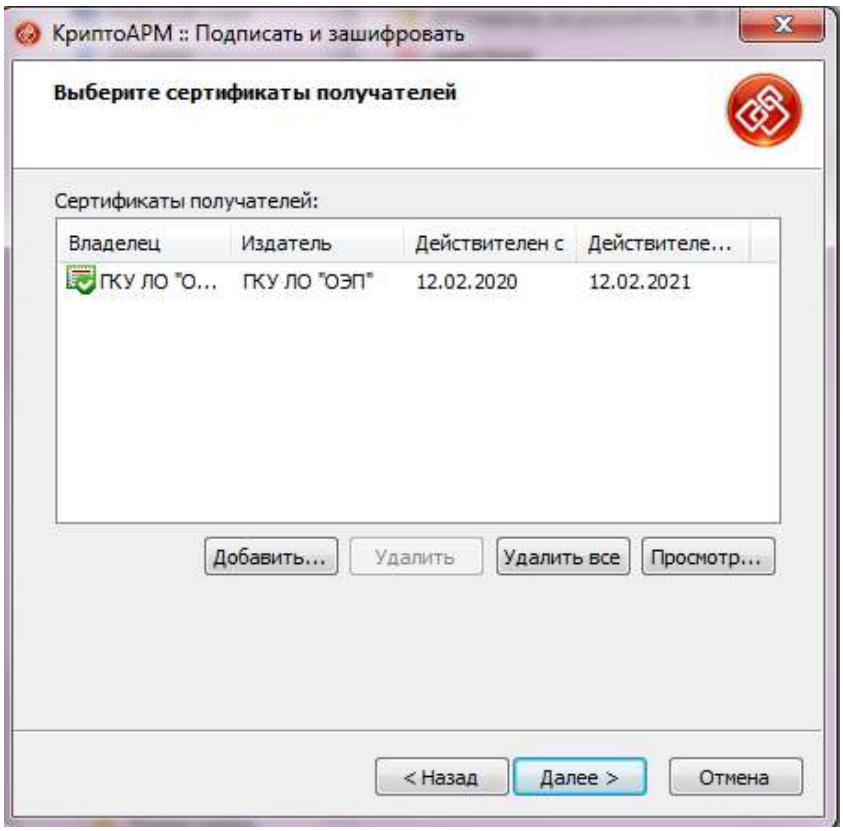
Далее в следующем окне необходимо выбрать используемый криптопровайдер, как и при создании запроса нужно обязательно выбрать Crypto-Pro GOST R 34/10-2012 Cryptographic Service Provider



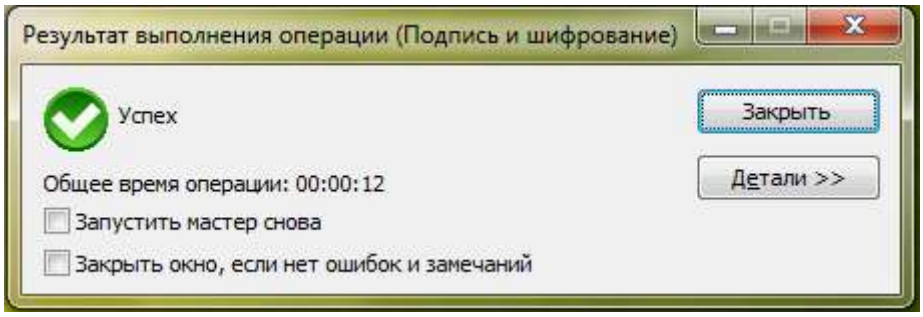
В окне выбора сертификата получателя, не забываем выбрать сертификат уполномоченного лица УЦ, для этого выберете вкладку «Личное хранилище сертификатов» и найдите сертификат уполномоченного лица УЦ.



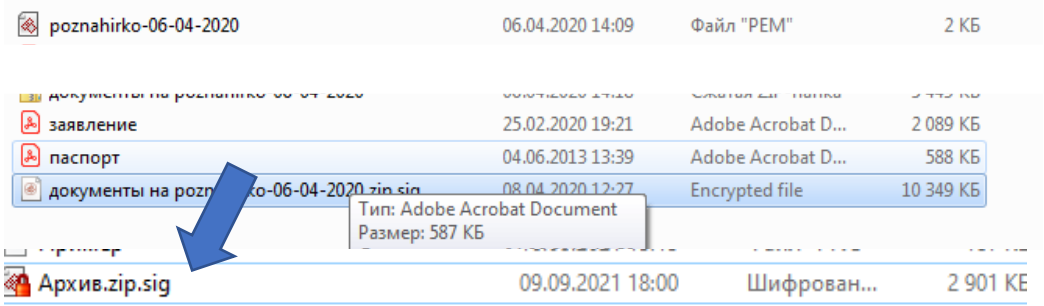
После выбора сертификата уполномоченного лица нажмите кнопку «Далее». Если требуется указать еще лицо в качестве получателя то повторите процедуру описанную выше.



по завершению должно появиться окно с успешным результатом выполнения процедуры подписания



Созданный зашифрованный файл с расширением sig необходимо направить на почту удостоверяющего центра udc@e-gov.lenobl.ru (Направляете только подписанный и зашифрованный архив, также не забудьте указать контактные данные).



Если вы отправляете несколько запросов их всех можно вложить в один архив и подписать (зашифровать) электронной подписью руководителя организации.