

Руководство по подготовке работы с электронной подписью для мобильного приложения EOSmobile и системы «ЭОС Совещания»

Москва
2024

В данном документе приведен порядок установки и настройки ЭП для мобильных подсистем EOSmobile и «ЕОС Совещания».

Книга не является полной документацией к программному обеспечению. Для использования программы необходимо наличие других книг, включаемых в комплект.

Подсистема постоянно совершенствуется и в связи с этим возможны некоторые несоответствия, касающиеся описания пользовательского интерфейса.

Документация разработана специалистами ГК «ЭОС».

Мобильные подсистемы являются торговой маркой ГК «ЭОС».

Право на тиражирование программных продуктов и документации принадлежит ГК «ЭОС».

Все упомянутые в данном издании товарные знаки и зарегистрированные товарные знаки принадлежат своим законным владельцам.

© ГК «ЭОС».

107113, Москва, ул. Шумкина, д. 20 стр. 1.
Тел/факс: (495) 221-24-31
e-mail: support@eos.ru
http://www.eos.ru

Оглавление

1. Условные обозначения 5
2. ЭП для ОС Android 6
2.1. Подготовка архива с ЭП (ОС Android) 6
2.2. Передача сертификата и ключа через CMP (ОС Android) 13
2.3. Загрузка из внутренней памяти (ОС Android) 18
2.4. Токен (ОС Android) 21
3. ЭП для ОС iOS 24
3.1. Подготовка архива с ЭП (ОС iOS) 24
3.2. Подготовка PFX-файла (для ОС iOS) 27
3.3. Передача сертификата и ключа через CMP (ОС iOS) 31
3.4. Загрузка из внутренней памяти (ОС iOS) 36
3.5. Токен (ОС iOS) 38
4. ЭП для ОС Аврора 40
4.1. Подготовка PFX-файла, архива с ЭП (ОС Аврора) 41
4.2. Передача сертификата и ключа через CMP (ОС Аврора) 45
4. ЭП для ОС Windows 50
4.3. Система «КАРМА» 50

1. Условные обозначения

- EOSmobile – наименование мобильного приложения
- «ЭОС Совещания» – наименование мобильного приложения
- МП – мобильное приложение (либо EOSmobile, либо «ЭОС Совещания»)
- Пользователь – мобильный пользователь, работающий в EOSmobile или «ЭОС Совещания»
- ОС – операционная система
- СМР – Сервер мобильных решений
- DMSIS – Сервис интеграции
- ЭП – электронная подпись
- КАРМА – универсальное программное решение для ЭП
- ДЛ – должностное лицо



Примечание:

Данный документ соответствует последней версии EOSmobile 4.X, последней версии «ЭОС Совещания» и последней версии СМР 4.X.

Для работы с ЭП необходимо в блоке «Электронная подпись» на сайте СМР включить хотя бы один из параметров (см. Рис. 1.1).

2. ЭП для ОС Android

Для обеспечения работы с ЭП на устройстве необходимо:

- либо на СМР загрузить ZIP-архив с ЭП и передать его в МП;
- либо загрузить из внутренней памяти устройства;
- либо подключить поддерживаемый внешний носитель с загруженными на него сертификатами.



Важно:

На устройствах Android должна быть введена лицензия КриптоПро версии 5.0.12922 и выше (лицензия приобретается отдельно).

2.1. Подготовка архива с ЭП (ОС Android)



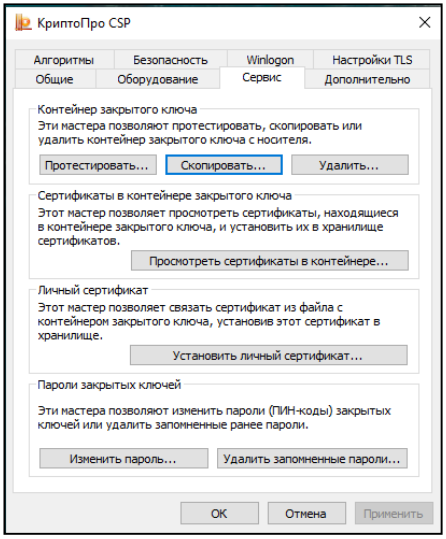
Важно:

Для копирования контейнера требуется установленная на компьютере программа КриптоПро CSP.

Для подготовки ZIP-архива с ЭП необходимо произвести следующую последовательность действий:

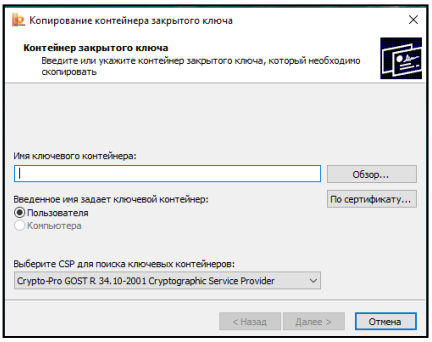
1. Копирование контейнера закрытого ключа с носителя Рутокен:
    1.1. подключить носитель к компьютеру;
    1.2. запустить программу КриптоПро CSP, перейти на закладку «Сервис» и нажать на кнопку «Скопировать» (см. Рис. 2.1.1):

Рис. 2.1.1 – Настройка сервиса КриптоПро CSP



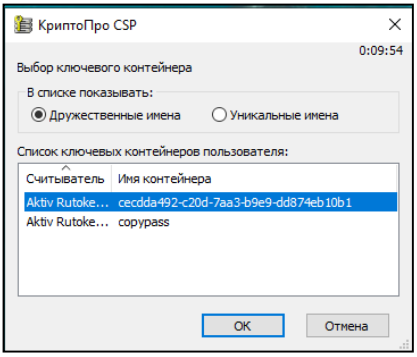
2. Нажать на кнопку «Обзор»:

Рис. 2.1.2 – Просмотр имени ключевого контейнера



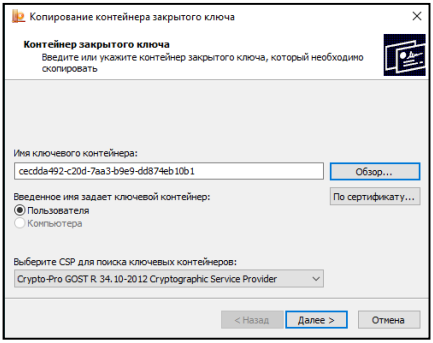
3. Выделить нужный ключевой контейнер и нажать кнопку «ОК»:

Рис. 2.1.3 – Выбор имени ключевого контейнера



4. Нажать на кнопку «Далее»:

Рис. 2.1.4 – Копирование закрытого ключа

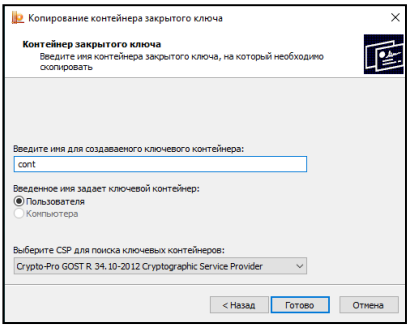


5. Ввести имя для создаваемого ключевого контейнера и нажать «Готово»:

Важно:

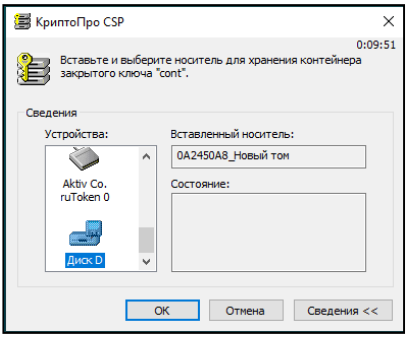
Имя контейнера в окне ниже не должно превышать 8 символов, иначе в дальнейшем работа с ЭП на мобильном устройстве будет невозможна!

Рис. 2.1.5 – Имя контейнера закрытого ключа



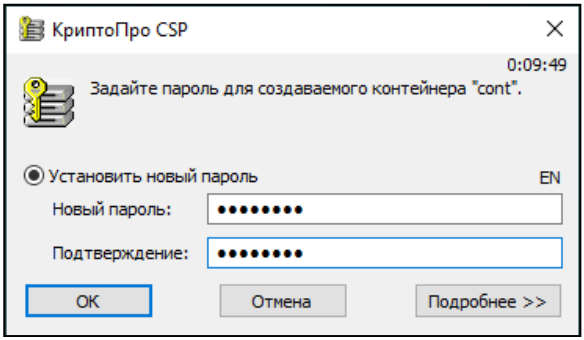
6. Выбрать диск для сохранения контейнера и нажать «ОК»:

Рис. 2.1.6 – Выбор диска для хранения контейнера закрытого ключа



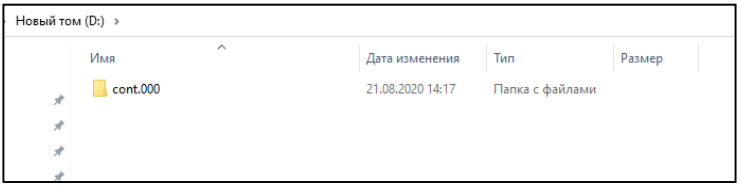
7. Установить пароль для создаваемого контейнера и нажать «ОК»:

Рис. 2.1.7 – Пароль для контейнера закрытого ключа



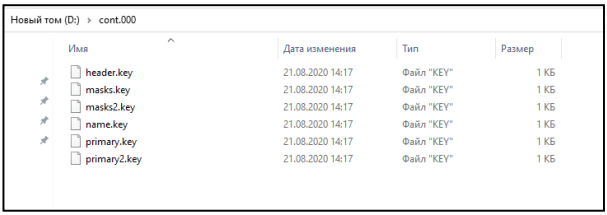
8. После успешного копирования перейти на диск, куда был скопирован контейнер:

Рис. 2.1.8 – Переход на диск с контейнером закрытого ключа



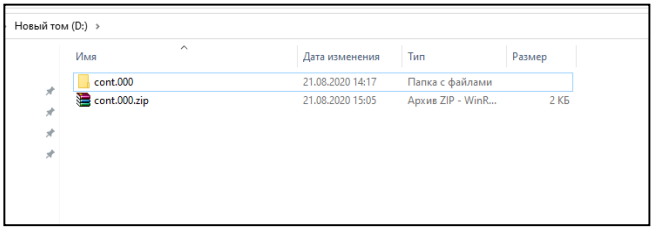
9. Зайти в папку и проверить, чтобы в ней находились 6 файлов с именами и расширением как показано ниже:

Рис. 2.1.9 – Отображение файлов в контейнере закрытого ключа



10. Далее папку с файлами (именно папку, а не файлы, находящиеся в данной папке) нужно добавить в .zip - архив с помощью программы для создания архивов (Winrar или другой). Формат архива .zip ОБЯЗАТЕЛЕН:

Рис. 2.1.10 – Помещение файлов контейнера в архив



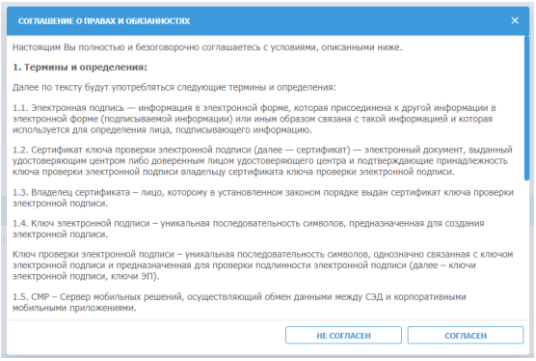
Важно:

Пароль на zip-архив устанавливать нельзя!
В противном случае архив не сможет быть распакован и автоматически применен.

2.2. Передача сертификата и ключа через СМР (ОС Android)

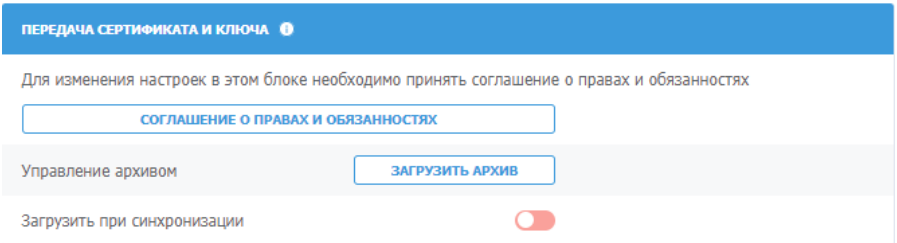
Для передачи сертификата и ключа в МП на сайте СМР в разделе «Настройки пользователя» блок «Передача сертификата и ключа» нажмите кнопку «Соглашение о правах и обязанностях». Произойдёт переход на страницу «Соглашение о правах и обязанностях» (см. Рис. 2.2.1).

Рис. 2.2.1 – Соглашение о правах и обязанностях



Прочтите внимательно «Соглашение о правах и обязанностях». Если вы не согласны с ним, нажмите кнопку «НЕ СОГЛАСЕН» слева внизу страницы, произойдёт переход на страницу настроек пользователя. Если вы согласны с ним, нажмите кнопку «СОГЛАСЕН» справа внизу страницы, кнопка «ЗАГРУЗИТЬ АРХИВ» станет доступной (см. Рис. 2.2.2).

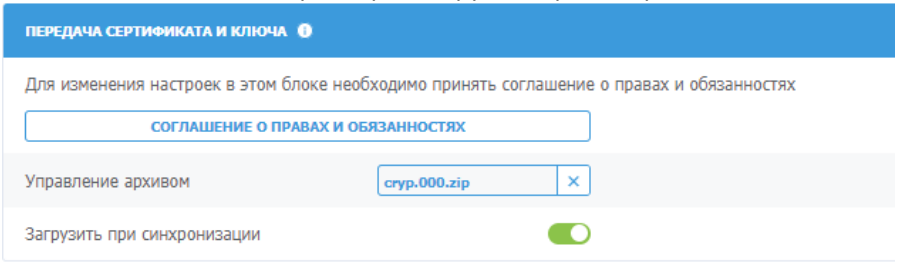
Рис. 2.2.2 – Доступность загрузки сертификата и ключей



На странице «Отправка сертификата и ключей» нажмите кнопку «ЗАГРУЗИТЬ АРХИВ». Откроется окно проводника, в котором нужно выбрать ранее подготовленный zip-архив, содержащий сертификат и ключи (подробнее про подготовку zip-архива см. п. 2.1 текущего документа).

После того как zip-архив с сертификатом и ключом выбран, информация о нём отобразится на странице СМР, параметр «Загрузить при синхронизации» будет автоматически переведен в положение ВКЛ (см. Рис. 2.2.3).

Рис. 2.2.3 – Включение параметра «Загрузить при синхронизации»



Примечание:

- Если необходимо обновить/заменить сертификат и ключ в МП, то необходимо загрузить новый zip-архив.
- Zip-архив будет храниться на СМР до тех пор, пока технолог не удалит его по кнопке «Х» справа.
- Для загрузки zip-архива необходимо в блоке «Электронная подпись» включить хотя бы один из параметров (см. Рис. 2.2.4).

Рис. 2.2.4 – Параметры ЭП на СМР во вкладке «Документооборот»

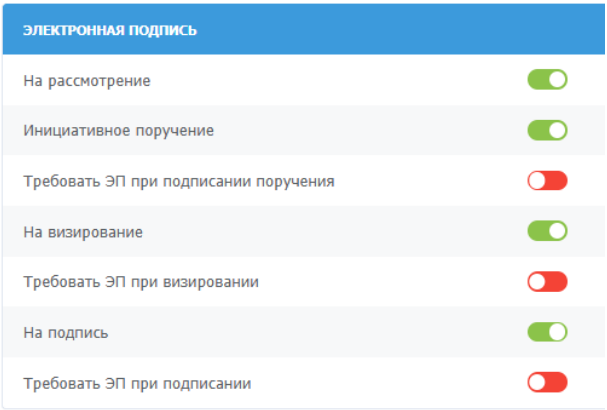


Рис. 2.2.5 – Параметры ЭП на СМР во вкладке «Совещания»



Пункт «На рассмотрение»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю будет доступна возможность использовать ЭП для подписания поручений. Соответственно мобильному пользователю в настройках EOSmobile будет доступен (отображен) раздел «Электронная подпись», а также доступна (отображена) кнопка «Направить на исполнение (с ЭП)».

Пункт «Инициативное поручение»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю будет доступна возможность использовать ЭП для подписания инициативных поручений.

Пункт «Требовать ЭП при подписании поручения»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю при работе с проектами поручений будет доступна ТОЛЬКО кнопка «Направить на исполнение (с ЭП)». Кнопка «Направить на исполнение» (без использования ЭП) не будет доступна (отображаться) в EOSmobile.



Пример / Совет:

Рекомендуется включить данный параметр, если мобильный пользователь планирует всегда подписывать электронной подписью проекты поручений. Вместе с тем, это упростит взаимодействие мобильного пользователя с интерфейсом EOSmobile.

Пункт «На визирование»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю при работе с проектами документов будет доступно использование ЭП.



Пример / Совет:

Данный параметр не требует от мобильного пользователя строгого использования ЭП при визировании проекта документа, соответственно пользователь может завизировать проект документа с или без использования ЭП.

Пункт «Требовать ЭП при визировании»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильный пользователь сможет завизировать проект документа ТОЛЬКО с использованием ЭП. Визирование без ЭП будет недоступно.



Пример / Совет:

Включение данного параметра может потребоваться, если пользователю необходимо все визировать с использованием ЭП. Соответственно данный параметр исключит вероятность, что пользователь завизирует проект документа без использования ЭП.

Пункт «На подпись»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю при работе с проектами документов будет доступно использование ЭП.

Пункт «Требовать ЭП при подписании»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильный пользователь сможет подписать проект документа ТОЛЬКО с использованием ЭП. Подписание без ЭП будет недоступно.

Пункт «Использовать электронную подпись»

По умолчанию ВКЛ. Если параметр ВЫКЛ., то мобильный пользователь не сможет подписать мнение или голос с использованием ЭП. Подписание с ЭП будет недоступно.

2.3. Загрузка из внутренней памяти (ОС Android)



Важно:

Для копирования контейнера требуется установленная на компьютере программа КриптоПроCSP.



Важно:

После установки МП при первом входе в приложение или во время работы приложения следует обязательно предоставить приложению требуемые права.

1. Подготовка архива с ЭП.

Для подготовки ZIP-архива с ЭП необходимо произвести последовательность действий, описанную в п. 2.1. текущего документа.

2. Установка ключа и сертификата в МП Android:

2.1. Подключить устройство к компьютеру в режиме передачи файлов.

2.2. Скопировать созданный zip-архив (в примере cont.000.zip) во внутреннюю память устройства (например, в папку Download).

2.3. Важно! Для установки сертификата и ключа на устройство требуется, чтобы в параметрах пользователя на СМР в разделе

«Электронная подпись» был включен как минимум один параметр из следующих параметров:

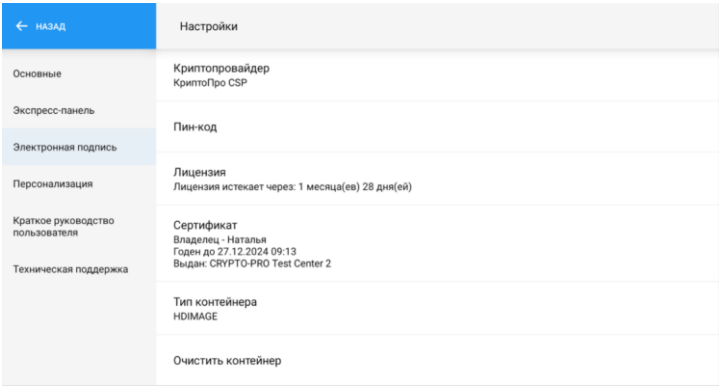
- На рассмотрение
- Инициативное поручение
- На визирование
- На подпись

Нажать на кнопку «Синхронизация» в МП.

2.4. После синхронизации приложения с СМР зайти в раздел «Настройки» - «Электронная подпись».

2.5. По нажатию на строку «Тип контейнера» выбрать «HDIMAGE». Нажать на строку «Выбрать контейнер» и в появившемся окне выбрать загруженный в память zip-архив.

Рис. 2.3.1 – Настройка ЭП в МП



После выбора загруженного zip-архива будет произведена установка контейнера во внутреннее хранилище КриптоПро. После успешной установки на экране отобразится сертификат ЭП.

2.6. Нажать на строку «Лицензия» и в окне ввести лицензию КриптоПро CSP. После успешного ввода в строке будет показано время до

истечения срока лицензии.

2.7. По нажатию на строку «Пин-код» в окне можно задать пароль, который был введен при создании контейнера в шаге 7 п.2.1 текущего документа. Если пароль не вводить в данном окне, то он будет запрошен непосредственно при подписании.



Важно:

После установки zip-архив не будет удален из памяти устройства. Если требуется удаление архива, то пользователь может удалить его сам через файловый менеджер устройства или через подключение к компьютеру.



Важно:

Строка «Очистить контейнер»: после нажатия на эту строку и подтверждения операции будет произведено удаление ключевого контейнера, установленного из памяти устройства, а также введенного в п.2.7 пин-кода.

2.4. Токен (ОС Android)

Для работы с ЭП к устройству на Android может быть подключен внешний носитель ключевой информации.



Важно:

При работе с криптопровайдером КриптоПро CSP на внешних носителях необходимо, чтобы на мобильном устройстве было установлено программное обеспечение «Панель управления Рутокен» последней версии (для сертификатов на носителях Рутокен) https://play.google.com/store/apps/details?id=ru.rutoken .
В приложениях EOSmobile и «ЭОС Совещания» необходимо вводить лицензию для КриптоПро версии 5.0.12922 и выше (лицензия приобретается отдельно).



Примечание:

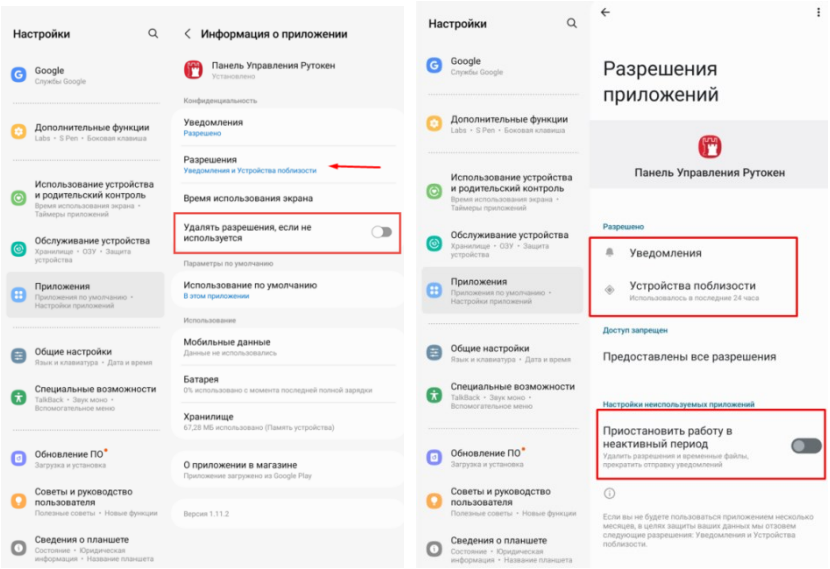
Для стабильной работы соединения устройства с bluetooth-токеном, не следует работать в режиме экономии заряда батареи, а также с низким уровнем заряда батареи.

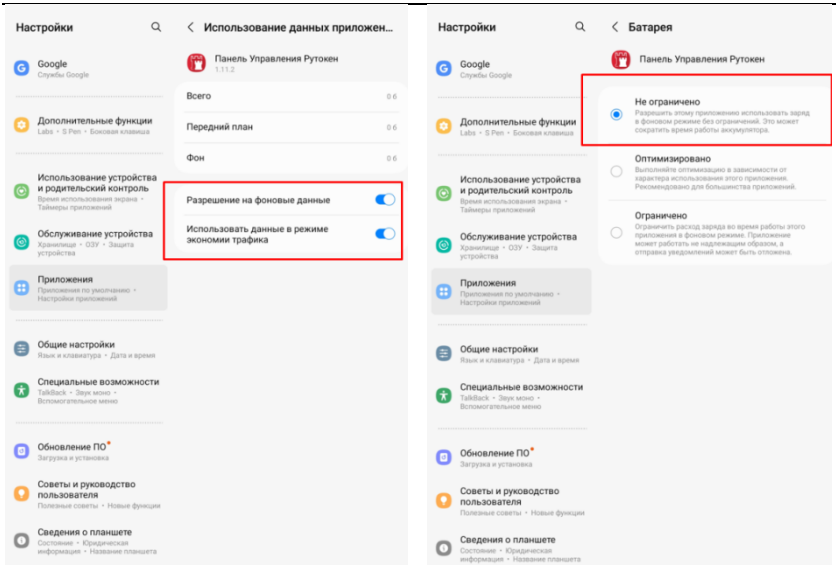
Для корректной работы Рутокен потребуются дополнительные настройки:

1. выгрузить из памяти устройства приложение «Панель управления Рутокен» и мобильное приложение,
2. зайти в настройки устройства -> Приложения -> «Панель управления Рутокен»,

3. дать разрешения приложению и выставить настройки (см. Рис. 8.3.4.3),
4. запустить «Панель управления Рутокен», убедиться, что токен отображается,
5. запустить мобильное приложение, в настройках ЭП выбрать криптопровайдера, выбрать тип контейнера и осуществить поиск сертификатов.

Рис. 8.3.4.3 – Настройки «Панель Управления Рутокен»





Выбрать тип контейнера Activ Rutoken ECP BT 1(2) при работе криптопровайдера КриптоПро с Bluetooth-носителями Рутокен.

3. ЭП для ОС iOS

Для обеспечения работы с ЭП на устройстве необходимо:

- либо на СМР загрузить ZIP-архив с ЭП и передать его в МП;
- либо загрузить из внутренней памяти устройства;
- либо подключить поддерживаемый внешний носитель с загруженными на него сертификатами.



Важно:

На устройствах iOS должна быть введена лицензия КриптоПро версии 5.0.12922 и выше (лицензия приобретается отдельно).

3.1. Подготовка архива с ЭП (ОС iOS)

Для подготовки ZIP-архива с ЭП необходимо произвести следующую последовательность действий:

Этап 1 – подготовка компонентов ЭП:

1. Скачать и установить программу КриптоПро CSP [1] – https://www.cryptopro.ru/products/csp/downloads

[1] Для доступа к данному разделу сайта необходимо быть авторизированным.



Примечание:

Данная программа требуется для работы с ключами.
Скачиваемая версия КриптоПро CSP зависит от следующих условий: используемая версия КриптоПро CSP в организации и лицензионного ключа клиенткой версии.

2. Запустить программу экспорта ключей и сертификатов [2] CryptoExportForm (подробнее см. далее). С помощью неё выгрузить из контейнера ключей следующие файлы:
    - Зашифрованный ключ, состоящий из трех файлов:
        - с расширением .salt
        - с расширением .vector
        - с расширением .key12
    - Сертификат, хранящийся в контейнере (формат DER с расширением .cer)

Этап 2 – подготовка ZIP-архива[3]:

1. Необходимо поместить в ZIP-архив:
    a) Все файлы из этапа №1
    b) Корневой сертификат удостоверяющего центра
    c) Все промежуточные сертификаты при их наличии

Этап 3 – загрузка ZIP-архива на СМР:

1. Загрузить ZIP-архив на СМР
2. Взвести флаг «Загрузить при синхронизации»
3. Запустить синхронизацию в МП

[2] Выдачу квалифицированных сертификатов можно заказать у любого поставщика ЭП, являющимся партнером КриптоПро
[3] Наименование ZIP-архива может быть любым

Этап 4 – распаковка и активация ЭП. Если ZIP-архив был правильно подготовлен, то он автоматически будет скачан мобильным приложением и распакован. Далее пользователю необходимо:

1. выбрать криптопровайдер КриптоПро,
2. ввести ключ лицензии КриптоПро,
3. выбрать ранее загруженный сертификат (полученный из ZIP-архива),
4. если предполагается автоматический ввод пин-кода, то ввести пин-код.

Обновление сертификата в МП.

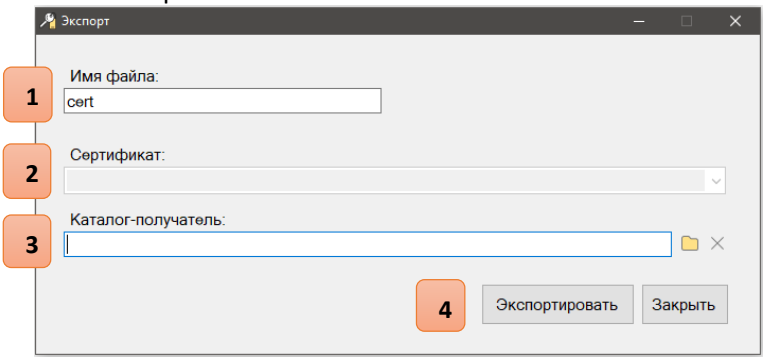
Подготовка и отправка обновленного сертификата аналогична.

Запустить программу «Crypto_Export_Form» и далее следуйте инструкции.

ШАГИ:

1. Поле «Имя файла» – наименование файла сертификата после экспорта. Заполнить поле «Имя файла» или оставить его по умолчанию.
2. Выбрать контейнер закрытых ключей КриптоПро.
3. Выбрать папку для сохранения экспортированного сертификата. Если папка не выбрана или выбрана некорректно, то сертификат будет экспортирован в директорию с программой.
4. Нажать кнопку «Экспортировать» и дождаться сообщения об успешном экспорте или об ошибке (см. Рис. 3.1.1).

Рис. 3.1.1 – Экспорт



Подготовка PFX-файла описана ниже.

3.2. Подготовка PFX-файла (для ОС iOS)

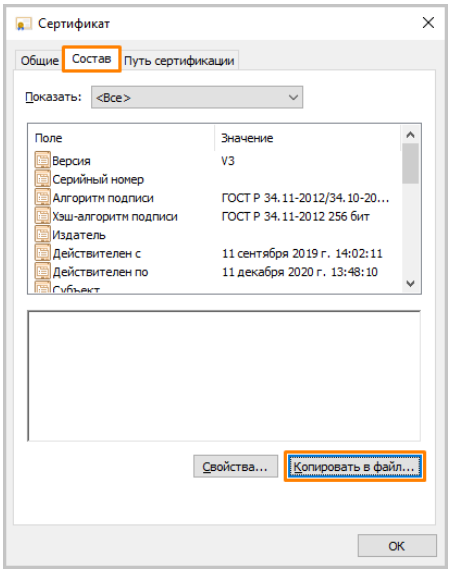
Экспортирование PFX-файла

1. Откройте оснастку работы с сертификатами:

— Пуск → Все программы → КриптоПро → Сертификаты

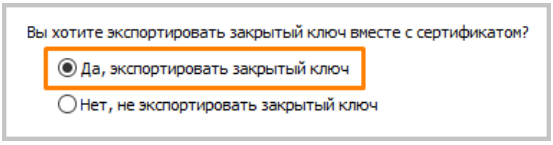
2. Откройте сертификат, который нужно скопировать. На вкладке «Состав» нажмите «Копировать в файл» (см. Рис. 3.2.1).

Рис. 3.2.1 – Экспорт сертификата



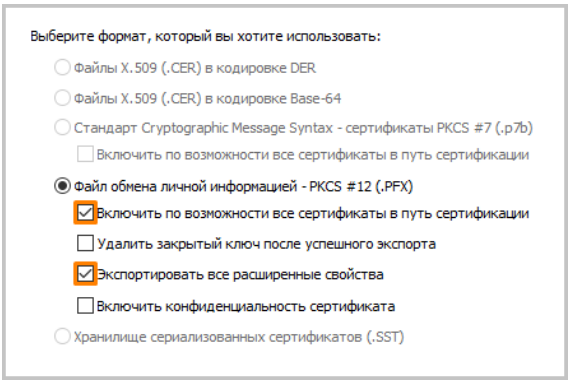
3. В «Мастере экспорта сертификтов» нажмите «Далее» и выберите пункт «Да, экспортировать закрытый ключ». Нажмите «Далее» (см. Рис. 3.2.2).

Рис. 3.2.2 – Мастер экспорта



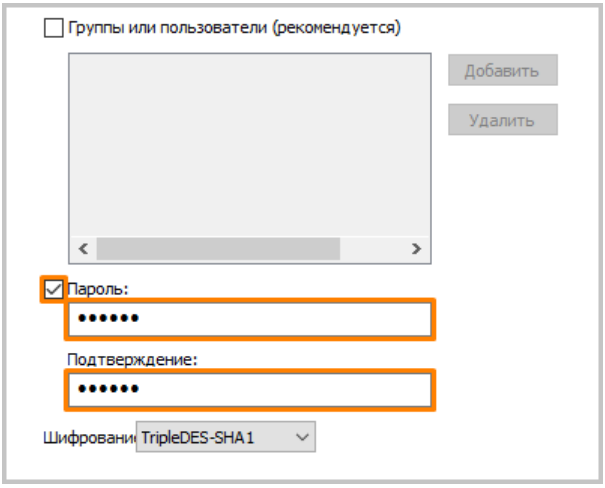
4. На следующем этапе поставьте галочки у пунктов «Включить по возможности все сертификаты в путь сертификации» и «Экспортировать все расширенные свойства», остальные галочки необходимо убрать. Нажмите «Далее» (см. Рис. 3.2.3).

Рис. 3.2.3 – Выбор формата



5. Обязательно задайте пароль для экспортируемого файла. Данный пароль не рекомендуется сообщать по электронной почте. Нажмите «Далее» (см. Рис. 3.2.4).

Рис. 3.2.4 – Пароль для экспортируемого файла



6. Укажите имя файла, выберите путь сохранения и нажмите «Далее», затем нажмите «Готово» (см. Рис. 3.2.5).

Рис. 3.2.5 – Имя файла



7. Экспортируйте открытый ключ сертификата (см. Экспорт открытого ключа).

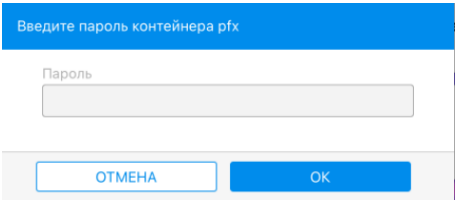
8. Заархивируйте полученные файлы форматов .pfx и .cer.

Импортирование PFX-контейнера с ЭП

Для импорта PFX-файла необходимо выполнить следующие шаги:

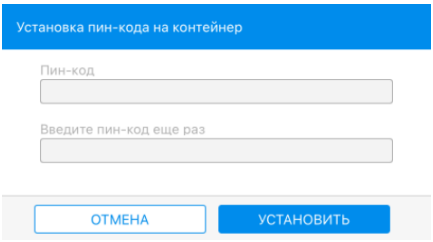
1. Создать PFX-файл и поместить его в .ZIP-архив (пароль на архив не устанавливать),
2. Загрузить .ZIP-архив в профиль пользователя на СМР. Параметр «Загрузить при синхронизации» ВКЛ,
3. Ввести пароль к PFX-файлу, установленного администратором (технологом) (см. Рис. 3.2.6),

Рис. 3.2.6 – Пароль контейнера с ЭП



4. Установить ПИН-код к контейнеру с ЭП (см. Рис. 3.2.7).

Рис. 3.2.7 – ПИН-код к контейнеру с ЭП

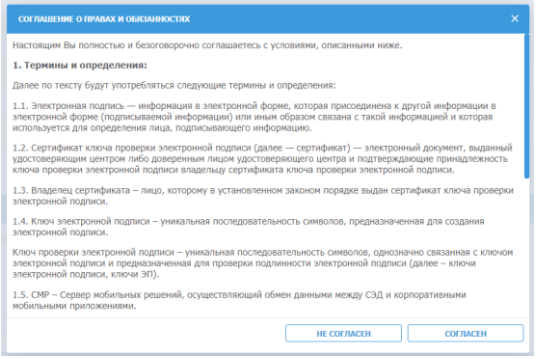


ПИН-код на контейнер с ЭП устанавливается на усмотрение пользователя, либо регламента, принятого в организации.

3.3. Передача сертификата и ключа через СМР (ОС iOS)

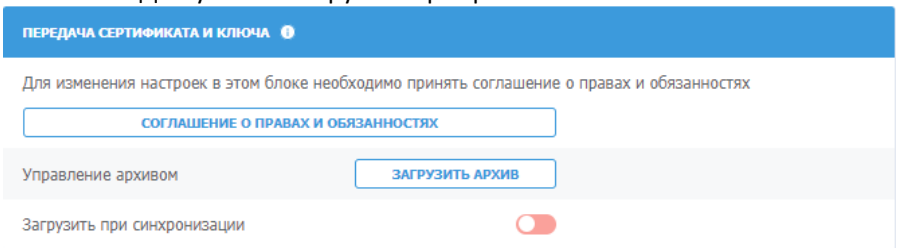
Для передачи сертификата и ключа в МП на сайте СМР в разделе «Настройки пользователя» блок «Передача сертификата и ключа» нажмите кнопку «Соглашение о правах и обязанностях». Произойдёт переход на страницу «Соглашение о правах и обязанностях» (см. Рис. 3.3.1).

Рис. 3.3.1 – Соглашение о правах и обязанностях



Прочтите внимательно «Соглашение о правах и обязанностях». Если вы не согласны с ним, нажмите кнопку «НЕ СОГЛАСЕН» слева внизу страницы, произойдёт переход на страницу настроек пользователя. Если вы согласны с ним, нажмите кнопку «СОГЛАСЕН» справа внизу страницы, кнопка «Загрузить архив» станет доступной (см. Рис. 3.3.2).

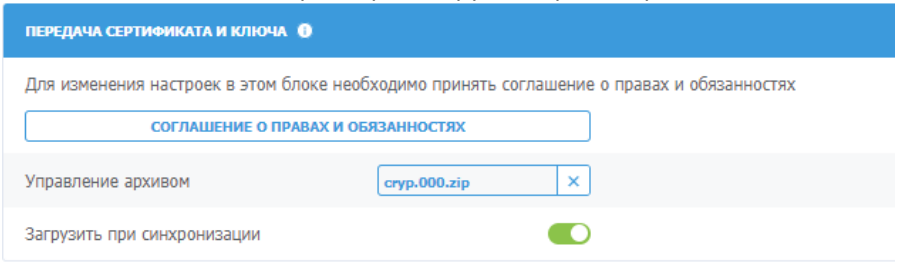
Рис. 3.3.2 – Доступность загрузки сертификата и ключей



На странице «Отправка сертификата и ключей» нажмите кнопку «ЗАГРУЗИТЬ АРХИВ». Откроется окно проводника, в котором нужно выбрать ранее подготовленный zip-архив, содержащий сертификат и ключи (подробнее про подготовку zip-архива см. п. 3.1 текущего документа).

После того как zip-архив с сертификатом и ключом выбран, информация о нём отобразится на странице СМР, параметр «Загрузить при синхронизации» будет автоматически переведен в положение ВКЛ (см. Рис. 3.3.3).

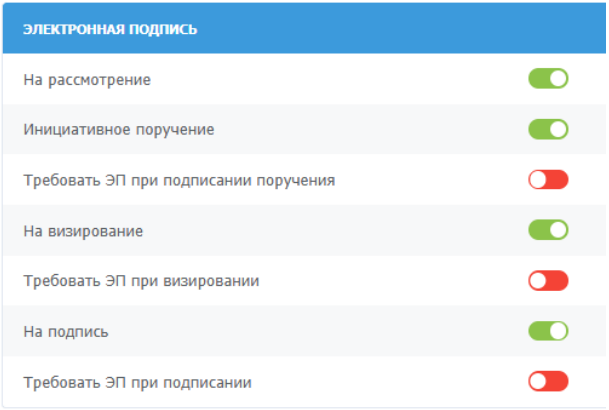
Рис. 3.3.3 – Включение параметра «Загрузить при синхронизации»



Примечание:

- Если необходимо обновить/заменить сертификат и ключ в МП, то необходимо загрузить новый zip-архив.
- Zip-архив будет храниться на СМР до тех пор, пока технолог не удалит его по кнопке «Х» справа.
- Для загрузки zip-архива необходимо в блоке «Электронная подпись» включить хотя бы один из параметров (см. Рис. 3.3.4).

Рис. 3.3.4 – Параметры ЭП на СМР во вкладке «Документооборот»



Пункт «На рассмотрение»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю будет доступна возможность использовать ЭП для подписания поручений. Соответственно мобильному пользователю в настройках EOSmobile будет доступен (отображен) раздел «Электронная подпись», а также доступна (отображена) кнопка «Направить на исполнение (с ЭП)».

Пункт «Инициативное поручение»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю будет доступна возможность использовать ЭП для подписания инициативных поручений.

Пункт «Требовать ЭП при подписании поручения»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю при работе с проектами поручений будет доступна ТОЛЬКО кнопка «Направить на исполнение (с ЭП)». Кнопка «Направить на исполнение» (без использования ЭП) не будет доступна (отображаться) в EOSmobile.



Пример / Совет:

Рекомендуется включить данный параметр, если мобильный пользователь планирует всегда подписывать электронной подписью проекты поручений. Вместе с тем, это упростит взаимодействие мобильного пользователя с интерфейсом EOSmobile.

Пункт «На визирование»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю при работе с проектами документов будет доступно использование ЭП.



Пример / Совет:

Данный параметр не требует от мобильного пользователя строгого использования ЭП при визировании проекта документа, соответственно пользователь может завизировать проект документа с или без использования ЭП.

Пункт «Требовать ЭП при визировании»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильный пользователь сможет завизировать проект документа ТОЛЬКО с использованием ЭП. Визирование без ЭП будет недоступно.



Пример / Совет:

Включение данного параметра может потребоваться, если пользователю необходимо все визировать с использованием ЭП. Соответственно данный параметр исключит вероятность, что пользователь завизирует проект документа без использования ЭП.

Пункт «На подпись»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю при работе с проектами документов будет доступно использование ЭП.

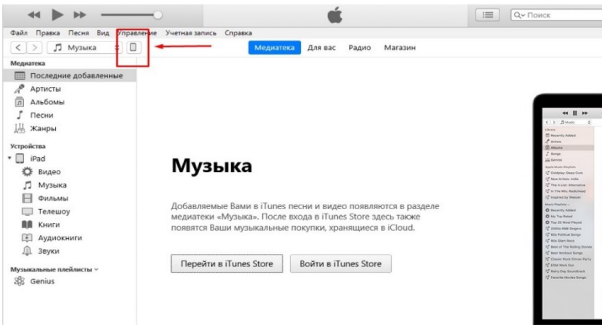
Пункт «Требовать ЭП при подписании»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильный пользователь сможет подписать проект документа ТОЛЬКО с использованием ЭП. Подписание без ЭП будет недоступно.

3.4. Загрузка из внутренней памяти (ОС iOS)

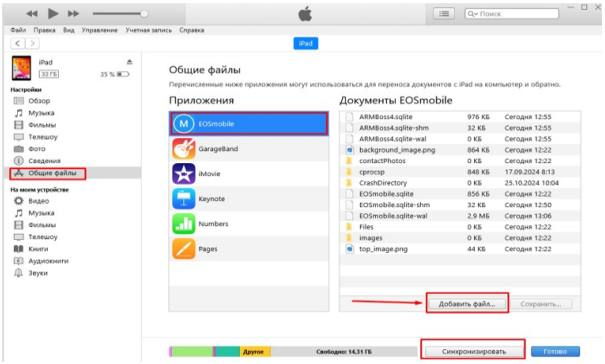
1. Ввести лицензию КриптоПро (версия 5) в мобильном приложении в настройках ЭП. Выгрузить приложение.
2. Установить на компьютере (Windows) iTunes: https://www.apple.com/itunes/
3. Подключить к компьютеру iPad.
4. Выбрать устройство (см. Рис. 3.4.1).

Рис. 3.4.1 – Выбор устройства



5. Перейти в «Общие файлы», выбрать приложение EOSmobile (см. Рис. 3.4.2).

Рис. 3.4.2 – Выбор приложения



6. Далее нажимаем «Добавить файл».

   Внимание: Файл должен быть с наименованием certs.zip. Синхронизируем с устройством кнопкой «Синхронизировать».

7. Запустить приложение на устройстве.
8. Ввести пароль (установленный при создании контейнера), если это контейнер с pfx-файлом.
9. Ввести пин-код и установить (по желанию пользователя).

3.5. Токен (ОС iOS)

SDK КриптоПро 5 может зачитывать сертификаты Рутокен, а также их использовать.

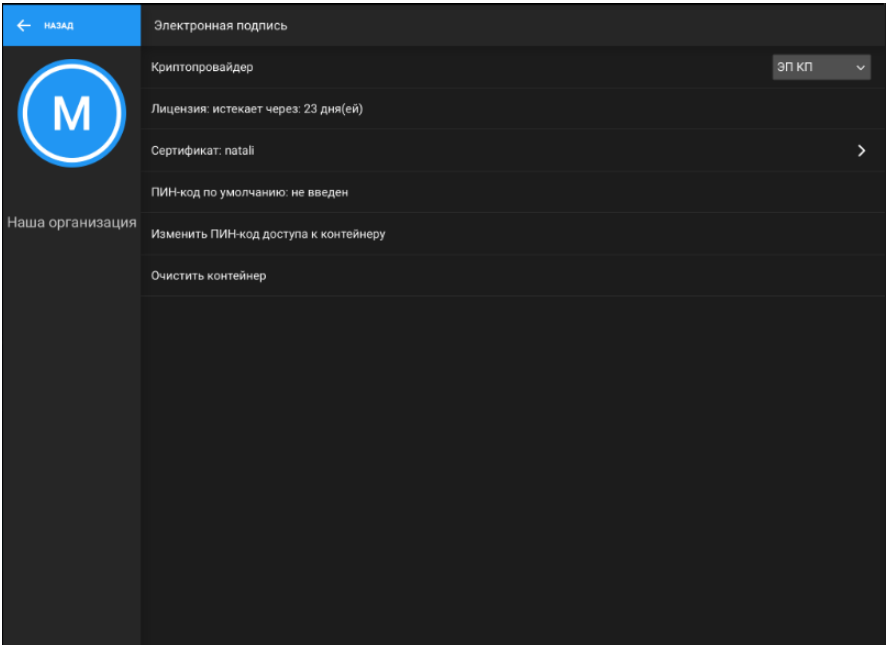


Важно:

Не рекомендуется в контейнер Рутокен записывать более 5 сертификатов.

1. Включить bluetooth в настройках планшета, включить Bluetooth-токен, дождаться подключения,
2. Зайти в Настройки мобильного приложения в раздел Электронная подпись и выбрать «ЭП КП» (см. Рис. 3.5.1),
3. Ввести лицензию КриптоПро (версия 5 и выше),
4. Перейти в раздел Сертификат, выбрать нужный (если их несколько),
5. Ввести пин-код и установить (по желанию пользователя).

Рис. 3.5.1 – Настройки ЭП



4. ЭП для ОС Аврора



Важно:

Для обеспечения работы с ЭП на устройстве необходимо:

- наличие приложения КриптоПро версии 5.0.12922 и выше на устройстве с введенной лицензией (приобретается отдельно);
  - для ввода лицензии откройте приложение КриптоПРО CSP, зажмите экран в любом месте и потяните сверху вниз, в появившейся вверху области выберите «Ввести лицензию», введите серийный номер (лицензионный ключ) CSP 5.0. Нажмите кнопку «ОК».
- загружен на СМР ZIP-архив с ЭП и МП успешно распаковало его.



Примечание:

Загрузка из внутренней памяти устройства не предусмотрена на текущий момент, так же не предусмотрена работа с внешними носителями ЭП.

4.1. Подготовка PFX-файла, архива с ЭП (ОС Аврора)

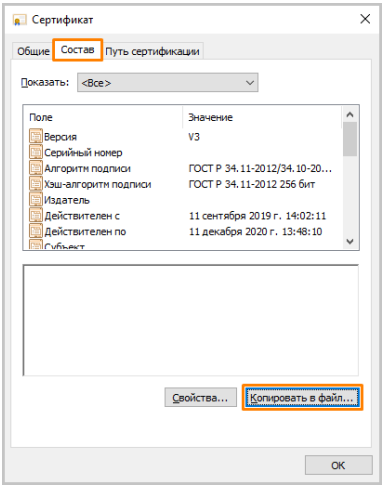
Экспортирование PFX-файла

1. Откройте оснастку работы с сертификатами:

Пуск → Все программы → КриптоПро → Сертификаты

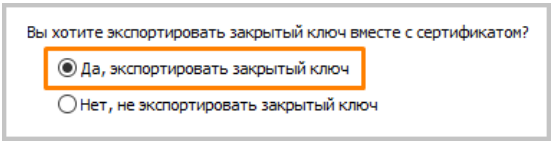
2. Откройте сертификат, который нужно скопировать. На вкладке «Состав» нажмите кнопку «Копировать в файл» (см. Рис. 4.1.1).

Рис. 4.1.1 – Окно работы с сертификатами



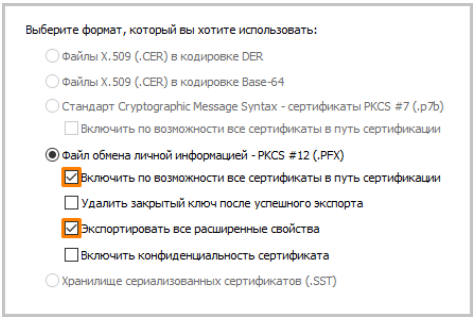
3. В «Мастере экспорта сертификтов» нажмите «Далее» и выберите пункт «Да, экспортировать закрытый ключ». Нажмите «Далее» (см. Рис. 4.1.2).

Рис. 4.1.2 – Мастер экпорта сертификатов



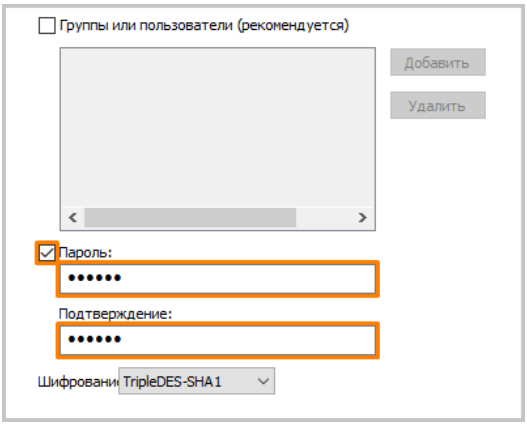
4. На следующем этапе поставьте галочки у пунктов «Включить по возможности все сертификаты в путь сертификации» и «Экспортировать все расширенные свойства», остальные галочки необходимо убрать. Нажмите «Далее» (см. Рис. 4.1.3).

Рис. 4.1.3 – Выбор формата



5. Обязательно задайте пароль для экспортируемого файла. Данный пароль не рекомендуется сообщать по электронной почте. Нажмите «Далее» (см. Рис. 4.1.4).

Рис. 4.1.4 – Пароль для экспортируемого файла



6. Укажите имя файла, выберите путь сохранения и нажмите «Далее», затем нажмите «Готово» (см. Рис. 4.1.5).

Рис. 4.1.5 – Имя экспортируемого файла



7. Экспортируйте открытый ключ сертификата (см. Экспорт открытого ключа).

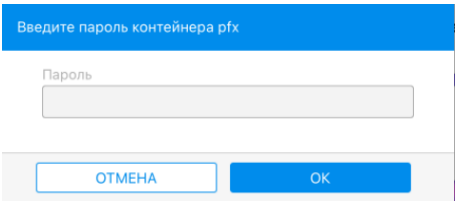
8. Заархивируйте полученные файлы форматов .pfx и .cer.

Импортирование PFX-контейнера с ЭП

Для импорта PFX-файла необходимо выполнить следующие шаги:

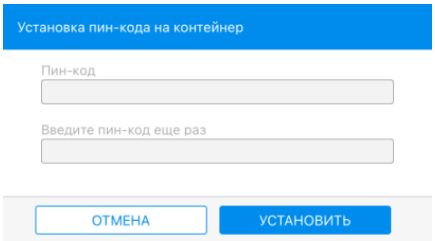
5. Создать PFX-файл и поместить его в .ZIP-архив (пароль на архив не устанавливать),
6. Загрузить .ZIP-архив в профиль пользователя на СМР. Параметр «Загрузить при синхронизации» ВКЛ,
7. Ввести пароль к PFX-файлу, установленный администратором (технологом) (см. Рис. 4.1.6),

Рис. 4.1.6 – Пароль контейнера с ЭП



8. Установить ПИН-код к контейнеру с ЭП (см. Рис. 4.1.7).

Рис. 4.1.7 – ПИН-код к контейнеру с ЭП

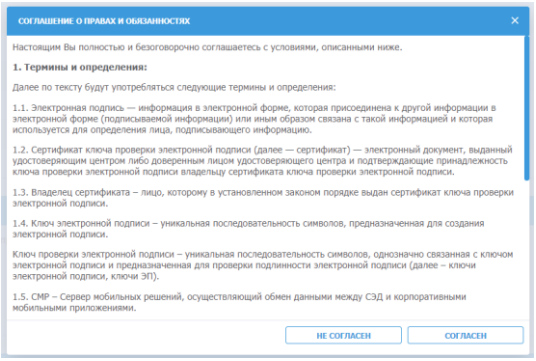


ПИН-код на контейнер с ЭП устанавливается на усмотрение пользователя, либо регламента, принятого в организации.

4.2. Передача сертификата и ключа через СМР (ОС Аврора)

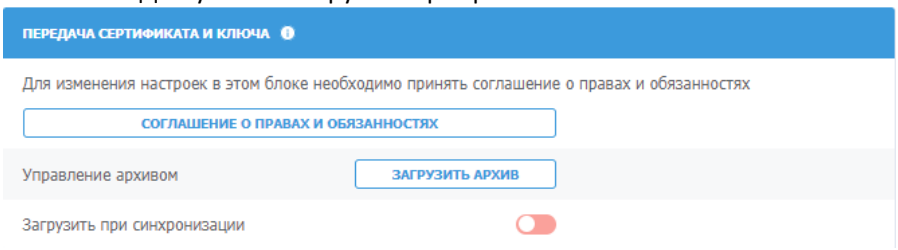
Для передачи сертификата и ключа в МП на сайте СМР в разделе «Настройки пользователя» блок «Передача сертификата и ключа» нажмите кнопку «Соглашение о правах и обязанностях». Произойдёт переход на страницу «Соглашение о правах и обязанностях» (см. Рис. 4.2.1).

Рис. 4.2.1 – Соглашение о правах и обязанностях



Прочтите внимательно «Соглашение о правах и обязанностях». Если вы не согласны с ним, нажмите кнопку «НЕ СОГЛАСЕН» слева внизу страницы, произойдёт переход на страницу настроек пользователя. Если вы согласны с ним, нажмите кнопку «СОГЛАСЕН» справа внизу страницы, кнопка «Загрузить архив» станет доступной (см. Рис. 4.2.2).

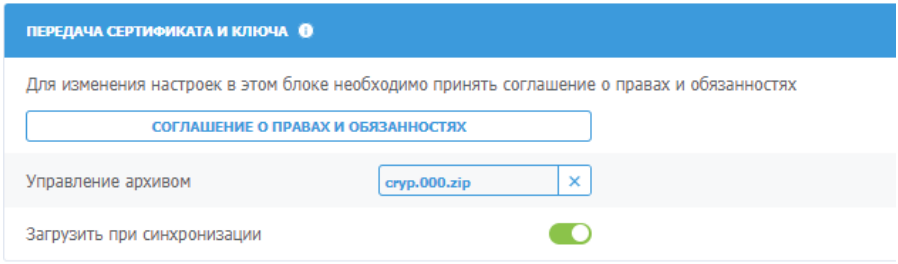
Рис. 4.2.2 – Доступность загрузки сертификата и ключей



На странице «Отправка сертификата и ключей» нажмите кнопку «ЗАГРУЗИТЬ АРХИВ». Откроется окно проводника, в котором нужно выбрать ранее подготовленный zip-архив, содержащий сертификат и ключи (подробнее про подготовку zip-архива см. п.4.1 текущего документа).

После того как zip-архив с сертификатом и ключом выбран, информация о нём отобразится на странице СМР, параметр «Загрузить при синхронизации» будет автоматически переведен в положение ВКЛ (см. Рис. 4.2.3).

Рис. 4.2.3 – Включение параметра «Загрузить при синхронизации»

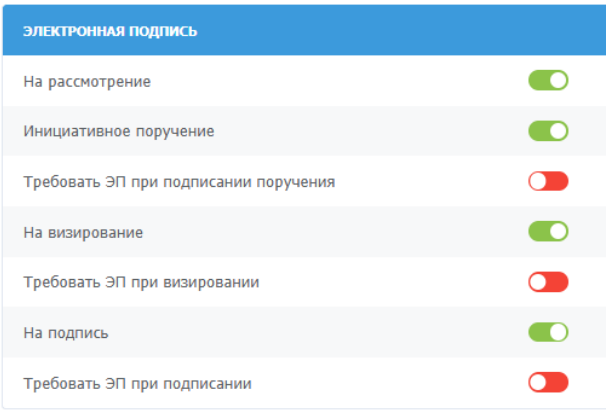


Примечание:

- Если необходимо обновить/заменить сертификат и ключ в МП, то необходимо загрузить новый zip-архив.

- Zip-архив будет храниться на СМР до тех пор, пока технолог не удалит его по кнопке «Х» справа.
- Для загрузки zip-архива необходимо в блоке «Электронная подпись» включить хотя бы один из параметров (см. Рис. 4.2.4).

Рис. 4.2.4 – Параметры ЭП на СМР во вкладке «Документооборот»



Пункт «На рассмотрение»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю будет доступна возможность использовать ЭП для подписания поручений. Соответственно мобильному пользователю в настройках EOSmobile будет доступен (отображен) раздел «Электронная подпись», а также доступна (отображена) кнопка «Направить на исполнение (с ЭП)».

Пункт «Инициативное поручение»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю будет доступна возможность использовать ЭП для подписания инициативных поручений.

Пункт «Требовать ЭП при подписании поручения»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю при работе с проектами поручений будет доступна ТОЛЬКО кнопка «Направить на исполнение (с ЭП)». Кнопка «Направить на исполнение» (без использования ЭП) не будет доступна (отображаться) в EOSmobile.



Пример / Совет:

Рекомендуется включить данный параметр, если мобильный пользователь планирует всегда подписывать электронной подписью проекты поручений. Вместе с тем, это упростит взаимодействие мобильного пользователя с интерфейсом EOSmobile.

Пункт «На визирование»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю при работе с проектами документов будет доступно использование ЭП.



Пример / Совет:

Данный параметр не требует от мобильного пользователя строгого использования ЭП при визировании проекта документа, соответственно пользователь может завизировать проект документа с или без использования ЭП.

Пункт «Требовать ЭП при визировании»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильный пользователь сможет завизировать проект документа ТОЛЬКО с использованием ЭП. Визирование без ЭП будет недоступно.



Пример / Совет:

Включение данного параметра может потребоваться, если пользователю необходимо все визировать с использованием ЭП. Соответственно данный параметр исключит вероятность, что пользователь завизирует проект документа без использования ЭП.

Пункт «На подпись»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю при работе с проектами документов будет доступно использование ЭП.

Пункт «Требовать ЭП при подписании»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильный пользователь сможет подписать проект документа ТОЛЬКО с использованием ЭП. Подписание без ЭП будет недоступно.

5. ЭП для ОС Windows

5.1 Система «КАРМА»

Важно

Для использования ЭП на устройстве, где установлено приложение EOSmobile (Windows), должны быть установлены следующие компоненты:

- система «КАРМА»,
- ПО криптопровайдера (в зависимости от криптопровайдера).

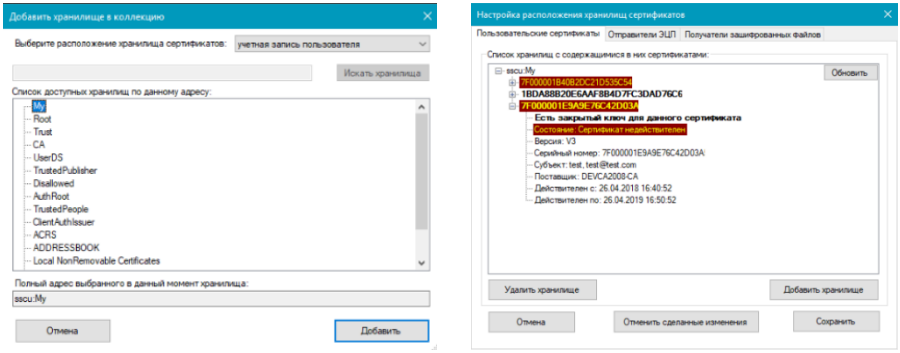
Примечание:

Т.к. Windows устройства позволяют использовать связку «КАРМА» & CryptoAPI & криптопровайдер, то ключевой контейнер может быть расположен на USB или Bluetooth токене, или в реестре Windows, или в «контейнере» на несистемном диске, или на отчуждаемом носителе.

Важно:

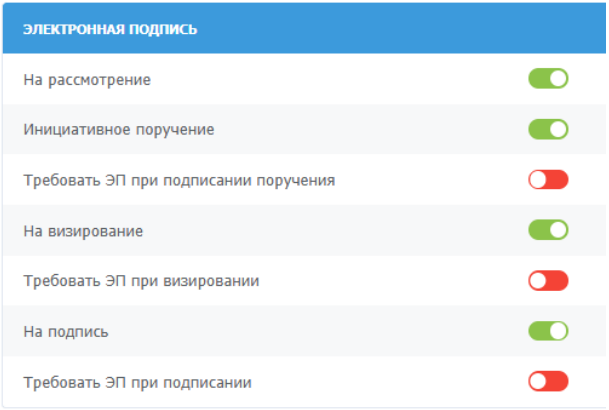
Валидный сертификат должен быть установлен в локальное хранилище пользователя.
Далее в настройках «КАРМА» должно быть выбрано хранилище «My» (личное). Путь: Обязательные -> Настройка адресов хранилищ сертификатов -> Добавить хранилище -> Выбрать «My» (см. Рис. 4.1.1).

Рис. 5.1.1 – Выбор хранилища сертификата в настройках «КАРМА»



Для работы с ЭП необходимо в блоке «Электронная подпись» на сайте СМР включить хотя бы один из параметров (см. Рис. 5.1.1).

Рис. 5.1.1 – Параметры ЭП на СМР во вкладке «Документооборот»



Пункт «На рассмотрение»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю будет доступна возможность использовать ЭП для подписания поручений. Соответственно мобильному пользователю в настройках EOSmobile будет доступен (отображен) раздел «Электронная подпись», а также доступна (отображена) кнопка «Направить на исполнение (с ЭП)».

Пункт «Инициативное поручение»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю будет доступна возможность использовать ЭП для подписания инициативных поручений.

Пункт «Требовать ЭП при подписании поручения»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю при работе с проектами поручений будет доступна ТОЛЬКО кнопка «Направить на исполнение (с ЭП)». Кнопка «Направить на исполнение» (без использования ЭП) не будет доступна (отображаться) в EOSmobile.



Пример / Совет:

Рекомендуется включить данный параметр, если мобильный пользователь планирует всегда подписывать электронной подписью проекты поручений. Вместе с тем, это упростит взаимодействие мобильного пользователя с интерфейсом EOSmobile.

Пункт «На визирование»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю при работе с проектами документов будет доступно использование ЭП.



Пример / Совет:

Данный параметр не требует от мобильного пользователя строгого использования ЭП при визировании проекта документа, соответственно пользователь может завизировать проект документа с или без использования ЭП.

Пункт «Требовать ЭП при визировании»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильный пользователь сможет завизировать проект документа ТОЛЬКО с использованием ЭП. Визирование без ЭП будет недоступно.



Пример / Совет:

Включение данного параметра может потребоваться, если пользователю необходимо все визировать с использованием ЭП. Соответственно данный параметр исключит вероятность, что пользователь завизирует проект документа без использования ЭП.

Пункт «На подпись»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильному пользователю при работе с проектами документов будет доступно использование ЭП.

Пункт «Требовать ЭП при подписании»

По умолчанию ВЫКЛ. Если параметр ВКЛ., то мобильный пользователь сможет подписать проект документа ТОЛЬКО с использованием ЭП. Подписание без ЭП будет недоступно.