

# Передача документов с использованием электронной подписи

Руководство по установке и настройке.



# Содержание

<input type="checkbox"/> Общие сведения об электронной подписи   Комплект ЭЦП	3	<input type="checkbox"/> Заполнение Карточки регистрации запроса	14
<input type="checkbox"/> Комплект ЭЦП   Краткое описание программного обеспечения	4	<input type="checkbox"/> Получение и импорт сертификатов	15
<input type="checkbox"/> Загрузка драйверов Рутокен   Учетные записи Рутокен	5	<input type="checkbox"/> Установка и настройка File-PRO   Личный сертификат	16
<input type="checkbox"/> Установка Admin-PKI v5*   Подготовка к генерации запроса	6	<input type="checkbox"/> Сертификат шифрования   Сертификаты УЦ	17
<input type="checkbox"/> Порядок выдачи сертификата	7	<input type="checkbox"/> Настройка обработки файлов в File-PRO	18
<input type="checkbox"/> Порядок выдачи сертификата   Личное присутствие	8	<input type="checkbox"/> Подпись и шифрование файла	19
<input type="checkbox"/> Порядок выдачи сертификата   Доверенность	9	<input type="checkbox"/> Подпись и шифрование файла   Вид конечного файла	20
<input type="checkbox"/> Генерация запроса на сертификат	10	<input type="checkbox"/> Передача файла в банк	21
<input type="checkbox"/> Параметры запроса сертификата	11	<input type="checkbox"/> Получение файлов из банка   Расшифровка	22
<input type="checkbox"/> Сохранение запроса сертификата	12	<input type="checkbox"/> Получение файлов из банка   Проверка подписи	23
<input type="checkbox"/> Печать запроса	13	<input type="checkbox"/> Учетная запись Администратора   Разблокировка PIN Пользователя	24
		<input type="checkbox"/> Контакты DCS	25



## ➤ **Электронная подпись (ЭП) –**

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».

## ➤ **ЭП используется для передачи некоторых типов документов в банк**

(в связи с вступлением в силу Инструкции Банка России № 138-И), а также для удаленного заключения договоров, подписания заявок и прочих юридически значимых документов. Согласно 63-ФЗ усиленная ЭП, используемая Ситибанком, является полным аналогом собственноручной подписи и печати организации. Таким образом, дополнительно предоставлять уполномочивающие документы не требуется, достаточно выпустить сертификаты ЭП. Ситибанк вправе ограничивать список документов, принимаемых с электронной подписью, оставляя возможность принять их только на бумаге.

Для начала использования ЭП 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
- **Заявление** на выдачу USB-токена

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

## USB-токен Rutoken 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.

## File-PRO v2.5.0.0\*



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

## Admin-PKI v5\*



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).

# Загрузка драйверов Рутокен | Учетные записи Рутокен



Загрузите последнюю версию драйверов с официального сайта:

<http://www.rutoken.ru/support/download/drivers-for-windows/>

## ↓ Драйверы Рутокен для Windows, EXE

Версия: 4.8.8.0 от 17.09.2020  
Поддерживаемые ОС: 32- и 64-разрядные Microsoft Windows

В файловой системе Рутокен ЭЦП существует 2 учетных записи. Нажмите **[Ввести PIN-код]** для того, чтобы увидеть возможные варианты входа в систему.

### Пользователь

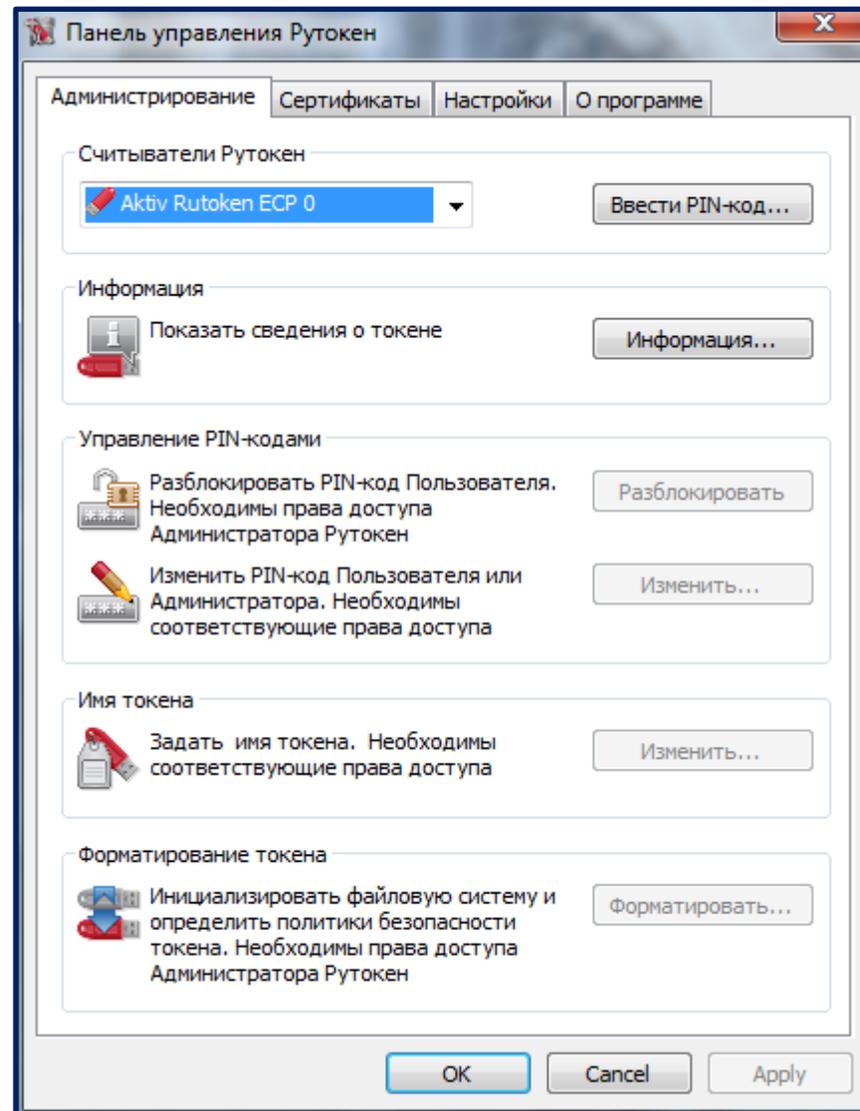
Учетная запись предусмотрена для повседневной работы с токеном. PIN рекомендуется заменить на уникальный.

**Пин-код по умолчанию:**  
**12345678**

### Администратор

Учетная запись предусмотрена для разблокировки PIN-кода пользователя и форматирования токена.

**Пин-код по умолчанию:**  
**87654321**



1

Дистрибутивы можно скачать по ссылке:

[https://www.e-notary.ru/files/products/update/citibank/customers/adm\\_file\\_esp\\_win.zip](https://www.e-notary.ru/files/products/update/citibank/customers/adm_file_esp_win.zip)

Пароль к архиву: **citibank2019**

2

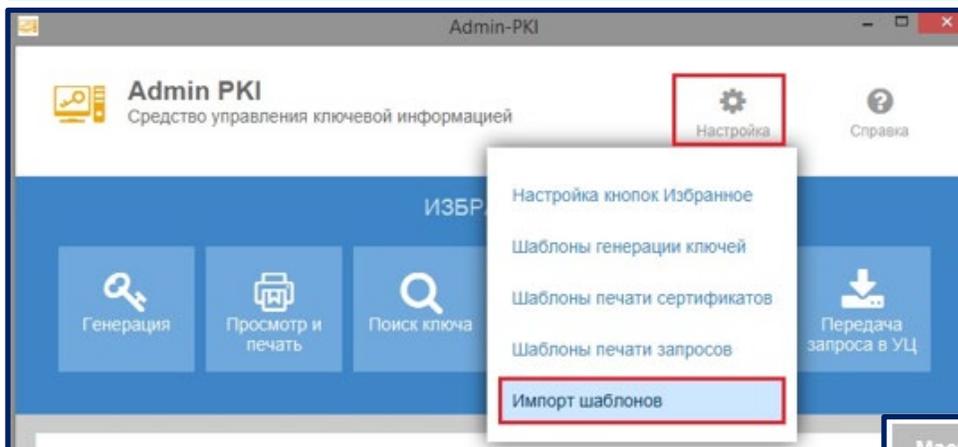
Откройте инструкцию с помощью PDF Reader и сохраните приложенные к инструкции файлы на компьютер («Сохранить вложение как...»)

3

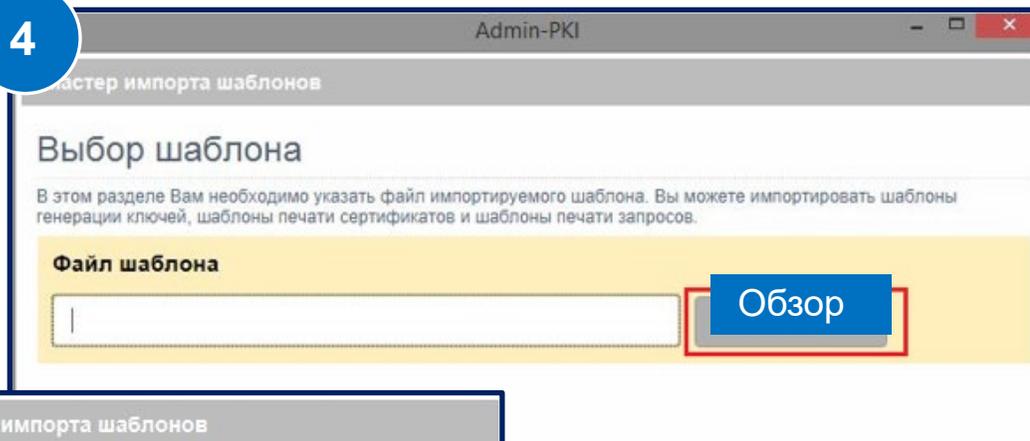


В программе Admin-PKI нажмите **Настройка > Импорт шаблонов > Обзор** и добавьте поочередно файлы шаблонов в программу

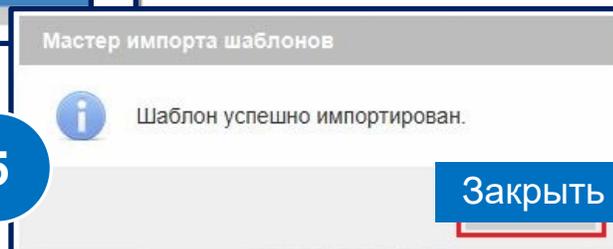
- ✓ [5.2.3]\_GOST\_2012\_default\_keygen\_template.tpl
- ✓ Citibank Request Print Template 2020.tpl



4



5



# 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 электронную подпись в Удостоверяющем центре Ситибанка, нужно подтвердить Вашу личность одним из двух способов:

## Лично приехать в офис Ситибанка



Личная идентификация производится в офисе Ситибанка по адресу: г. Москва, ул. Гашека, 8-10, стр. 1, метро "Маяковская".

При себе необходимо иметь паспорт и Карточку регистрации запроса на сертификат.  
**\*\*\*** Если Карточка была направлена ранее в оригинале, то при себе можно иметь только паспорт.

## Оформить в компании специальную доверенность / доверенности



Доверенность на осуществление идентификации лица, получающего сертификат ЭП, оформляется **перед** подачей запросов на сертификат в банк.

**ВНИМАНИЕ:** Доверенное лицо и владелец сертификата не должны совпадать.



Нажмите, чтобы открыть вложения к PDF и скачать бланки Доверенности

1

Владелец сертификата направляет Электронный файл запроса (файл с расширением .pem) на адрес [cert.ru@citi.com](mailto:cert.ru@citi.com).

**Внимание!** В теме письма обязательно укажите базовый номер компании и ФИО владельца сертификата.

2

Владелец сертификата направляет скан-копию распечатанной Карточки регистрации запроса на сертификат на адрес [ru.tfa@citi.com](mailto:ru.tfa@citi.com).

Карточка заверяется подписью:

- **Владельца сертификата** (поле «Личная подпись владельца ключа»)
- **Уполномоченного представителя компании** (поле «Руководитель организации»)

**Внимание!** Поле «Личность владельца сертификата установлена» требуется оставить пустым.

3

После получения Карточки регистрации запроса на сертификат Банк начинает обработку запроса и проводит сверку Карточки регистрации запроса на сертификат и файла электронного запроса с расширением .pem.

4

По завершении обработки Банк направляет владельцу сертификата архив с **неактивным сертификатом** и уведомление о необходимости лично посетить офис Банка по адресу: Москва, ул. Гашека, 8-10, стр. 1 для прохождения процедуры идентификации.

При себе необходимо иметь паспорт и оригинал Карточки регистрации запроса на сертификат.

5

После завершения идентификации владельца сертификата Банк активирует сертификат пользователя.

# Порядок выдачи сертификата | Доверенность

1

Определите в Вашей Компании лицо, которое будет осуществлять личную идентификацию лиц, запрашивающих электронную подпись и получающих сертификаты электронной подписи

2

Заполните и отправьте по e-мейлу документы на адрес [ru.tfa@citi.com](mailto:ru.tfa@citi.com).

- **запрос на выдачу доверенности для представителя** (руководителем организации или уполномоченным лицом с общей (генеральной) доверенностью или с доверенностью на подписание документов, связанных с получением ЭП/оформлением сертификата ЭП;
- **шаблон доверенности** (заполняется в файле Word, не заверяется);
- **копия паспорта**

3

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

4

Владелец сертификата направляет Электронный файл запроса (файл с расширением .pem) на адрес [cert.ru@citi.com](mailto:cert.ru@citi.com).

**Внимание!** В теме письма обязательно укажите базовый номер компании и ФИО владельца сертификата.

5

Владелец сертификата направляет скан-копию распечатанной Карточки регистрации запроса на сертификат адрес [ru.tfa@citi.com](mailto:ru.tfa@citi.com).

**Карточка заверяется подписью:**

- **Владельца сертификата** (поле «Личная подпись владельца ключа»)
- **Уполномоченного представителя компании** (поле «Руководитель организации»)
- **Представителя** (поле «Личность владельца сертификата установлена»).

6

По завершении обработки Банк направляет владельцу сертификата архив с **неактивным сертификатом** и копию(бланк) сертификата ЭП Доверенному лицу по электронной почте

7

Доверенное лицо ставит подпись в поле «Личность владельца сертификата установлена», указывает дату, а владелец сертификата расписывается в поле «Сертификат получен лично».

**Внимание!** Дата на документе должна совпадать с датой начала действия сертификата, поле «Действителен с » (3-я строка документа).

8

Сканированная копия подписанного Сертификата ЭП направляется на адрес [ru.tfa@citi.com](mailto:ru.tfa@citi.com)

После завершения идентификации Банк активирует сертификат пользователя.

9

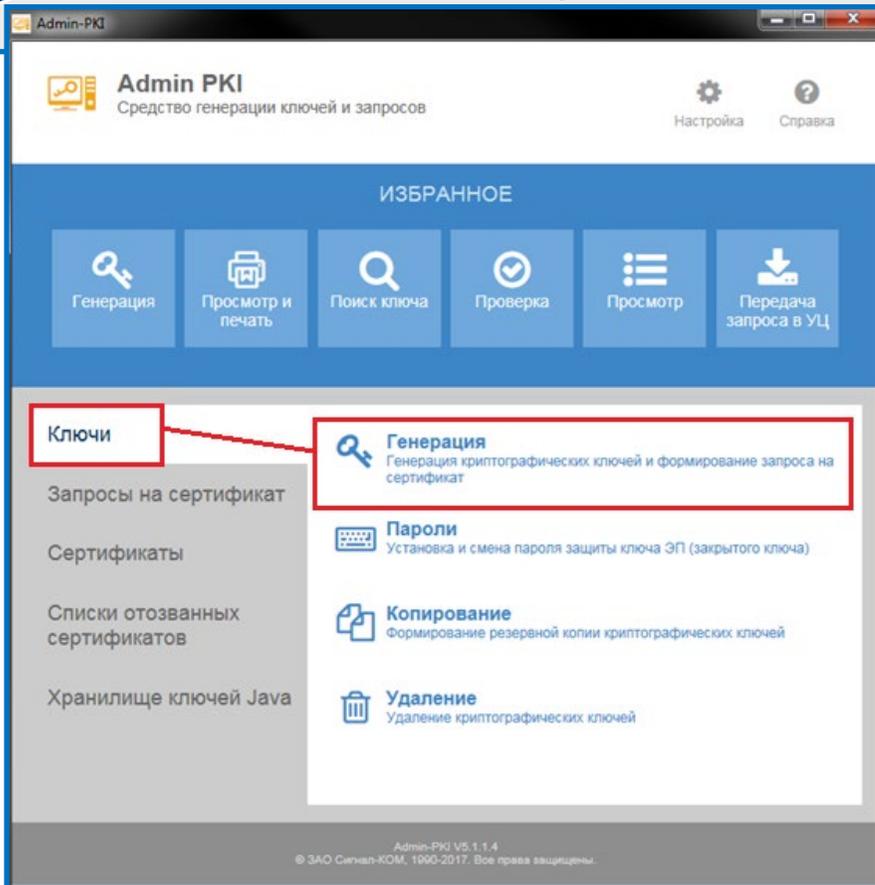
Оригиналы Карточки и Сертификата передаются в офис Банка:

- г. Москва, ул. Гашека, 8-10, стр. 1 или
- г. Санкт-Петербург, Итальянская, д.5.

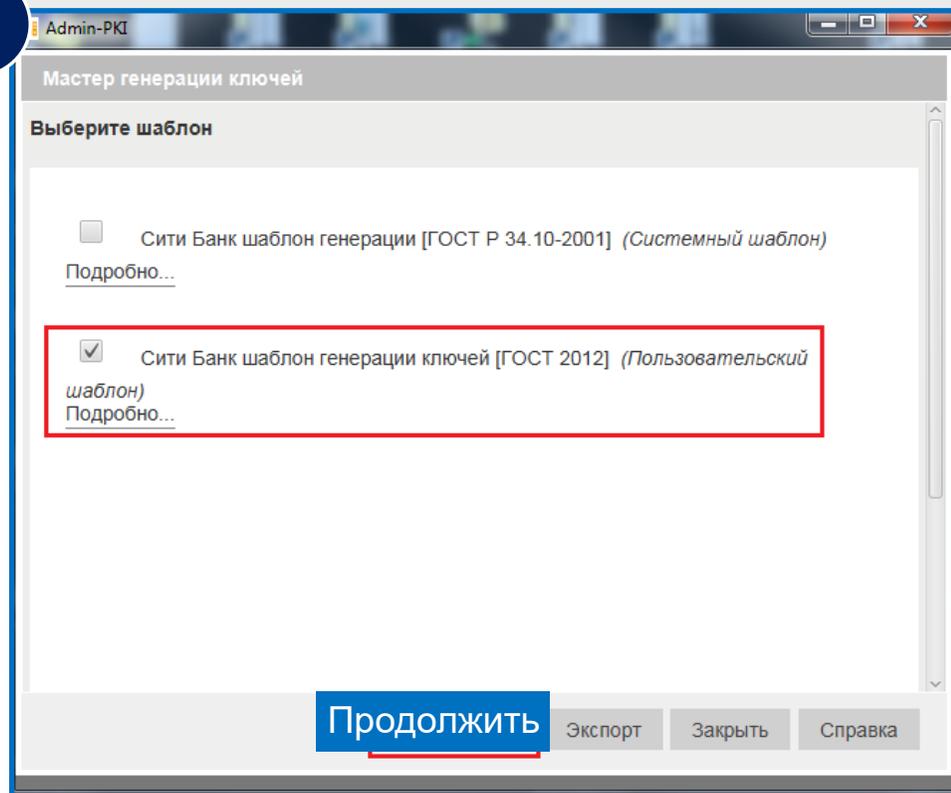
**Внимание!** Оригиналы должны быть переданы в течении **30 календарных дн.** В противном случае выпущенный сертификат будет заблокирован.

# Генерация запроса на сертификат

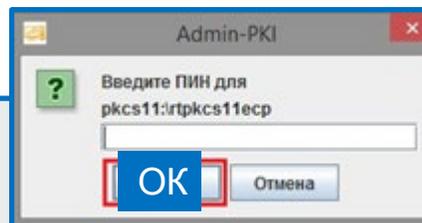
1 В программе Admin-PKI выберите пункт «Ключи» > «Генерация»



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



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



# Параметры запроса сертификата

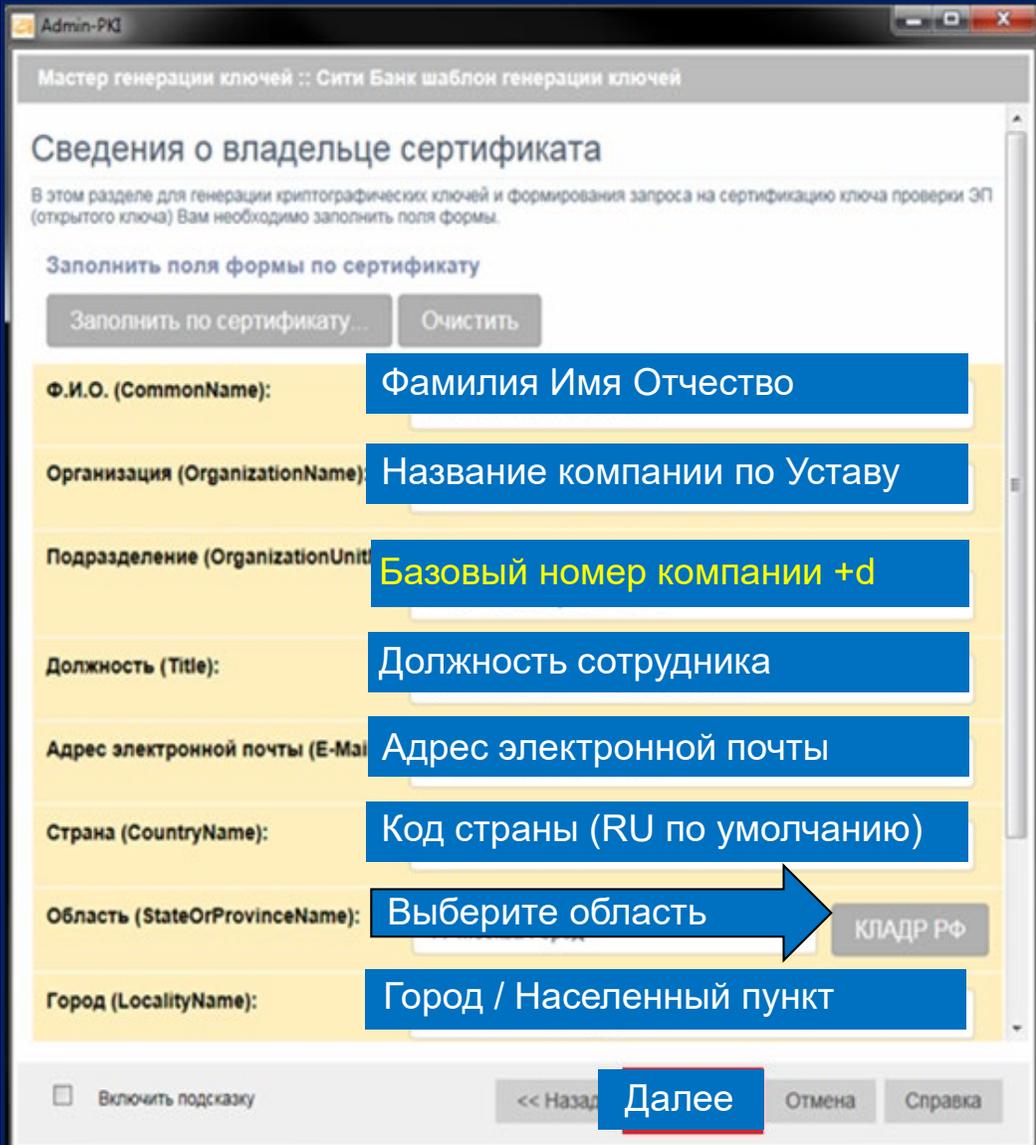
4

Все выделенные желтым поля являются обязательными для заполнения.

- Для сертификата для документов (гарантии, кредитные заявки, факторинг и пр.) укажите **базовый номер+d** (например, 123456d) в поле «Подразделение»
- Для сертификата для корпоративных карт укажите **базовый номер+d** (например, 123456d) в поле «Подразделение» и **Программный администратор** в поле «Должность»

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

 Страна, область и город должны быть указаны исходя из **фактического местонахождения владельца сертификата**



Admin-ПК  
 Мастер генерации ключей :: Сити Банк шаблон генерации ключей

### Сведения о владельце сертификата

В этом разделе для генерации криптографических ключей и формирования запроса на сертификацию ключа проверки ЭП (открытого ключа) Вам необходимо заполнить поля формы.

Заполнить поля формы по сертификату

Заполнить по сертификату... Очистить

Ф.И.О. (CommonName): **Фамилия Имя Отчество**

Организация (OrganizationName): **Название компании по Уставу**

Подразделение (OrganizationUnit): **Базовый номер компании +d**

Должность (Title): **Должность сотрудника**

Адрес электронной почты (E-Mail): **Адрес электронной почты**

Страна (CountryName): **Код страны (RU по умолчанию)**

Область (StateOrProvinceName): **Выберите область** → КЛАДР РФ

Город (LocalityName): **Город / Населенный пункт**

Включить подсказку

<< Назад **Далее** Отмена Справка

# Сохранение запроса сертификата

5

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

i

**У каждого сертификата должен быть свой закрытый ключ.**

В случае появления окна, как на скриншоте ниже, на токене уже ранее генерировался ключ.

Нажмите «**НЕТ**», чтобы ключевая пара Запрос < > Закрытый ключ сформировалась корректно.

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



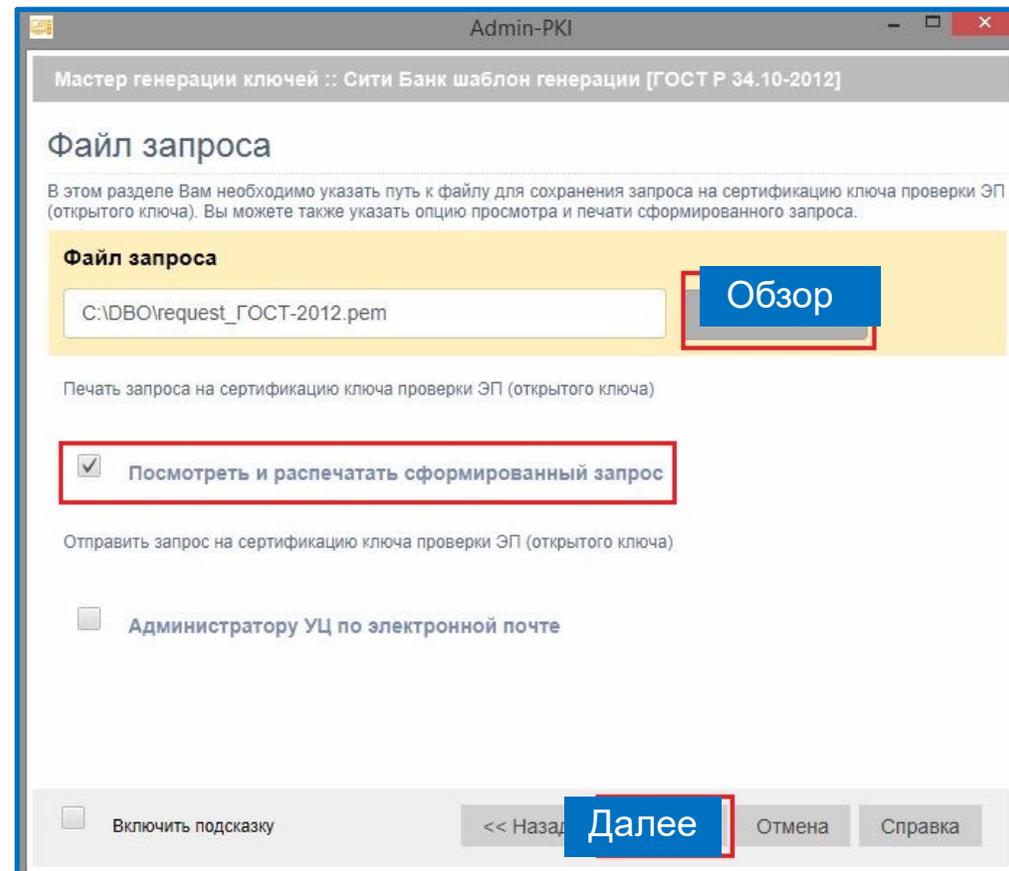
Мастер генерации ключей



Ключ ЭП (закрытый ключ) уже существует. Для формирования запроса на сертификат использовать существующий ключ ЭП?

Да

Нет



# Печать запроса

**6** Admin-PKI

просмотра и печати запросов

Поле	Значение
Версия	0
Владелец	CN= [REDACTED]
Открытый ключ	Algorithm: GOSTR3410-2012-256 ...
Расширенное использование ключа	Extended Key Usage
Расширения в запросе	Extension
Сертификационные политики	Certificate Policies
Подпись	Signature Algorithm: GOSTR3411...
Текст запроса	CertificationRequest: [ Versi...
Запрос	PKCS#10

Включить подсказку << Назад **Далее** Отмена Справка

**7** Admin-PKI

просмотра и печати запросов

### Выбор шаблона печати запроса

Шаблон просмотра и печати запроса.

Выберите шаблон печати запроса

**Citibank Request Print Template 2020**

Включить подсказку << Назад **Далее** Отмена Справка

**8** просмотра и печати запросов

### КАРТОЧКА РЕГИСТРАЦИИ ЗАПРОСА НА СЕРТИФИКАТ АБОНЕНТА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

1. Наименование организации: АО КБ Ситибанк
2. Юридический адрес: \_\_\_\_\_
3. Почтовый адрес: \_\_\_\_\_
4. Наименование документа о регистрации, кем и когда выдан: \_\_\_\_\_
5. Тел. \_\_\_\_\_ 6. Факс \_\_\_\_\_
7. Примечания: \_\_\_\_\_
8. Сведения об абоненте: \_\_\_\_\_

Включить подсказку << Назад **Далее** Отмена Справка

**i** В случае необходимости генерации нескольких 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.

# Заполнение Карточки регистрации запроса

## КАРТОЧКА РЕГИСТРАЦИИ ЗАПРОСА НА СЕРТИФИКАТ АБОНЕНТА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

- Наименование организации: **автоматически из Admin-PKI**
- Юридический адрес: **юридический адрес компании**
- Почтовый адрес: **фактический адрес пользователя (не обязательно)**
- Наименование документа о регистрации, кем и когда выдан:  
**ОГРН (не обязательно)**
- Тел. **номер телефона** 6. Факс
- Примечания:
- Сведения об абоненте:  
 Страна: **автоматически из Admin-PKI**  
 Область/Район: **автоматически из Admin-PKI**  
 Город/Село: **автоматически из Admin-PKI**  
 Организация: **автоматически из Admin-PKI**  
 Подразделение: **автоматически из Admin-PKI**  
 Должность: **автоматически из Admin-PKI**  
 Фамилия, имя, отчество: **автоматически из Admin-PKI**  
 E-mail адрес: **автоматически из Admin-PKI**  
 Удостоверение личности: паспорт \_\_\_\_\_ сер. **серия паспорта** N **номер паспорта**  
 выдан **дата выдачи** г. \_\_\_\_\_ кем выдан \_\_\_\_\_

**9** Распечатайте карточку регистрации запроса на сертификат и заполните пустые поля (выделены синим).  
  
Некоторые поля подтянут информацию автоматически из программы Admin-PKI (выделены красным)

**Открытый ключ владельца:**  
 Algorithm: ECGOST3410 (1.2.643.2.2.19)  
 Parameters: CP-A (1.2.643.2.2.35.1)  
 PublicKey: 26-5f62:dc-69-38:e5-9b:dd-10-ac-1b:c6-50-50-f1-1f-49-0b:ac-97-62:cd-5f-2e-7b-7a-9b-96-f7-7d-43-17-c3-32-53-a3-8d-7c-5f-83-da-26-7e-3a-b8-76-1c-e8-74-67-14-39-e1-92-c4-37-01-94-2f-68-87-2e-a2

**Текст запроса на сертификат открытого ключа в формате PEM:**

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBWzCCAXACAQAwggECMQswCQYDVQQGEwJVSUVEVMBMGA1UECAwMOKDRj9C30LDRQ
vdGMMRUwEwYDVQQHDAzQcNGP0LFQsNC90YwxJzA1BgnVBAoMHTCX0JDQniDQmtCR
ICLQodC40YLQuNcX0LDQvdC6IjENMAsGA1UECwwERFNIRDEdMBsGA1UEDAwUOKKHQ
v9C10YbQuNCw0LrQuNGB0YIxQzBBBgNVBAMM0tC10LXRgNC10YnQtdC90LrQviDQ
mNGA0LjQvdCwInCa0L7QvdGB0YLQsNC90YLQuNC90L7QstC90LAXkTAnBgkqhkiG
9w0BCEwGmlYaW5hLnR1cmVzY2hlbmtvQGNpdGkuY29tMGwHAYGKoUDAgITMBIG
ByqFAwICiWEGByqFAwICgEDQwAEQCZfYtXp00Wb3RdsG8ZQUPEfSQuS12LNxy57
epuW931DF8MyU6ONfF+D2iZ+Wrh2H0h0ZxQ54ZLENwGUL2iHLqKgADAKBgYqhQMC
AgMFAANBAH/faFfTKcyM8KVkOVlxJi4igpRhMBtzuHbPCVmhRBJpGDrF5RKB9/NGe
IyS/bL6ObVz481J/4SIzowEdIqH0TR0=
-----END CERTIFICATE REQUEST-----
```

**i** Если поля для подписи Доверенного лица нет в Карточке регистрации, то можно дописать это поле в Карточке от руки

**Личная подпись владельца ключа:**  
 \_\_\_\_\_ /  
 (подпись) / (расшифровка подписи)  
 Достоверность приведенных данных подтверждаю

**Руководитель организации:**  
 \_\_\_\_\_ /  
 (подпись) / (расшифровка подписи)

**Личность владельца сертификата установлена**  
 \_\_\_\_\_ /  
 (подпись) / (расшифровка подписи)

" \_\_\_\_ " \_\_\_\_\_ **дата** \_\_\_\_\_ 20 \_\_\_\_ г. |  
 \_\_\_\_\_ **М.П.** \_\_\_\_\_ **печать компании**

# Получение и импорт сертификатов

Полученный zip-архив с сертификатами нужно распаковать, поменять расширение файлов с **.ce\_** на **.cer** и сохранить на компьютер:

- Личный сертификат пользователя
- Encryption 2021.cer
- cacert\_enotary 2021.cer
- SubCA\_citibank 2021.cer



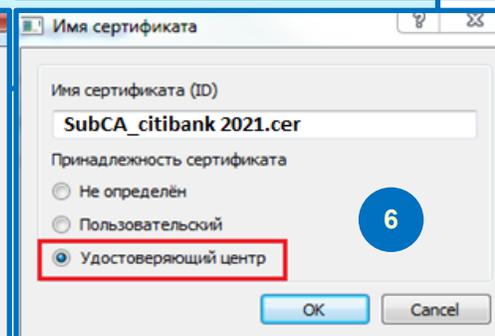
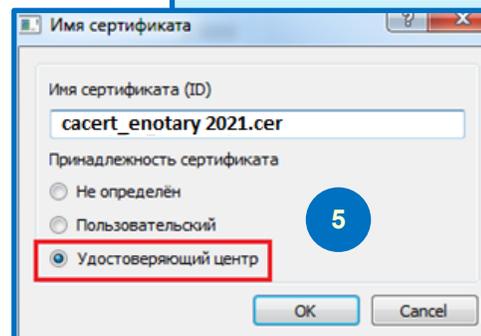
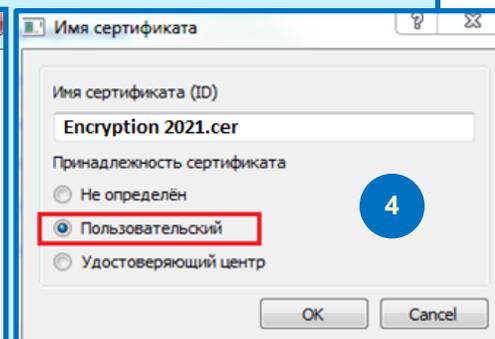
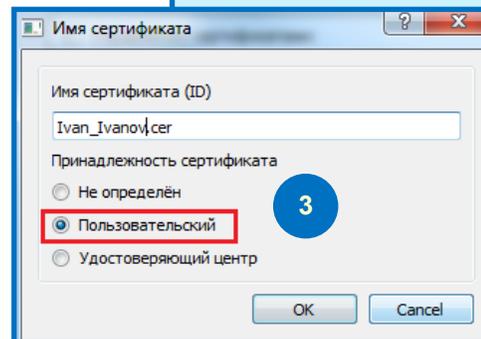
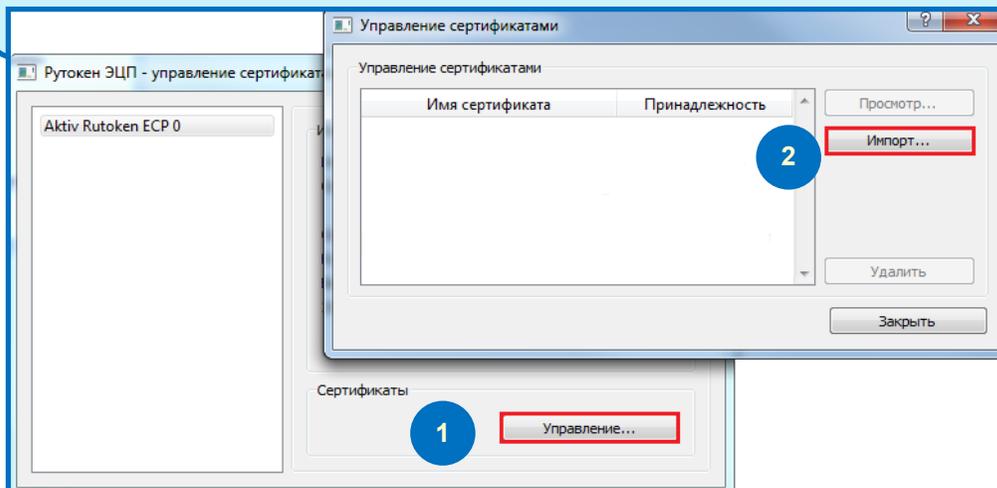
Срок действия сертификатов с момента выпуска – **3 года**

⚙ Скачайте утилиту для импорта сертификатов:

[https://www.e-notary.ru/files/download/rutoken/rutoken\\_utility.zip](https://www.e-notary.ru/files/download/rutoken/rutoken_utility.zip)

Выберите с компьютера файлы сертификатов и импортируйте их на токен, установив принадлежность.

Запустите файл **rutoken\_utility.exe**  
Нажмите кнопку **Управление**, затем **Импорт**

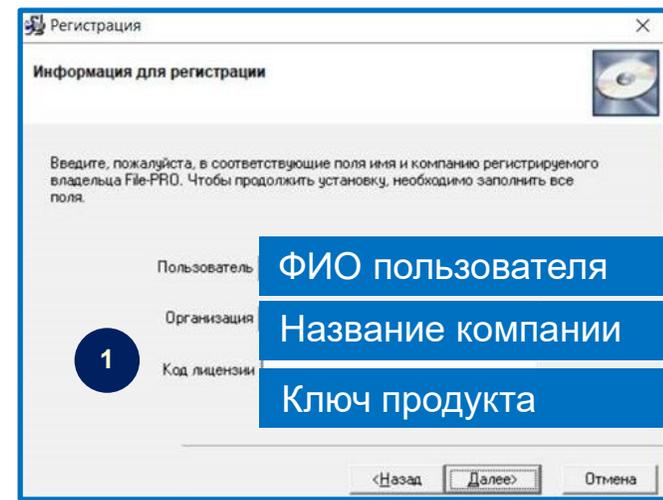


# Установка и настройка File-PRO | Личный сертификат

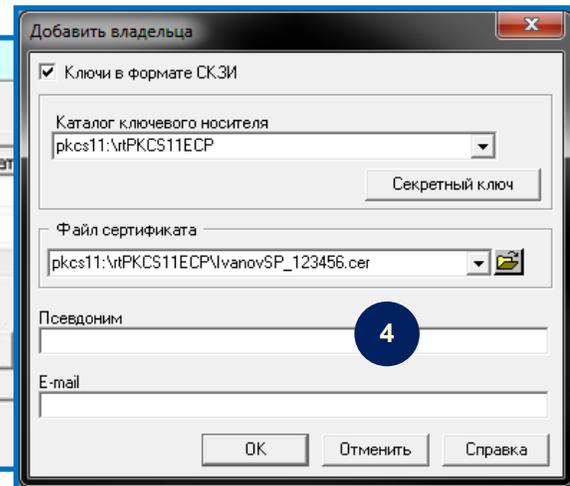
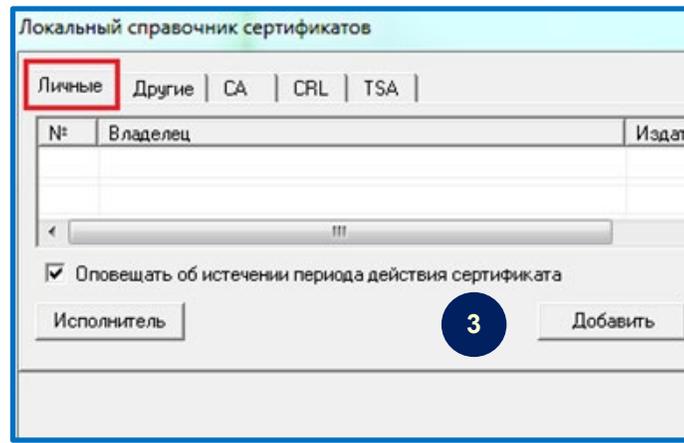
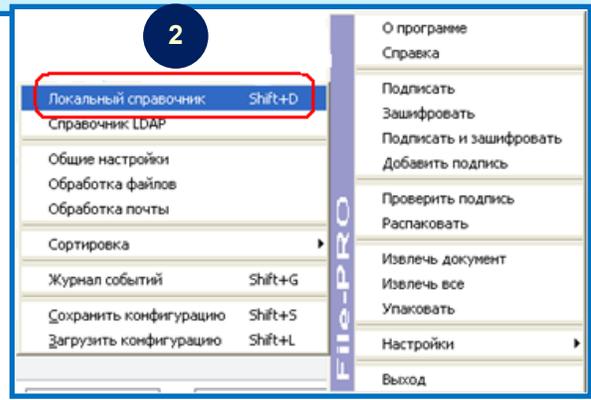
1. Запустите установочный файл File-PRO.exe и следуйте указаниям мастера установки.

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 сопроводительной документации.



2. Щелкните мышью на иконке File-PRO и выберите **Настройки > Локальный справочник**

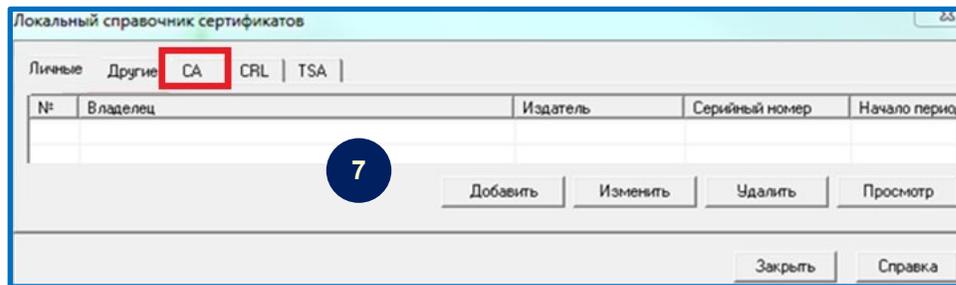
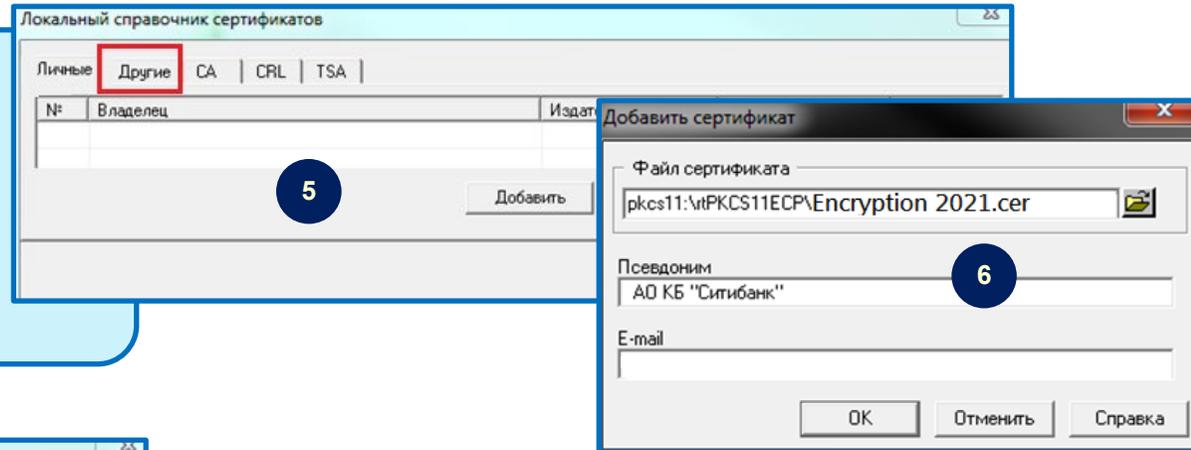


3. На вкладке **Личные** нажмите **Добавить**.

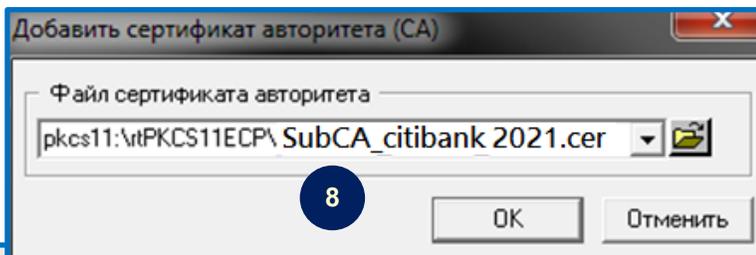
4. В качестве каталога ключевого носителя выберете **pkcs11:\rtPKCS11ECP**  
 Укажите файл сертификата в формате **pkcs11:\rtPKCS11ECP\ivanovSP\_123456.cer**,  
 где **ivanovSP\_123456.cer** – название файла сертификата, затем нажмите **OK**

# Сертификат шифрования | Сертификаты УЦ

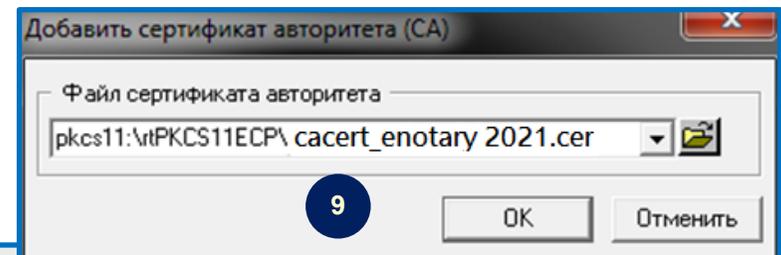
5. На вкладке **Другие** нажмите **Добавить**
6. Укажите **Файл сертификата** в формате **pkcs11:\rtPKCS11ECP\Encryption 2021.cer** где Encryption 2021.cer – название файла сертификата
- Нажмите **ОК**, чтобы завершить установку.



7. Зайдите на вкладку **CA** и нажмите **Добавить**, чтобы начать импорт новых сертификатов.



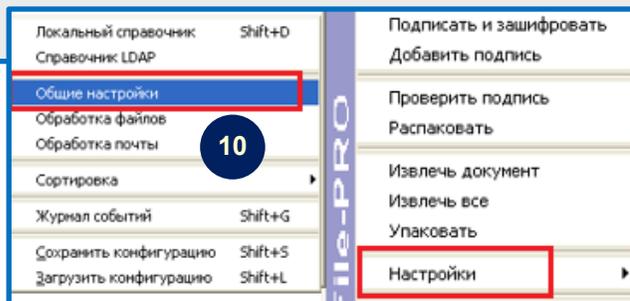
8. Укажите файл сертификата авторитета в формате: **pkcs11:\rtPKCS11ECP\SubCA\_citibank 2021.cer**



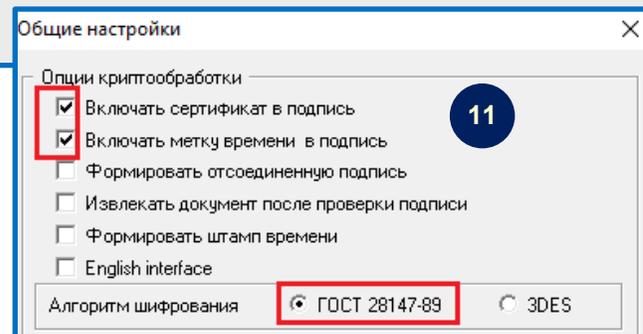
9. Укажите файл сертификата авторитета в формате: **pkcs11:\rtPKCS11ECP\cacert\_enotary 2021.cer**

# Настройка обработки файлов в File-PRO

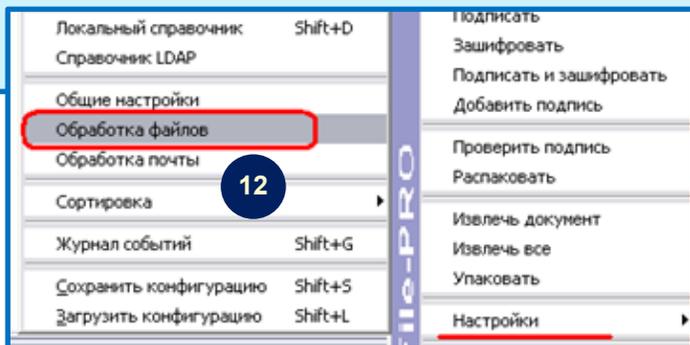
10. Настройки формата подписи происходят в меню **File-PRO > Настройки > Общие настройки**



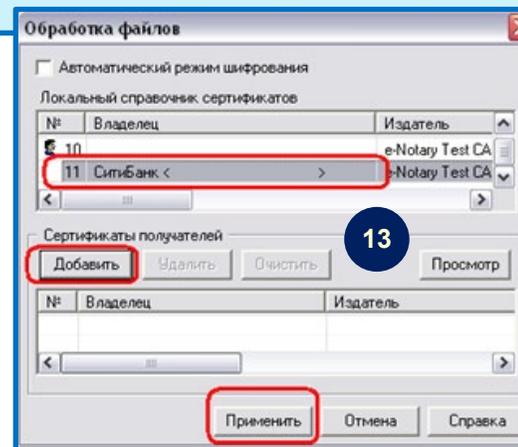
11. Отметьте нужные опции, если они не установлены, а также проверьте алгоритм шифрования



12. Настройка автоматического выбора получателя при подписи и шифровании файла происходят в меню **File-PRO > Настройки > Обработка файлов**



13. Выберите личный сертификат и сертификат банка в Локальном справочнике сертификатов, нажмите поочередно кнопку **Добавить**, затем **Применить**



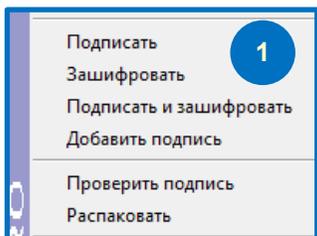
Настройка программы File-PRO завершена

# Подпись и шифрование файла

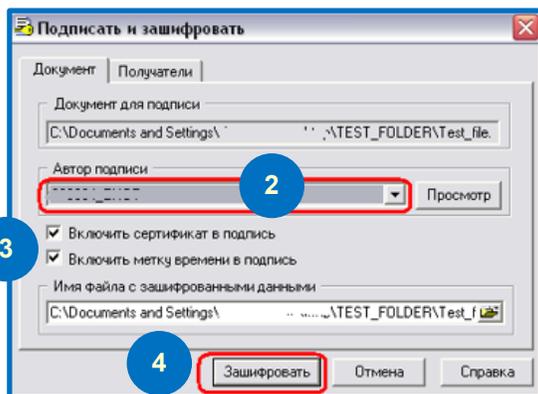


При передаче документов на обработку в банк файлы, содержащие документы, должны быть подписаны электронной подписью уполномоченного лица и зашифрованы, затем заархивированы в ZIP-архив.

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



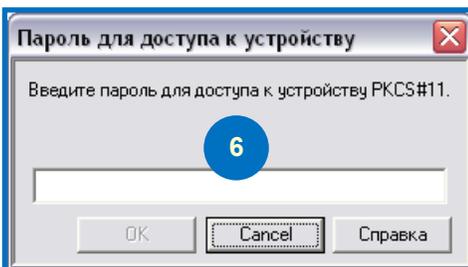
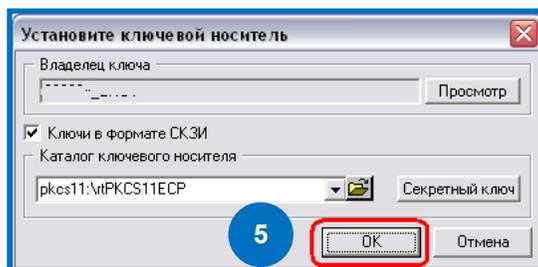
1. Щелкните мышью на иконке File-PRO и выберите нужное Вам действие: **Подписать** и **Зашифровать**, либо по отдельности **Подписать** или **Зашифровать**



2. В поле **Автор подписи** указывается сертификат подписанта. Если у Вас несколько сертификатов, то в этом поле нужно выбрать нужный

3. Убедитесь, что отмечены параметры **Включить сертификат в подпись** и **Включить метку времени в подпись**

4. Нажмите кнопку **Зашифровать**

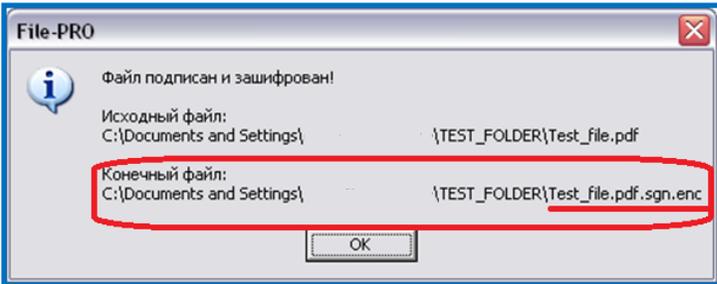


5. Нажмите **OK**

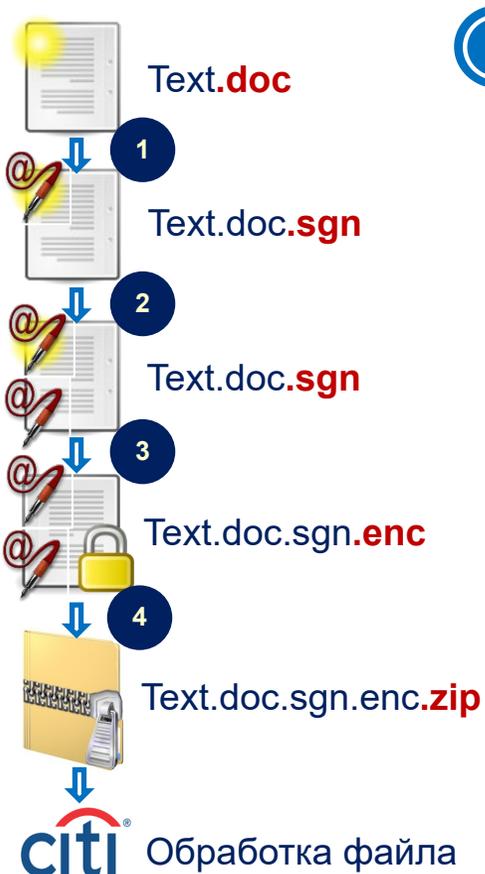
6. Введите пин-код для USB-токена и нажмите **OK** (по умолчанию, пин **12345678**, если его не менял пользователь)

Откроется окно с результатом и указанием местонахождения файлов. Нажмите кнопку **OK**.

# Подпись и шифрование файла | Вид конечного файла



- 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 (результатирующий)** файл с расширением **.sgn.enc**



**i** Если документ подписывается несколькими ЭП, пользователи могут подписывать его в любом порядке на свое усмотрение. Подписывающий файл последним должен его зашифровать, заархивировать и направить в банк.

Функции шифрования, упаковки и отправки файла в банк **могут быть переданы другим пользователям (исполнителям)**. Электронная подпись или иные документы для таких пользователей не требуются.

1. Для подписи документа используйте функцию **Подписать**
2. Для повторной подписи нажмите либо **Подписать**, чтобы передать документ далее на шифрование или еще одну подпись, либо **Подписать и Зашифровать**, если данная подпись – последняя. Для подписи уже подписанного ранее документа нужно подписывать файл с расширением .sgn
3. Для шифрования документа используйте функцию **Зашифровать**.
4. Для Заархивируйте документ в ZIP-архив для передачи в банк

# Передача файла в банк



При передаче документов на обработку в банк файлы, содержащие документы, должны быть подписаны электронной подписью уполномоченного лица и зашифрованы, затем заархивированы в ZIP-архив.

- В названии файла допустимы ТОЛЬКО латинские буквы и цифры
- В одном zip-архиве должен содержаться только один файл
- Максимально допустимый размер файла .zip не может превышать 5Mb
- Максимально допустимый размер файла в ZIP-архиве не может превышать 5Mb
- В письме при передаче файлов в банк может содержаться несколько ZIP-архивов общим размером не более 10 МБ

FileName.sgn.enc.zip



При передаче документов по электронной почте файл с данными должен быть последовательно:

1. Подписан,
2. Зашифрован
3. Заархивирован (ZIP).

Для передачи подписанного, зашифрованного и заархивированного файла прикрепите файл к электронному письму и отправьте его на адрес

**[eforms.ru@citi.com](mailto:eforms.ru@citi.com)**

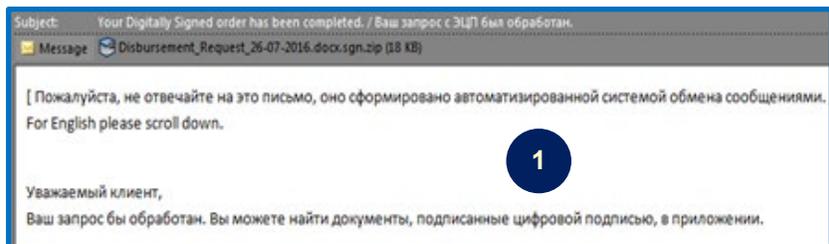


В теле письма Вы также можете указать дополнительные сведения, однако информация, переданная таким образом не может рассматриваться как юридически значимая, и не наследует признаков ЭП и шифрования файла, прикреплённого к сообщению.

# Получение файлов из банка | Расшифровка

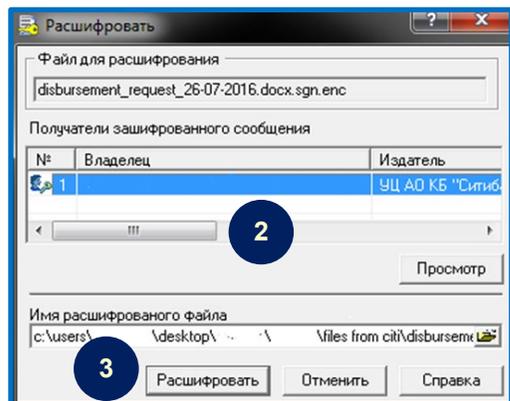


Вы не сможете расшифровать файл, полученный из банка, если Ваш токен будет утерян, поврежден или форматирован, а также если истечет личный сертификат пользователя. Пожалуйста, расшифруйте и сохраните документ сразу после получения.



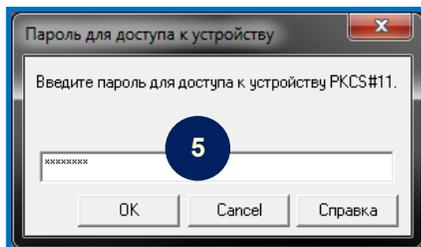
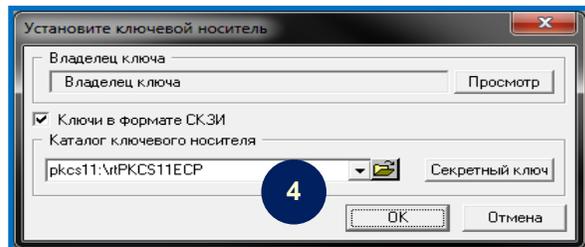
1. Для проверки электронной подписи и хранения файла сохраните/откройте вложение, присланное банком, и разархивируйте с помощью **Secure ZIP**

Если Secure Zip не установлен, то можно воспользоваться бесплатным ПО: <https://www.pkware.com/zip-reader>



2. Откройте разархивированный файл двойным щелчком мыши, после чего автоматически откроется окно проверки подписи File-PRO.

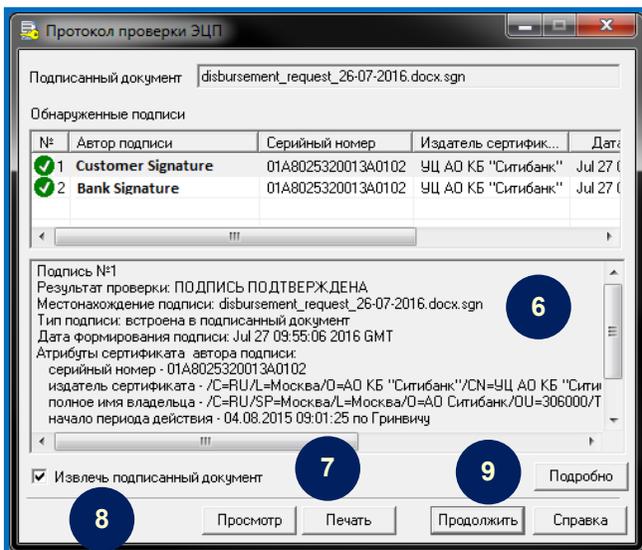
3. Выберите сертификат, которым подписывался отправленный в банк файл (это не требуется если Вы используете только один сертификат), затем нажмите **Расшифровать**



4. Убедитесь, что USB-токен вставлен в USB-порт компьютера, и нажмите **OK**

5. Введите пин-код для USB-токена и нажмите **OK** (по умолчанию, пин **12345678**, если его не менял пользователь)

# Получение файлов из банка | Проверка подписи



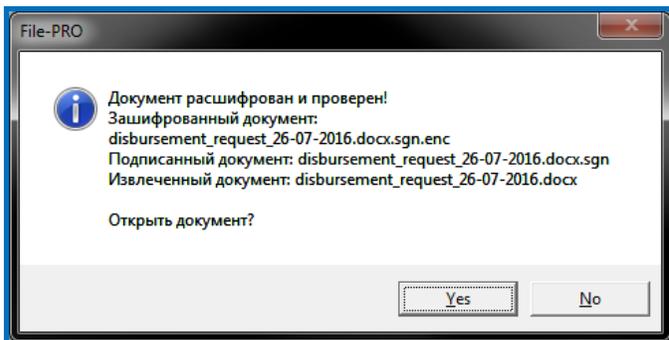
6. Открывшееся окно продемонстрирует подписи на файле и их корректность.

Зеленая отметка и фраза **ПОДПИСЬ ПОДТВЕРЖДЕНА** в окне с подробностями ниже указывает на то, что:

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

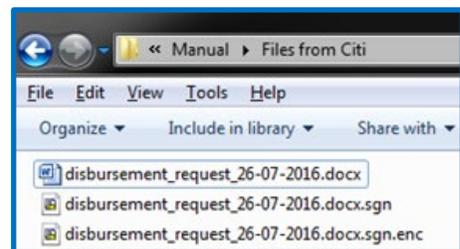
7. Нажав **Печать**, можно напечатать Протокол проверки ЭП

8. Поставьте галочку **Извлечь подписанный документ** и Просмотр, если требуется открыть **исходный** файл без подписи и шифрования



9. Нажмите **Продолжить**, чтобы завершить процедуру проверки электронной подписи

10. Нажмите **Yes**, если Вы хотите открыть *исходный* файл (расшифрованный и со снятыми подписями). Нажмите **No**, чтобы закрыть это окно.



11. Файлы можно различить по расширению.

Имя файла.doc.sgn.enc – подписанный и зашифрованный файл

Имя файла.doc.sgn – подписанный файл без шифрования

Имя файла.doc – исходный файл без подписи и шифрования

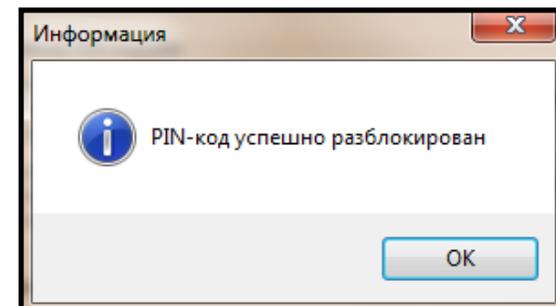
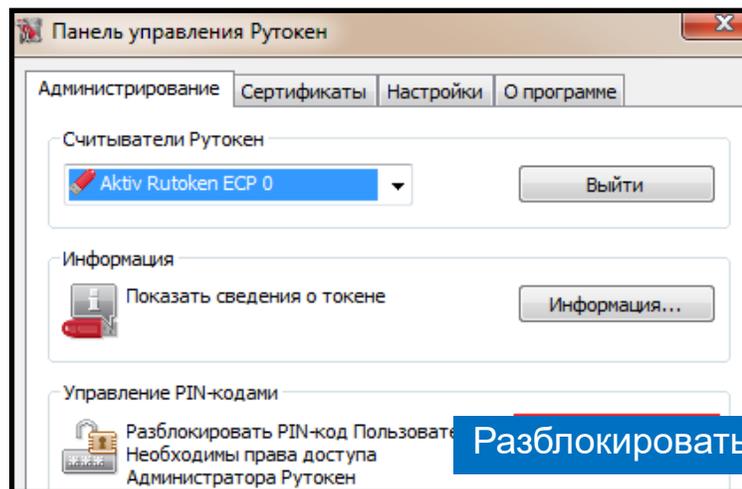
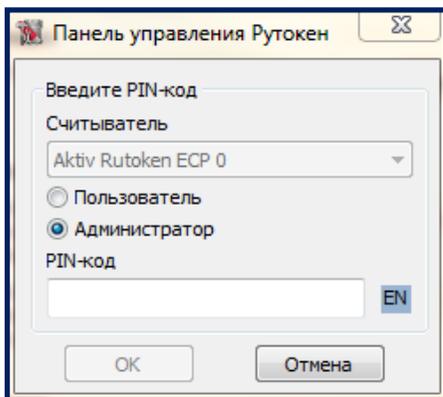
# Учетная запись Администратора | Разблокировка PIN Пользователя



Если неправильно набрать PIN-код Пользователя несколько раз подряд, то он блокируется. В этом случае с помощью учетной записи Администратора можно разблокировать PIN-код Пользователя.

Откройте «Панель управления Рутокен», нажмите на кнопку **[Ввести пин-код]**, выберите учетную запись **[Администратор]**, введите пин-код администратора (по умолчанию, если его не меняли, **87654321**).

Для разблокировки пин-кода пользователя нажмите кнопку **[Разблокировать] / Unblock**.



# Техническая поддержка DCS

## Контактная информация

### E-mail:

[ebs.russia@citi.com](mailto:ebs.russia@citi.com)

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

