

Подготовка компьютера к работе в системе интернет-банк «Faktura»

ВНИМАНИЕ!!! Для работы в системе интернет-банк «Faktura» необходимо использовать браузер (интернет-обозреватель) Internet Explorer 11 или Google Chrome

1. Откройте браузер и перейдите по ссылке: <https://business.faktura.ru/f2b/faq?article=2-1>
2. Скачайте программное обеспечение для Windows 7, 8, 10.
3. Запустите файл мастера настройки «InternetBankSetup.exe».
4. Следуйте дальнейшим указаниям в окне установки.
5. Нажмите «Завершить» по завершении установки.
6. Если для работы используется браузер Google Chrome – дополнительно установите расширение.

Получение личного сертификата безопасности для работы в системе интернет-банк «Faktura»

ВНИМАНИЕ!!! Все нижеописанные действия необходимо выполнять с использованием браузера (интернет-обозревателя) Internet Explorer 11 или Google Chrome

Шаг 1. Установить считыватель со смарт-картой в USB-порт рабочей станции (компьютера).

Шаг 2. Начать процедуру создания личного сертификата, ввести (скопировать) ссылку в адресную строку браузера:

<https://ca.faktura.ru/ca/new-certificate?agentId=5162>

Получение сертификата

С посещением банка

Подайте заявление в банк лично и получите сертификат:

1. Заполните заявление.
2. Распечатайте и подпишите заявление.
3. Посетите банк, чтобы подтвердить личность и подать заявление в бумажном виде.
4. Сохраните сертификат.

Заполнить заявление

После нажатия кнопки «Заполнить заявление» появится регистрационная форма (рисунок 1).

Шаг 3. Заполнить регистрационную форму (рисунок 1): указать устройство хранения сертификата - **Смарт-ключ (ГОСТ)**, нажать кнопку «Подтвердить». Система предложит ввести секретный PIN-код (рисунок 2).

ВНИМАНИЕ!!! PIN-код пользователь придумывает и вводит самостоятельно, его необходимо запомнить и не сообщать сторонним лицам.

https://ca.faktura.ru/ca/app/v1/ru x +

ca.faktura.ru/ca/app/v1/new-certificate?0&agentId=5162

Заявление на получение сертификата

Место хранения сертификата
Смарт-ключ (ГОСТ)

Убедитесь что смарт-ключ подключен!

Фамилия Имя

Отчество

Я получаю сертификат как юридическое лицо

Если вы ИП - получайте сертификат физического лица.

ИНН / КИО организации

Наименование организации

Документ, на основании которого действую

Необходимо указать наименование, номер и дату документа, на основании которого действует уполномоченное лицо (устав, доверенность и тп)

Страна Город

E-mail Телефон

На указанный e-mail придёт ссылка для сохранения сертификата и будут приходить уведомления об истечении срока действия сертификата

Далее

Рисунок 1



Рисунок 2

ВНИМАНИЕ!!! В случае использования смарт-ключа Рутокен-ЭЦП (красный ключ с надписью Faktura.ru) по умолчанию установлен пароль пользователя –«12345678», пароль администратора – «87654321»

Шаг 4. Далее необходимо задать код разблокирования (нужен в случае троекратного ошибочного ввода PIN-кода) (рисунок 3).

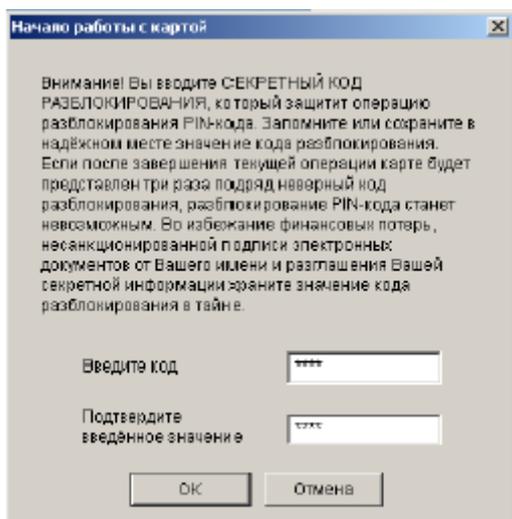


Рисунок 3

ВНИМАНИЕ!!! В случае троекратного неверного ввода секретного кода (PIN-кода) смарт-карта блокируется. Разблокировка производится с помощью кода разблокирования. В случае троекратного неверного ввода кода разблокирования смарт-карта более не может быть использована в дальнейшем.

Шаг 5. После создания PIN-кода и кода разблокирования система повторно запросит PIN-код (Рисунок 4)

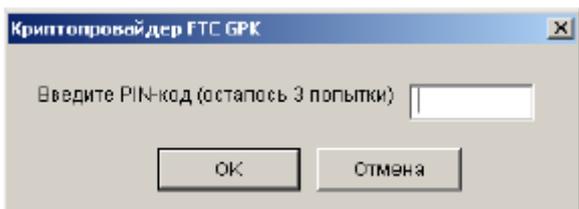


Рисунок 4

Шаг 5.1 При первом обращении к Рутокену система предложит вам сменить PIN-код пользователя нажимайте **ОК**

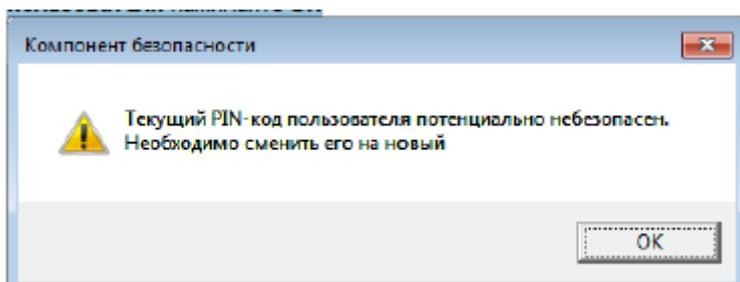


Рисунок 5

PIN-код пользователя по умолчанию (старый) «12345678» новый PIN-код должен содержать **не менее 6 и не более 8 символов**

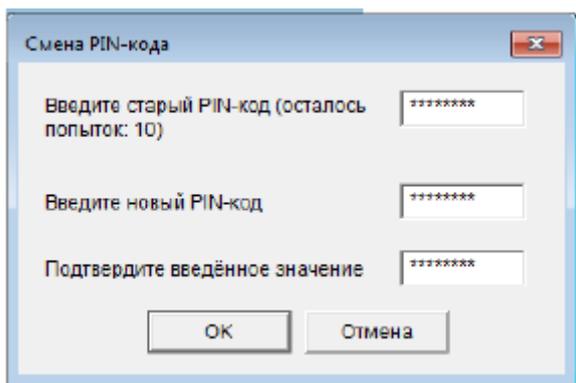


Рисунок 6

Шаг 5.2 Смена PIN-кода Администратора (будет вам необходим в случае блокировки PIN-кода пользователя). PIN-код Администратора по умолчанию (старый) «87654321» новый PIN-код должен содержать **не менее 6 и не более 8 символов**

Шаг 5.3 Система попросит ввести PIN-код пользователя (который вы придумали)

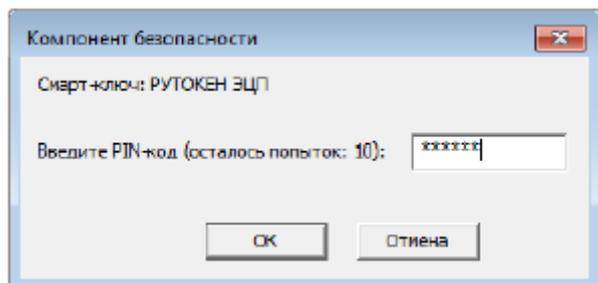


Рисунок 7

Шаг 6. Проверить правильность введенных данных, представленных латинскими буквами. В таком виде данные владельца сертификата хранятся в системе и в самом сертификате (рисунок 15).

Проверьте написание Ваших данных латинскими буквами

Ваше полное имя (Ф.И.О.)	<input type="text" value="Bogomolov Evgenij Nikolaevich"/>	Наименование организации	<input type="text" value="RNKO R-INKAS OOO"/>
ИНН/КИО	<input type="text" value="7707377237"/>		
Страна	<input type="text" value="RU"/>	Город	<input type="text" value="Moskva"/>

Ваши контактные данные

Следующие поля не используются при регистрации сертификата, но используются как дополнительная информация о Вас при подписи сертификата

Адрес	<input type="text" value="127051 Москва Малый Каретный переулок д.8"/>	Телефон	<input type="text" value="+7(495)393-48-98"/>
E-mail	<input type="text" value="ben1@rinkas.ru"/>		

[Назад](#)

[Отправить запрос](#)

Рисунок 8

Шаг 7. Отправить данные в Удостоверяющий центр: кнопка «Отправить запрос».

Внимание!!! В случае если идентификаторы запроса на сертификат дублируют существующую запись в базе, система сгенерирует ошибку (рисунок 9). Необходимо внести изменения в запрос на сертификат (например, изменить ФИО: добавить символ или заменить имеющийся – Ivanov Ivan Ivanovichh).

Ошибка!

В системе уже есть запрос на сертификат с такими данными. Для получения сертификата измените данные в форме запроса.

[Получите сертификата](#)

Рисунок 9

Шаг 8. После успешного отправления запроса необходимо перейти по ссылке (рисунок 10) для печати заявления на получение сертификата для юридических лиц.

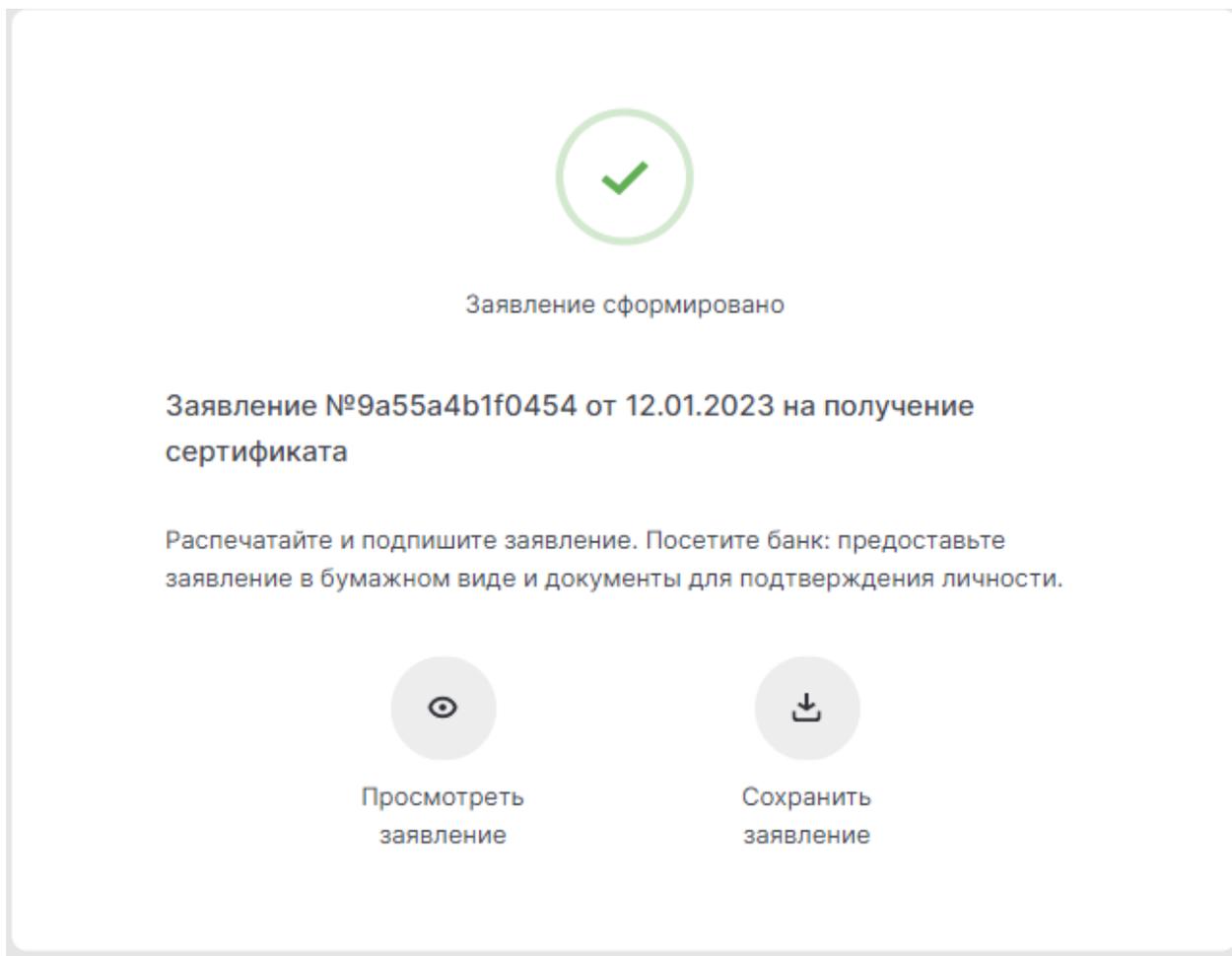


Рисунок 10

Шаг 9. Ввести ФИО заявителя (пользователя сертификата) (рисунок 11 п.1).

Шаг 10. Ввести наименование организации (рисунок 11 п.2).

Шаг 11. Ввести повторно ФИО заявителя (пользователя сертификата) (рисунок 11 п.3).

Печать заявления - Chromium-Gost

ca.faktura.ru/ca/docs?lang=ru&document=application&id=2715082016359508&class=2&email=ben1@r-inkas.ru&phone=79687830399&client=Тестов+...

Агенту Удостоверяющего центра «AUTHORITY»
РНКО "Р-ИНКАС" (ООО)
/ в Удостоверяющий центр «AUTHORITY»

Заявление на выдачу Сертификата ключа проверки электронной подписи

Прошу Удостоверяющий центр «AUTHORITY» создать и выдать уполномоченному лицу организации ООО "Тестовая компания" (наименование организации), действующ(-ему)(-ей) на основании _____, Сертификат ключа проверки электронной подписи (Класс 2 Сертификата) с параметром Идентификатора владельца сертификата: CN=Testov Test Testovich, OU=UTC 185A5B0B76D, O=ООО "Тестовая компания", L=Moskva, C=RU (ФИО \ псевдоним уполномоченного лица организации / наименование \ псевдоним организации). Уникальный номер запроса: 9a55a4b1f0454.

С Правилами Электронного документооборота корпоративной информационной Системы «BeSafe» (далее – «Система «BeSafe»»), которые размещены в сети Интернет на сайте www.besafe.ru ознакомлены, согласны и обязуемся соблюдать и выполнять.

Признаю, что получение документа, подписанного Электронной подписью Участника Системы «BeSafe» (далее – «Участник») юридически эквивалентно получению документа на бумажном носителе, подписанного собственноручными подписями уполномоченных лиц Участника и заверенного печатью Участника, если документ на бумажном носителе должен быть заверен печатью. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Ключ электронной подписи, Электронная подпись и Сертификат ключа проверки электронной подписи Участника созданы и используются в соответствии с Правилами работы Удостоверяющего центра «AUTHORITY».

Реквизиты Клиента:

ФИО уполномоченного лица организации	Тестов Тест Тестович
Наименование организации	ООО "Тестовая компания"
Контактный телефон	79687830399
E-mail	ben1@r-inkas.ru

Настоящим соглашаюсь с обработкой своих персональных данных, в том числе с использованием технических средств, Закрытым акционерным обществом «Центр Цифровых сертификатов», а также Агентом (Доверенным лицом) Удостоверяющего центра «AUTHORITY».

Признаю, что мои персональные данные, включенные в Сертификат, будут внесены Удостоверяющим центром в реестр Сертификатов. Реестр Сертификатов доступен в сети Интернет на сайте www.authority.ru.

Понимаю, что Удостоверяющий центр обрабатывает мои персональные данные, включенные в Сертификат и размещенные в реестре Сертификатов, для выполнения обязанностей по ведению реестра Сертификатов, включению содержащихся в Сертификатах персональных данных в реестр Сертификатов и обеспечению доступа лиц к информации, содержащейся в реестре Сертификатов с использованием сети Интернет, которые возложены на Удостоверяющий центр частью 2 статьи 13 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Понимаю, что в соответствии с пунктом 2 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» выполнение Удостоверяющим центром обязанностей, возложенных на него частью 2 статьи 13 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», является правовым основанием обработки моих персональных данных, включенных в Сертификат.

принято Агентом Удостоверяющего центра/ Удостоверяющим центром:

<u>РНКО "Р-ИНКАС" (ООО)</u>	(полное наименование)	_____	(подпись уполномоченного лица организации)
_____	(дата)	_____	(Ф.И.О. уполномоченного лица организации)
_____	(подпись уполномоченного лица)	Тестов Тест Тестович	
_____	(ФИО уполномоченного лица)		

М.П. М.П. (если применимо)

Рисунок 11

Шаг 12. Распечатать заявление в двух экземплярах: кнопка «Распечатать», далее поставить подпись и печать организации. Готовое заявление предоставить операционному работнику Банка. При себе иметь документ, удостоверяющий личность.

Сохранение личного сертификата безопасности на смарт-карту.

Внимание!!! После того, как вы принесете подписанный запроса в Банк, на указанный Вами в запросе на выдачу сертификата электронный адрес придет ссылка (примерное содержимое на рисунке 12).

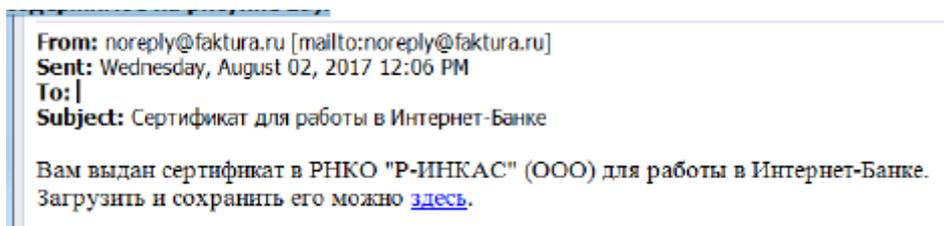


Рисунок 12

Внимание!!! Все нижеописанные действия необходимо выполнять с использованием браузера (интернет-обозревателя) Internet Explorer.

Шаг 1. Перейти по полученной ссылке, кликнув левой кнопкой мыши, либо ввести в адресную строку браузера методом «копировать-вставить».

Шаг 2. Распечатать Акт приема-передачи сертификата открытого ключа, кликнув по ссылке в появившемся окне (рисунок 13).

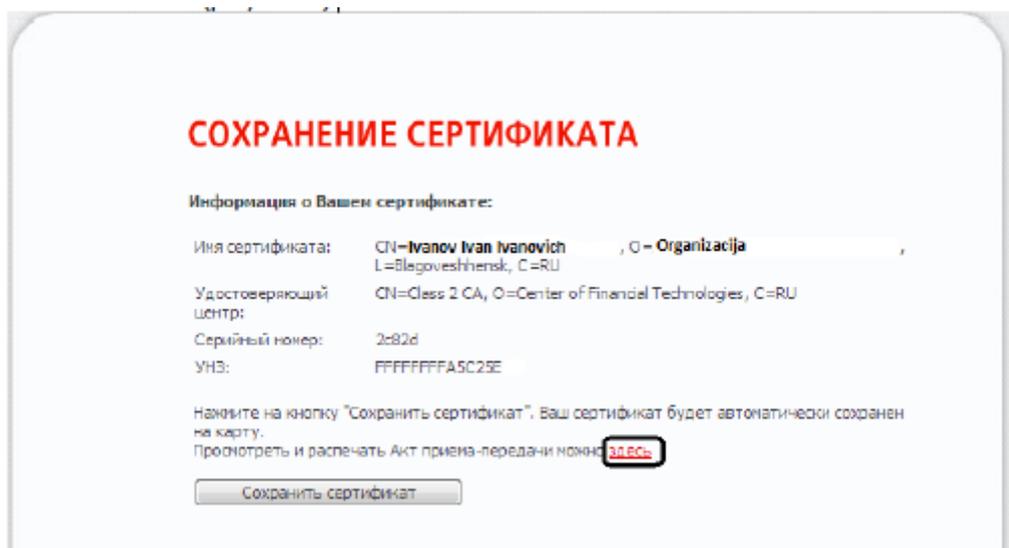


Рисунок 13

Шаг 3. Установить считыватель со смарт-картой в USB-порт рабочей станции (компьютера).

Шаг 4. Сохранить сертификат на смарт-карту: кнопка «Сохранить сертификат». Система предложит ввести PIN-код для доступа к смарт-карте (рисунок 14).

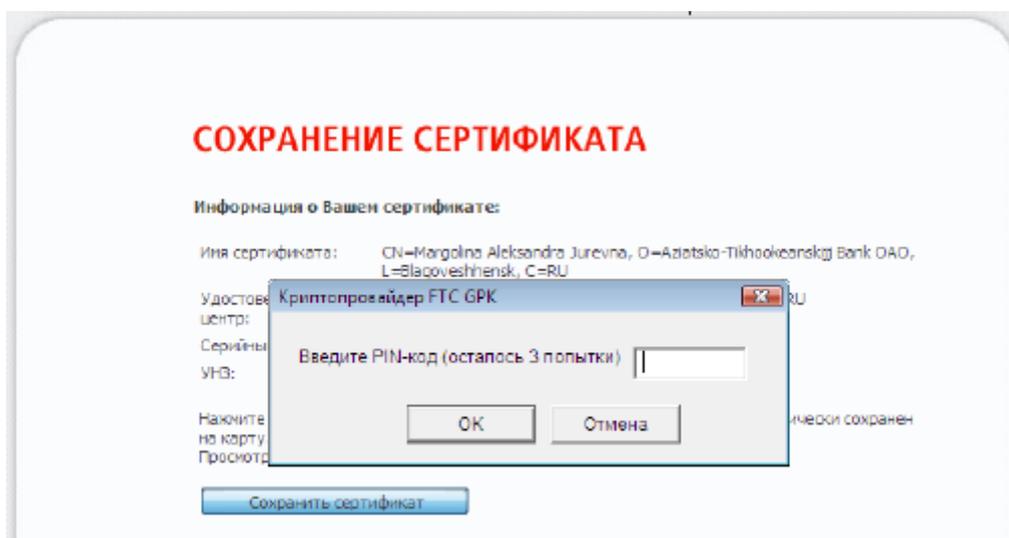


Рисунок 14

Шаг 5. Подтверждаем сохранение сертификата (рисунки 15-16).

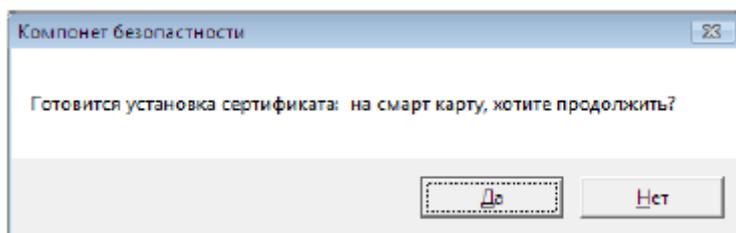


Рисунок 15

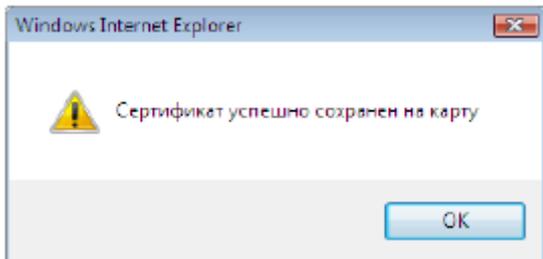


Рисунок 16

Шаг 6. Подписанный Акт приема-передачи сертификата необходимо передать операционному работнику РНКО. На основании данного акта наши сотрудники подключат ваш сертификат (свяжут сертификат и ваш счет).

ВНИМАНИЕ!!! После получения сертификата компьютер готов для работы в системе интернет-банк «Faktura», ярлык для запуска рабочего места находится на рабочем столе.