1. *Выполнение первого входа в систему.*

Для входа в систему запустите Интернет-клиент с помощью ярлыка на рабочем столе, либо перейдите в Internet Explorer по адресу https://bc.rshb.ru (Рисунок 1).

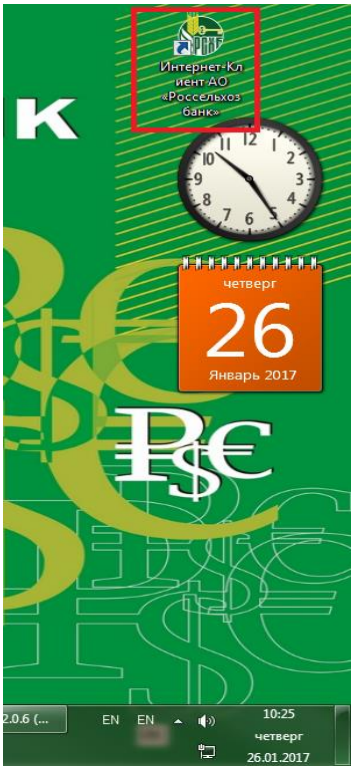

Рисунок 1. Ярлык Системы "Интернет-Клиент" на рабочем столе.

При входе появится окно ввода логина и пароля (Рисунок 2).

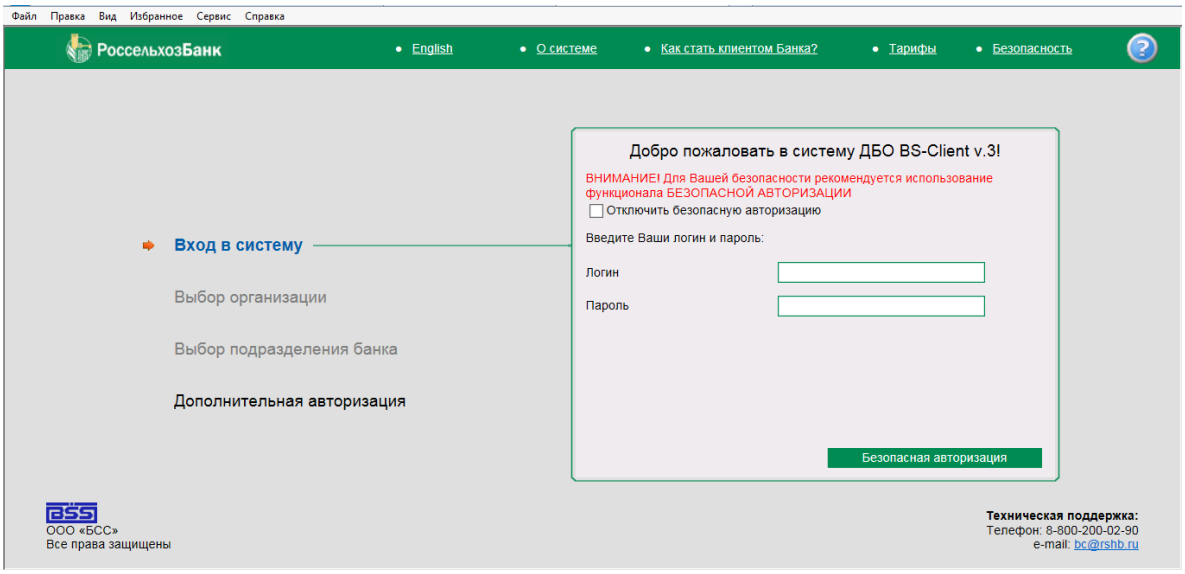

Рисунок 2. Вход в Систему "Интернет-Клиент".

Введите логин и пароль для входа в систему «Интернет-Клиент». Логин и пароль указаны на бумажном носителе, выданном Вам в отделении Банка.

Вы можете использовать безопасную авторизацию с использованием виртуальной клавиатуры. Для этого нажмите кнопку «Безопасная авторизация». Откроется окно виртуальной клавиатуры, в котором последовательно необходимо набрать логин и пароль (Рисунок 3).

Рисунок 3. Безопасная авторизация.

Также Вы можете использовать для ввода логина и пароля обычную клавиатуру. Для этого установите флажок «Отключить безопасную авторизацию», введите логин и пароль и нажмите кнопку «Далее» (Рисунок 4).

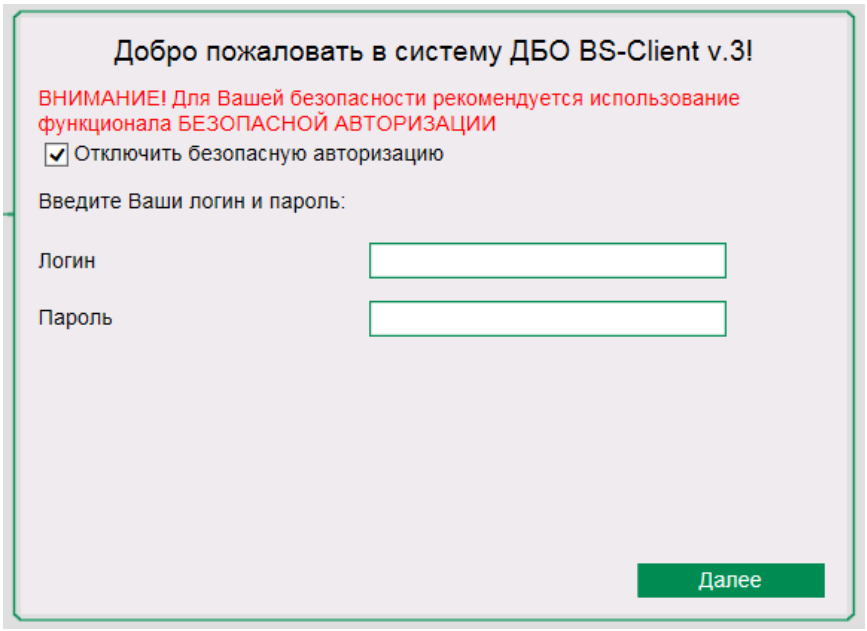

Рисунок 4. Отключение безопасной авторизации.

После ввода логина и пароля будет запрошена установка сертификатов Удостоверяющего Центра (УЦ) Банка (Рисунок 5).

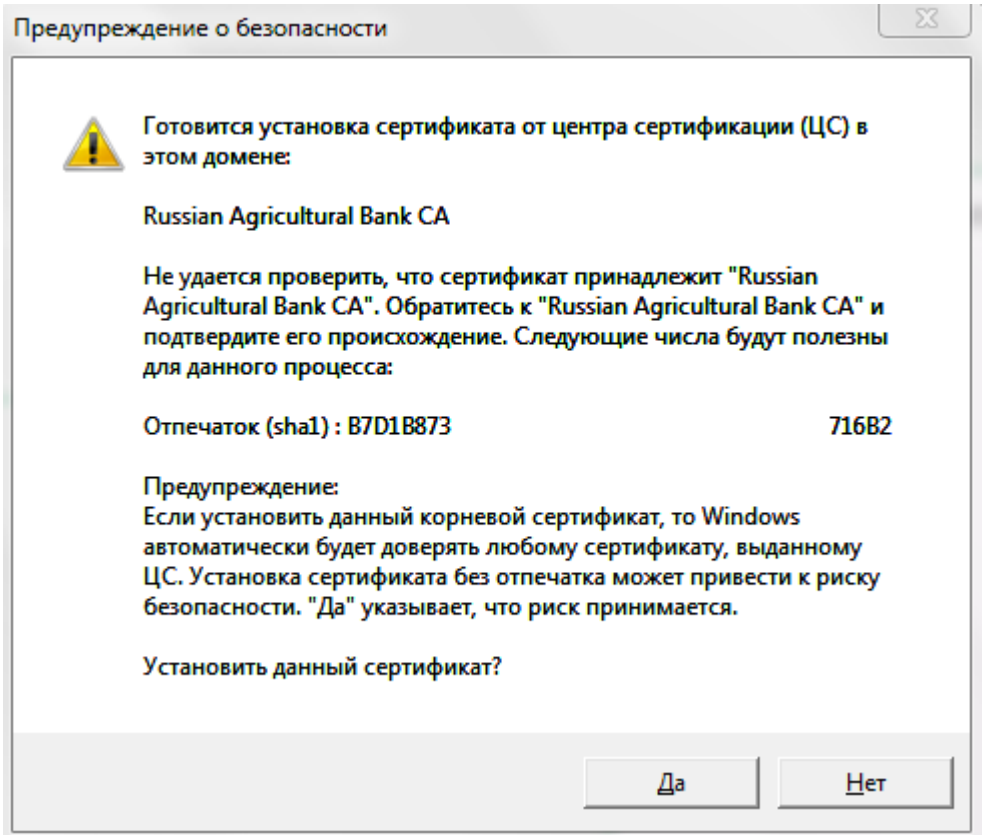

Рисунок 5. Запрос на установку сертификатов УЦ Банка.

ВАЖНО! Подобные окна появятся на Вашем экране 6-7 раз. Для корректной работы Интернет-клиента обязательно соглашайтесь на установку сертификатов УЦ Банка, нажимая «Да».

Далее появится окно выбора абонента для дополнительной авторизации (Рисунок 6).

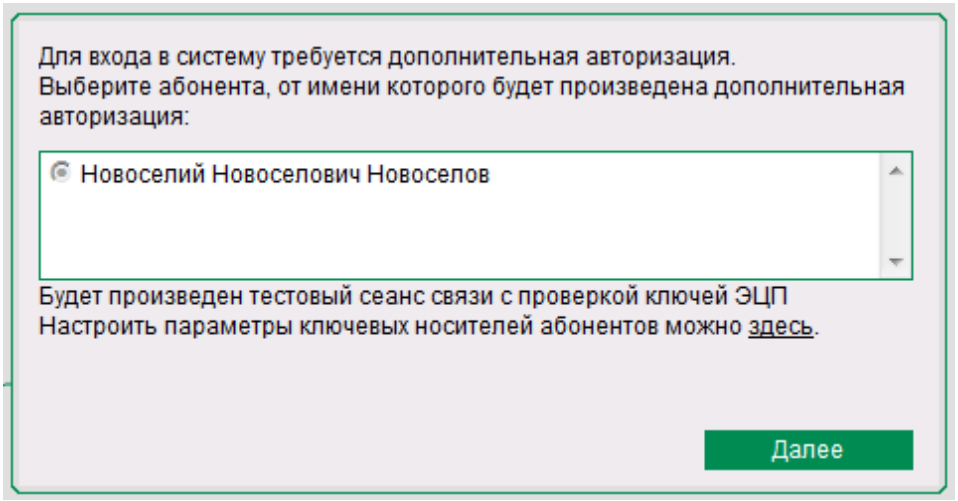

Рисунок 6. Окно дополнительной авторизации.

В этом окне необходимо выбрать абонента, вставить функциональный ключевой носитель eToken, выданный на указанного в окне дополнительной авторизации абонента в USB порт компьютера и нажать кнопку «Далее».

ВАЖНО! После вставки токена в USB-порт, возможно появление окна для смены пароля (PIN-кода) на eToken (Рисунок 7).

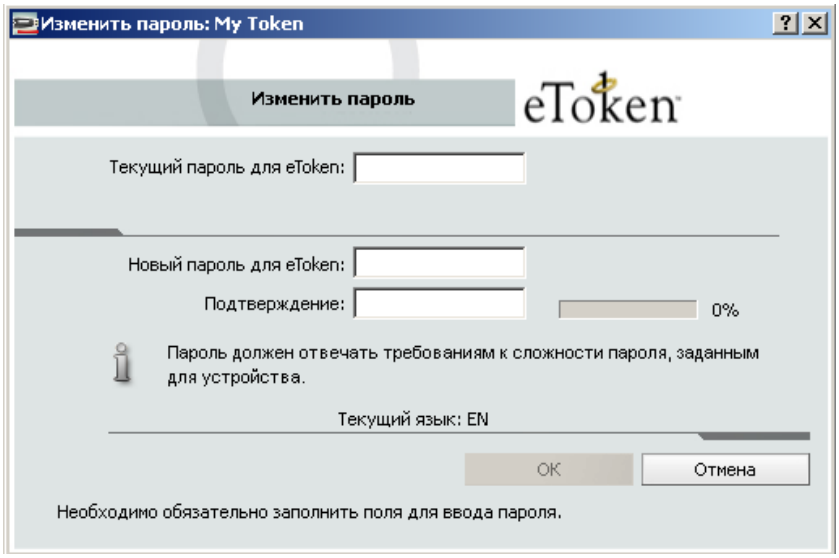

Рисунок 7. Окно смены пароля (PIN-кода) на eToken.

Во время установки системы «Интернет-Клиент» менять PIN-код не нужно, это окно необходимо закрыть, либо нажать кнопку «Отмена». Смену PIN-кода рекомендуется произвести уже после принятия постоянного сертификата (принятие описано в Рисунок 28).

Далее в процессе входа в систему будет запрошен пароль (PIN-код) для контейнера. Необходимо ввести PIN-код (по умолчанию - 1234567890) и нажать «ОК» (Рисунок 8).

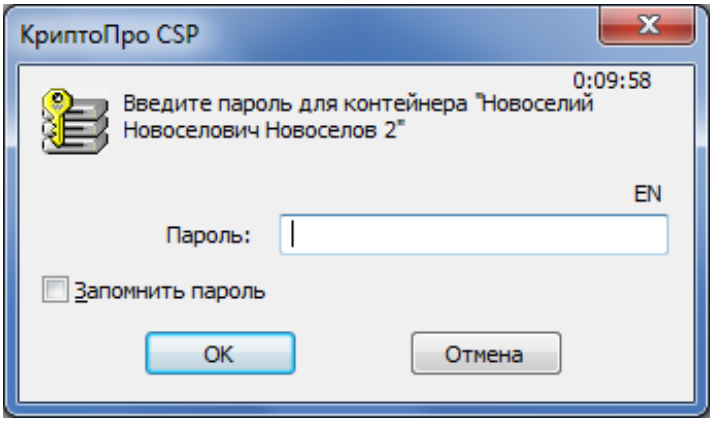

Рисунок 8. Запрос PIN-кода (пароля) на контейнер.

Вводите PIN-код внимательно: после многократного ввода неверного пароля (15 попыток) eToken заблокируется. Единственным выходом после этого будет возврат токена в отделение банка для перевыпуска ключа. Если PIN-код введен неверно, появится окно (Рисунок 9).

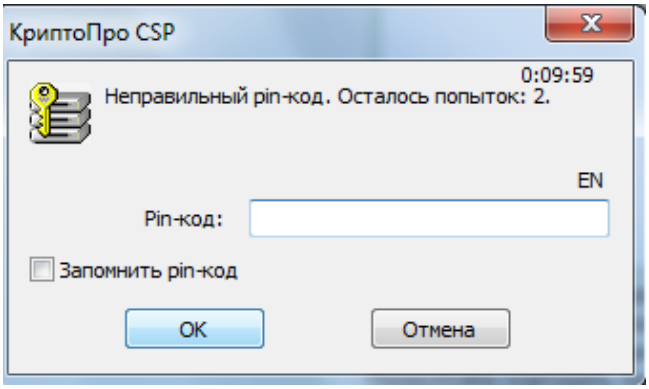

Рисунок 9. Сообщение о неверном пароле.

После корректного ввода PIN-кода откроется главное окно системы «Интернет-Клиент» (Рисунок 10).

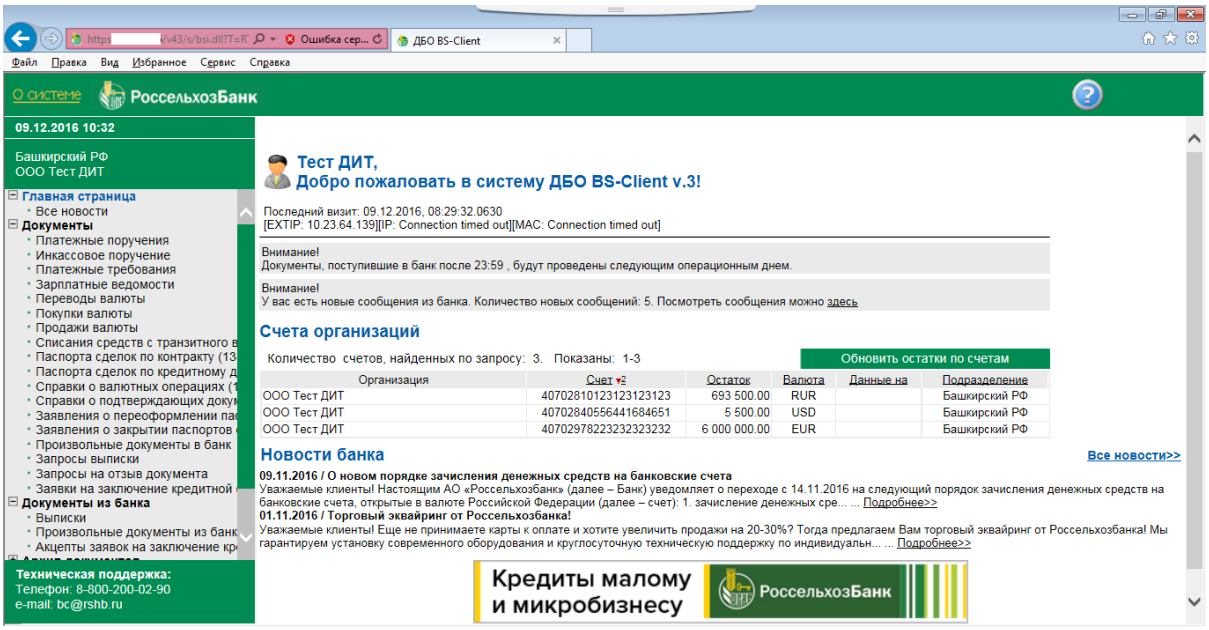

Рисунок 10. Главное окно Системы "Интернет-Клиент".

2. Создание запроса на генерацию.

После установки системы «Интернет-Клиент» в обязательном порядке необходимо перегенерировать комплект ключей. При каждом входе будет выводиться напоминание о необходимости перегенерации. Для продолжения нажмите «Далее» (Рисунок 11).

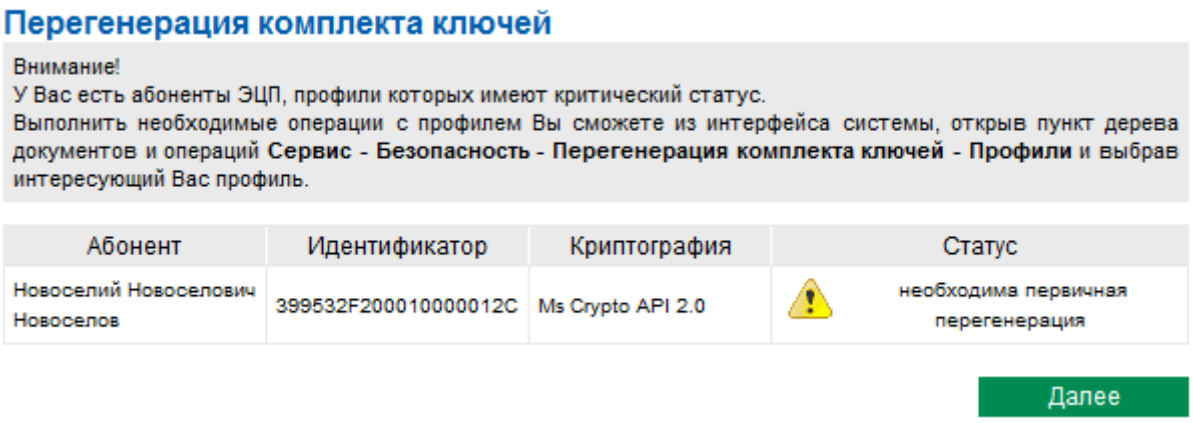

Рисунок 11. Предупреждение о необходимости перегенерации.

ВАЖНО! Во время создания запроса на перегенерацию ключей в USB-порт должен быть установлен eToken только того абонента, которому необходимо произвести перегенерацию.

Для перегенерации ключей зайдите в меню «Сервис – Безопасность – Перегенерация комплекта ключей - Профили» (Рисунок 12).

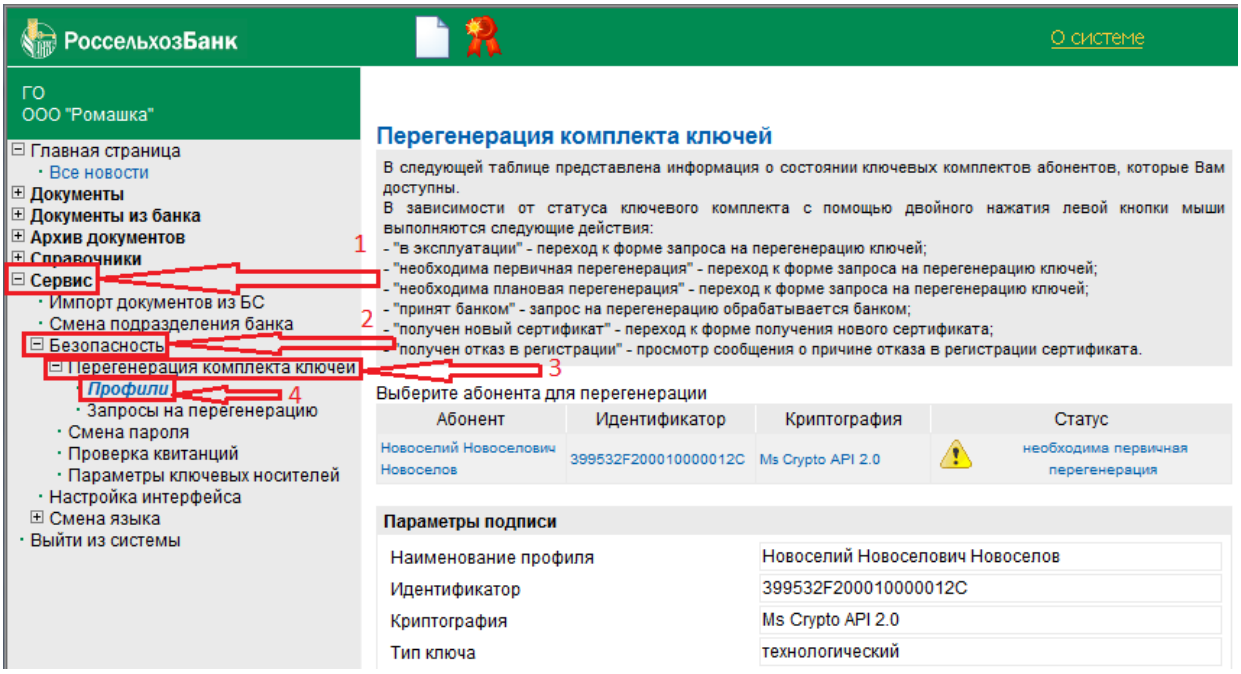

Рисунок 12. Переход к разделу "Профили".

После этого кликните по строке с ФИО абонента, появятся параметры подписи. Далее нажмите на кнопку «Создать запрос» (иконка с белым листом бумаги) (Рисунок 13).

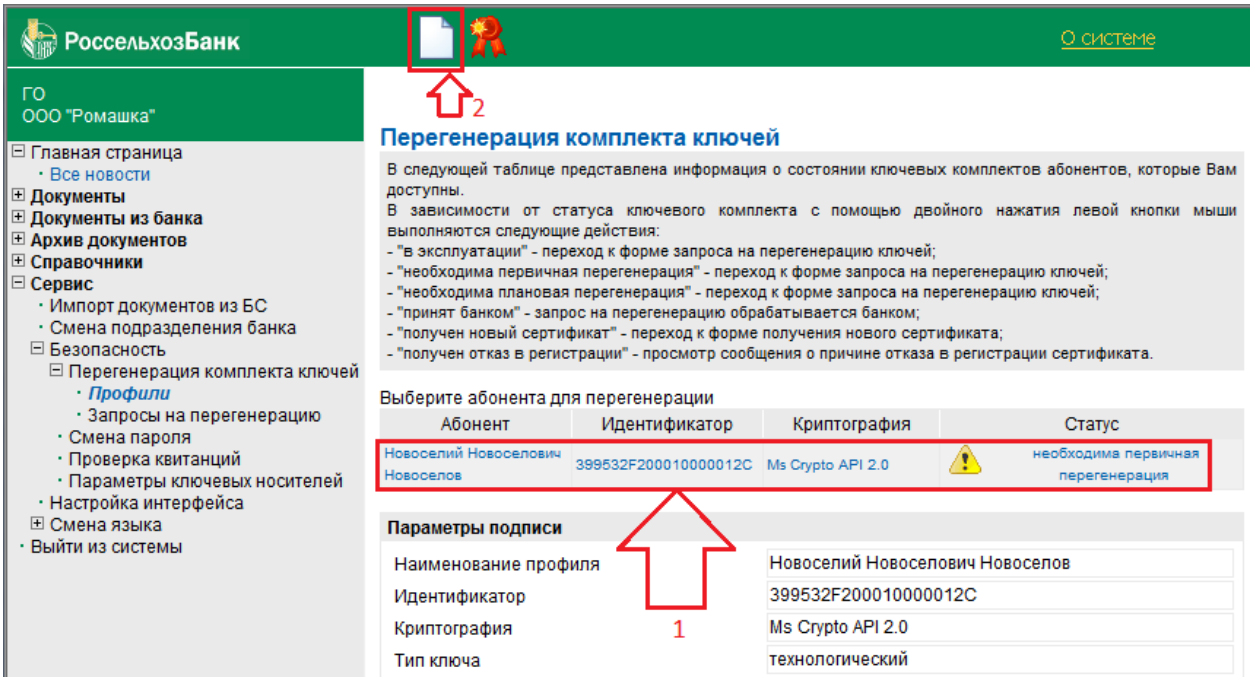

Рисунок 13. Создание нового запроса на генерацию.

Далее откроется окно перегенерации комплекта ключей. Нажмите кнопку отправки документа в Банк (иконка с белым листом и зелёной стрелкой) (Рисунок 14).

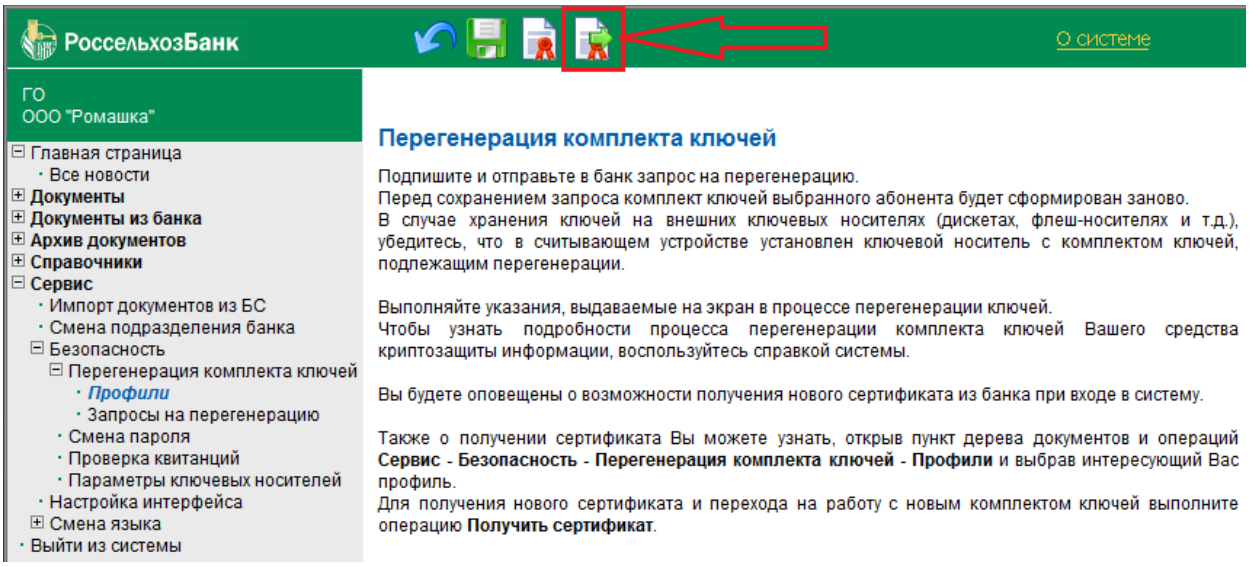

Рисунок 14. Отправка запроса на генерацию в Банк.

Затем откроется окно КриптоПро CSP, где нужно выбрать носитель, куда запишется ключ. В поле «Вставленный носитель» должно быть указано имя токена Etoken_JAVA_XXXXXXXX, где XXXXXXXX – номер токена. Этот номер можно найти в карточке специальных парольных фраз (выдаётся в отделении Банка среди прочей документации). Чаще всего этому носителю соответствуют устройства **Aladdin Token или AKS ifdh**. После выбора устройства нажмите ОК (Рисунок 15).

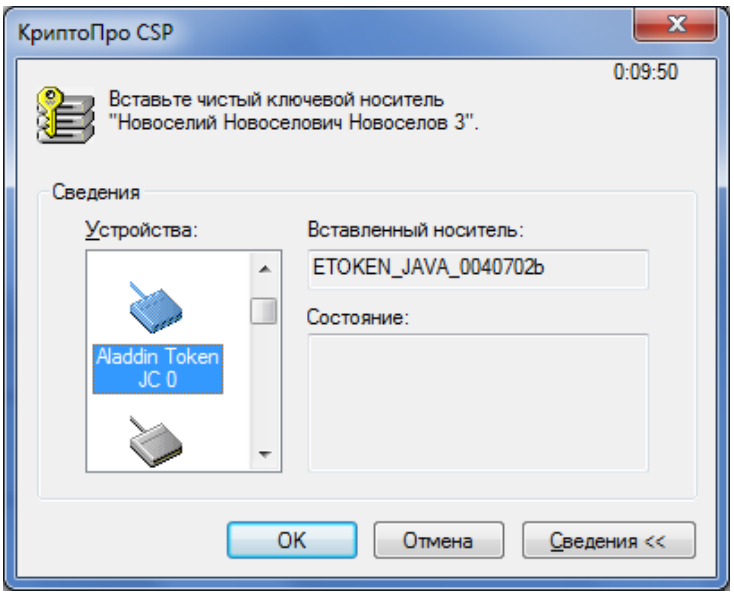

Рисунок 15. Выбор ключевого носителя.

ВАЖНО! Ни в коем случае не выбирайте в списке устройств «Реестр». В случае записи ключа в реестр, он считается скомпрометированным.

После этого произойдёт активация биологического датчика случайных чисел (рис. 35). Перемещайте указатель мыши в пределах этого окна до тех пор, пока не заполнится индикатор. Не закрывайте данное окно самостоятельно (Рисунок 16).

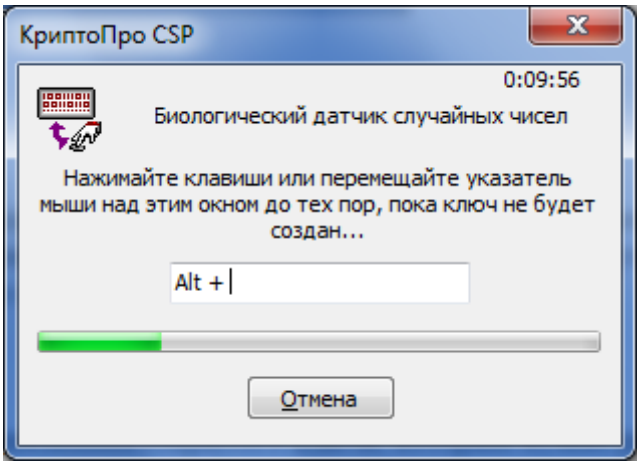

Рисунок 16. Биологический датчик случайных чисел.

После завершения работы датчика случайных чисел введите PIN-код (1234567890) на создаваемый контейнер с новым комплектом ключей (Рисунок 17).

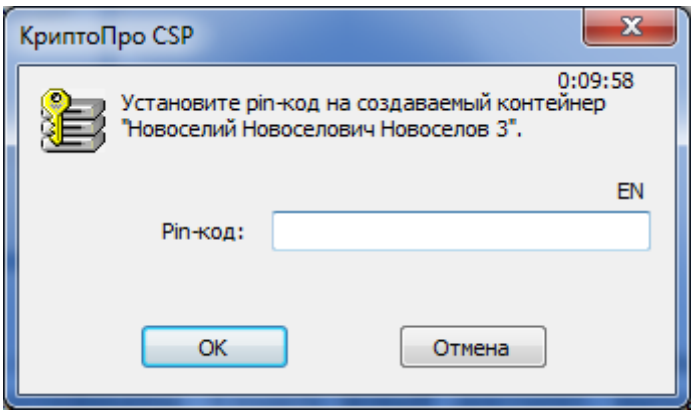

Рисунок 17. Установка PIN-кода на контейнер.

В следующем окне подпишите запрос на сертификат, нажав на «Подписать» (Рисунок 18).

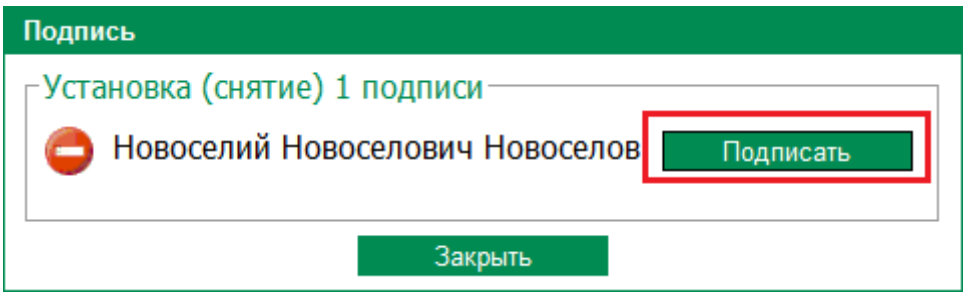

Рисунок 18. Подписание запроса на генерацию.

Будет выведен запрос на новый сертификат ключа проверки электронной подписи. Его необходимо распечатать в двух экземплярах, подписать в бумажном виде и предоставить в отделение Банка. Для печати запроса нажмите кнопку «Печать» (Рисунок 19).

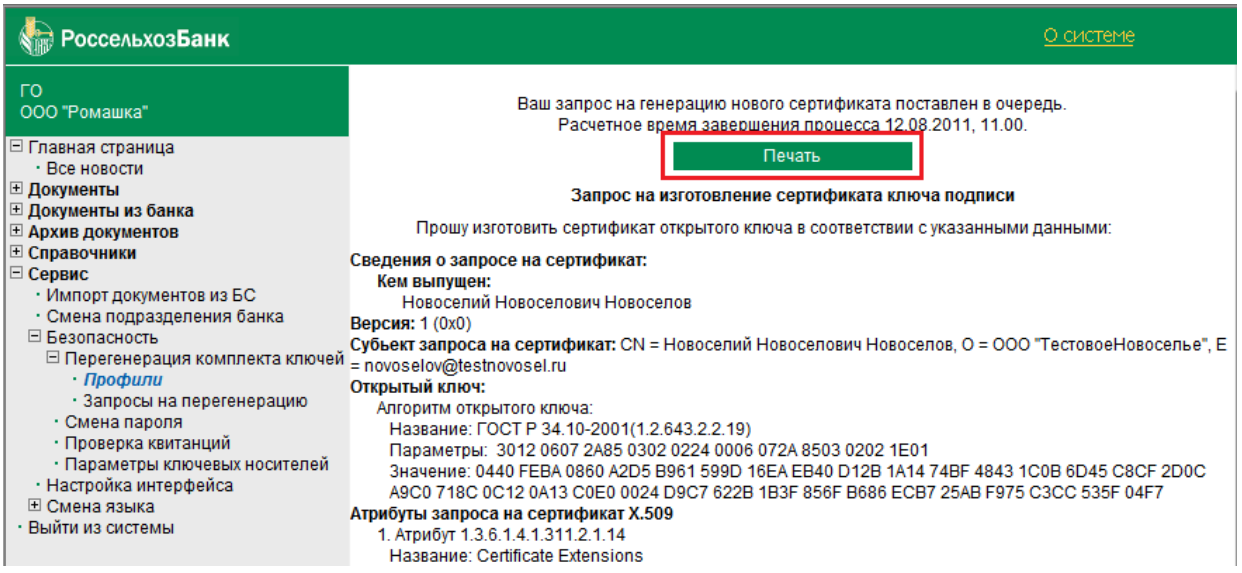

Рисунок 19. Печать запроса на генерацию.

Если в данный момент распечатать запрос не представляется возможным (например, к компьютеру не подключен принтер), это можно сделать позже. Для этого в меню «Профили» нажмите кнопку «Акт признания сертификата» (белый лист с лупой и красным бантом) (Рисунок 20).

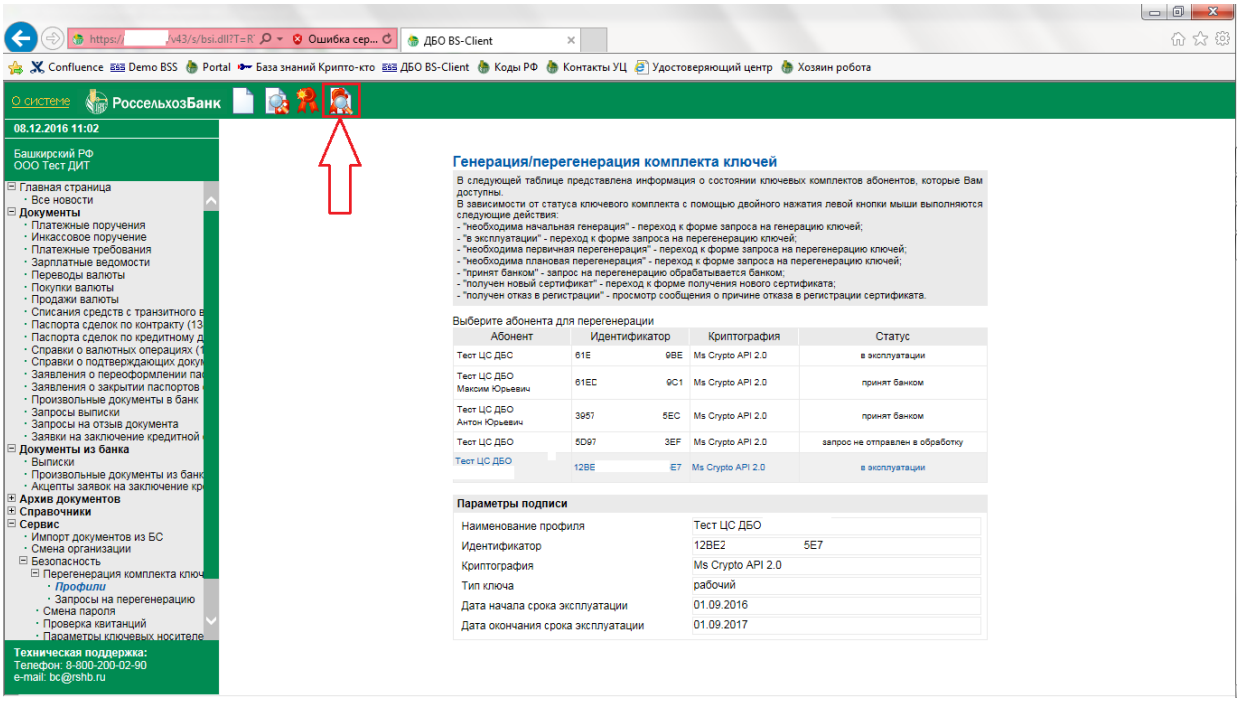

Рисунок 20. Просмотр акта признания.

Кроме того, возможно сохранить печатную форму запроса в файл. Перенеся его на компьютер с подключенным принтером, Вы сможете распечатать запрос.

Нажмите кнопку «Печать» (Рисунок 21).

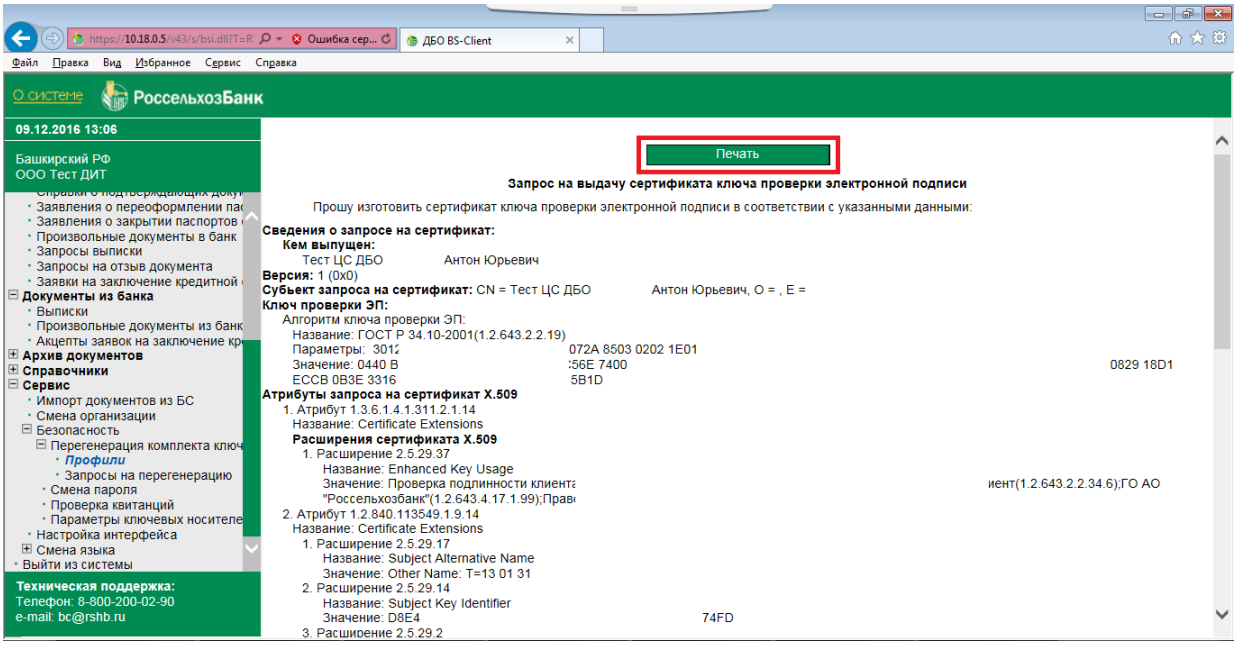

Рисунок 21. Печать акта признания.

Откроется окно выбора принтера. Необходимо найти виртуальный принтер Microsoft XPS Document Writer и нажать кнопку «Печать» (Рисунок 22).

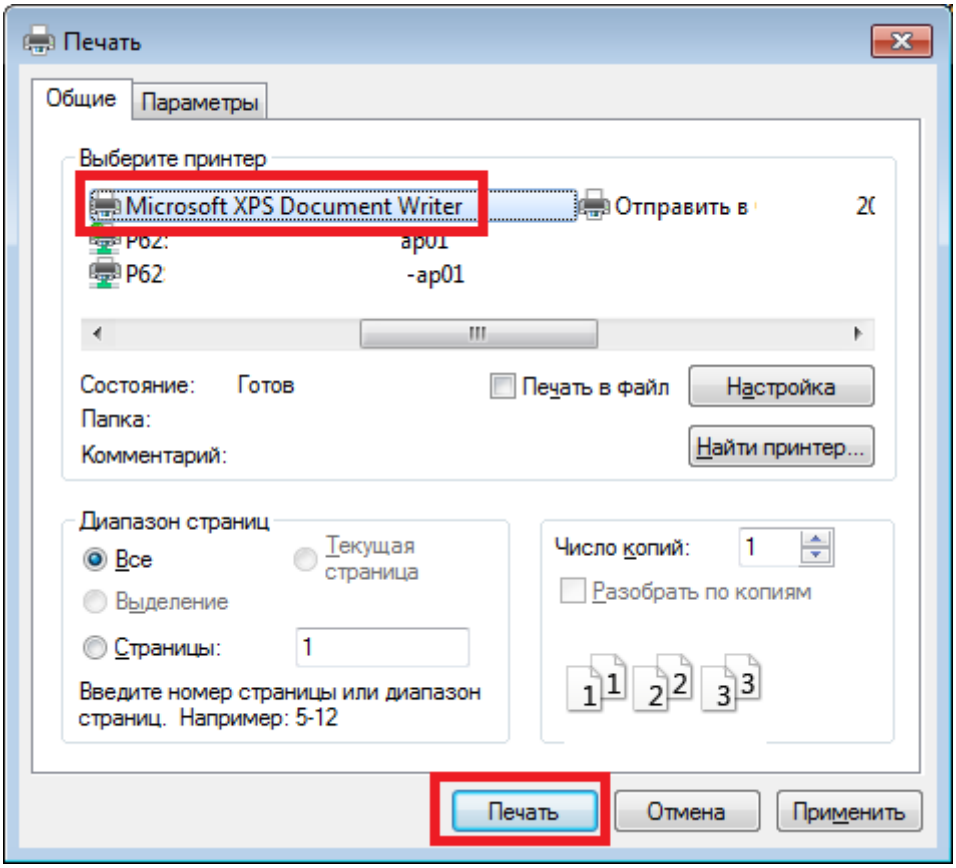

Рисунок 22. Выбор виртуального принтера.

В следующем окне укажите папку для сохранения файла, задайте ему произвольное имя и нажмите «Сохранить» (Рисунок 23).

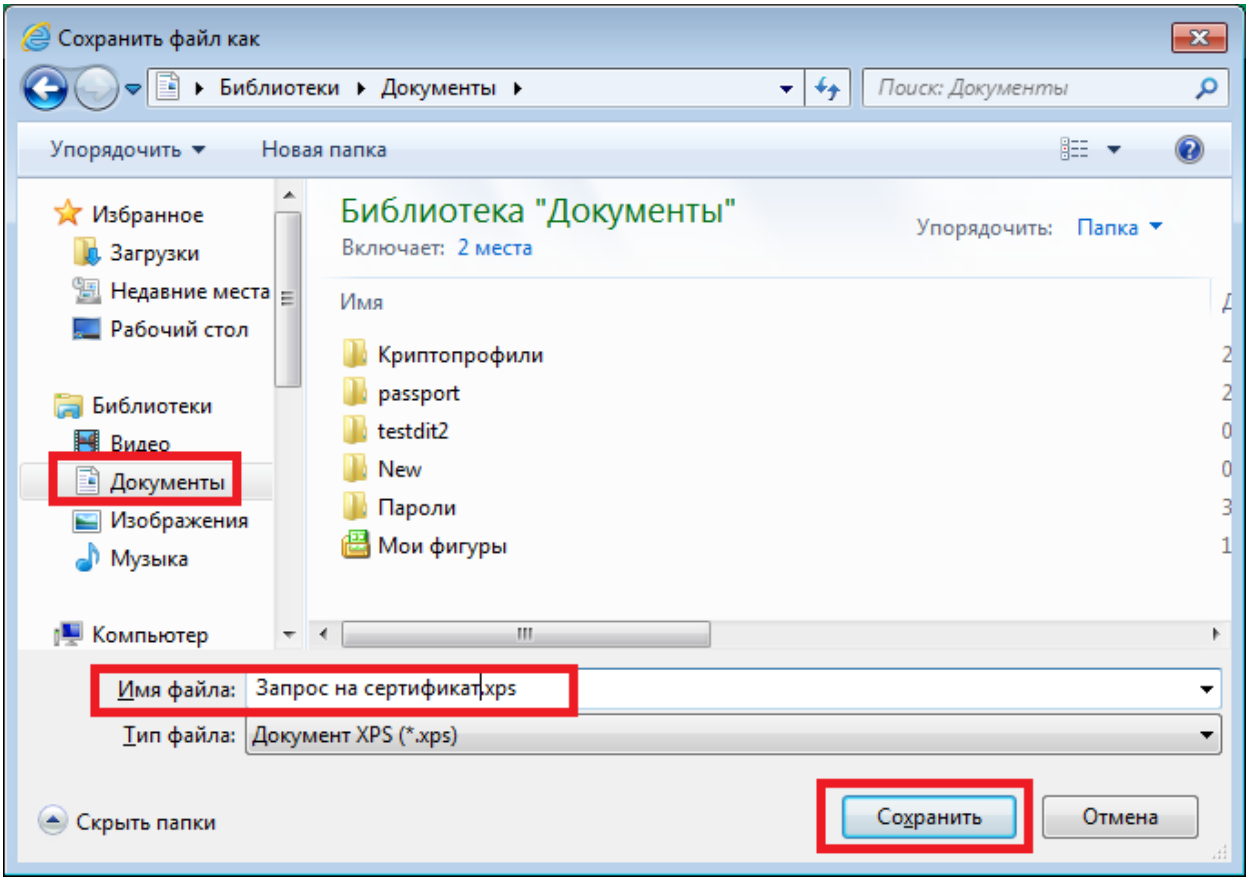

Рисунок 23. Сохранение печатной формы в файл.

Перенесите этот файл на компьютер с подключенным и установленным принтером. Откройте его. Выберите пункт меню «Файл», далее «Печать» (Рисунок 24).

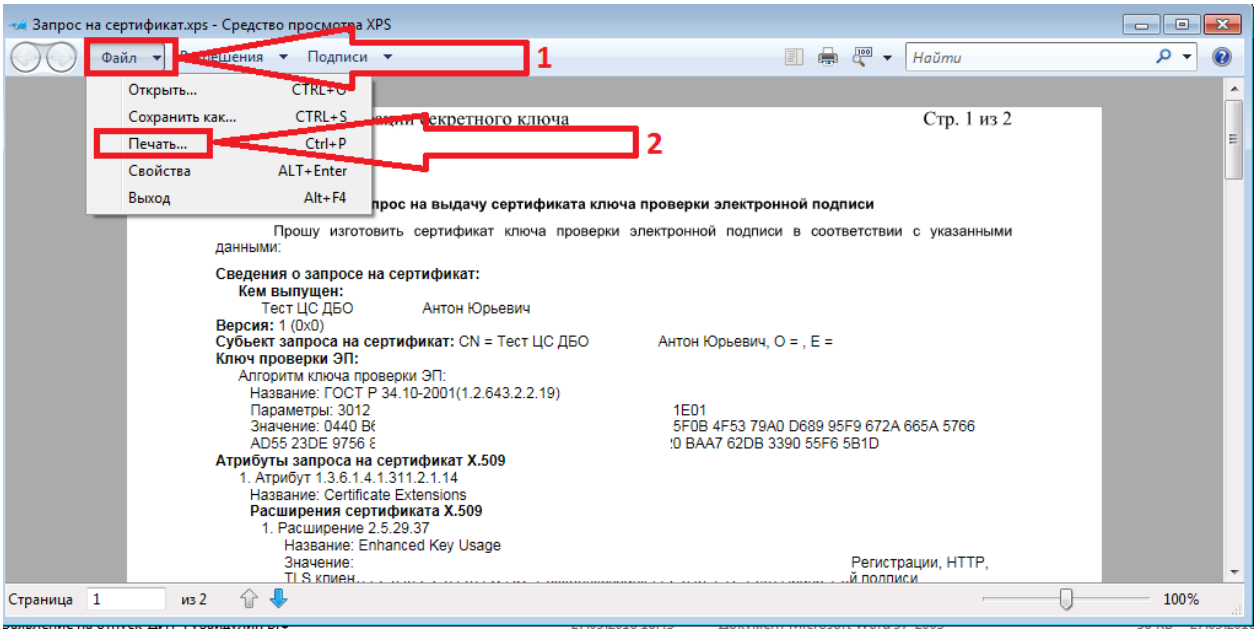

Рисунок 24. Печать из сохранённого файл.

ВАЖНО! После отправки запроса обязательно проверьте статус Вашего запроса на сертификат.

Перейдите в раздел «Сервис-Безопасность-Перегенерация комплекта ключей-Запросы на перегенерацию» (Рисунок 25).

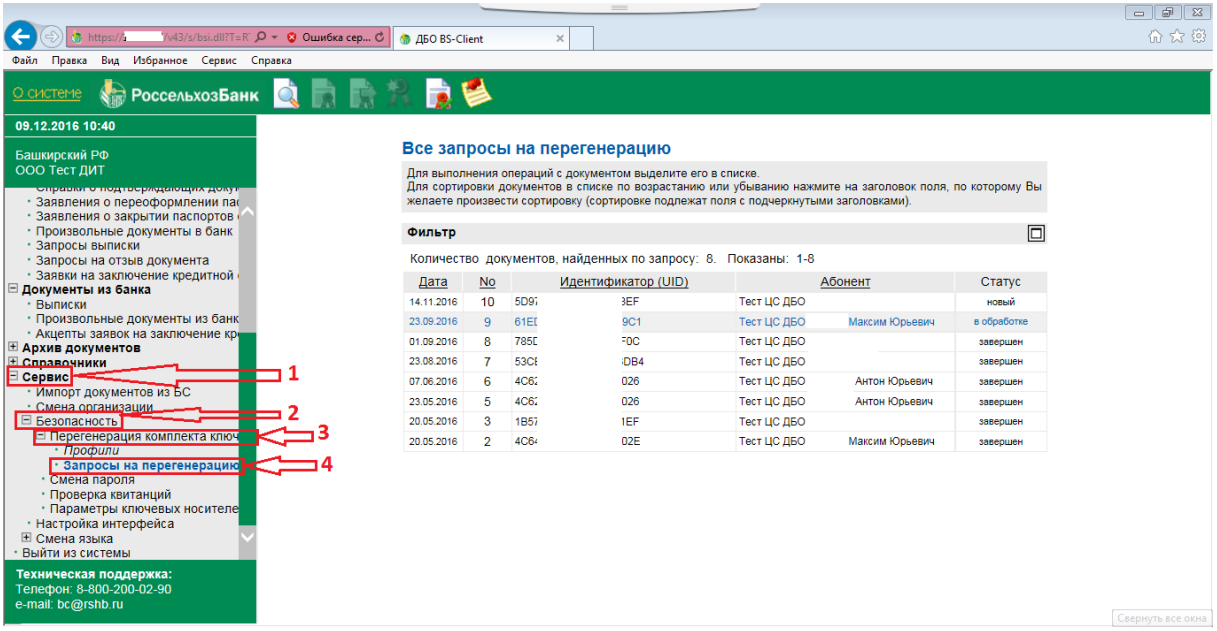

Рисунок 25. Переход к разделу "Запросы на перегенерацию".

В таблице справа Вы обнаружите Ваш запрос на сертификат, датированный днём его создания. При успешной отправке статус должен быть «Отправлен», либо «В обработке» (Рисунок 26).

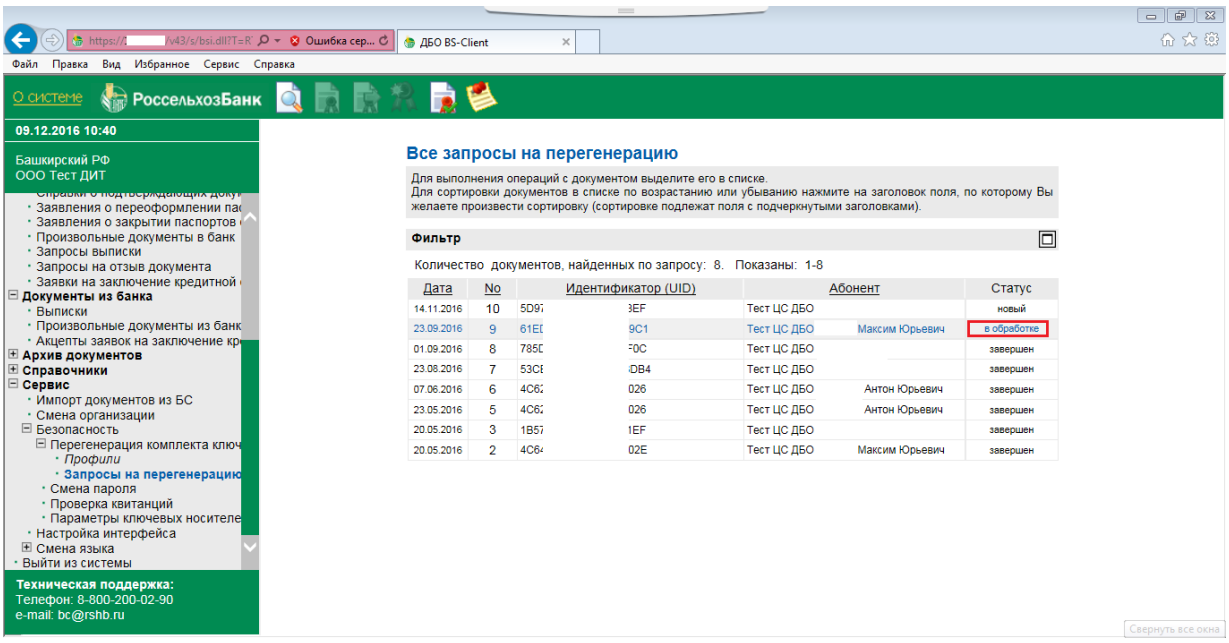

Рисунок 26. Статус запроса на генерацию.

ВАЖНО! Если статус у запроса «Подписан», либо «Новый», это означает, что в Банк он не был отправлен.

Для отправки выделите запрос в таблице, щёлкнув по нему. Далее нажмите кнопку «Отправить документ в Банк» (Рисунок 27).

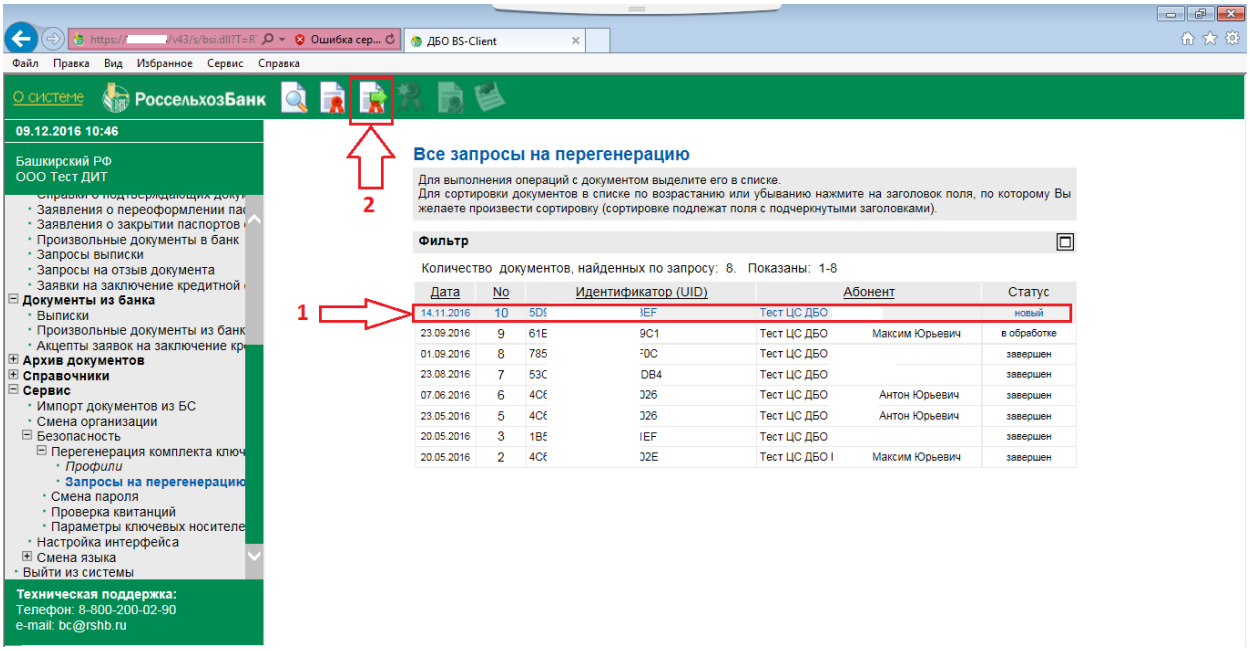

Рисунок 27. Отправка сохраненного запроса на генерацию.

3. Принятие выпущенного сертификата.

После отправки запроса электронным способом и предоставления запроса на бумажном носителе в Банк необходимо ожидать 2-3 рабочих дня.

ВАЖНО! При очередном входе в Интернет-клиент появится оповещение о выпуске нового сертификата. Его в обязательном порядке нужно принять. В противном случае сертификат не вступит в силу.

Для принятия нового сертификата ключа проверки электронной подписи необходимо выбрать «Сервис» - «Безопасность» - «Перегенерация комплекта ключей» - «Профили».

В открывшемся окне выбрать ФИО абонента, для которого осуществлялась перегенерация комплекта ключей, и нажать «Получить сертификат (ключ)» (иконка с изображением красного банта) (Рисунок 28).

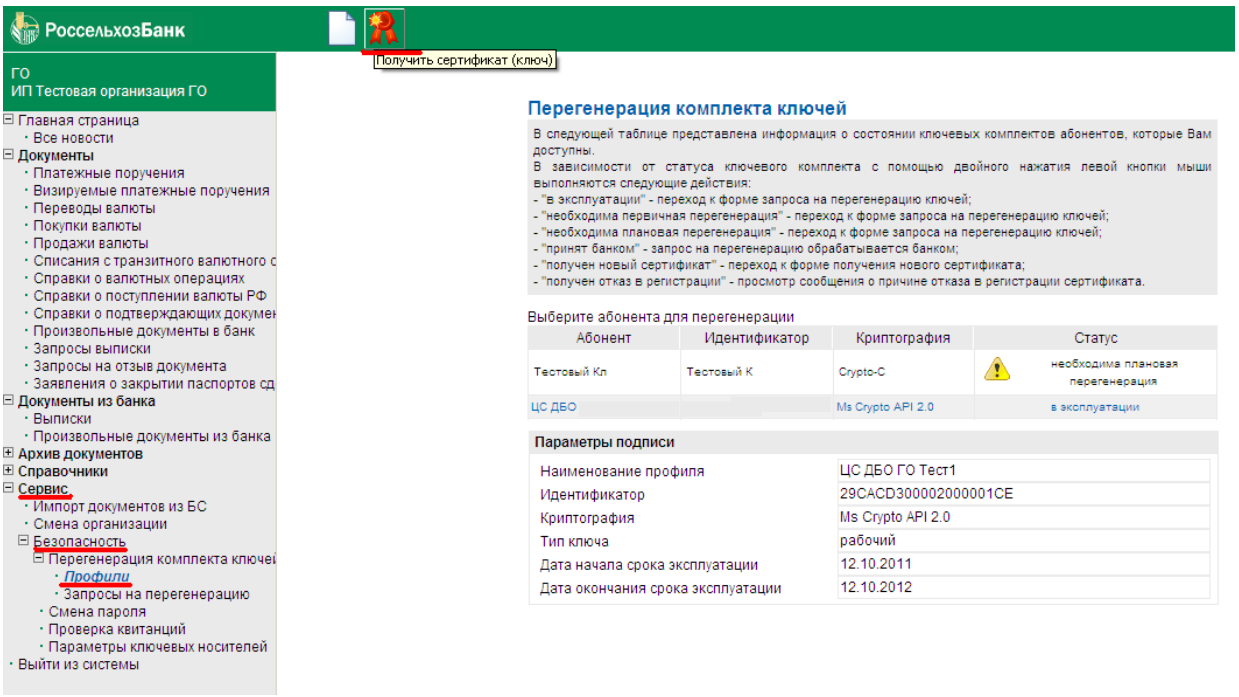

Рисунок 28. Получение выпущенного сертификата.

По окончании процедуры появится сообщение «Вы переведены на работу с новым комплектом ключей». Только после этого сертификат считается принятым и вступает в действие.

Если сертификат получен успешно, абонент примет статус «В эксплуатации» (Рисунок 29).

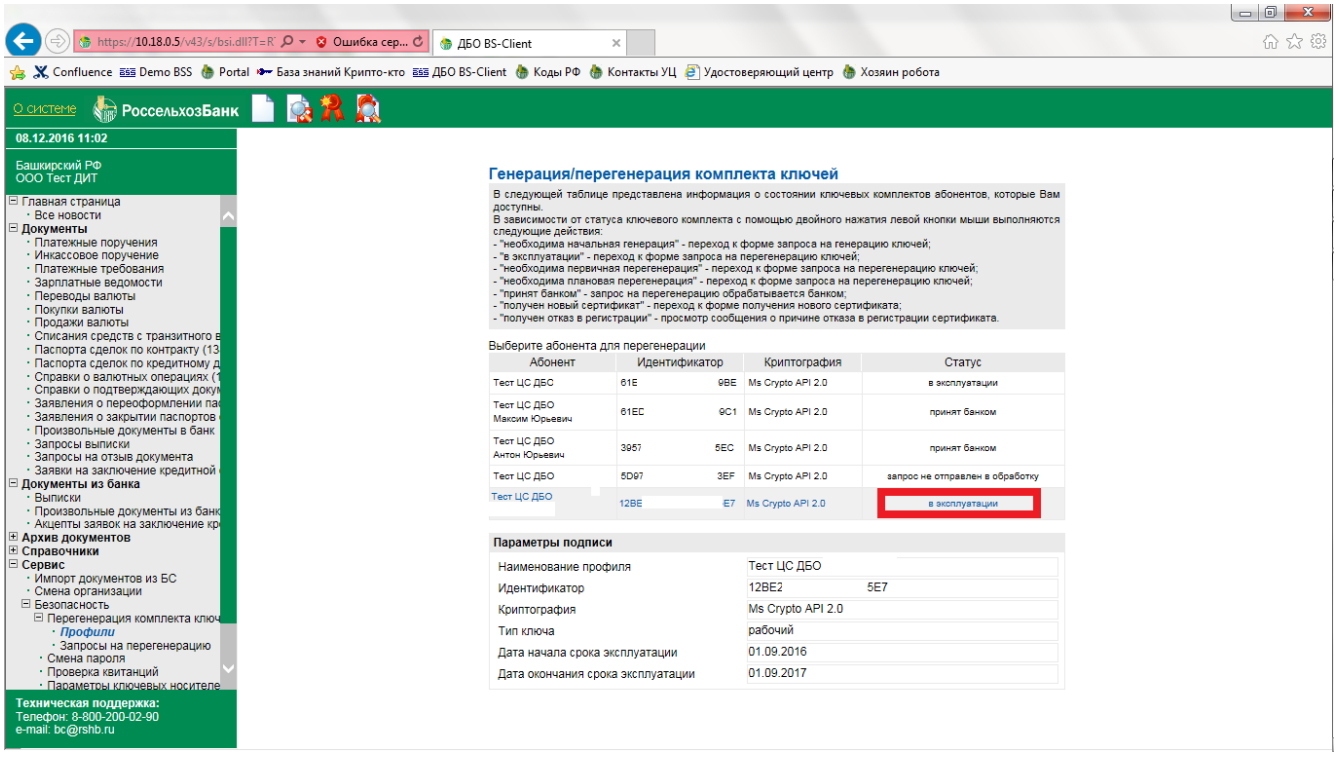

Рисунок 29. Статус выпущенного сертификата.