Treasury and Trade solutions

Передача документов с использованием электронной подписи.

Руководство пользователя

Общая информация об электронной подписи.

В данном руководстве подробно описана последовательность действий, которые необходимы для начала использования электронной подписи для удаленного заключения договоров с Ситибанком.

Общая информация об электронной подписи

Законодательные аспекты использования и комплект необходимой документации

- Электронная подпись – это инструмент, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования подписи и проверить принадлежность подписи конкретному лицу. Использование электронной подписи регулируется Федеральным законом N 63-ФЗ «Об электронной подписи».

- В настоящее время электронная подпись используется для удаленного заключения договоров, подписания заявок и прочих юридически значимых документов. Согласно 63-ФЗ усиленная электронная подпись, используемая Ситибанком, является полным аналогом собственноручной подписи и печати организации. Ситибанк вправе ограничивать список документов, принимаемых с электронной подписью, оставляя возможность принять их только на бумаге.

Для начала использования электронной подписи при электронном обмене документами необходимо подписать следующие документы:

- **Заявление о присоединении к Договору о порядке обмена документами и информацией в электронном виде при обслуживании корпоративных клиентов**

  С Договором и Правилами обмена электронными документами можно ознакомиться, перейдя по ссылке: http://www.citibank.ru/russia/corporate/rus/edm.htm

- **Заявление о присоединении к Регламенту Удостоверяющего Центра**

  В настоящее время в качестве Удостоверяющего Центра используется УЦ «e-Notary», предоставляемый компанией «Сигнал-КОМ».

- **Заявление на выдачу USB-токена**

Общая информация об электронной подписи

Комплект поставки, краткое описание программного обеспечения

После подписания необходимой документации на электронную подпись каждый пользователь ЭП получает следующий набор программного и технического обеспечения:

- **USB-токен «Rutoken ЭЦП 2.0»**

  USB-токен используется для создания и хранения ключей электронной подписи. Так как ключ ЭП хранится на отдельном специальном физическом носителе, практически исключается возможность компрометации ключа и увеличивается общая безопасность информационной системы.

- «**Admin-PKI**»

  Программное обеспечение, позволяющее создать и записать на USB-токен уникальный ключ пользователя, а также создать и распечатать запрос на регистрацию данного сертификата (необходим для предоставления в банк).

- «**FilePro**»

  Программное обеспечение, позволяющее подписывать и шифровать файлы пользователя на компьютере, а также проверять авторство подписанных документов.

  Дистрибутивы можно скачать по ссылке:
  https://www.e-notary.ru/files/products/update/citibank/customers/adm_file_esp_win.zip

  Пароль к архиву: **citibank2019**

Общая информация об электронной подписи

Порядок обмена документами между АО КБ «Ситибанк» и клиентами

Некоторые документы можно передавать через модуль Delphi в системе CitiDirect, а некоторые – отправлять на выделенный email адрес. Возможно использовать следующие форматы документов: DOC, PDF, RTF.

Отправка документов через модуль Delphi	Отправка документов на выделенный email адрес
Необходимо добавить подписанный файл в архив ZIP, выбрать продукт «**ElectronicBanking**» в модуле Delphi системы CitiDirect и подгрузить архив. Предоставить уполномоченным лицам доступ к продукту «**ElectronicBanking**» в модуле Delphi можно, отправив запрос в DCS HelpDesk (техническая поддержка).	Подписанный документ можно отправить на выделенный email адрес – eforms.ru@citi.com

При передаче документов по электронным каналам обязательно использование Электронно-Цифровой Подписи, шифрования и архивирования(ZIP).

Программа для архивирования и разархивирования файлов – SECURE ZIP.

В настоящий момент в названии файла допустимы ТОЛЬКО латинские буквы и цифры.

Пожалуйста, обратите внимание, что документы будут приняты в обработку текущим днем, только если они были отправлены до 15-00 Московского времени.

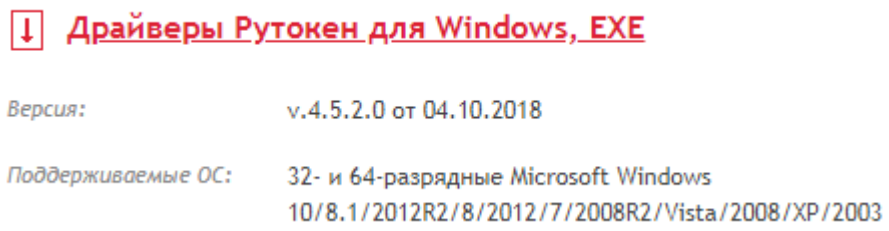
Подготовка USB-токена к работе.

Установка драйверов «Рутокен ЭЦП», руководство по использованию устройства.

Подготовка USB-токена к работе

Загрузка драйверов «Rutoken ЭЦП»

Загрузите драйверы с официального сайта: http://www.rutoken.ru/support/download/drivers-for-windows/



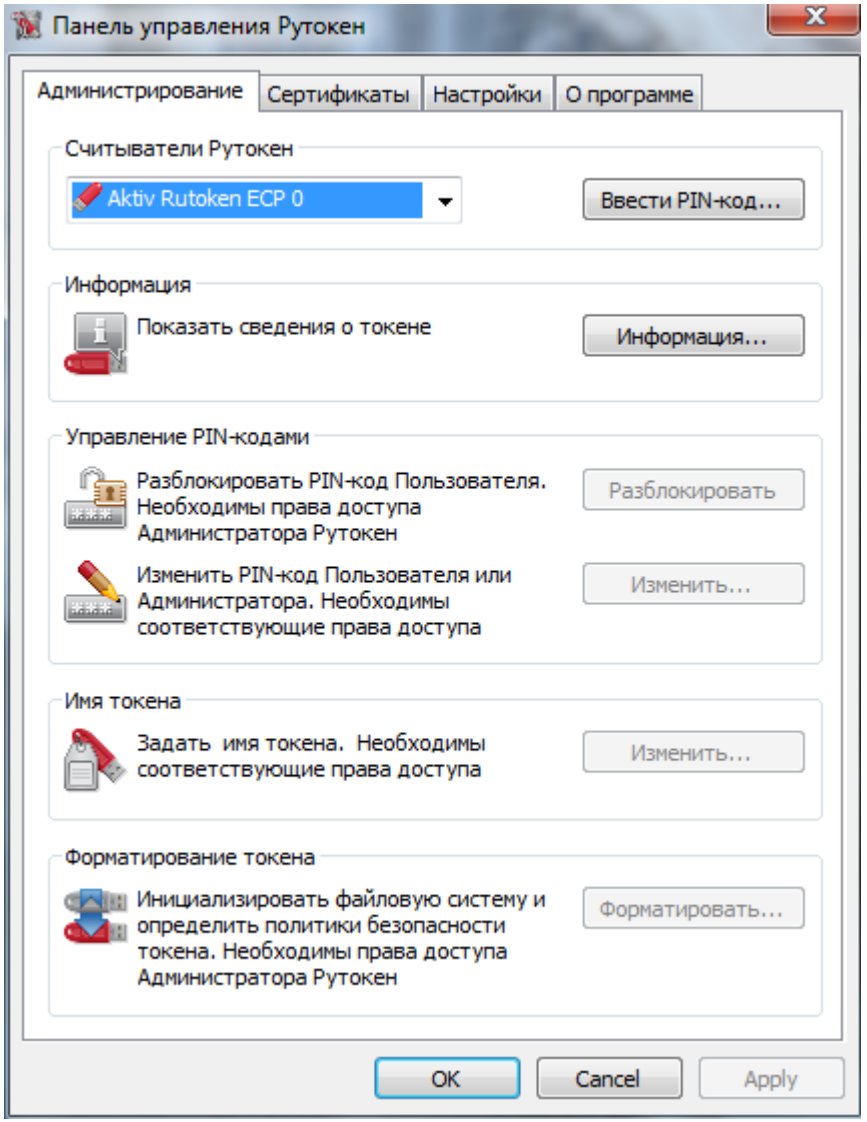
Для установки драйверов необходимы права администратора. Отсоедините Rutoken от USB-порта компьютера. Запустите программу установки и следуйте указаниям.

Для корректной работы устройства после установки драйвера **обязательно перезагрузите компьютер**.

После подключения на USB-токене должен загореться светодиод. Это говорит о том, что Rutoken корректно распознан операционной системой и готов к работе

Подготовка USB-токена к работе

Учетные записи Рутокен



Откройте «Панель управления Рутокен». По умолчанию ярлык панели прописывается на «Рабочем столе» и в меню «Все программы». В файловой системе Рутокен ЭЦП существует учетная запись Администратора и учетная запись Пользователя. Нажмите [Ввести PIN-код] для того, чтобы увидеть возможные варианты входа в систему.

1. Учетная запись **Пользователя** предусмотрена для задания имени токена и генерации запроса на сертификат в программе Admin-PKI.

Пин-код пользователя по умолчанию:
12345678

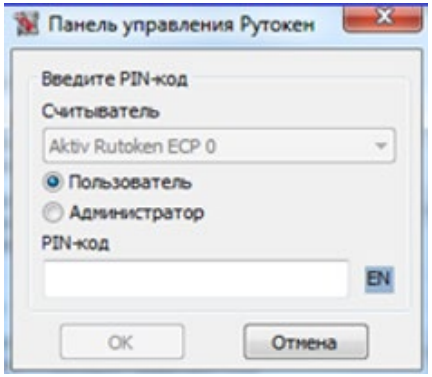
2. Учетная запись **Администратора** предусмотрена для разблокировки PIN-кода пользователя (на значение по умолчанию) и форматирования токена (удаление всех имеющихся данных, создание новой файловой системы).

Пин-код администратора по умолчанию:
87654321

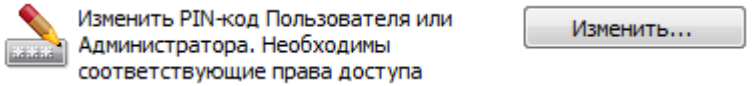
Подготовка USB-токена к работе

Смена PIN-кода.

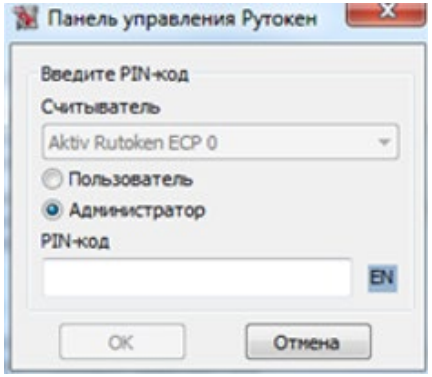
Внимание! В целях безопасности PIN-код администратора и пользователя необходимо заменить на **уникальный**.



Для того, чтобы изменить пин-код, в «Панели управления Рутокен» нажмите **[Ввести PIN-код]**, в появившемся окне выберите **Пользователь/Администратор** и нажмите на кнопку **[Изменить]**.



Для обеспечения безопасности:



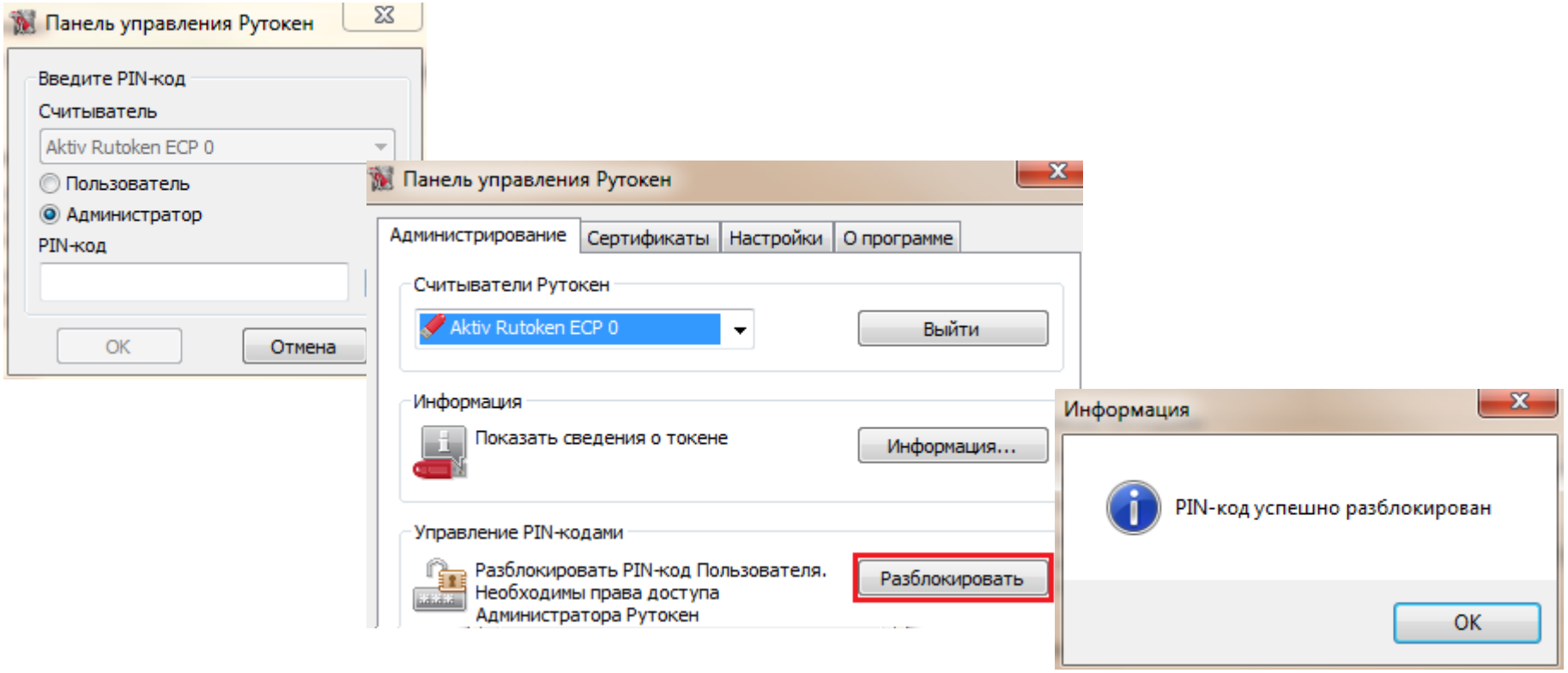
1. Не устанавливайте PIN-код менее 8 символов.
2. Не сообщайте ваш PIN-код никому из коллег или знакомых.
3. Храните устройство бережно, тогда оно прослужит долго.
4. При блокировке PIN-кода Пользователя обратитесь к Администратору.
5. Если был заблокирован PIN-код Администратора, то вопрос можно решить только полным очищением памяти, с потерей всех данных. Продолжить работу с ЭЦП в этом случае будет невозможно без создания нового ключа и предоставления нового запроса на сертификат в Банк.

Подготовка USB-токена к работе

Возможности учетной записи Администратора. Разблокировка PIN-кода Пользователя

Если неправильно набрать PIN-код Пользователя несколько раз подряд, то он блокируется. Rutoken ограничивает число неверных попыток ввода PIN-кода (по умолчанию 10). В этом случае Администратор Rutoken может разблокировать PIN-код Пользователя.

Откройте «Панель управления Рутокен», нажмите на кнопку **[Ввести PIN]**, выберите [Администратор], введите PIN-код. Для разблокировки PIN-кода пользователя нажмите кнопку **[Разблокировать].**



Установка программы “Admin-PKI”.

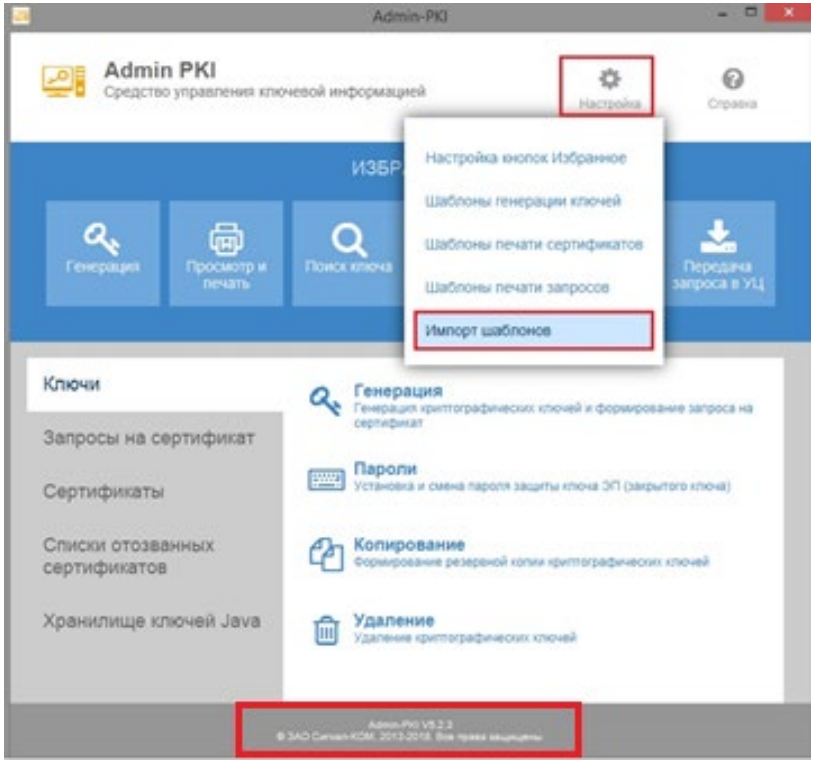
Установка программного обеспечения «Admin-PKI». Программа используется для создания запроса на сертификата электронной подписи.

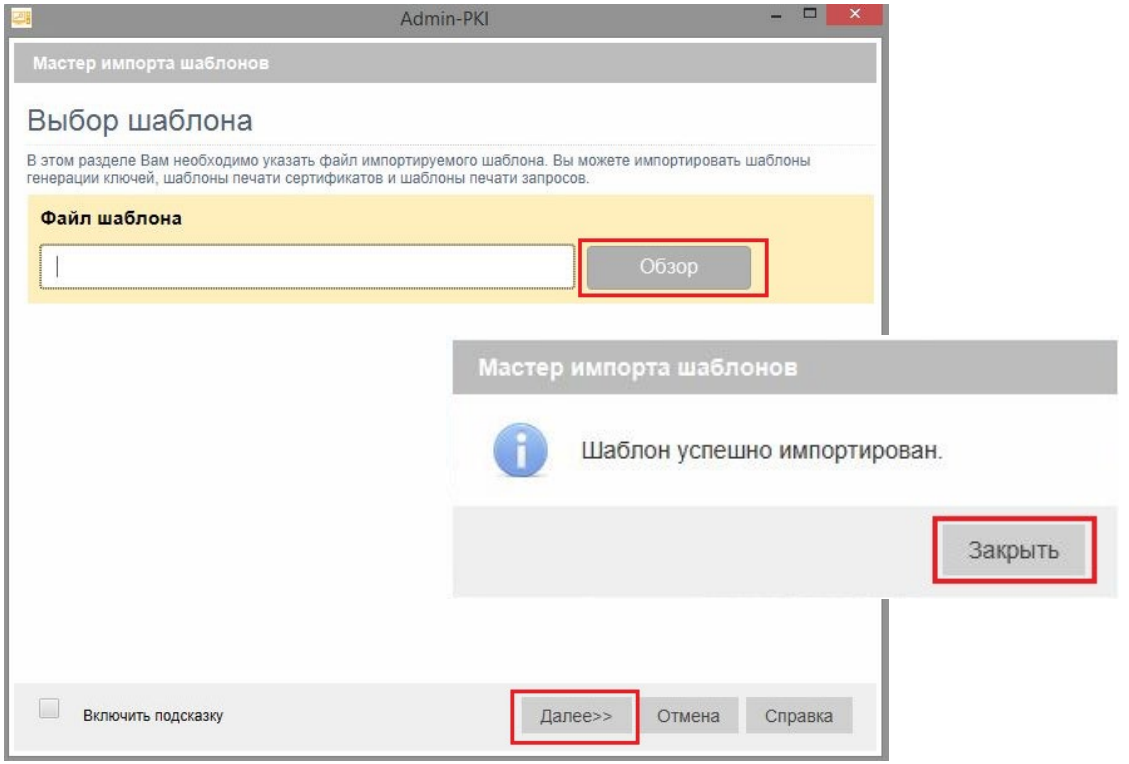
Установка “Admin-PKI”.

Установка и подготовка Admin-PKI к генерации запроса

Запустите установочный файл **[admin-pki_v.5***.exe]** с CD-диска «E-Notary. Криптографическая защита данных» с программным обеспечением (находится в пакете с USB-токеном) и следуйте указаниям.

Сохраните приложенный к данной инструкции файл: ***[5.2.3]_GOST_2012_default_keygen_template.tpl***, нажмите в программе Настройка > Импорт шаблонов > Обзор и выберите файл шаблона.





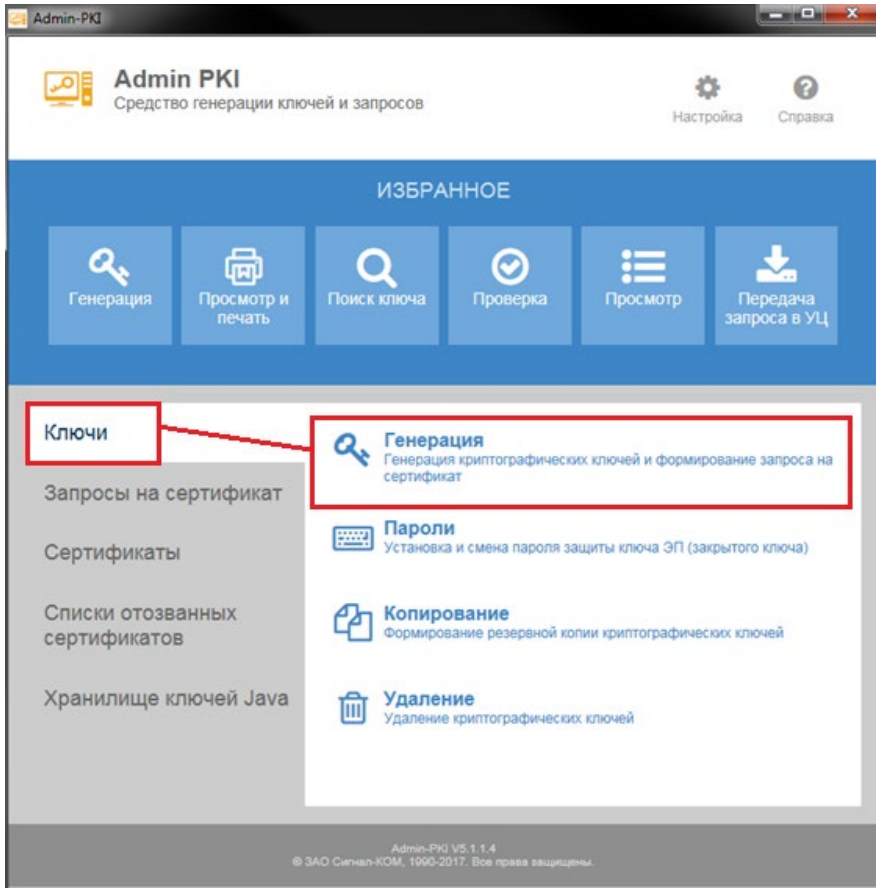
Создание запроса на сертификат электронной подписи.

Генерация запроса в программе Admin-PKI и последующая регистрация в Удостоверяющем Центре.

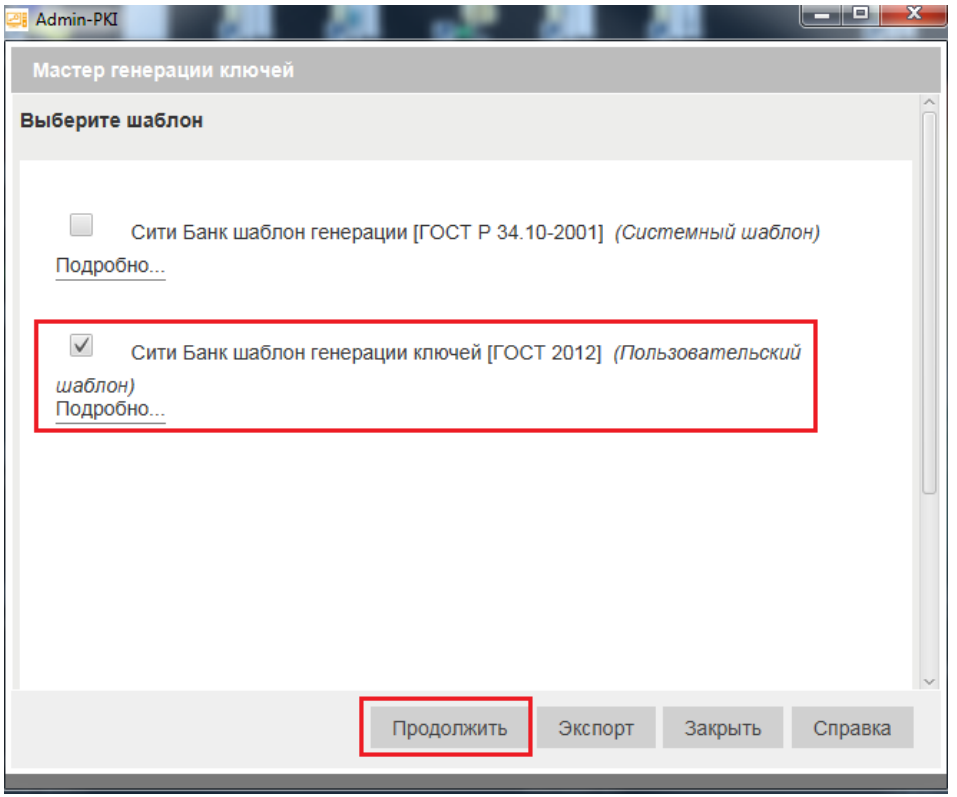
Создание сертификата электронной подписи

Генерация запроса на сертификат

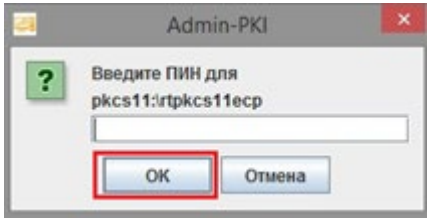
- Выберите пункт «Ключи» > «Генерация».



- Выберите пользовательский шаблон для генерации ключей [ГОСТ 2012] и нажмите «Продолжить»



- Введите PIN Пользователя для Рутокена, нажмите ОК и затем «Далее».



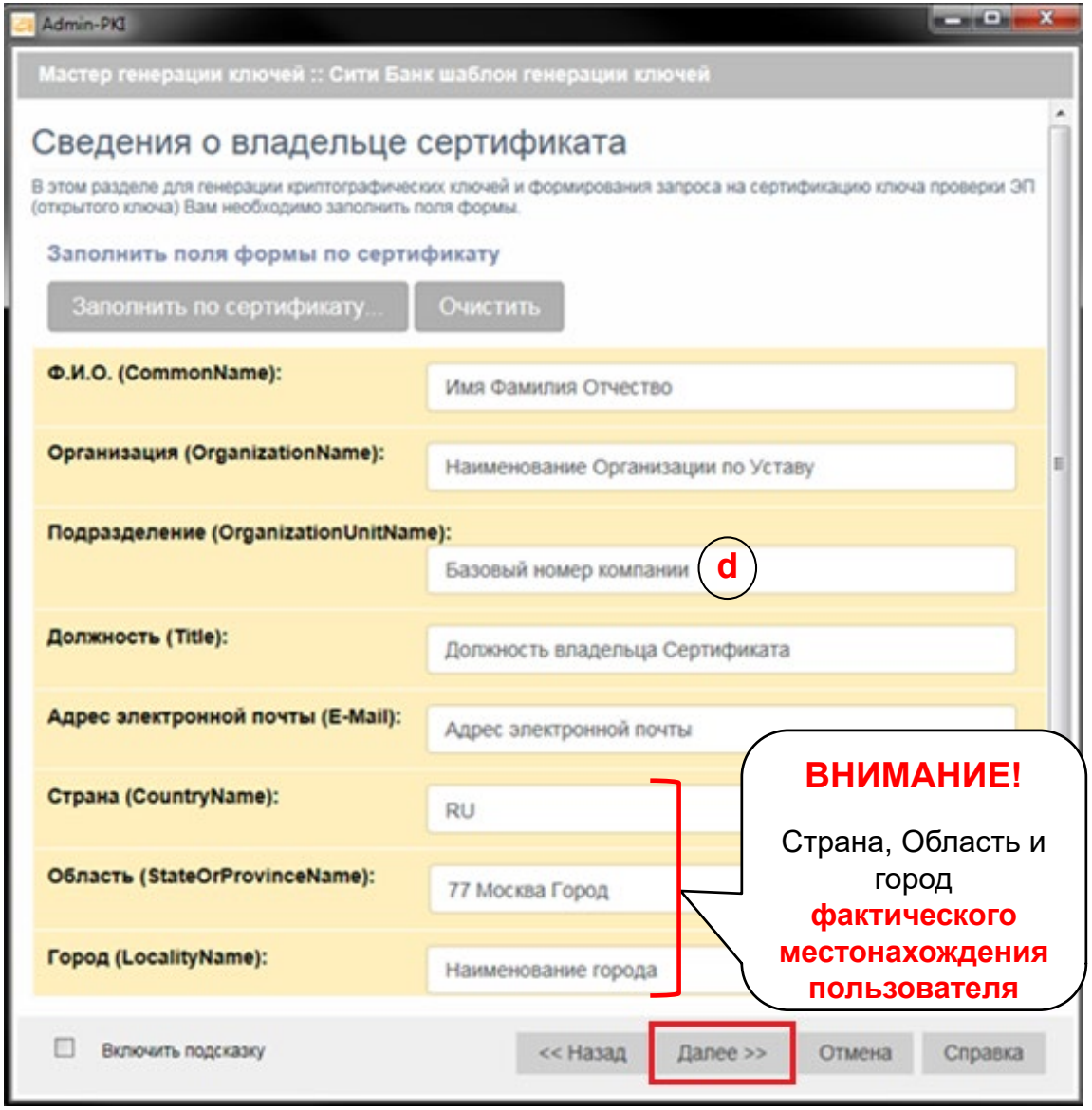
Создание сертификата электронной подписи

Параметры запроса сертификата

Внимание!
Все поля являются обязательными для заполнения.
Неправильно заполненное или оставленное пустым поле будет являться причиной для отказа в регистрации сертификата.

В целях информационной безопасности электронный сертификат пользователя вы сможете получить только на указанный E-mail адрес.

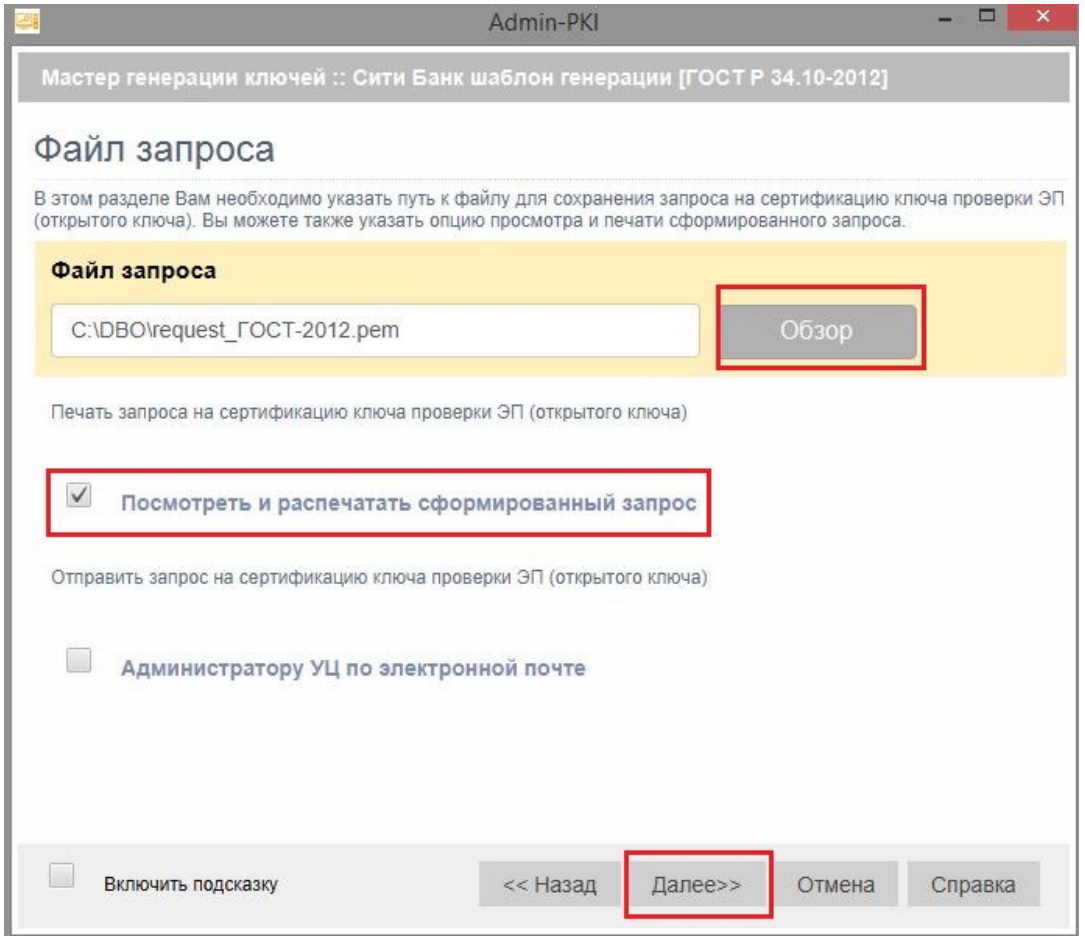
- Если Вы выпускаете сертификат для отправки **документов для факторинга, аккредитивов и гарантий**, то в поле Подразделение **укажите базовый номер компании + d** (например, **123456d**)
- Если Вы выпускаете сертификат для **продукта «Корпоративные карты»**, то в поле Подразделение **укажите базовый номер компании + d** (например, **123456d**), а в поле Должность укажите **Программный администратор**.



Создание сертификата электронной подписи

Параметры запроса сертификата

- Если требуется поменять расположение файла запроса, то нажмите кнопку «Обзор».
- Убедитесь, что галочка «Просмотреть и распечатать сформированный запрос» установлена
- Нажмите «Далее».



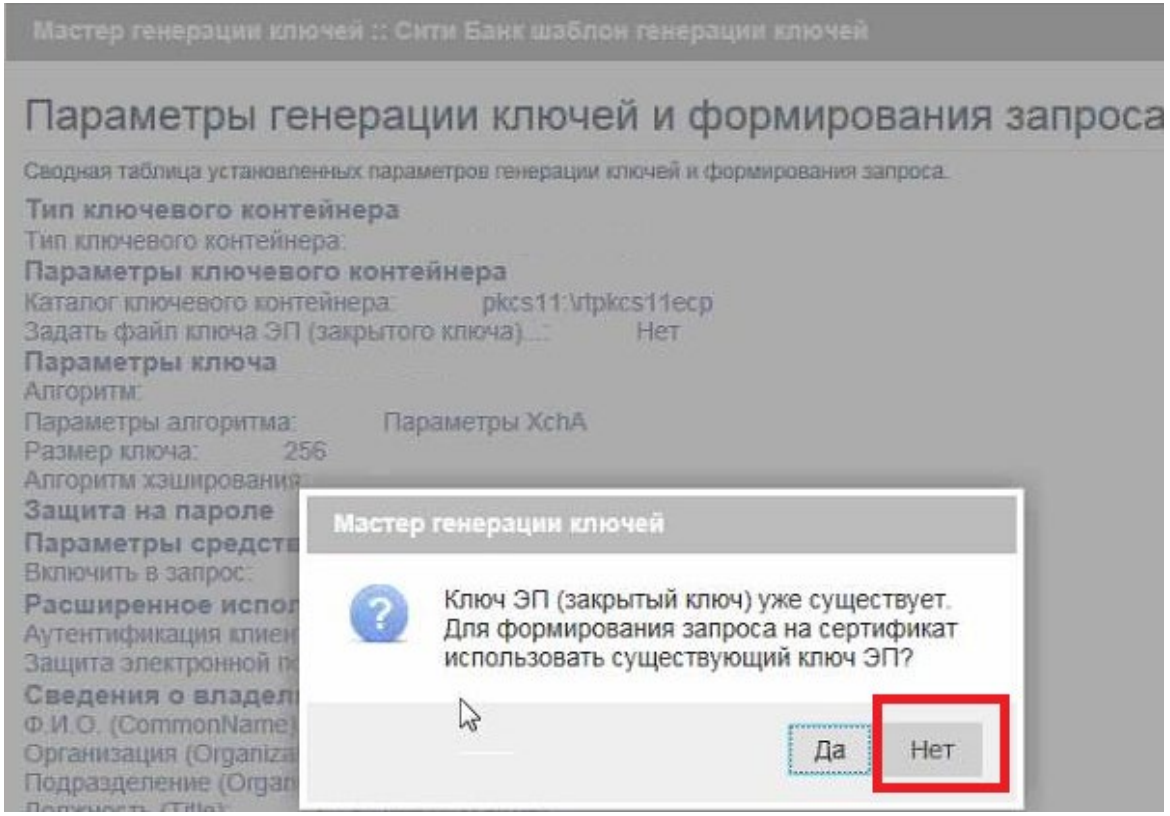
Создание сертификата электронной подписи

Параметры запроса сертификата

Обращаем Ваше внимание, что у **каждого сертификата должен быть свой закрытый ключ**. В случае появления окна, как на скриншоте ниже, на токене уже ранее генерировался ключ.

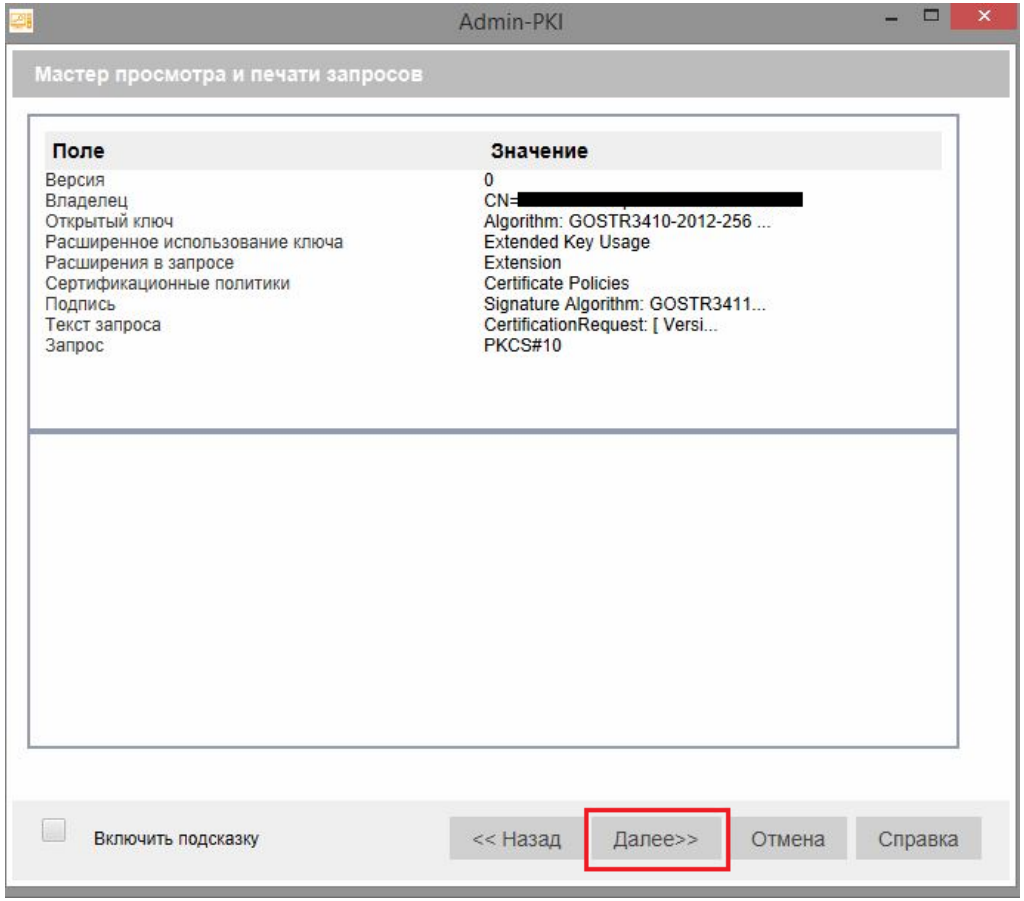
В этом случае нажмите «**НЕТ**», чтобы ключевая пара ***Запрос < > Закрытый ключ*** сформировалась корректно.

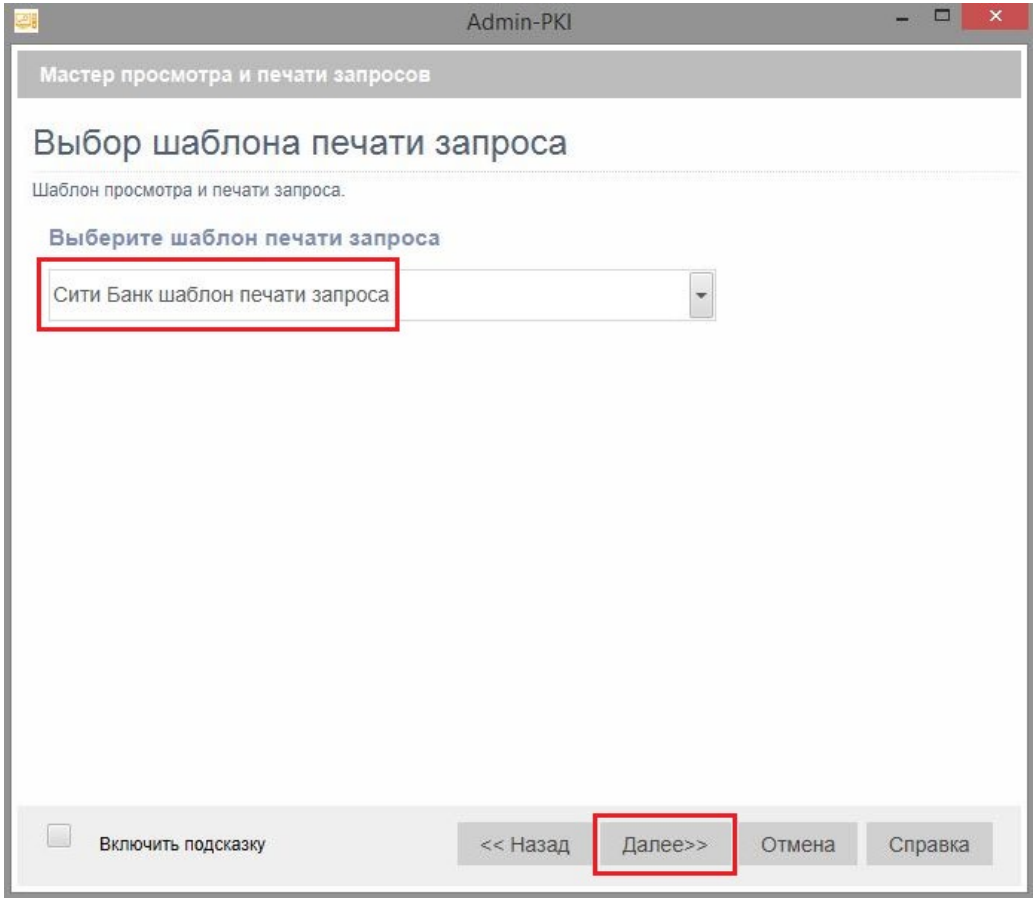
Если данное окно не появилось, то просто переходите к следующей странице инструкции.



Создание сертификата электронной подписи

Параметры запроса сертификата

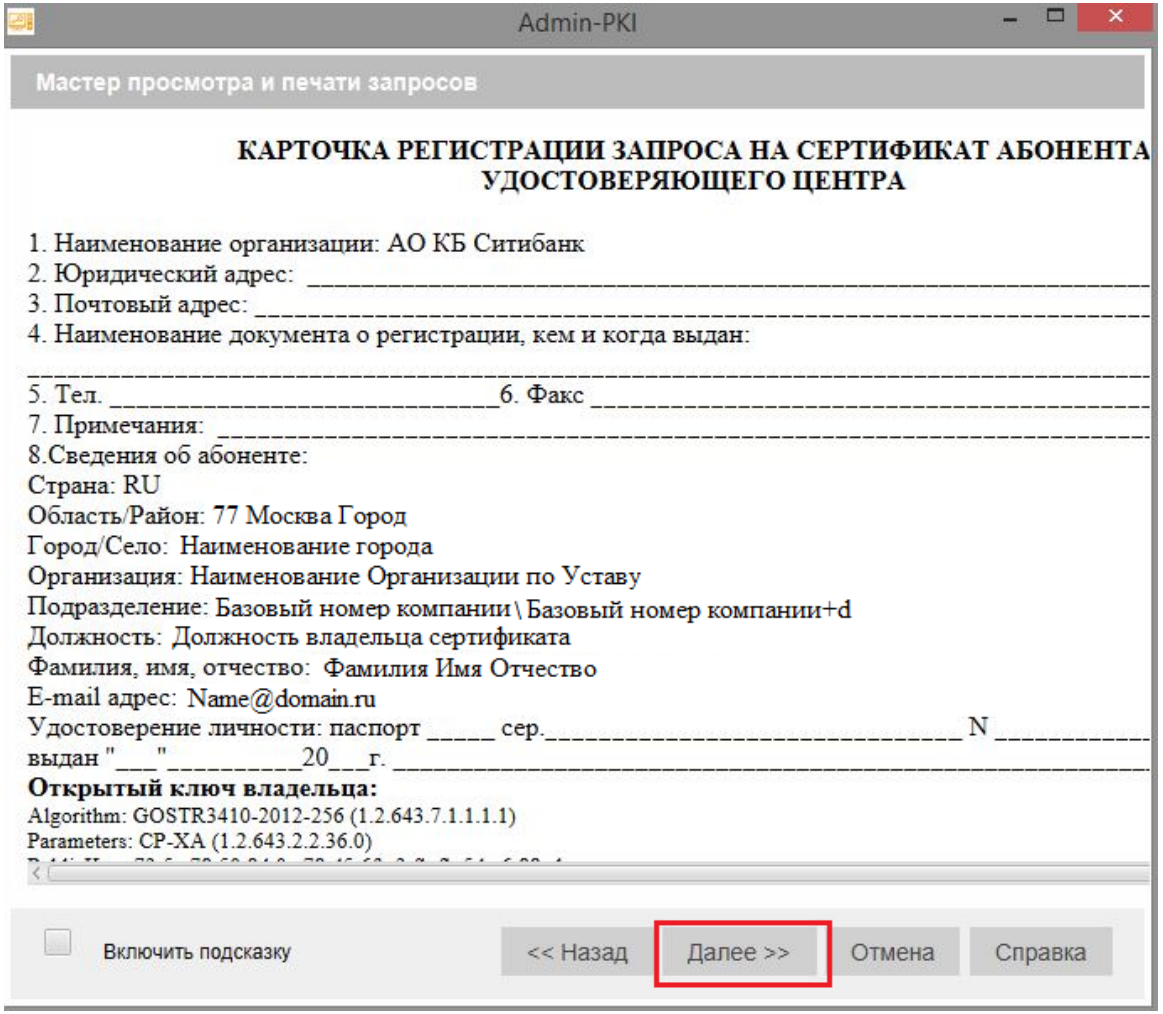




Создание сертификата электронной подписи

Параметры запроса сертификата

- В случае необходимости генерации нескольких ключей (сертификатов) – последовательность шагов следует повторить.
- В каждом случае в поле Файл запроса необходимо указать путь для сохранения файла, каждый раз указывая уникальное имя файла запроса на сертификат.
- Нажмите «Далее» для продолжения генерации.



Создание сертификата электронной подписи

Карточка регистрации запроса на сертификат абонента удостоверяющего центра

КАРТОЧКА РЕГИСТРАЦИИ ЗАПРОСА НА СЕРТИФИКАТ АБОНЕНТА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

1. Наименование организации: Наименование организации по Уставу
2. Юридический адрес: **юридический адрес по Уставу**
3. Почтовый адрес: **фактический адрес местонахождения**
4. Наименование документа о регистрации, кем и когда выдан:
номер ОГРН, кем и когда выдан
5. Тел. **контактный телефон** 6. Факс **факс (необязательно)**
7. Примечания: **дополнительная информация (необязательно)**
8. Сведения об абоненте:

Страна: RU
Область/Район: 77 Москва Город
Город/Село: Наименование города
Организация: Наименование организации по Уставу
Подразделение: Базовый номер компании \ Базовый номер компании+d
Должность: Должность владельца сертификата
Фамилия, имя, отчество: Фамилия Имя Отчество
E-mail адрес: Name@domain.ru
Удостоверение личности: паспорт _____ сер. **серия паспорта** N **номер паспорта**
выдан "**когда выдан** 20___г. **кем выдан**

Открытый ключ владельца:

Algorithm: GOST R 3410-2012-256 (1.2.643.7.1.1.1.1)
Parameters: CP-XA (1.2.643.2.2.36.0)
PublicKey: 73:5c:78:50:8d:0c:78:d5:6f:c3:fb:fb:5d:c6:88:ab:
5f:e1:c9:ce:fc:9d:0b:66:e3:0d:ac:b3:8e:03:85:71:
b6:d6:24:85:8e:b4:16:20:bd:9a:3c:03:68:3b:8a:bf:
73:36:3f:83:91:bd:c2:b7:b6:0a:48:6b:3a:a6:6f:23

Текст запроса на сертификат открытого ключа в формате PEM:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICLTCCAdgCAQAwggEZMRUwEwYDVQQHDAzQoNGP0LfQsNC90YwxLTArBgNVBAgM
JDYyINCg0Y/Qt9Cw0L3RgdC60LDRjyDQntCx0LvQsNGB0YLRjDELMAkGA1UEBhMC
UlUxJzAlBgkqhkiG9w0BCQEWGGlyaW5hLnZhbmVzaGluYUBjaXRpLmNvbTEhMB8G
A1UEDAwYRUJTINGB0L/QtdGG0LjQsNC70LjRgdGCMRAwDgYDVQQLDAdpdDM2NzI4
MSMwIQYDVQQKDBrQkNCeINCa0JEg0KHQuNGC0LjQsdCw0L3QujFEMD8GA1UEAww4
0JLQsNC90LXRiNC40L3QsCDQmNGA0LjQvdCwINCa0L7QvdGB0YLQsNC90YLQuNC9
0L7QstC90LAwZjAfBggqhQMHAQEBATATBgcqhQMCAiQABggqhQMHAQECAgNDAARA
clx4UIOMeNVvw/v7XcaIql/hyc78nQtm4w2ss44DhXG21iSFjrQWIL2aPANo04q/
czY/g5G9wre2Ckhr0q2vI6BOMEwGCSqGSIb3DQEJDjE/MD0wDAYDVR0TAQH/BAIw
ADAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwME
MAwGCCqFAwcBAQMCBQADQQB5wL400VEG7Z9Jj1NP9lwVzcmdDBJjxAMVGOMLGbIK
AZhlcE8X7dg/mlKiV0irx1NSfBd1FANWJHhF5e/03u0r
-----END CERTIFICATE REQUEST-----
```

Личная подпись владельца ключа:

подпись владельца ключа
_____/_____/
(подпись) / (расшифровка подписи)

Достоверность приведенных данных подтверждаю

Руководитель организации:

подпись руководителя
_____/_____/
(подпись) / (расшифровка подписи)

"**печать организации**20____г.
М.П.

Распечатайте карточку регистрации запроса на сертификат и заполните пустые поля (выделены красным).

Обратите внимание!

Поле «Удостоверение личности» обязательное для заполнения. Укажите паспортные данные в соответствии с документом, удостоверяющим личность.

Выпуск сертификата.

Порядок выдачи сертификата.

В связи с вступлением в силу требований ФЗ №476 от 27.12.2019 «Об электронной подписи» и статьи 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», начиная с 1 июля 2020 изменяется порядок приема/ выдачи заявлений на ЭП.

Чтобы получить подпись в Удостоверяющем центре Ситибанка, нужно **подтвердить Вашу личность** одним из двух способов:

1

Лично приехать в офис Ситибанка

«На Калужской»: в г. Москва, ул. Профсоюзная, 61А с паспортом и документом «Карточка регистрации запроса на сертификат абонента Удостоверяющего центра».

Подробнее об этом способе получения ЭЦП см. на **стр. 3**

2

Оформить на определенное лицо в компании специальную доверенность

на осуществление идентификации лица, получающего сертификат ЭЦП (владельца сертификата, далее – **Заявителя**).

Подробнее об этом способе получения ЭЦП см. на **стр. 4-5**

1. Выпуск сертификата с подтверждением личности в отделении банка.

Порядок выдачи сертификата.

1. • Заявитель направляет **Электронный файл запроса** (файл с расширением **.pem**) на адрес cert.ru@citi.com. **Внимание!** В теме письма обязательно укажите базовый номер компании и ФИО Заявителя.

2. • Заявитель направляет скан-копию распечатанной **Карточки регистрации запроса на сертификат** адрес RU.TFA@CITI.COM *. Карточка заверяется подписью:
   - **Заявителя** (поле «Личная подпись владельца ключа»)
   - **Уполномоченного представителя компании** (поле «Руководитель организации»)
   Внимание! Поле «Личность владельца сертификата установлена» требуется оставить пустым.

3. • При получении обеих версий запроса Банк проводит их обработку.

4. • По завершении необходимых действий Банк направляет уведомление Заявителю о необходимости лично посетить офис Банка по адресу: **Москва, Профсоюзная улица, дом 61А, м. Калужская** для прохождения процедуры идентификации и получения сертификата открытого ключа. При себе Заявителю необходимо иметь паспорт и оригинал Карточки регистрации запроса на сертификат абонента Удостоверяющего центра.

5. • По завершении указанных действий Банк направляет Заявителю сертификат подписи на электронный адрес, указанный в запросе на сертификат.

*В случае, если по каким-либо причинам отправка скан-копии заполненной Карточки регистрации запроса на сертификат абонента Удостоверяющего центра на адрес RU.TFA@CITI.COM является невозможной, то форма может быть направлена в Банк курьером либо передана заявителем лично.

2. Выпуск сертификата без личного присутствия

Порядок выдачи сертификата.

1

- Определите в Вашей Компании лицо (далее - **Представитель**), которое будет осуществлять личную идентификацию лиц, запрашивающих электронную подпись и получающих сертификаты электронной подписи

2

- Заполните и отправьте по электронной почте нижеуказанные документы на адрес RU.TFA@CITI.COM:
  - запрос на выдачу доверенности для представителя (заверяется любым лицом из КОП компании);
  - шаблон доверенности (заполняется в Word, не заверяется);
  - копия паспорта.

3

- При получении указанных документов Банк проводит их обработку, выдает доверенность и уведомляет владельца доверенности по e-mail, указанному в запросе на выдачу доверенности.

4

- После получения доверенности Заявитель направляет **Электронный файл запроса** (файл с расширением **.pem**) на адрес cert.ru@citi.com.
  Внимание! В теме письма обязательно укажите базовый номер компании и ФИО Заявителя.

5

- Заявитель направляет скан-копию распечатанной Карточки регистрации запроса на сертификат адрес RU.TFA@CITI.COM. Карточка заверяется подписью:
  - **Заявителя** (поле «Личная подпись владельца ключа»)
  - **Уполномоченного представителя компании** (поле «Руководитель организации»);
  - **Представителя** (поле «Личность владельца сертификата установлена».

6

- Подписанный документ передаётся в оригинале в офис Банка: г. Москва, Профсоюзная улица, дом 61А или г. Санкт-Петербург, ул. Итальянская, д.5.
  Внимание! Оригинал документа должен быть передан в Банк в течение **30 календарных дней**. В противном случае выпущенный сертификат будет заблокирован.

2. Выпуск сертификата без личного присутствия

Порядок выдачи сертификата.

7

- По факту получения сканированной копии «Карточки регистрации запроса на сертификат абонента УЦ» Банк направляет копию(бланк) сертификата ЭП Представителю, ответственному за личную идентификацию Заявителя, по e-mail, указанному в заявлении на выдачу доверенности.

8

- Представитель распечатывает копию Сертификата ЭП, производит личную идентификацию Заявителя и ставит подпись в поле «Личность владельца сертификата установлена», а также указывает дату.
  Внимание! Дата на документе должна совпадать с датой начала действия сертификата, указанной в поле «Действителен с » (3-я строка документа).

9

- Заявитель ставит подпись в поле «Сертификат получен лично».

10

- Сканированная копия заполненного «Сертификата» пересылается на адрес RU.TFA@CITI.COM

11

- По факту получения сканированной и заполненной копии «Сертификата» Банк направляет Заявителю сертификат подписи на электронный адрес, указанный в запросе на сертификат

12

- Подписанный документ передаётся в оригинале в офис Банка: г. Москва, Профсоюзная улица, дом 61А или г. Санкт-Петербург, ул. Итальянская, д.5.
  Внимание! Оригинал документа должен быть передан в Банк в течении **30 календарных дней**. В противном случае выпущенный сертификат будет заблокирован.

*По вопросам касательно предоставления копии паспорта и заполнения\заверения запроса на выдачу доверенности для представителя и шаблона доверенности Вы можете обратиться **к куратору компании в Ситисервисе.**

Получение и импорт сертификатов.

Информация о сертификатах и импорт на USB-токен.

Получение и импорт сертификатов

Информация о сертификатах

На указанный в карточке регистрации запроса на сертификат абонента УЦ e-mail вы получите .zip архив с сертификатами:

- Личный сертификат пользователя
- Сертификат удостоверяющего центра Ситибанка (Citibank_SubCA_G2012.cer)
- Сертификат удостоверяющего центра E-Notary (e-notary_CA_G2012.cer)
- Сертификат шифрования (Citibank_Encryption_G2012.cer)

Распакуйте данный архив и сохраните сертификаты на жесткий диск компьютера.

Внимание! Срок действия сертификатов с момента выпуска – **3 года**. Об истечении времени действия сертификата и необходимости его перевыпуска, Вы будете предупреждены заблаговременно по электронной почте.

Скачайте утилиту для работы с сертификатами: https://www.e-notary.ru/files/download/rutoken/rutoken_utility.zip

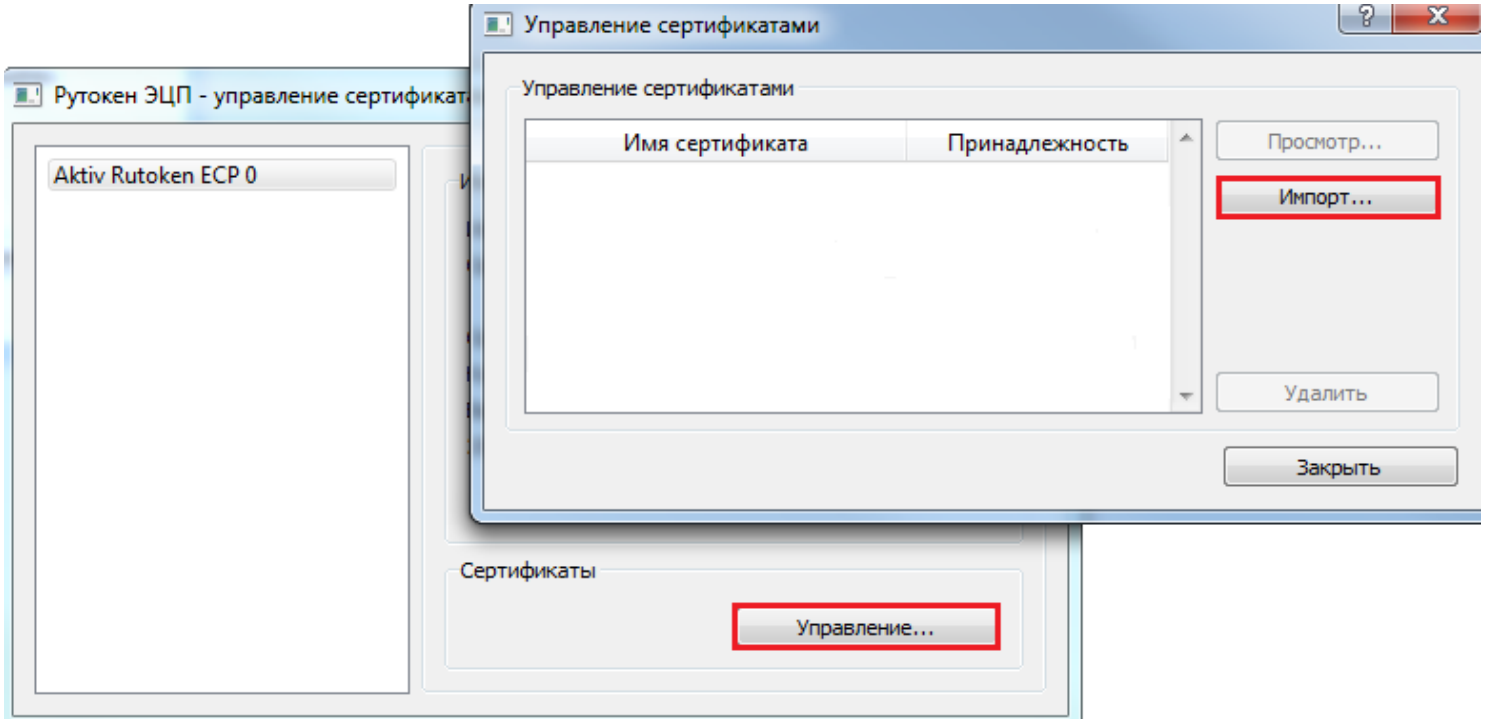
Получение и импорт сертификатов

Рутокен ЭЦП – управление сертификатами

Убедитесь, что файлы сертификатов, сохраненные на компьютере, имеют расширение .cer.=

Запустите файл rutoken_utility.exe Нажмите кнопку **Управление**.

В окне «Управление сертификатами» нажмите **Импорт** и в появившемся окне укажите папку с сертификатами.

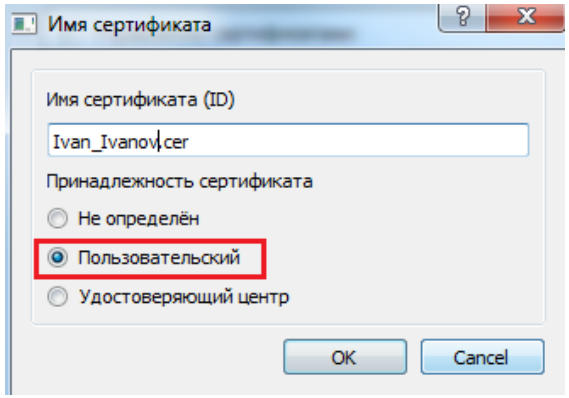


Получение и импорт сертификатов

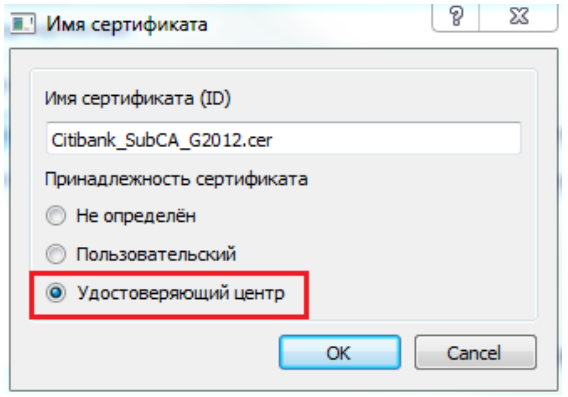
Импорт сертификатов на USB-токен

Импортируйте сертификаты в следующем порядке:

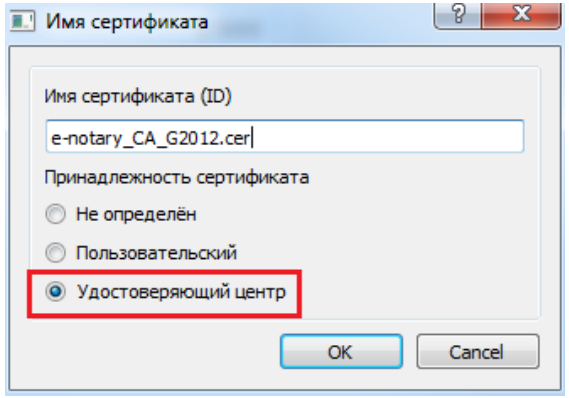
1.



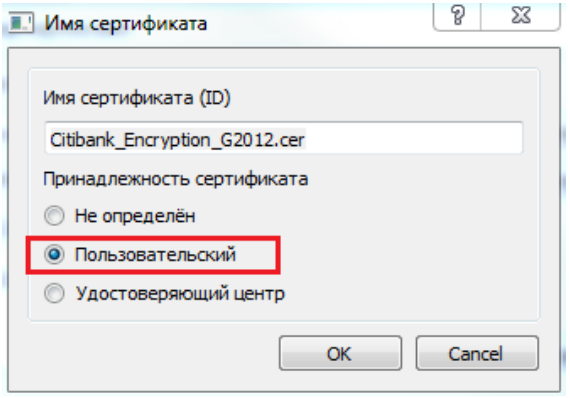
2.



3.



4.



Установка и использование программы «File-PRO»

Установка и настройка File-PRO – программного обеспечения для подписания файлов на ПК.

Установка программы «File-PRO»

Установка и настройка File-PRO – программного обеспечения для подписания файлов на ПК

Установка программного комплекса **“File-PRO”** выполняется с помощью программы установки **File-PRO.EXE**, которая включает в себя все необходимые для установки файлы.

Для установки запустите файл **File-PRO.EXE** на выполнение и следуйте инструкциям мастера установки.

Внимание: В меню «Выберите необходимые компоненты» чек-бокс «File-PRO Mail Client» следует оставить пустым.

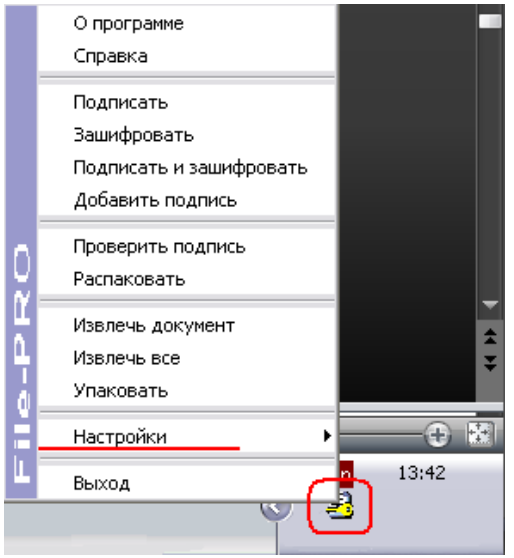
Для установки программы требуется лицензия. Лицензионный код выдается каждой компании при получении токена, он указан в документации.

Установка программы «File-PRO»

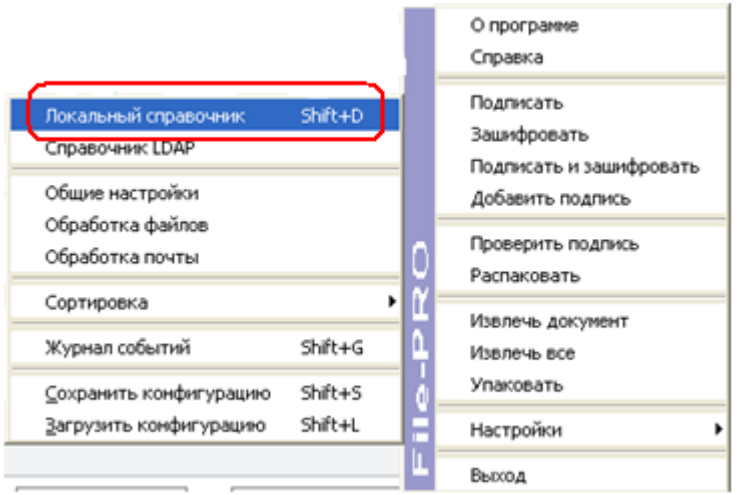
Установка и настройка File-PRO – программного обеспечения для подписания файлов на ПК

Настройка File-PRO

Для настройки программного комплекса необходимо щелкнуть мышью на иконке “File-PRO”, расположенной в области “Tray” системной панели задач, в результате чего на экране дисплея появится меню, включающее следующие пункты:



Затем выберите пункт меню «**Настройки ->Локальный справочник»**.

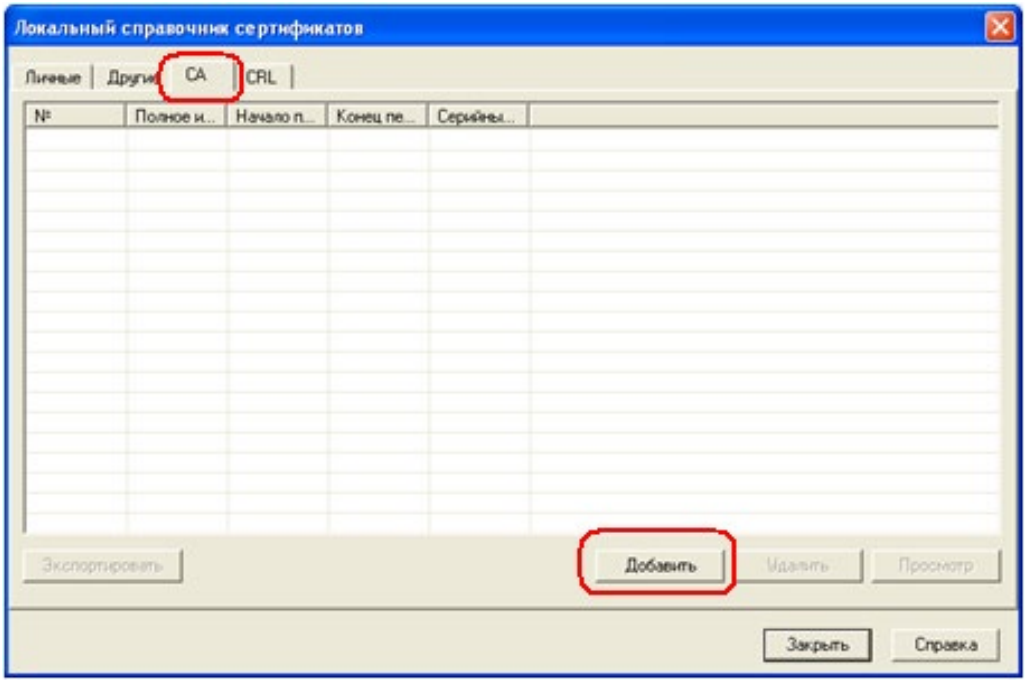


Установка программы «File-PRO»

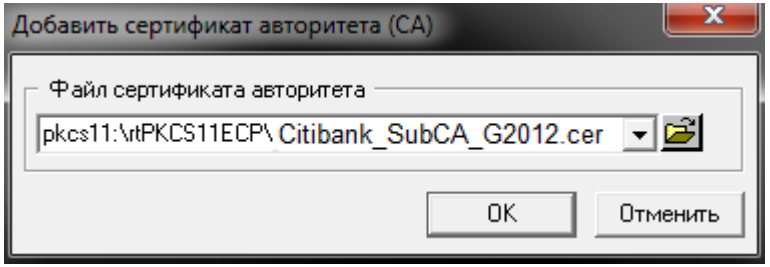
Установка и настройка File-PRO – программного обеспечения для подписания файлов на ПК

Пожалуйста, убедитесь что токен подключен к компьютеру.

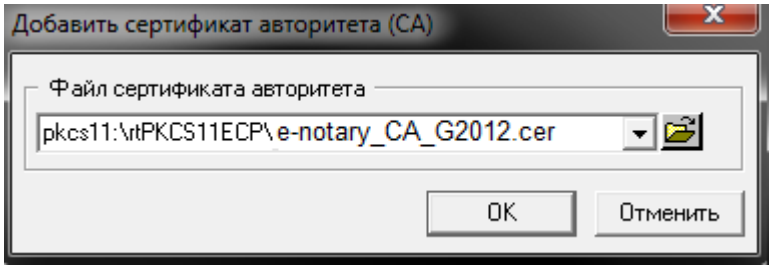
Зайдите на вкладку «CA» и начните импорт сертификатов.
Укажите файлы сертификатов в формате:



pkcs11:\rtPKCS11ECP\Citibank_SubCA_G2012.cer



pkcs11:\rtPKCS11ECP\e-notary_CA_G2012.cer

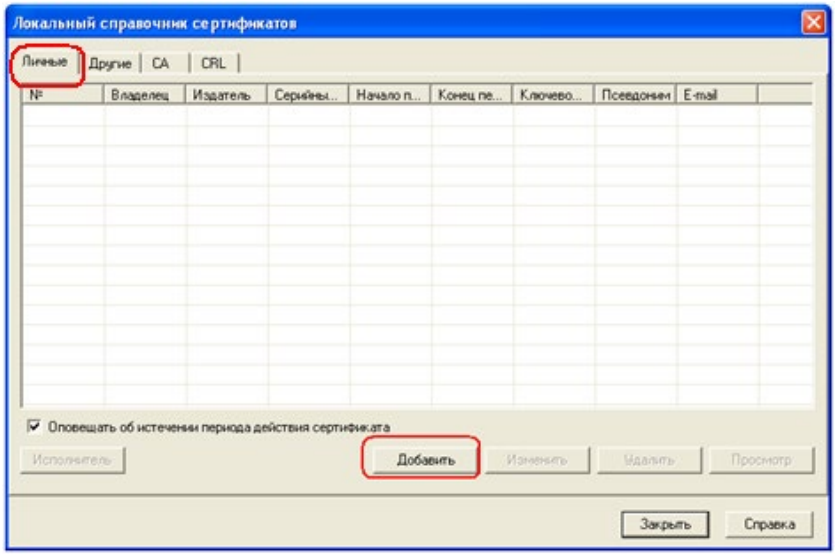


Нажмите «ОК», чтобы завершить установку.

Установка программы «File-PRO»

Установка и настройка File-PRO – программного обеспечения для подписания файлов на ПК

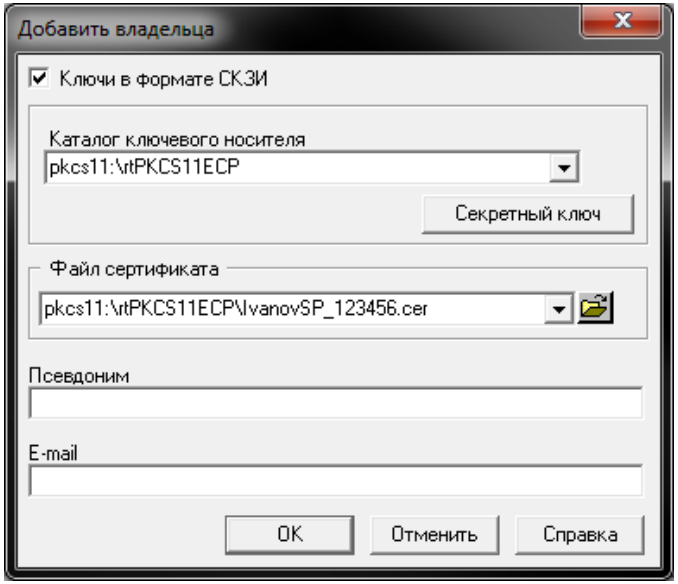
Аналогично устанавливается **личный сертификат**, для этого необходимо перейти на вкладку «**Личные**» и нажмите кнопку «Добавить».



В качестве каталога носителя выберете **pkcs11:\rtPKCS11ECP**

Укажите файл сертификата в формате **pkcs11:\rtPKCS11ECP\IvanovSP_123456.cer**

где IvanovSP_123456.cer – название файла сертификата



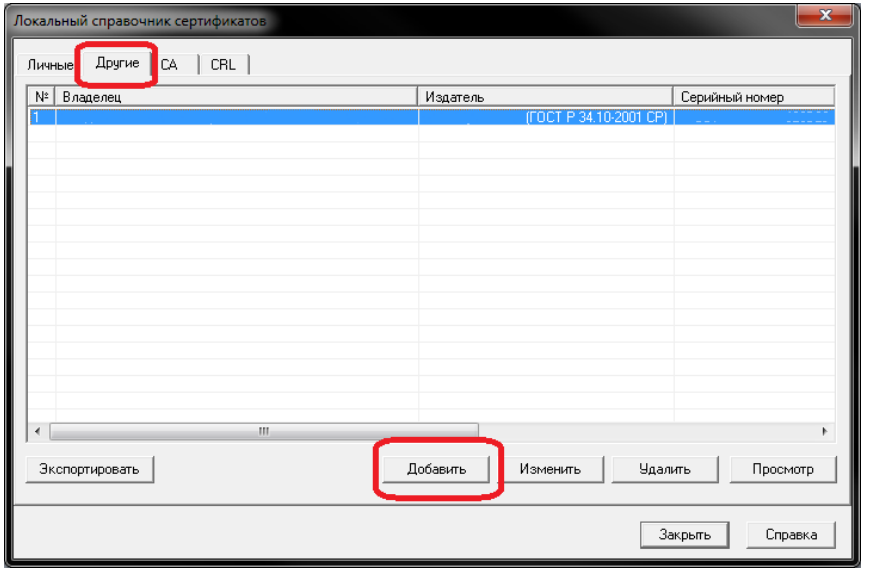
При правильном указании хранилища и наименования сертификата псевдоним и е-мейл отобразятся автоматически

Нажмите «ОК», чтобы завершить установку.

Установка программы «File-PRO»

Установка и настройка File-PRO – программного обеспечения для подписания файлов на ПК

Аналогично устанавливается **сертификат Шифрования**, для этого необходимо перейти на вкладку «**Другие**» и нажмите кнопку «Добавить».

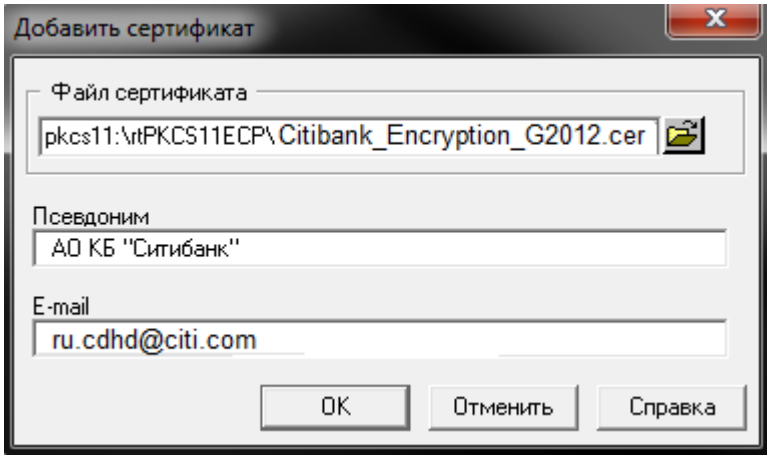


Зайдите на вкладку **«Другие»** и начните импорт сертификата.

Укажите файл сертификата в формате

pkcs11:\rtPKCS11ECP\Citibank_Encryption_G2012.cer

При правильном указании хранилища и наименования сертификата псевдоним и е-мейл отобразятся автоматически.

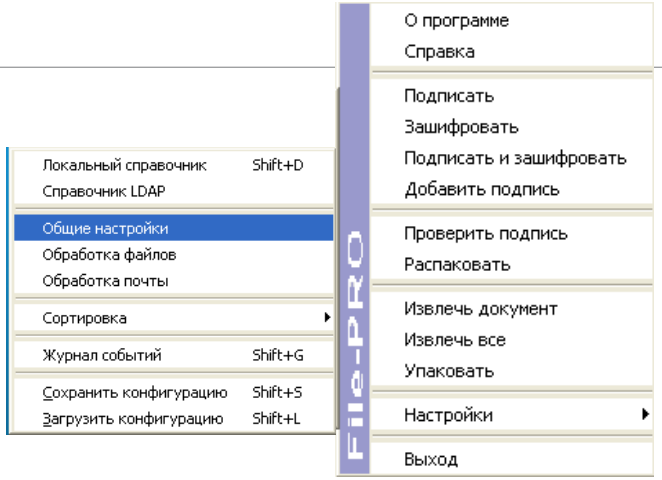


Нажмите «ОК», чтобы завершить установку.

Установка программы «File-PRO»

Настройки подписи

Настройки формата подписи происходят в меню
File Pro – Настройки – Общие настройки

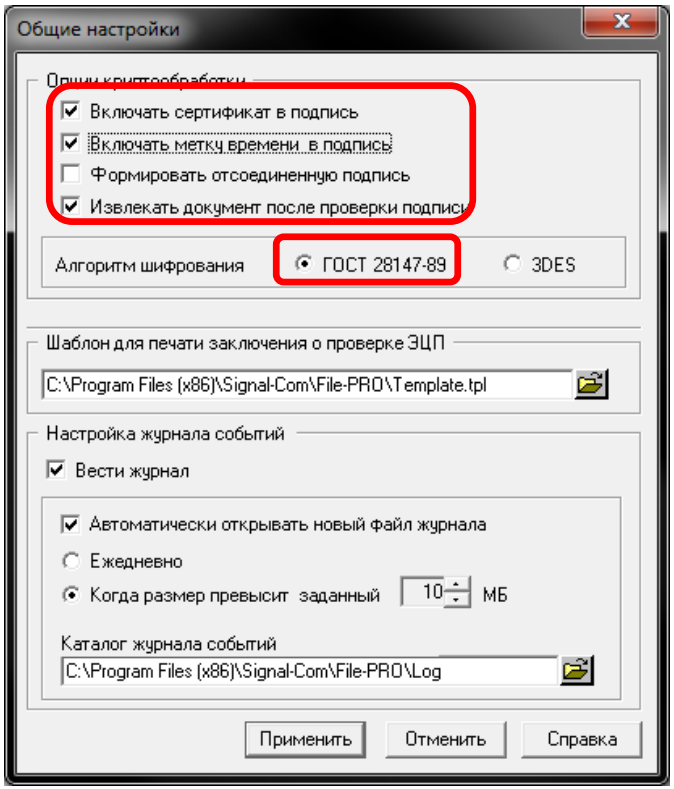


Подпись должна быть настроена следующим образом:

Опции Криптообработки

- Включать сертификат в подпись - Отмечено

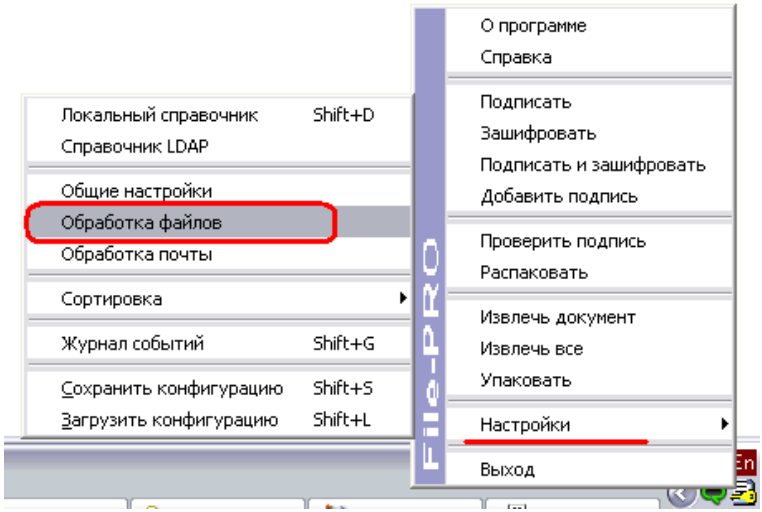
Алгоритм Шифрования - **ГОСТ 28147-89**



Установка программы «File-PRO»

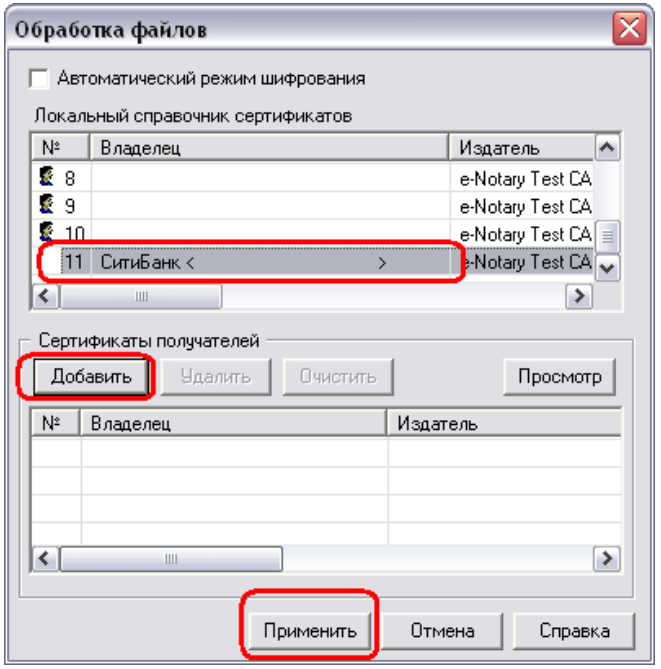
Настройки шифрования

Для автоматического выбора получателя при шифровании файла – сертификат получателя (для кого шифруется файл) следует указать в настройках обработки файлов.



Настройка Получателя по умолчанию происходят в меню **File Pro – Настройки – Обработка файлов**

Выберите сертификат получателя, нажмите кнопку «**Добавить**», затем «**Применить**».



Работа с системой «File-PRO»

Добавление подписи, шифрование файлов.

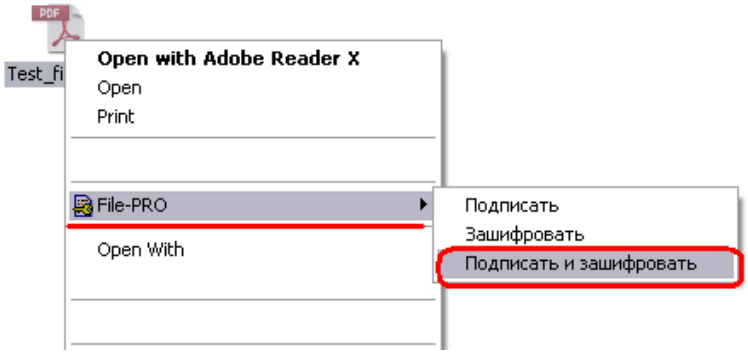
Работа с системой «File-PRO»

Добавление подписи, шифрование файлов.

При передаче документов на обработку в банк – файлы, содержащие документы, должны быть подписаны ЭЦП уполномоченного лица и зашифрованы.

В настоящий момент в названии файла допустимы ТОЛЬКО латинские буквы и цифры.

Для добавления Электронно-Цифровой подписи и шифрования файла необходимо выполнить следующие действия:



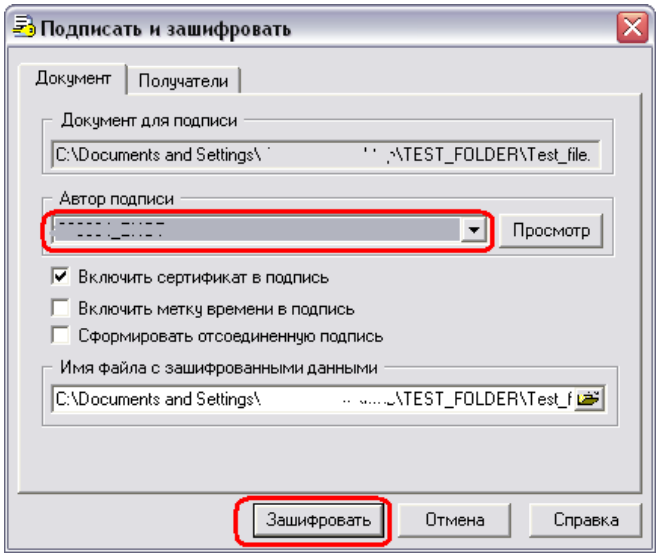
1. Щелкните **Правой клавишей** мыши на файле.

2. В открывшемся меню выберите **«File-PRO» -> «Подписать и зашифровать»**

3. В поле «Автор подписи» указывается название сертификата подписи которая будет использована. В случае когда в систему внесено несколько подписей – можно выбрать нужную подпись в этом поле.

   Убедитесь, что отмечен параметр «Включать сертификат в подпись»

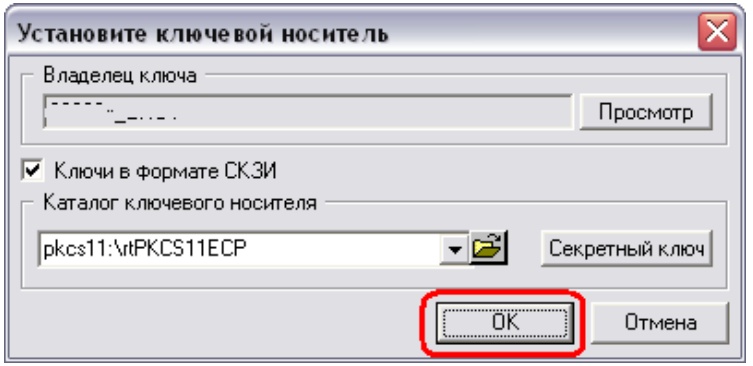
   Нажмите кнопку «**Зашифровать**».



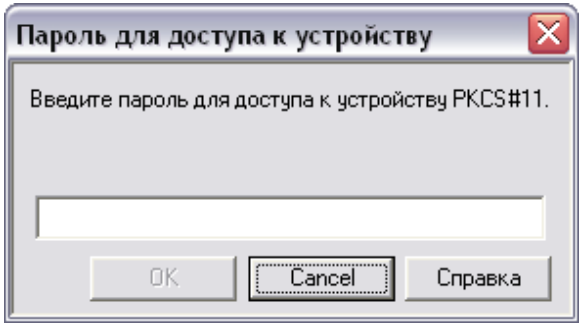
Работа с системой «File-PRO»

Добавление подписи, шифрование файлов.

1. Нажмите кнопку «**OK**».



2. Введите пароль к токену.



3. После установки подписи и шифрования откроется окно с результатом процедуры и указанием путей исходного и конечного файлов.

   Нажмите кнопку «**OK**».

Работа с системой «File-PRO»

Добавление подписи, шифрование файлов.

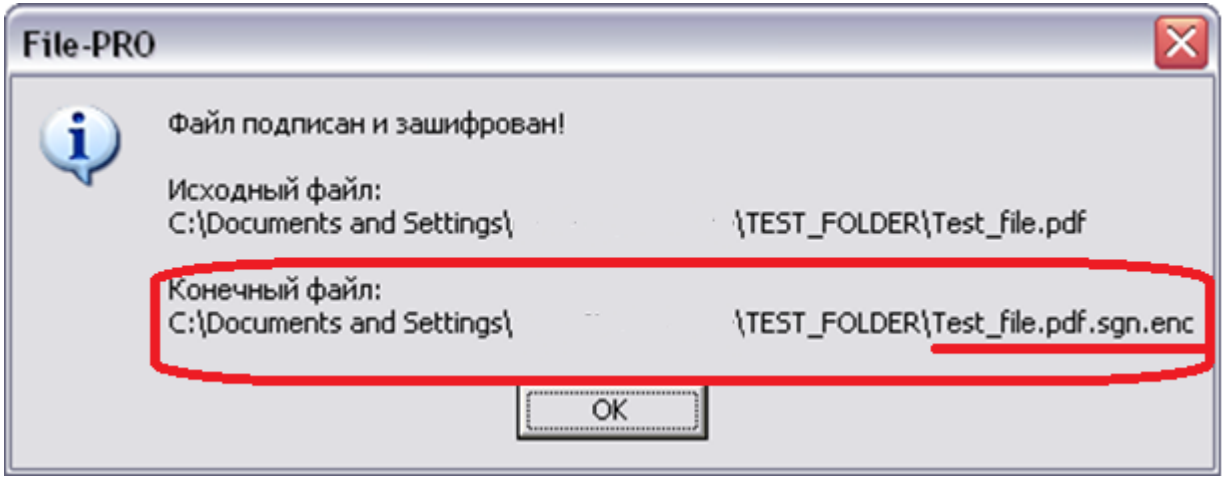
Пожалуйста обратите внимание:

- Результатом подписи и шифрования файла является создание дополнительного файла с расширением **.sgn.enc**

- Исходный файл остается неизменным.

- Архивировать и передавать в Банк следует отправлять именно *конечный* (результирующий) файл с расширением **.sgn.enc**

- Путь к подписанному и зашифрованному файлу указывается в сообщении о успехе операции (по умолчанию файл создается в той же папке, что и исходный файл):



Работа с системой «File-PRO»

Подписание документов несколькими подписями.

В случае если документ должен быть подписан несколькими ЭЦП – пользователи могут подписывать документ в любом порядке на свое усмотрение. Пользователь подписывающий файл последним должен его зашифровать, упаковать и передать файл в банк.

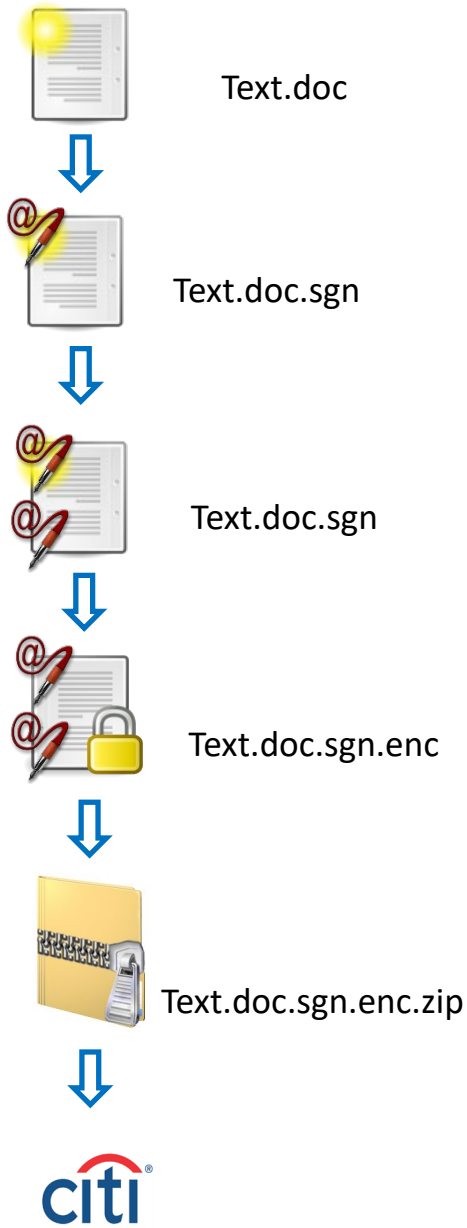
Пожалуйста обратите внимание - функции шифрования, упаковки и отправки файла в банк могут быть переданы другим пользователям(исполнителям). Электронная подпись или иные документы для таких пользователей не требуются.

Для того чтобы подписать документ – пожалуйста используйте функцию “Подписать”.
Все действия аналогичны указанным выше.

Для того чтобы зашифровать документ – пожалуйста используйте функцию “Зашифровать”.
Все действия аналогичны указанным выше.

Для подписи уже подписанного ранее документа – следует подписывать файл с расширением .sgn.

Для того чтобы проверить какие подписи уже поставлены на документ – дважды щелкните на документе – диалог проверки подписи откроется автоматически.



Работа с системой «File-PRO»

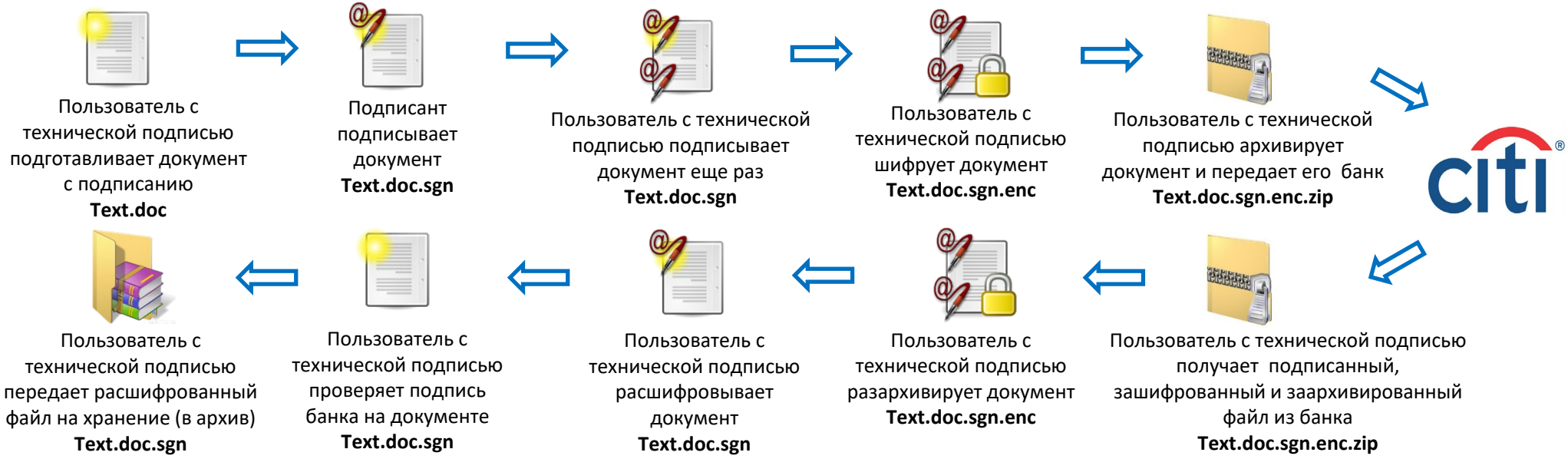
Роль технический подписи в подписании документов.

В некоторых случаях в процесс подписания документа добавляется еще один пользователь с так называемой «**технической подписью**». Этот пользователь может не иметь прав подписи, однако участвует в процессе подписания и шифрования документа наравне с остальными подписантами. Таким образом, пользователь, участвовавший в подписи документа, сможет в конечном итоге расшифровать поступивший из банка файл.

Права технической подписи в банке не проверяются, она не может выступать заменителем основной подписи. Технических подписей на документе может быть несколько, в зависимости от того, сколько пользователей должны иметь доступ в документу, поступающему из банка.

Техническая подпись обычно вводится для того, чтобы сократить и облегчить документооборот для подписантов компании. Основные функции по подготовке, шифрованию, передаче и получении файлов переходят на оператора (техническая подпись), от подписанта же потребуется только подпись.

Процесс подписи и шифрования может быть следующим:



Передача файлов в Банк

Передача подписанных и зашифрованных файлов через E-Mail и Delphi.

Передача файлов в Банк

Архивирование(сжатие) подписанных и зашифрованных файлов.

Перед отправкой подписанных и зашифрованных файлов в Банк – файлы следует заархивировать (сжать) в формат ZIP.

Рекомендуемая программа – SECURE ZIP.

В настоящий момент в названии файла допустимы ТОЛЬКО латинские буквы и цифры.

Пожалуйста, обратите внимание, что документы будут приняты в обработку текущим днем, только если они были отправлены до 15-00 Московского времени.

Для сжатия файлов вы можете воспользоваться любыми удобными вам приложениями поддерживающими формат ZIP.

Таким образом при передаче документов по электронным каналам файл с данными должен быть последовательно:
1. Подписан,
2. Зашифрован
3. Заархивирован (ZIP).

Ограничения, применяемые в настоящий момент:

1. В настоящий момент система поддерживает только **один** файл с данными в одном zip-архиве. (В дальнейшем система будет дорабатываться и будет поддерживать несколько файлов в одном zip-архиве.)
2. Максимально допустимый размер файлов ZIP не может превышать 5Mb.
3. Максимально допустимый размер файлов содержащихся внутри ZIP-архива не может превышать 5Mb.

Передача файлов в Банк

Передача подписанных и зашифрованных файлов по e-mail.

Для передачи подписанных, зашифрованных и заархивированных файлов по e-mail прикрепите файл как вложение к e-mail сообщению и отправьте его на адрес

eforms.ru@citi.com

В теле письма вы также можете указать сведения которые могли бы быть полезными при обработки ваших форм, однако информация переданная таким образом не может рассматриваться как юридически значимая и не наследует признаков ЭЦП и шифрования файла прикреплённого к сообщению.

Документы подписанные Банком. Расшифровывание, проверка подписи. Хранение документов.

Документы подписанные Банком. Расшифровывание, проверка подписи. Хранение документов.

Обратите внимание, что Вы не сможете расшифровать вложение, в случае если Ваш токен будет утерян, поврежден или форматирован. Пожалуйста, расшифруйте и сохраните документ после получения.

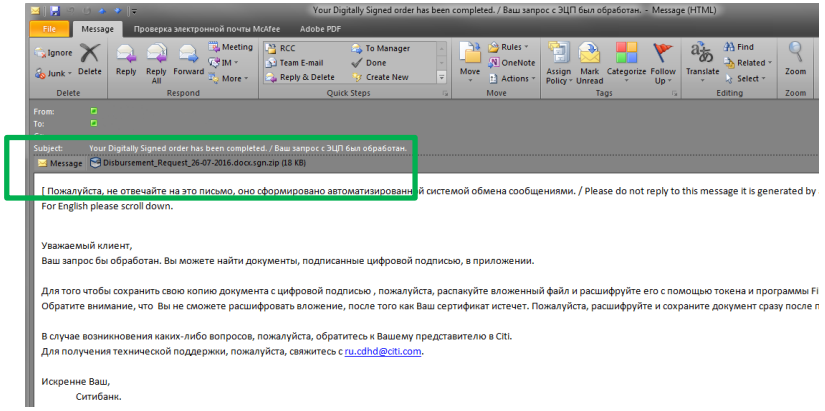
Если файл с цифровой подписью, который вы отправили первоначально, должен быть подписан как вами, так и Citi, то вы получите автоматически сгенерированное электронное письмо с приложенным документом, подписанным банком. Расшифровать документ может любой подписант из тех, кто изначально подписывал документ.

Полученный вами файл последовательно:

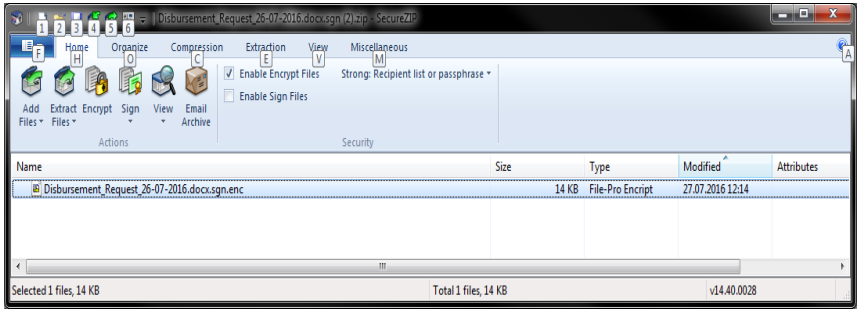
1. Подписан Клиентом (Ваш исходный документ)
2. Подписан Citi
3. Зашифрован на Ваш ключ (токен).
4. Упакован в ZIP

Для проверки валидности электронной подписи и хранения файла в расшифрованном виде – пожалуйста откройте вложение, разархивируйте с помощью Secure ZIP и затем расшифруйте файл, используя программу File-PRO и Ваш токен.

Откройте\Сохраните вложение



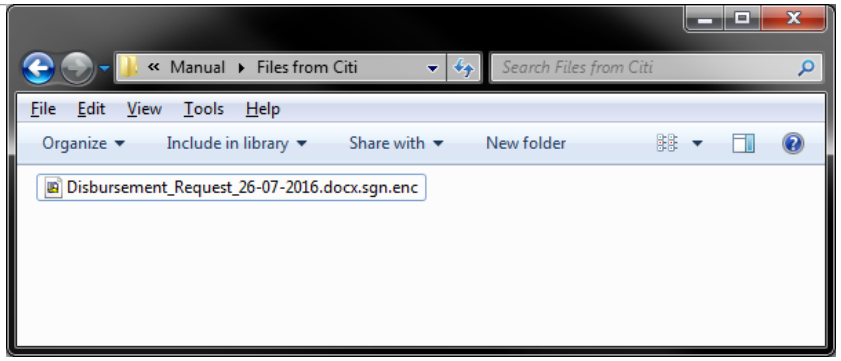
Извлеките файл в удобную вам папку на жёстком диске.



Документы подписанные Банком. Расшифровывание, проверка подписи. Хранение документов.

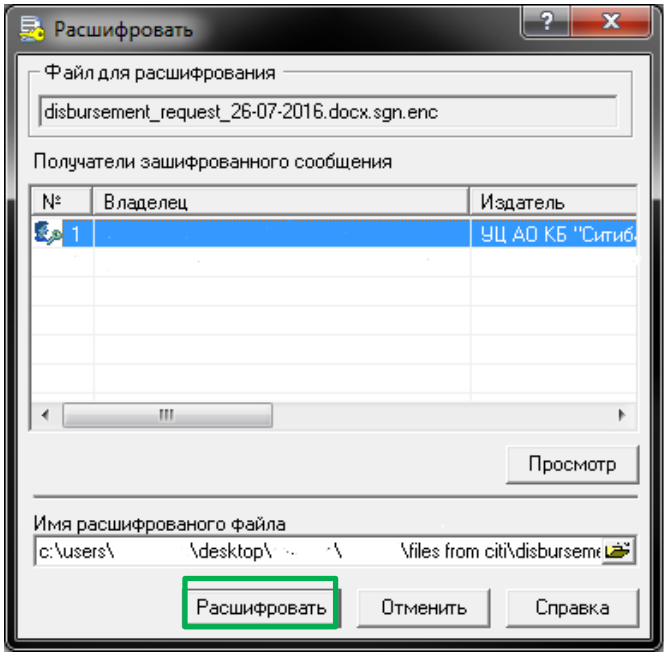
Чтобы расшифровать файл:

1. Откройте файл двойным щелчком мыши. (file_name.yyy.**sgn.enc**)

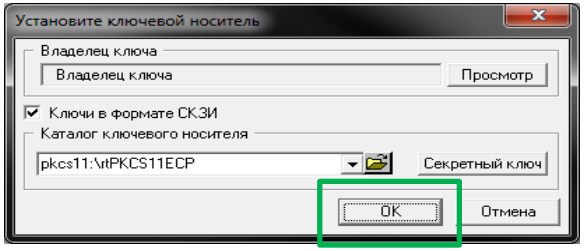


2. В открывшемся окне выберите подходящий сертификат (это не требуется если вы используете только один сертификат.)

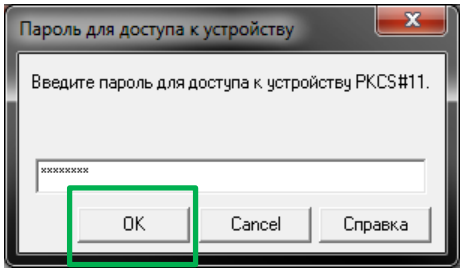
3. Нажмите “Расшифровать”.



4. Вставьте токен в USB-порт и нажмите OK

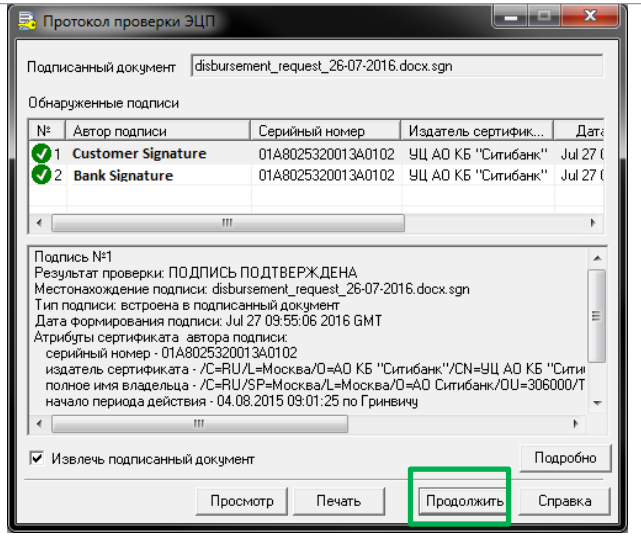


5. Введите пароль к токену и нажмите OK.



Документы подписанные Банком. Расшифровывание, проверка подписи. Хранение документов.

6. Открывшееся окно продемонстрирует подписи вложенные в файл их корректность.

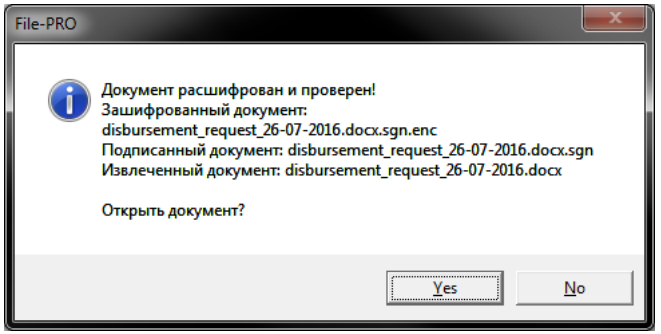


Зеленая отметка и фраза “ПОДПИСЬ ПОДТВЕРЖДЕНА” в окне с подробностями ниже указываете на то ,что:

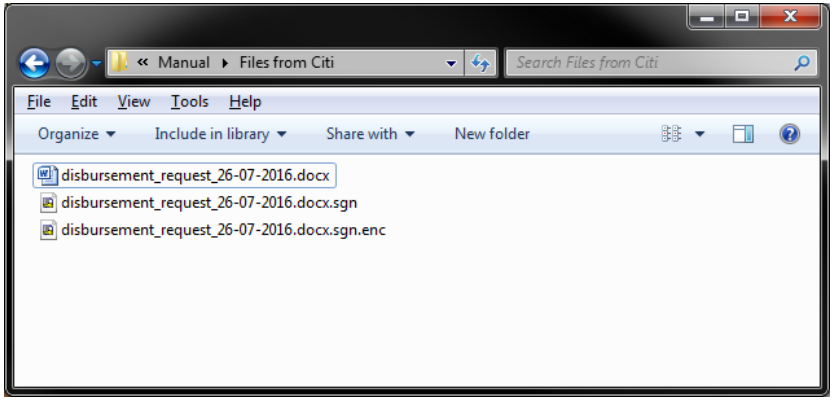
- Подпись верна
- Файл не был изменен с момента его подписания.

Нажмите “Продолжить” чтобы извлечь файлы.

7. Нажмите “Yes” если вы хотите открыть *исходный* файл (расшифрованный и со снятыми подписями). Нажмите “No” чтобы закрыть это окно.



8. Исходный файл, расшифрованный и подписанный файл будут распакованы в ту-же папку что и файл полученный из Citi.



file_name.yyy – исходный файл
file_name.yyy.**sgn** – подписанный и расшифрованный файл
file_name.yyy.**sgn.enc** - подписанный и зашифрованный файл

Возможности учетной записи Администратора Рутокен ЭЦП.

Форматирование USB-токена.

Возможности учетной записи Администратора Рутокен ЭЦП

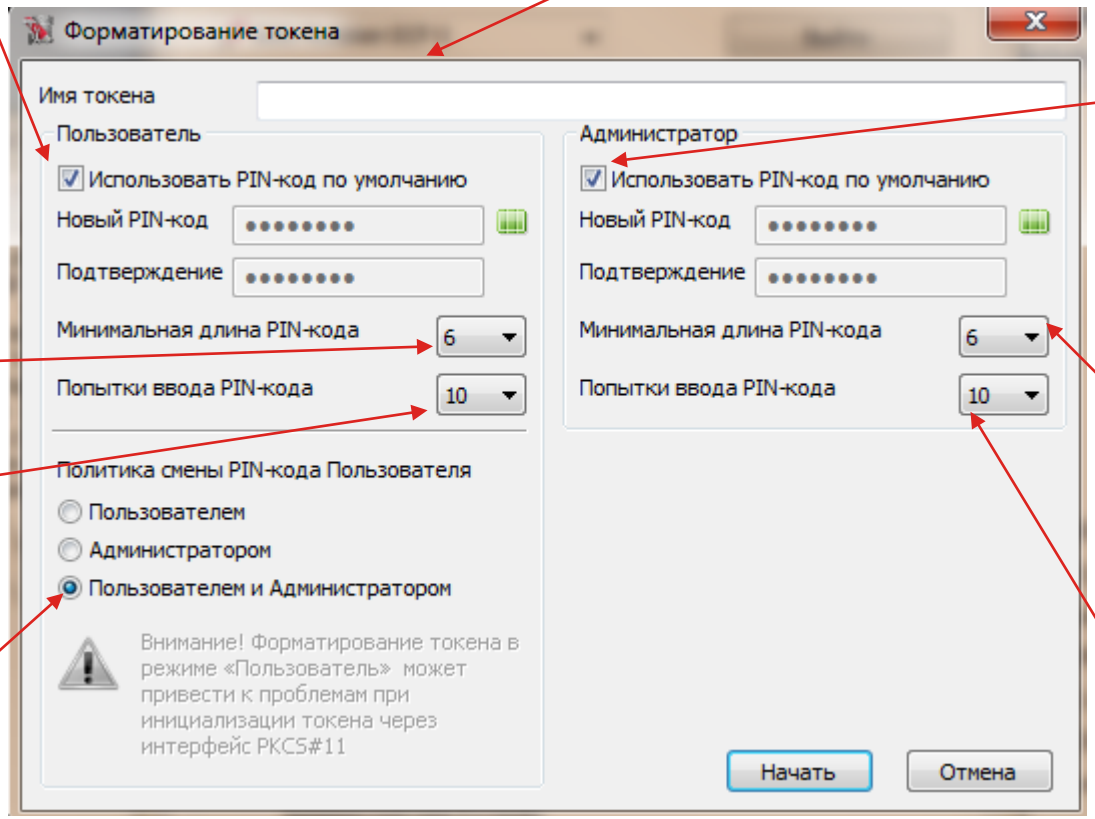
Форматирование USB-токена.

Откройте «Панель управления Рутокен», нажмите на кнопку **[Ввести PIN]**, выберите Администратор, введите PIN-код. После того, как вы получили Административный доступ к панели управления нажмите **[Форматировать]**.

Если установлена данная галочка, то после форматирования будет установлен PIN-код по умолчанию: 12345678. Если данная галочка не установлена, то вы можете задать PIN-код Пользователя, обратите внимание на индикатор, показывающий надежность PIN-кода.

Позволяет задать имя токена.

Если установлена данная галочка, то после форматирования, в качестве PIN-кода Администратора будет установлен PIN-код по умолчанию: 87654321. Если данная галочка не установлена, то вы можете задать PIN-код Администратора, обратите внимание на индикатор, показывающий надежность PIN-кода.



Минимальная длина PIN-кода Пользователя

Количество неправильных попыток ввода PIN-кода Пользователя, после которых PIN-код блокируется.

Позволяет задать под какой учетной записью можно будет сменить PIN-код Пользователя.

Минимальная длина PIN-кода Администратора.

Количество неправильных попыток ввода PIN-кода Администратора, после которых PIN-код блокируется.

Для того, чтобы произвести форматирование USB-токена нажмите кнопку **[Начать]**.

DCS
Техническая поддержка
Контактная информация

E-mail: ebs.russia@citi.com

Телефон: +7 495 725 67 95 (9:00-18:00 MSK)