Банк «Кузнецкий мост»
Акционерное общество

Установка системы Интернет Клиент-Банк при использовании ключевого носителя РуТокен ЭЦП 2.0.

Оглавление

Отдел организации и сопровождения электронного документооборота банка «Кузнецкий мост» АО
тел. (495) 510-63-91

Введение

Данная инструкция предназначена для клиентов, использующих в качестве средства защищенного хранения данных ключевой носитель **РуТокен ЭЦП 2.0**. Клиентам, использующим ключевой носитель **eToken**, необходимо ознакомиться с инструкцией «Установка системы Интернет Клиент-Банк при использовании ключевого носителя eToken». Чтобы определить, какой ключевой носитель вы используете, обратитесь к документу «Различия между eToken и РуТокен ЭЦП 2.0».

Все перечисленные документы доступны на сайте банка http://www.kmbank.ru в разделе «Корпоративным клиентам» - «Интернет Клиент-Банк».

Основные системные требования.

Для работы в системе "Интернет Клиент-Банк" необходимо использовать операционную систему Microsoft Windows 7, 8 или 10 и браузер Microsoft Internet Explorer версий 10 или 11. Также возможно использование актуальных версий браузеров Opera, Firefox и Chrome. На компьютере также должен быть установлены офисные программы Microsoft Word, Microsoft Excel версии 2003 или более поздней.

Корректная работа в устаревшей операционной системе Microsoft Windows XP, а также работа с использованием браузера Microsoft Internet Explorer версии 9 (и более ранних) невозможна. Просим Вас заблаговременно обновить Вашу операционную систему Microsoft Windows до одной из версий 7, 8, 10 и обновить браузер Microsoft Internet Explorer до актуальной версии. Обращаем внимание пользователей Windows 10, что работа в браузере Microsoft Edge не поддерживается. Используйте вместо него Internet Explorer (Пуск - список программ - «Стандартные - Windows» - «Internet Explorer»).

Более подробно о системных требованиях можно прочесть в Приложении № 2 к «Правилам обслуживания клиентов в системе дистанционного банковского обслуживания "Интернет Клиент-Банк» (документ доступен на сайте банка в разделе «Корпоративным клиентам» - «Интернет Клиент-Банк»).

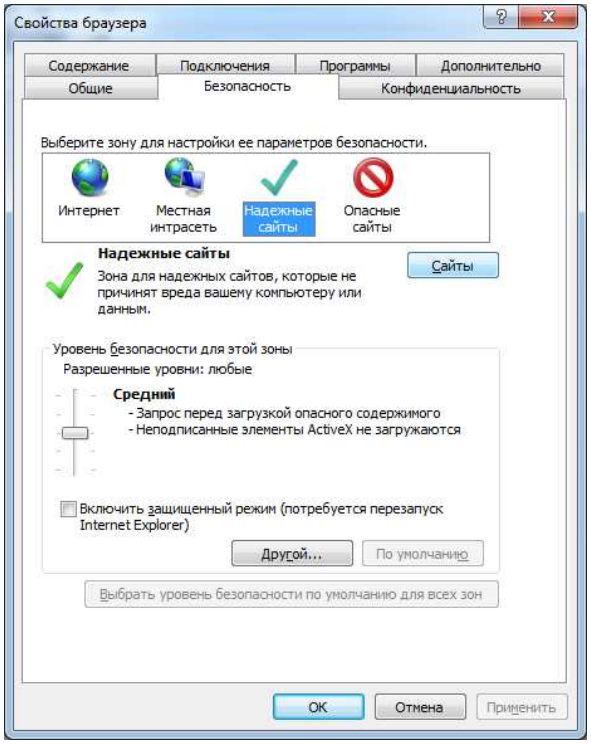
Особенности работы с носителем РуТокен ЭЦП 2.0.

Ключевой носитель **РуТокен ЭЦП 2.0** передается клиенту в запечатанном конверте, в который вложена листовка с указанными на ней пин-кодами пользователя и администратора. Пин-код пользователя необходим для работы в системе «Интернет Клиент-Банк». Пин-код администратора может потребоваться в случае необходимости разблокировки токена.

Работа с **РуТокен ЭЦП 2.0** в системе «Интернет Клиент-Банк» не требует установки драйверов. Клиент имеет возможность сменить пин-код, воспользовавшись ПО «Драйвер РуТокен для Windows», адрес для загрузки ПО: https://www.rutoken.ru/support/download/drivers-for-windows. Рекомендуемая длина пин-кода 6 символов, пин-код должен содержать большие и маленькие буквы латинского алфавита и цифры. Ввод пин-кода пользователя требуется при входе в систему, при генерации запросов на сертификат и при установке подписи на документы.

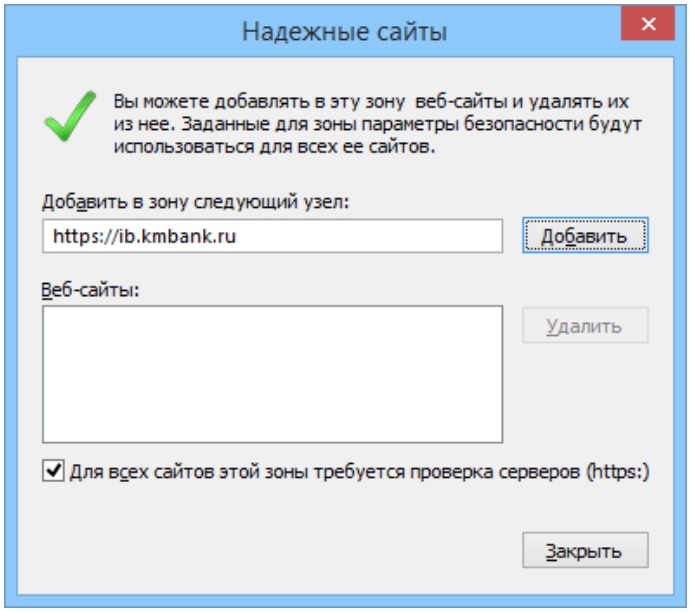
Установка Плагина
(на примере браузера Internet Explorer версии 11).

Запустите браузер Internet Explorer. Добавьте сайт Интернет Клиент-Банка в надежные сайты. Для этого зайдите в меню «Сервис» - «Свойства браузера», вкладка «Безопасность». Выберите «Надежные сайты»:



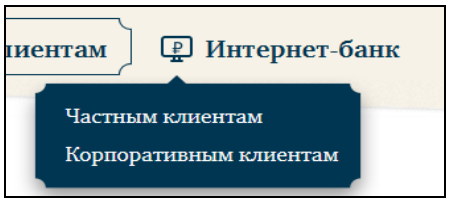
Нажмите кнопку «Сайты».

В открывшемся окне добавьте адрес https://ib.kmbank.ru в список доверенных сайтов кнопкой «Добавить», после чего нажмите «Закрыть»:

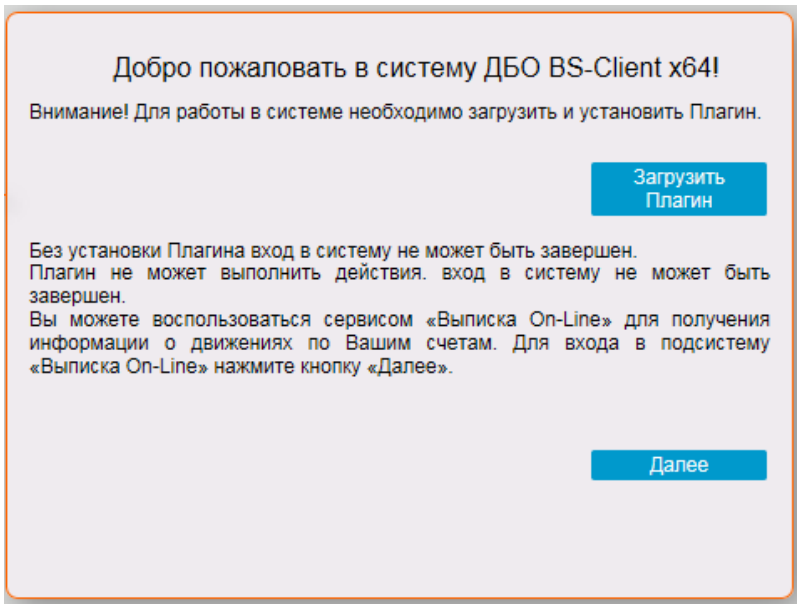


Вы также можете добавить адрес https://ib.kmbank.ru в закладки или вывести ярлык на рабочий стол для удобства последующего обращения к системе «Интернет Клиент-Банк».

Откройте страницу системы «Интернет Клиент-Банк» по адресу https://ib.kmbank.ru. На страницу системы «Интернет Клиент-Банк» также можно попасть через корпоративный сайт банка http://www.kmbank.ru, воспользовавшись ссылкой «Интернет-Банк» - «Корпоративным клиентам» на главной странице сайта:

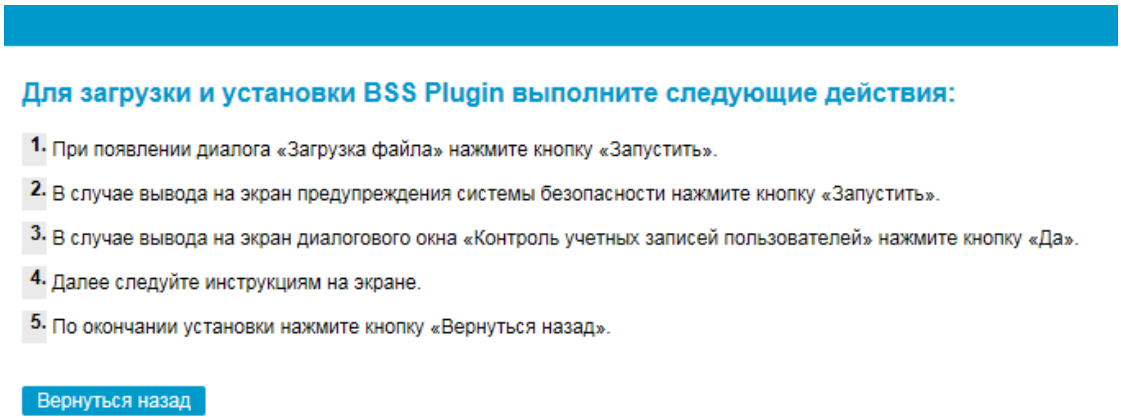


После загрузки страницы появится сообщение:



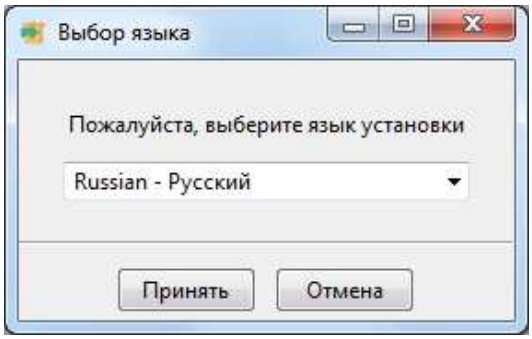
Нажмите «Загрузить Плагин».

Откроется страница с инструкцией по установке Плагина:

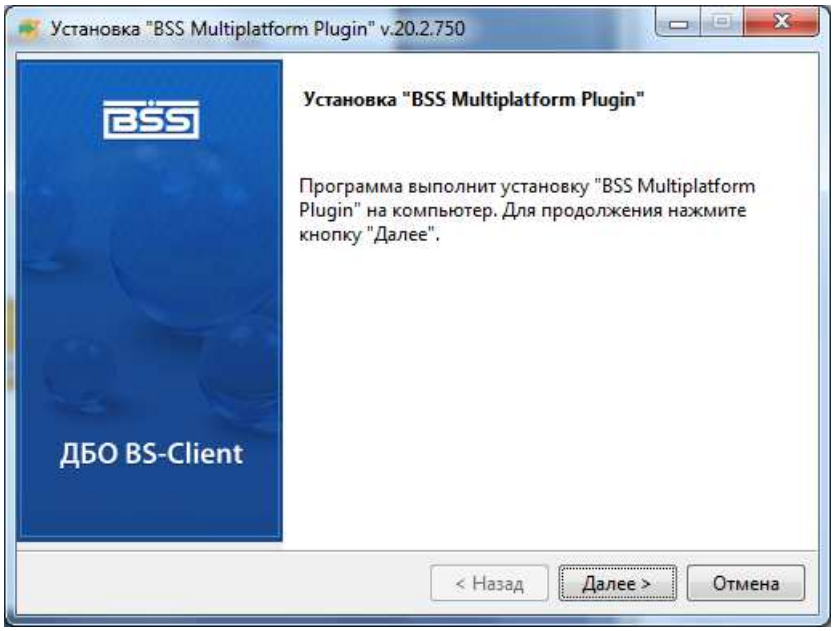


В нижней части страницы отобразится сообщение о загрузке установочного файла Плагина BssPluginSetup.exe:

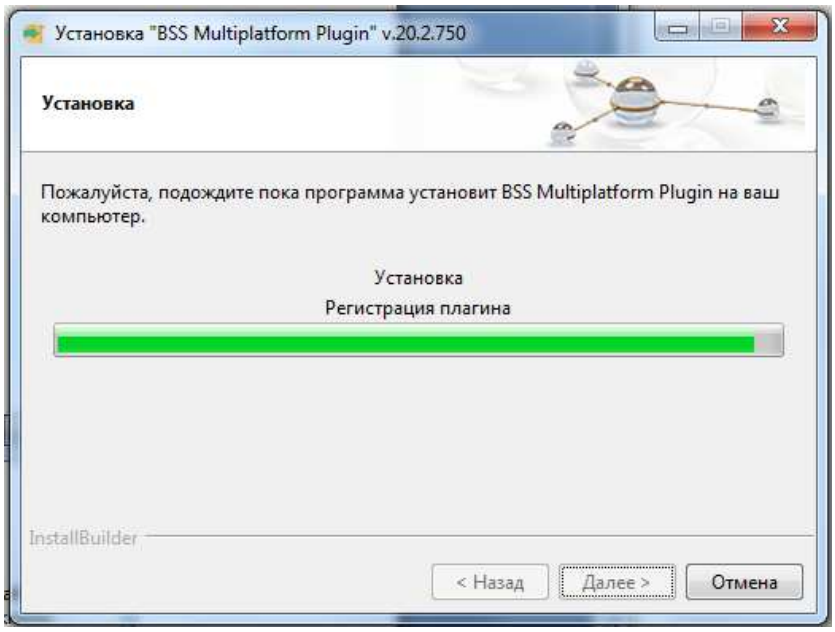
Нажмите «Выполнить». Начнется процесс установки Плагина.



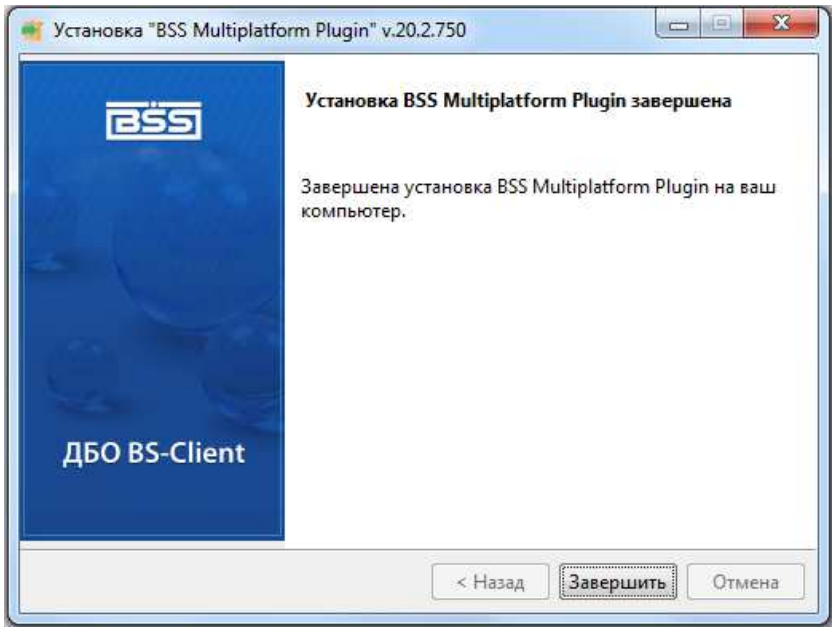
Нажмите «Принять».



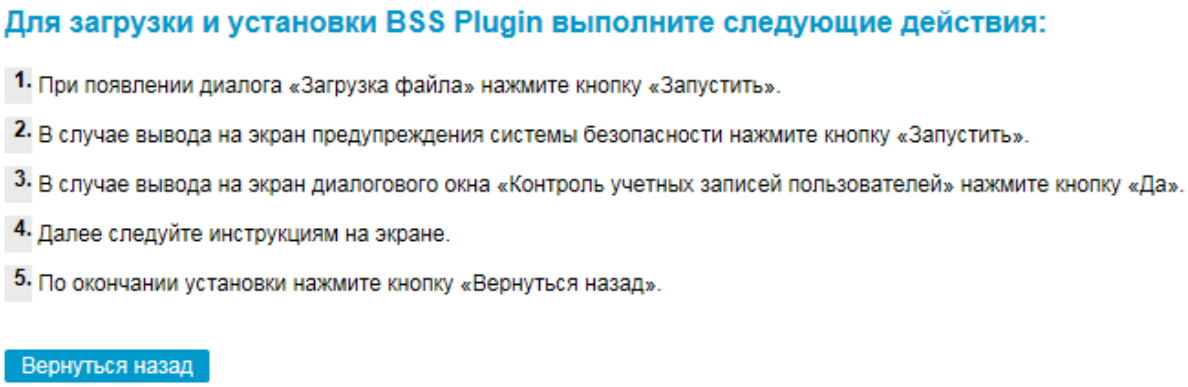
Нажмите «Далее».



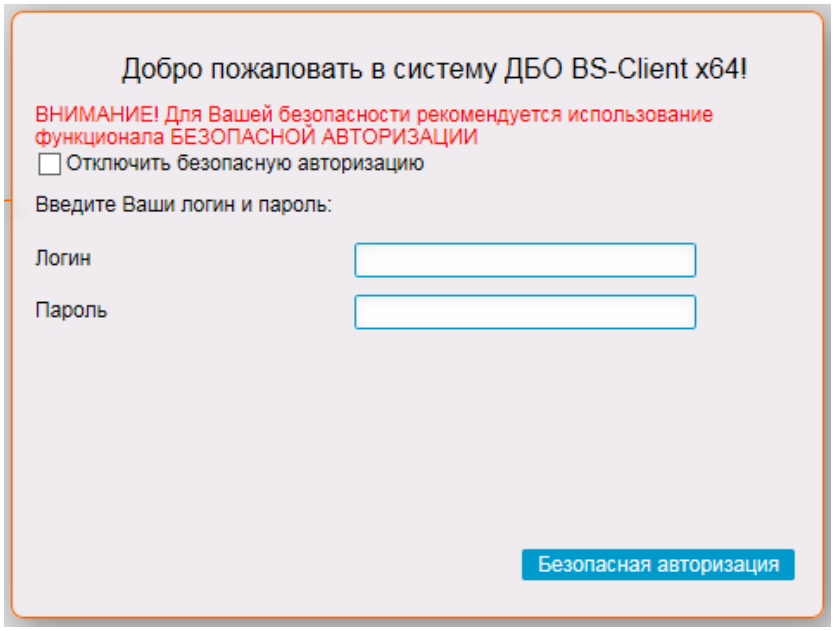
Ожидайте завершения установки.



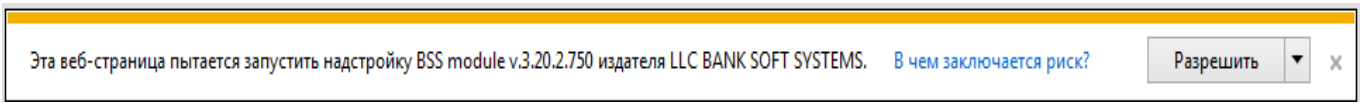
Нажмите «Завершить».



Нажмите «Вернуться назад» или заново откройте страницу «Интернет Клиент-Банк» https://ib.kmbank.ru. Отобразится окно для ввода логина и пароля пользователя Системы:



В нижней части страницы может отобразиться сообщение об использовании надстройки:



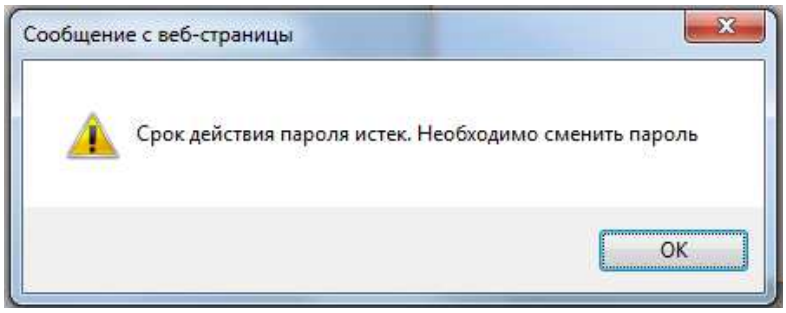
Нажмите «Разрешить».

Первый вход в Интернет Клиент-Банк.

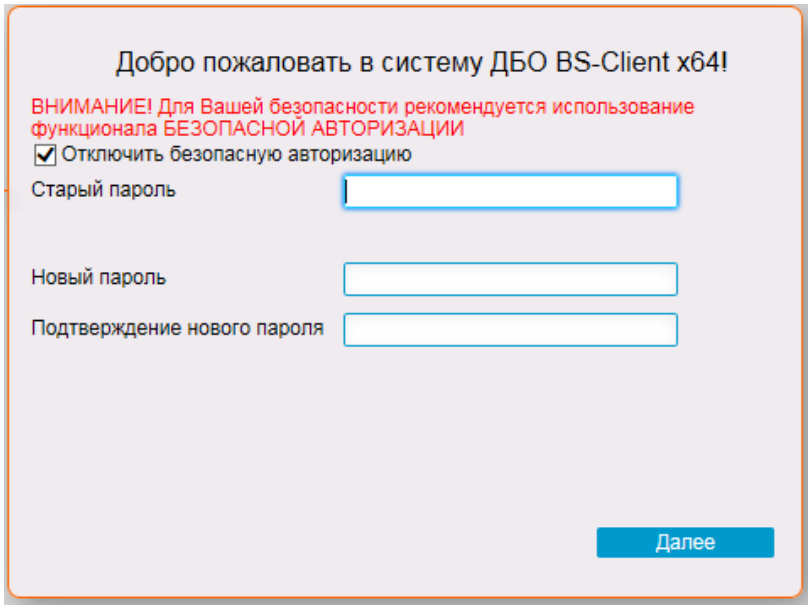
Поставьте галочку на пункте «Отключить безопасную авторизацию».

Заполните поля Логин и Пароль. Подробнее о том, где находится логин и пароль, смотрите в Приложении 1 к данной инструкции.

При первом входе система предложит изменить пароль для входа в систему:



Нажмите ОК. Отобразится окно смены пароля:

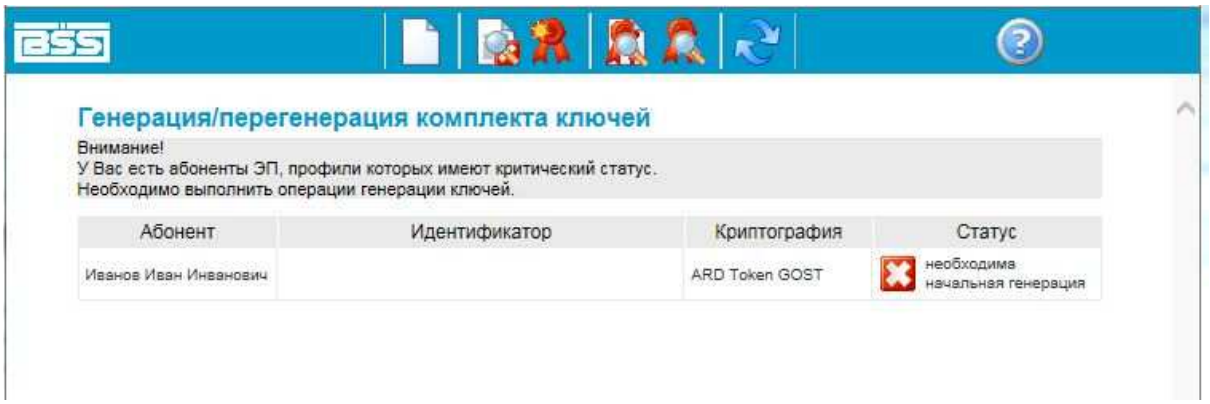


Введите ваш старый пароль пользователя системы, новый пароль и еще раз новый пароль в соответствующие поля формы. Новый пароль должен состоять из не менее 6 и не более 10 символов. Пароль должен содержать большие и маленькие буквы латинского алфавита, а также цифры. Пароль чувствителен к регистру. Нажмите «Далее».

Создание запроса на сертификат.

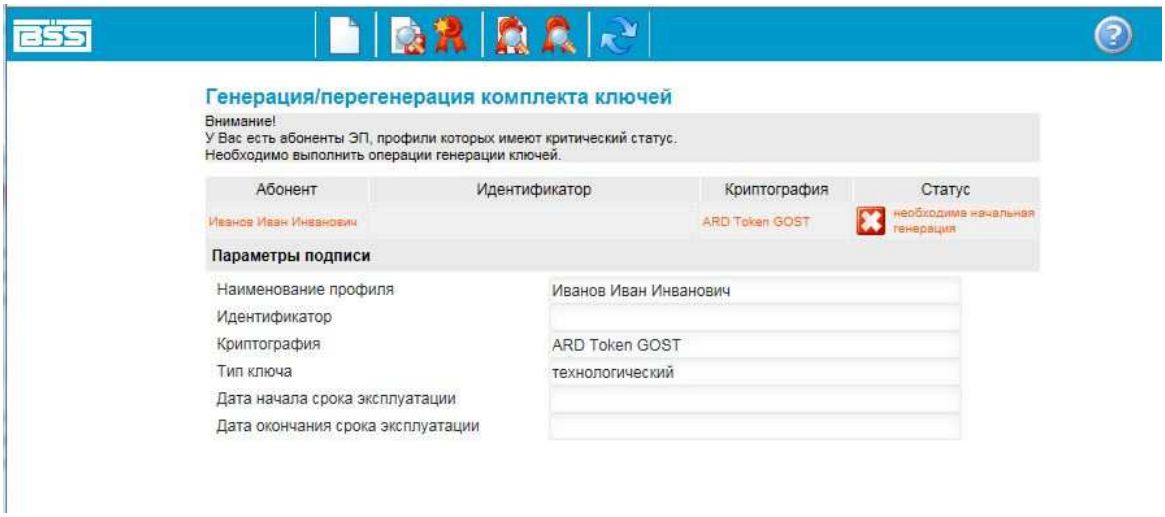
Создание запроса и получение сертификата производится на странице «Генерация / перегенерация комплекта ключей». В верхней части страницы отображаются шесть иконок. Назначение каждой из иконок показано на рисунке:

При первом входе в систему «Интернет Клиент-Банк» у Вас появится предупреждение о необходимости начальной генерации ключей:

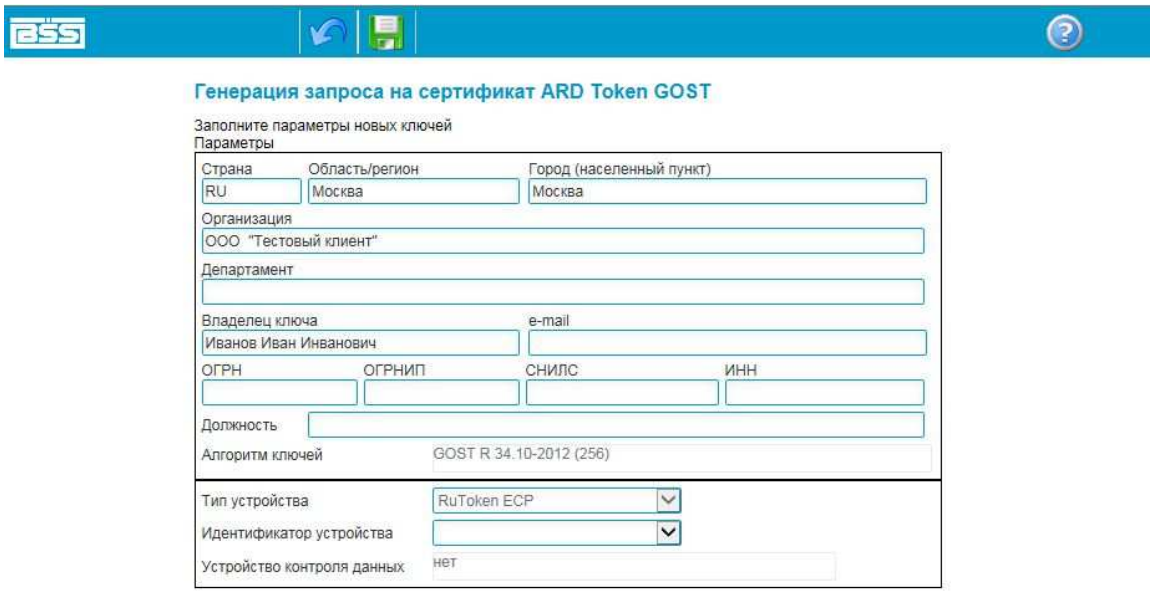


Вставьте токен в разъем USB компьютера.

Нажмите левой кнопкой мыши на ФИО абонента, для которого Вы будете запрос на сертификат. Отобразятся параметры подписи для этого абонента.

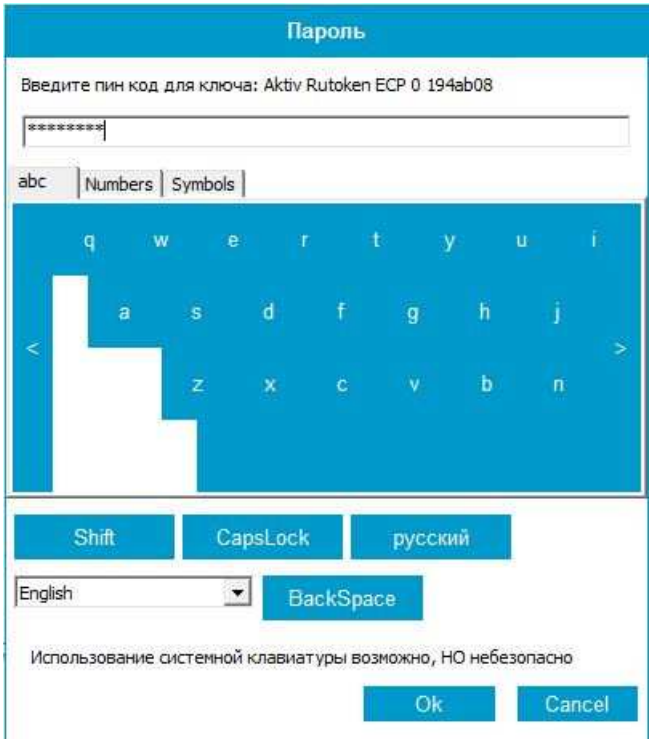


Далее нажмите на иконку «Создать запрос на генерацию/перегенерацию» (крайняя левая иконка в ряду). Откроется окно генерации запроса на сертификат:



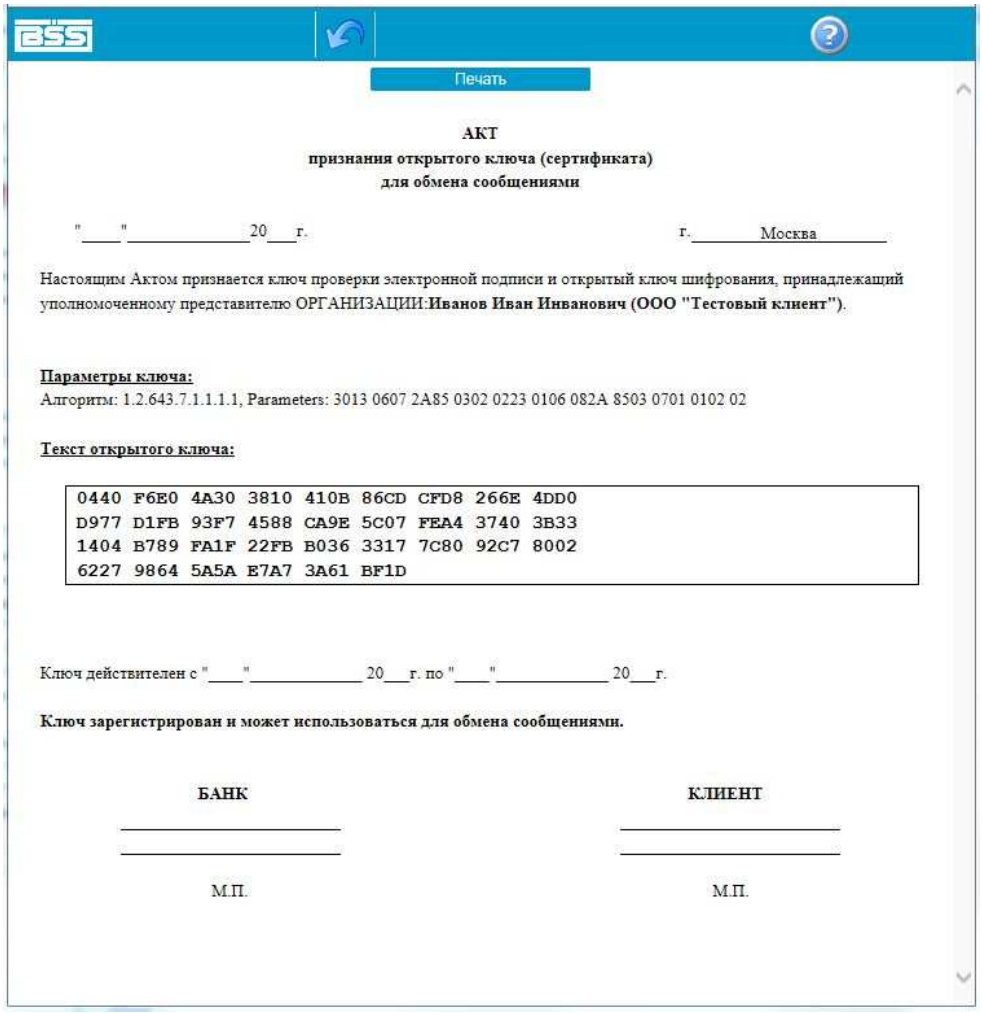
Проверьте правильность указания наименования организации и ФИО пользователя. Заполните поле «Идентификатор устройства», выбрав идентификатор подключенного ключевого носителя:

Остальные поля (Департамент, ОГРН, ОРГНИЛ, СНИЛС, ИНН, Должность) заполнять не нужно. Щелкните левой кнопкой мыши по иконке с изображением дискеты  , чтобы сохранить запрос. Отобразится запрос пин-кода устройства РуТокен ЭЦП 2.0.



Введите пин-код и нажмите «ОК».

В банк автоматически отправится запрос на сертификат, при этом на ваш РуТокен ЭЦП 2.0 запишется ключ подписи. На экране отобразится «АКТ признания открытого ключа (сертификата) для обмена сообщениями»:



Печать

АКТ
признания открытого ключа (сертификата)
для обмена сообщениями

"____"_____20___г. г._____Москва_____

Настоящим Актом признается ключ проверки электронной подписи и открытый ключ шифрования, принадлежащий уполномоченному представителю ОРГАНИЗАЦИИ:**Иванов Иван Инванович (ООО "Тестовый клиент")**.

Параметры ключа:
Алгоритм: 1.2.643.7.1.1.1.1, Parameters: 3013 0607 2A85 0302 0223 0106 082A 8503 0701 0102 02

Текст открытого ключа:

```
0440 F6E0 4A30 3810 410B 86CD CFD8 266E 4DD0
D977 D1FB 93F7 4588 CA9E 5C07 FEA4 3740 3B33
1404 B789 FA1F 22FB B036 3317 7C80 92C7 8002
6227 9864 5A5A E7A7 3A61 BF1D
```

Ключ действителен с "____"_____ 20___г. по "____"_____ 20___г.

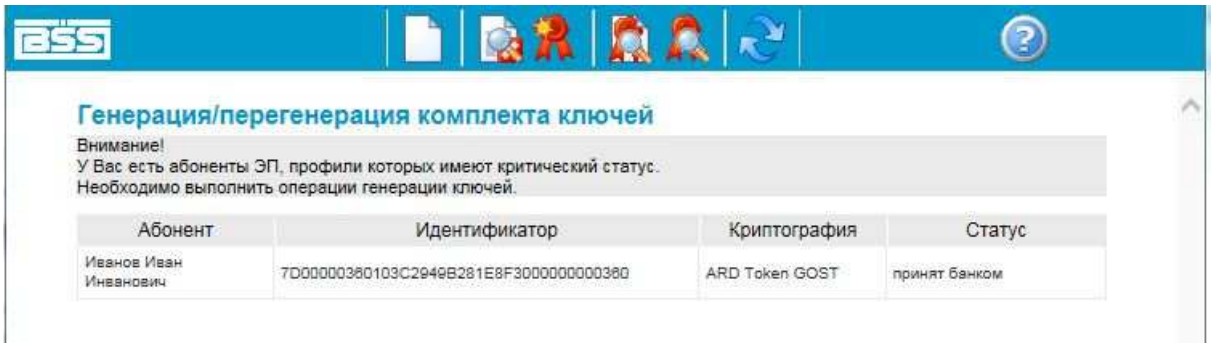
Ключ зарегистрирован и может использоваться для обмена сообщениями.

БАНК	**КЛИЕНТ**
_____	_____
_____	_____
М.П.	М.П.

Нажмите кнопку «Печать», расположенную над заголовком Акта, и распечатайте документ в 2 (двух) экземплярах. Далее оба экземпляра Акта необходимо подписать у руководителя, поставить печать организации и передать в Операционное управление Банка «Кузнецкий мост» АО.

Получение сертификата и начало работы в системе.

После подачи запроса на сертификат, статус абонента изменится на «принят банком».

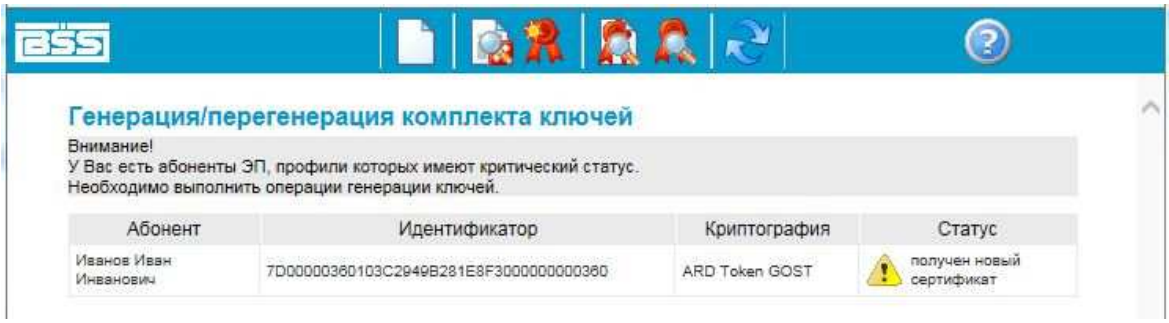


Генерация/перегенерация комплекта ключей

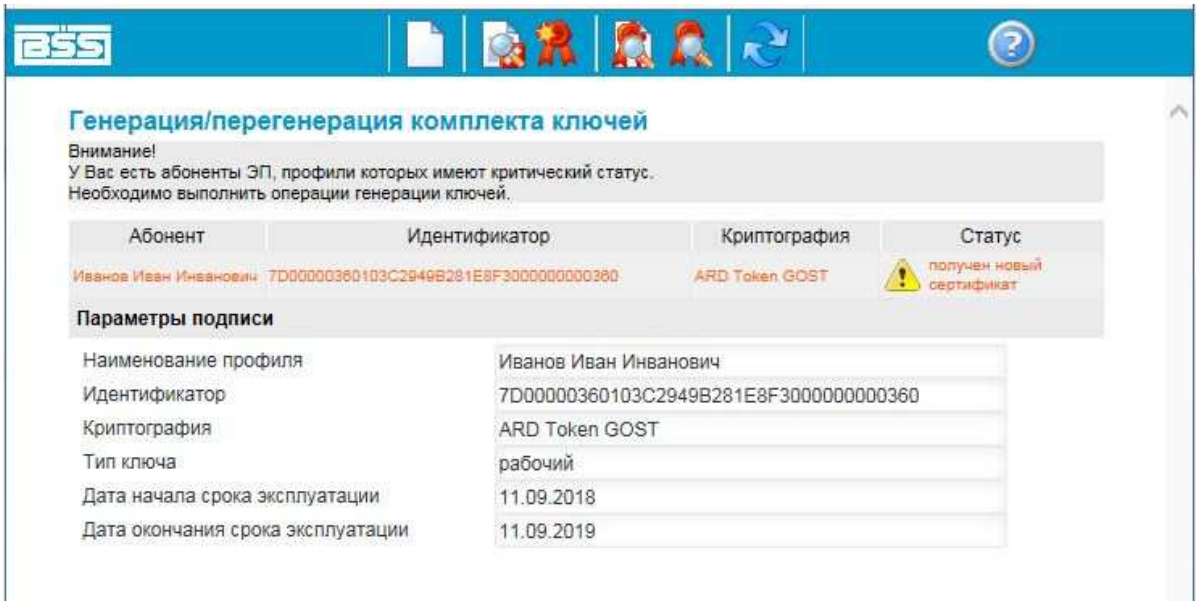
Внимание!
У Вас есть абоненты ЭП, профили которых имеют критический статус.
Необходимо выполнить операции генерации ключей.

Абонент	Идентификатор	Криптография	Статус
Иванов Иван Инванович	7D00000360103C2949B281E8F3000000000360	ARD Token GOST	принят банком

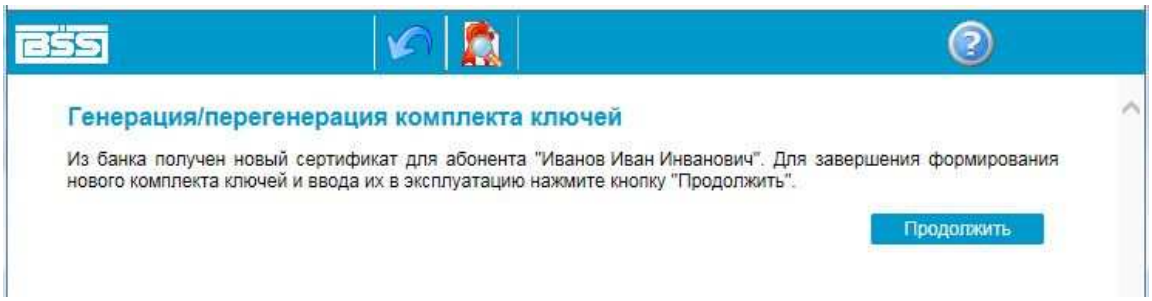
После того, как клиент передаст в банк подписанный и заверенный печатью «Акт признания открытого ключа», банк обработает запрос, сверит открытую часть ключа и активирует сертификат абонента. При следующем входе в систему клиент увидит, что статус абонента изменился на «Получен новый сертификат»:



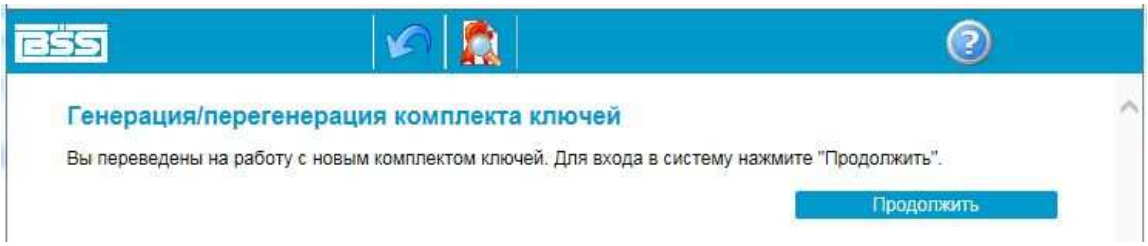
Кликните левой кнопкой мыши на ФИО абонента, для которого получен сертификат. Отобразятся параметры подписи для этого абонента.



Кликните по иконке «Получить сертификат (ключ)» (средняя кнопка в ряду).

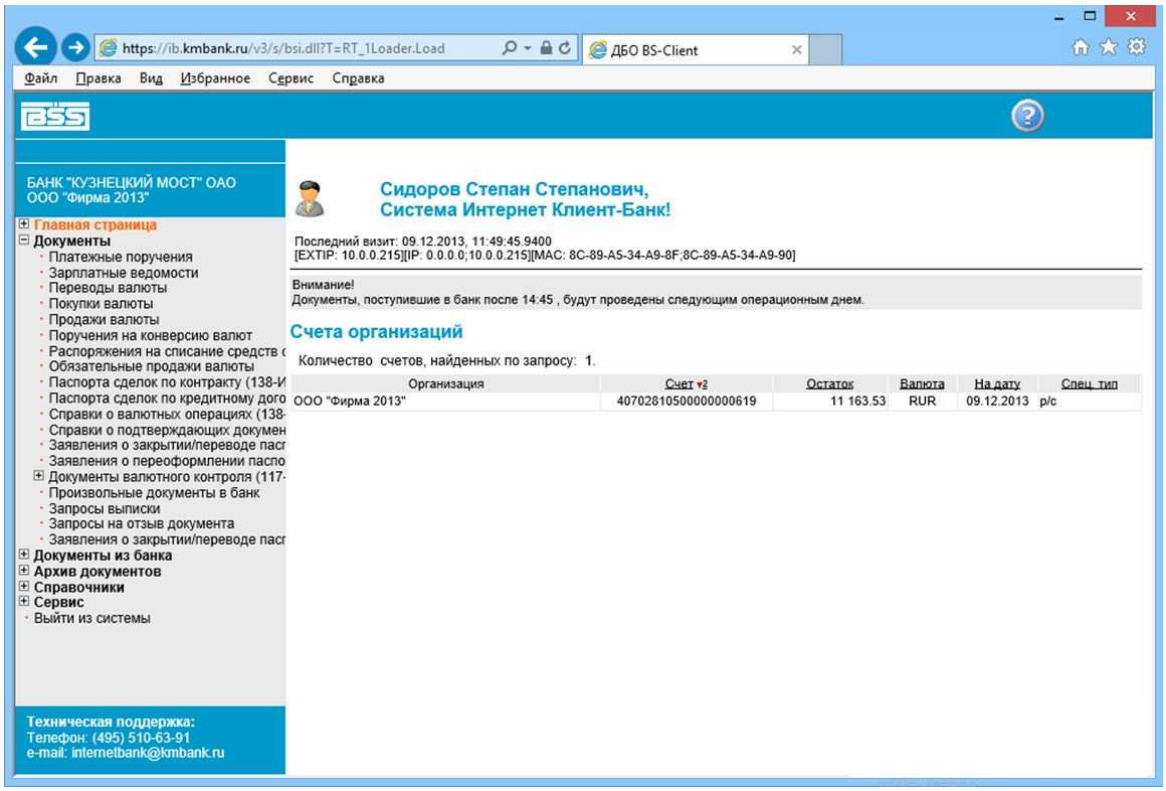


Нажмите «Продолжить»



Нажмите «Продолжить»

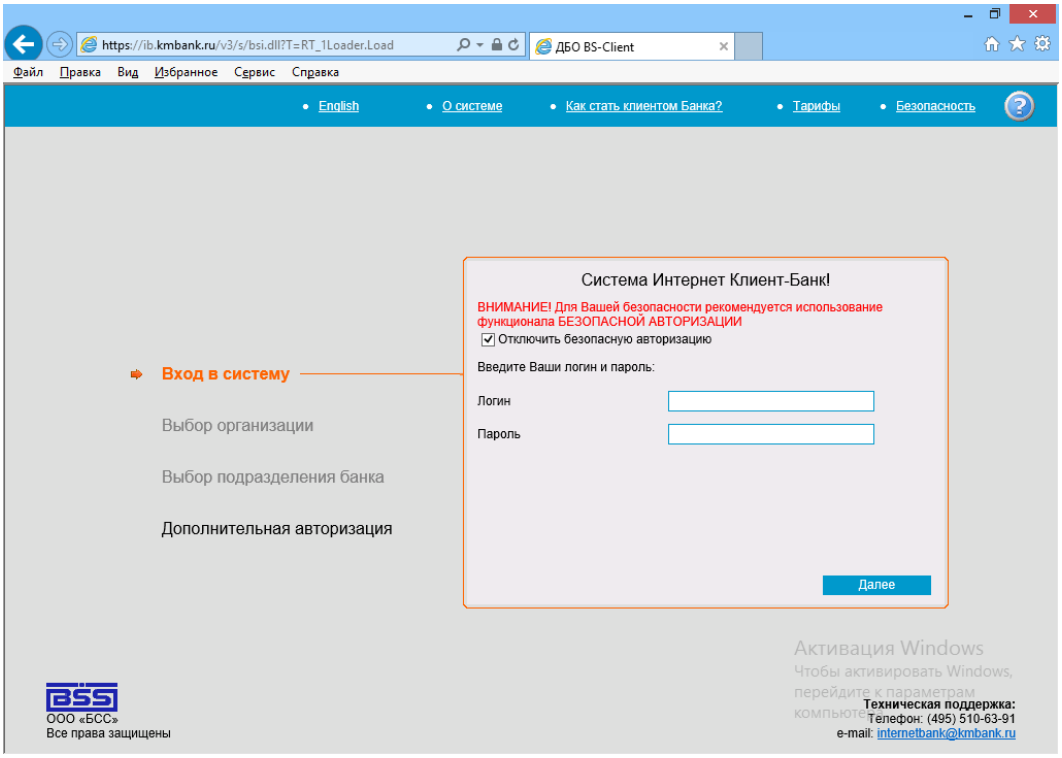
Отобразится главная страница системы «Интернет Клиент-Банк»:



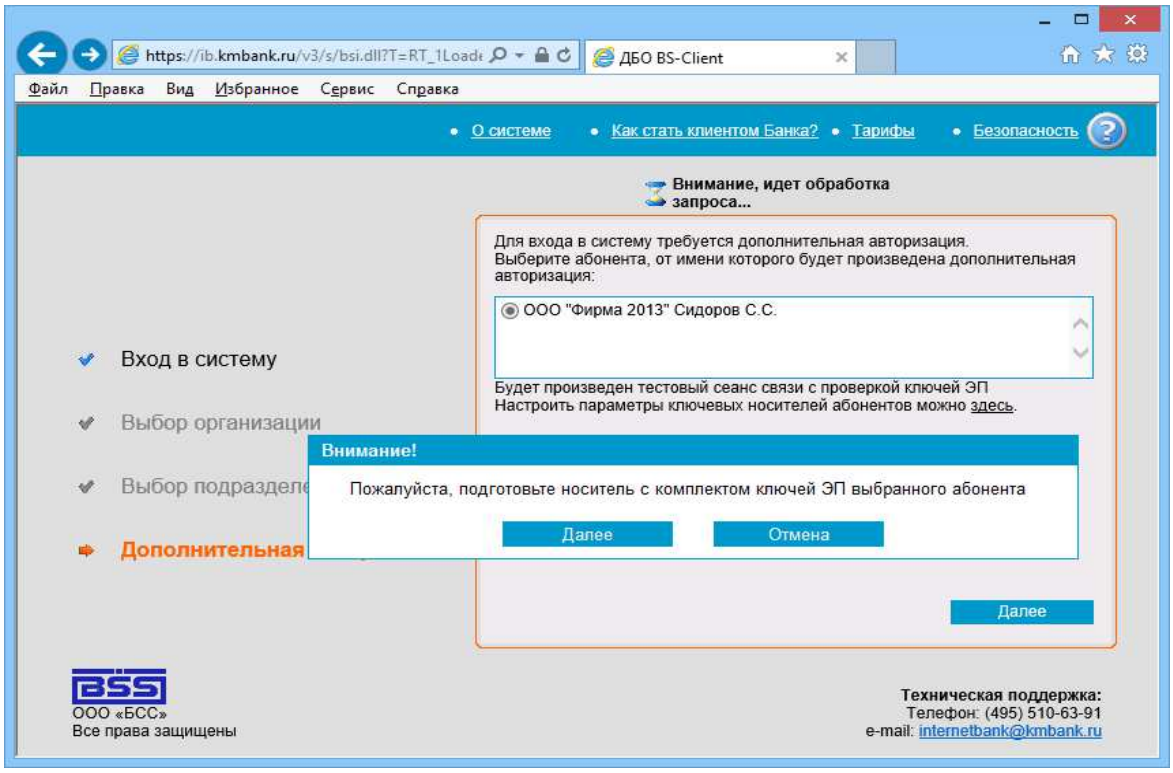
Статус ключей абонента изменится на «в эксплуатации» (статус можно посмотреть, выбрав в меню «Сервис» - «Безопасность» - «Профили»).

Ежедневная работа в системе Интернет Клиент-Банк

Откройте страницу https://ib.kmbank.ru в браузере Internet Explorer. Установите галочку «Отключить безопасную авторизацию». Введите логин и пароль, нажмите «Далее»:

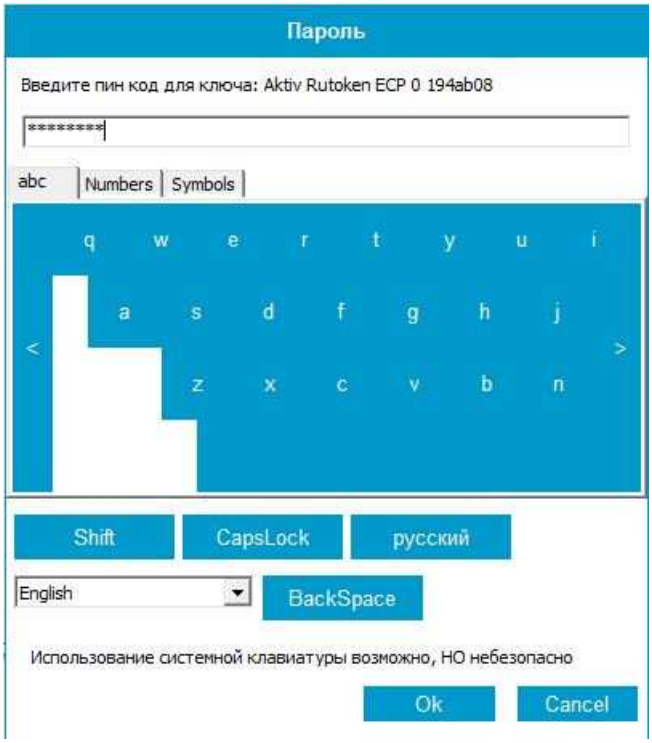


Отобразится предупреждение системы «Пожалуйста, подготовьте носитель ключей ЭП выбранного абонента». Вставьте ключевой носитель в разъем USB компьютера и нажмите «Далее».

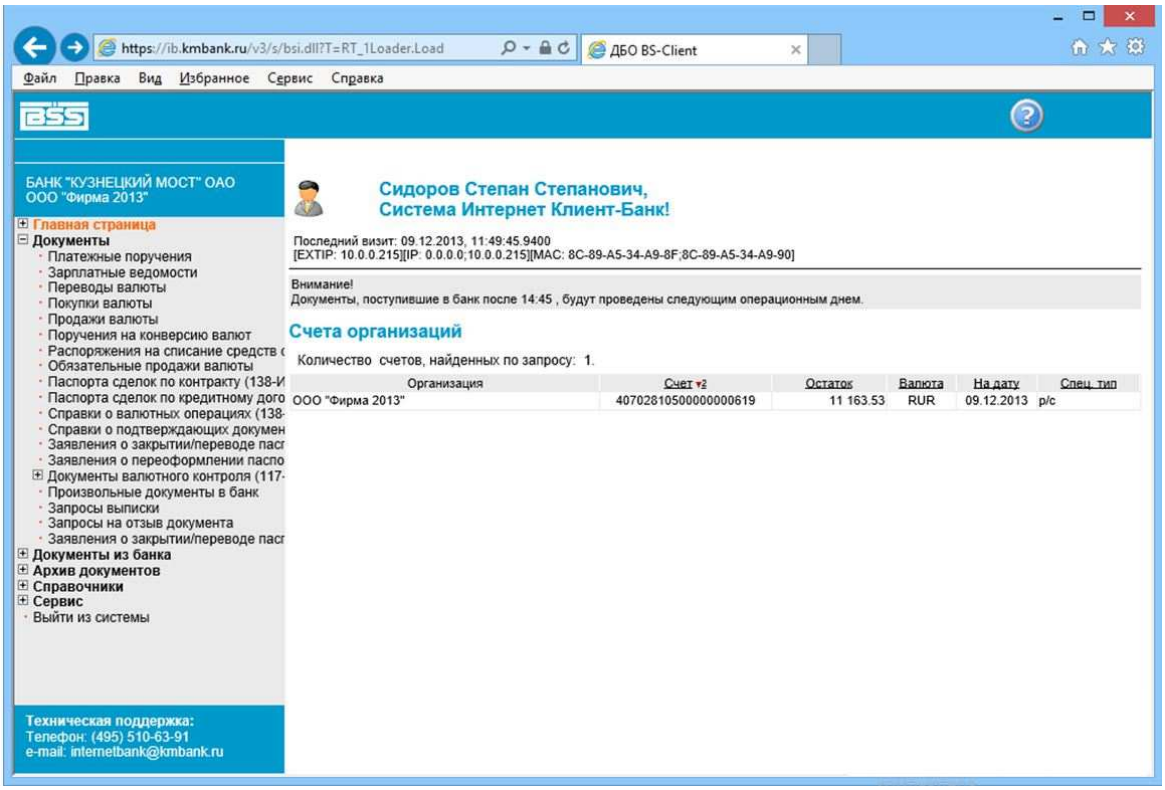


Система запросит у вас пин-код для ключа.

Обратите внимание, что после 10 попыток неправильного ввода пин-кода ваш РуТокен ЭЦП 2.0 будет заблокирован.



После ввода пин-кода вы попадете в рабочий интерфейс системы «Интернет Клиент-Банк».



Настоятельно рекомендуем:

- при работе в системе Интернет Клиент-Банк должны быть открыты только браузер, в котором вы работаете с системой, и, если необходимо, бухгалтерская программа для подготовки платежных поручений;

- начинать работу в системе Интернет Клиент-Банк с прочтения Сообщений из Банка и Новостей!

- Подключать ключевой носитель РуТокен ЭЦП 2.0 только на время работы в системе Интернет Клиент-Банк и не забывать отсоединять его сразу после завершения работы. Ключевой носитель необходимо хранить в недоступном для посторонних лиц месте, рекомендуется использовать сейф.

- При создании запроса на сертификат, а также при повседневной работе с системой Интернет Клиент-Банк к компьютеру должен быть подключен **только один ключевой носитель** (относящийся к пользователю, вошедшему в систему). Работа с системой Интернет Клиент-Банк с одновременным подключением двух и более токенов (в том числе, токенов, относящихся к другим банкам и другим клиентам) **не допускается**!

Приложение 1. Где найти логин и пароль для входа в систему «Интернет Клиент-Банк»?

Логин для входа в систему «Интернет Клиент-Банк» находится в Карточке пользователя (распечатка находится конверте с договором, который Вы получали в Банке).

БАНК "КУЗНЕЦКИЙ МОСТ" АО

Карточка пользователя подсистемы «Интернет-Клиент»

Ф.И.О. пользователя: Сидоров Степан Степанович

Логин	9876543210	Дата активации пароля	09.12.2013
Идентификатор пароля	3386940537	Дата оконч. действия пароля	-

Адреса доступа к сервисам:

Интернет-Клиент (Платеж.)	Выписка-Онлайн (Информ.)	Мобильный клиент (Информ.)
https://ib.kmbank.ru/	https://ib.kmbank.ru/	

Пароль для входа в систему «Интернет Клиент-Банк» находится в реквизитах персонального пароля (еще одна распечатка также находится в конверте с договором).

Конфиденциально. Персональный пароль клиента.

Реквизиты персонального пароля:

Идентификатор	**3386940537**
Пароль	**5810611336**

Внимание! Этот пароль предоставляется для первичного входа в систему Интернет Клиент-Банк. **Настоятельно рекомендуем** поменять этот пароль после первичной регистрации в системе «Интернет Клиент-Банк».

Отдел организации и сопровождения электронного документооборота банка «Кузнецкий мост» АО: **(495) 510-63-91.**