



Система дистанционного банковского обслуживания

ОАО «Банк Санкт-Петербург»

Инструкция по установке ЭП с диска для подсистемы «Банк-Клиент»





Содержание

1. НАСТРОЙКА ПАРАМЕТРОВ КЛЮЧЕВЫХ НОСИТЕЛЕЙ АБОНЕНТОВ ЭП.....	3
2. ПЕРЕГЕНЕРАЦИЯ КОМПЛЕКТА КЛЮЧЕЙ.....	7
3. ПЕЧАТЬ СЕРТИФИКАТА.....	9

1. Настройка параметров ключевых носителей абонентов ЭП

1. Получите диск с ЭП подсистемы «Банк-Клиент». Диск содержит папку, включающую технологические ключи и сертификаты ключей проверки электронной подписи абонентов клиента, например, 1472E9B4000000000A89.
2. Скопируйте папку, содержащую ключи (в нашем примере 1472E9B4000000000A89), с диска на свой компьютер. Путь выбирается произвольно, например, C:\Volin\Crypto.
3. Выберите пункт меню **Настройки** → **КриптоЗащита** → **Мастер настройки абонентов СКЗИ**.
4. Откроется окно **Мастер настройки криптозащиты (1)**.



Рис. 1.1 Окно Мастер настройки криптозащиты (1)

5. Отметьте действие **Импортировать криптографический профиль** и нажмите кнопку **Далее>**.
6. Откроется окно **Мастер настройки криптозащиты (2)**.

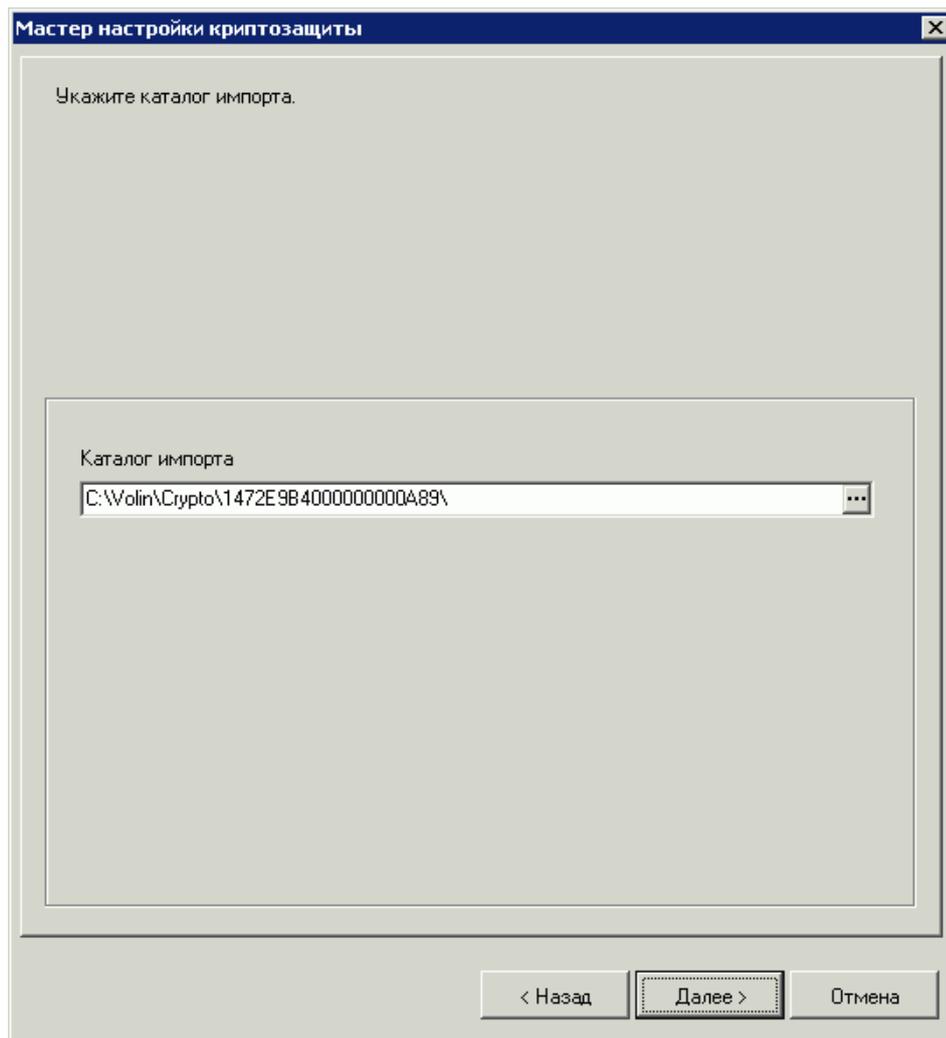
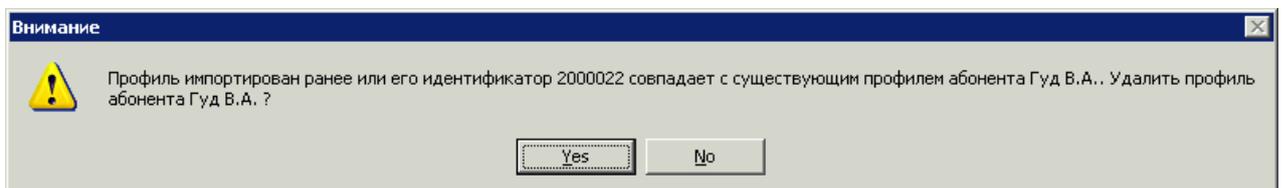


Рис. 1.2 Окно Мастер настройки криптозащиты (2)

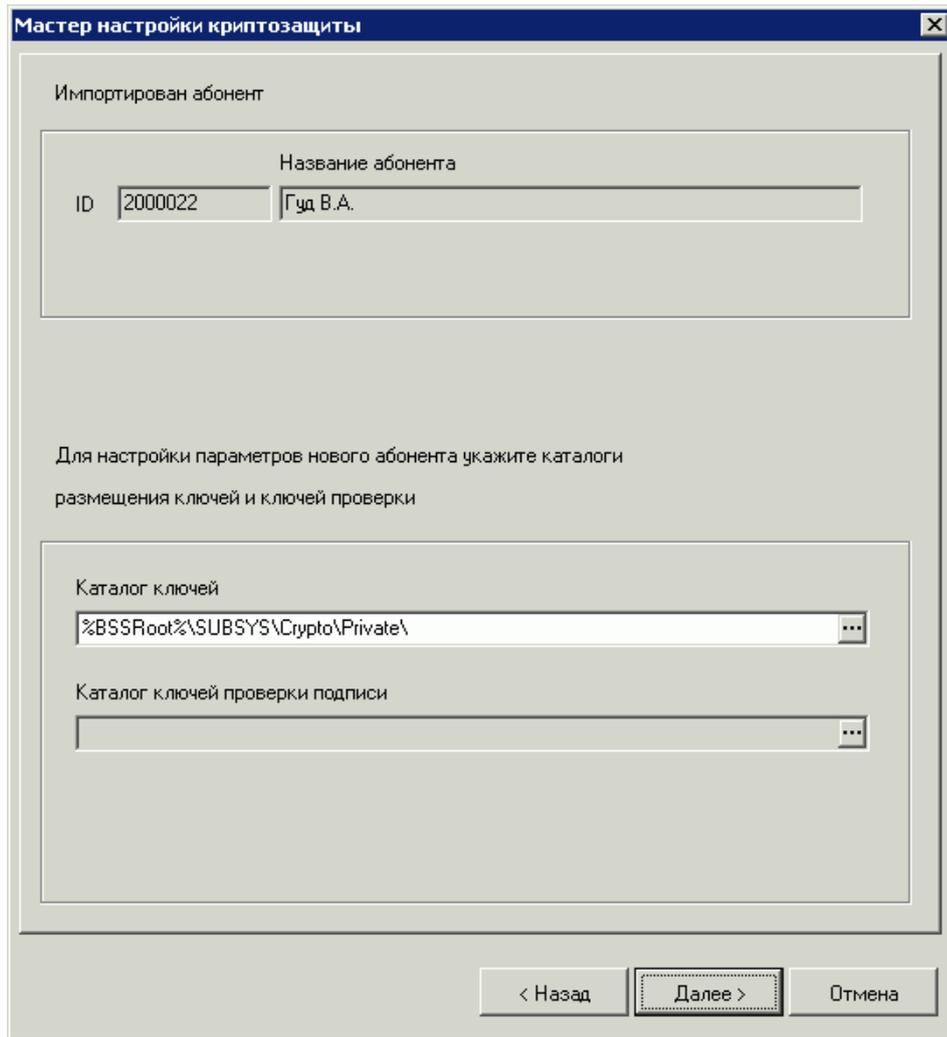
7. Выберите каталог, из которого будут импортированы ключи, и нажмите кнопку **Далее>**.

Примечание: Если импортируемый криптопрофиль уже существует, будет отображено предупреждение:



При нажатии кнопки **No**, импорт криптопрофиля осуществлен не будет.

8. При нажатии кнопки **Yes** откроется следующее окно:



Мастер настройки криптозащиты

Импортирован абонент

Название абонента

ID 2000022 Гуд В.А.

Для настройки параметров нового абонента укажите каталоги размещения ключей и ключей проверки

Каталог ключей
%BSSRoot%\SUBSYS\Crypto\Private\

Каталог ключей проверки подписи

< Назад Далее > Отмена

Рис. 1.3 Окно Мастер настройки криптозащиты (3)

9. Выберите каталог, в который будут установлены ключи электронной подписи, и нажмите кнопку **Далее>**.

Примечание: Указанный на рисунке каталог служит лишь для примера. В целях предотвращения несанкционированного использования системы ключи электронной подписи рекомендуется хранить на съемном носителе (дискета, FLASH-накопитель).

Примечание: Каталог ключей для каждого распорядителя должен быть различным.

10. Откроется окно **Мастер настройки криптозащиты (4)**.

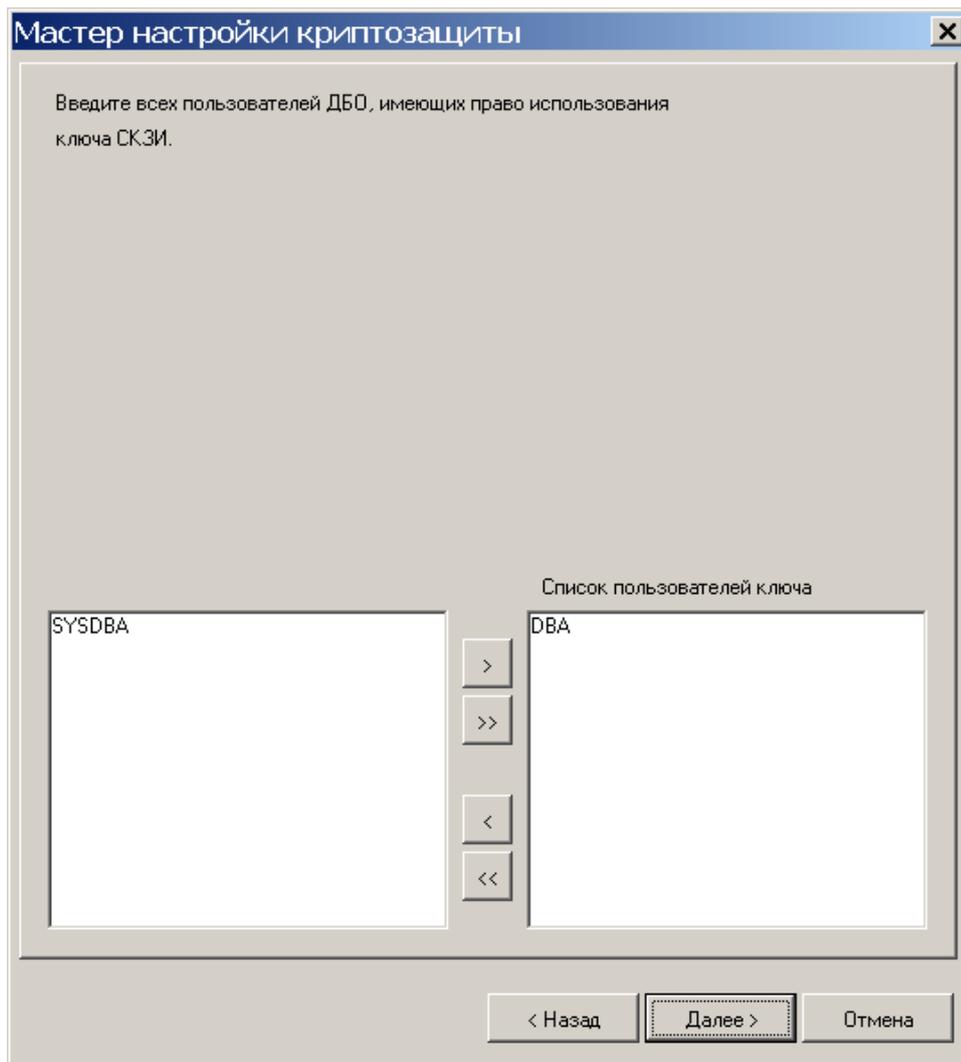


Рис. 1.4 Окно Мастер настройки криптозащиты (4)

11. Выберите пользователей, которым необходимо дать право использования импортируемого ключа, и нажмите кнопку **Далее>**.

Примечание: Стандартно это пользователь DBA.

12. При успешном импорте криптопрофиля Вы увидите сообщение об этом:

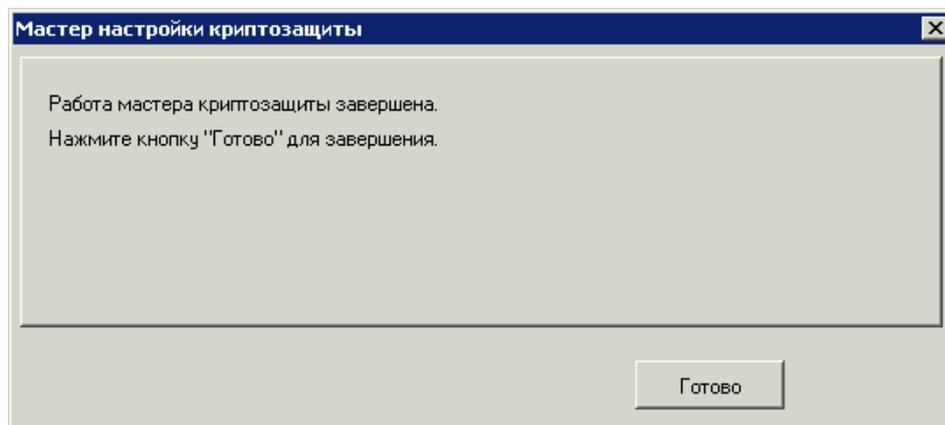


Рис. 1.5 Окно Мастер настройки криптозащиты (5)

13. Нажмите кнопку **Готово**.
14. Вы импортировали технологические ключи. Для того чтобы Вы могли подписывать и отправлять в банк документы, Вам необходимо выполнить процедуру регенерации комплекта ключей и предоставить распечатанные и подписанные сертификаты в банк (см. далее).

2. Регенерация комплекта ключей

Для регенерации ключей:

1. Выполните команды меню **Настройки** → **Криптозащита** → **Запросы на регистрацию сертификатов**.
2. Откроется страница **Запросы на сертификаты**.

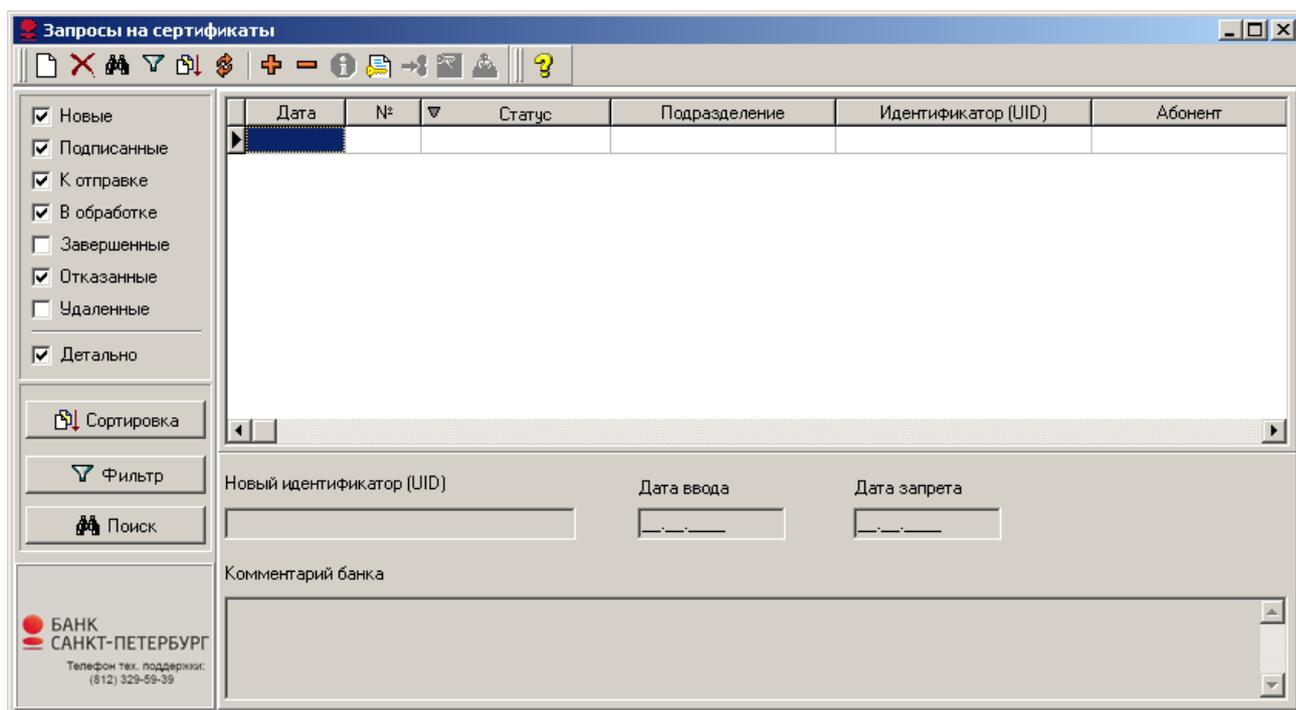


Рис. 2.1 Окно Запросы на сертификаты

3. Нажмите кнопку  на панели инструментов страницы.
4. Откроется окно **Удаленная регенерация**.

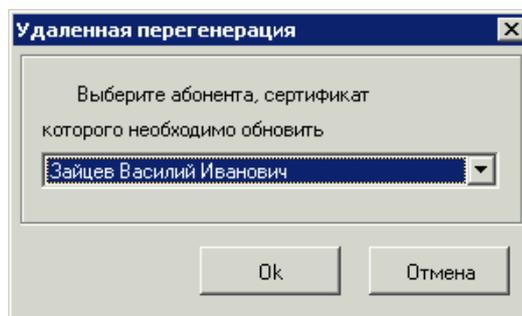


Рис. 2.2 Окно Удаленная регенерация (1)

5. Выберите абонента и нажмите кнопку **Ок**.
6. Появится сообщение:

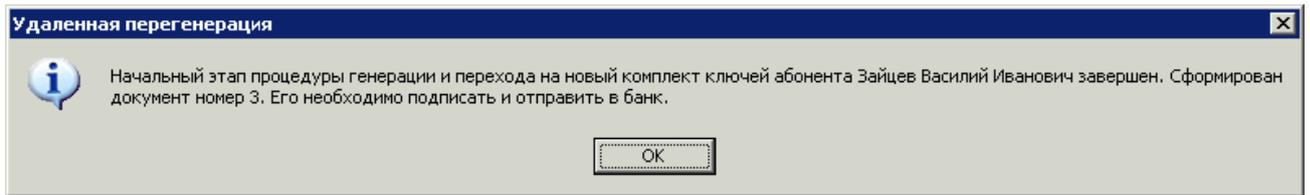


Рис. 2.3 Окно Удаленная регенерация (2)

7. Нажмите кнопку **ОК**.
8. В окне **Запросы на сертификаты** появится документ в статусе «новый».

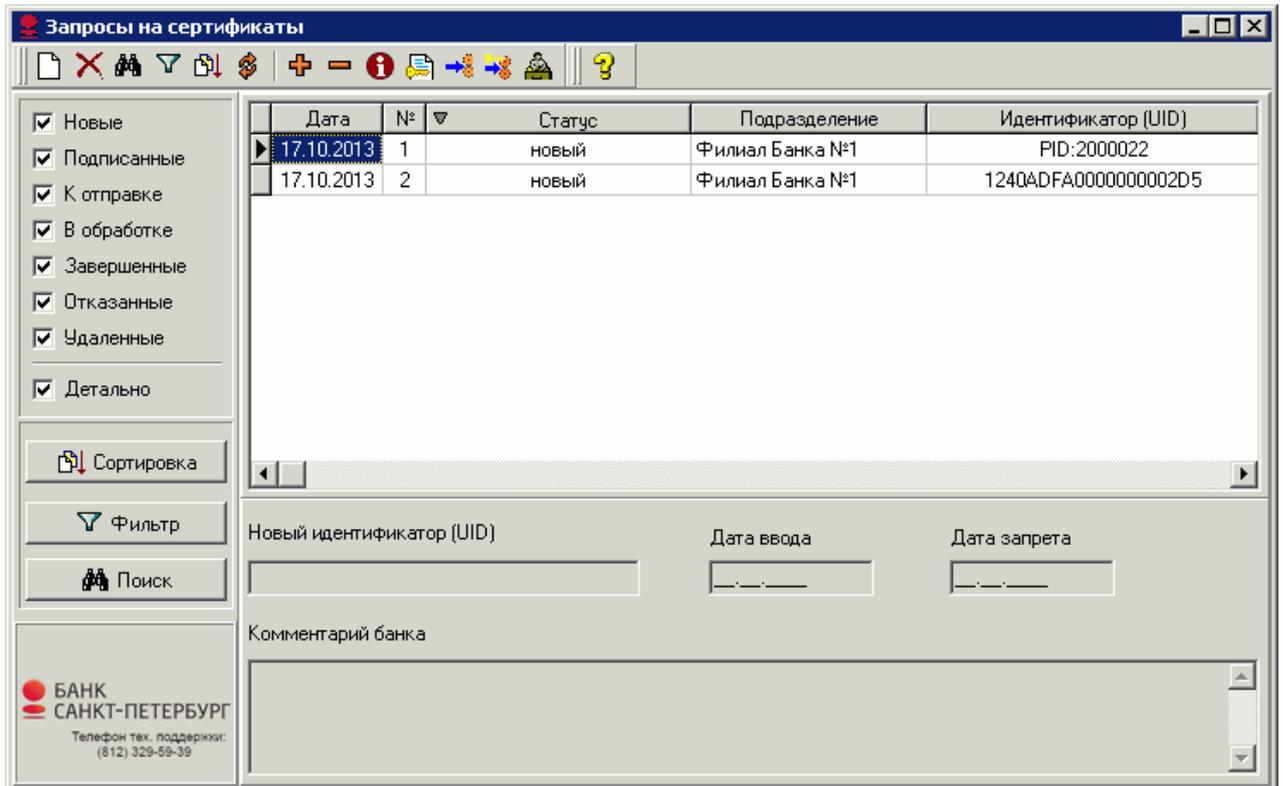


Рис. 2.4 Окно Запросы на сертификаты с новым запросом

9. Если абонентов, имеющих право подписи несколько, то выполните п.п. 3-8 данной инструкции для каждого абонента.

Примечание: Для каждого абонента можно создать только один запрос.

10. Для отправки запросов в банк выделите в списке нужные документы и нажмите кнопку  на панели инструментов окна.
11. Для отслеживания изменений статусов документов поставьте все флаги в левой части окна **Запросы на сертификаты** (см. Рис. 2.4).
12. Для проведения сеанса связи с банком нажмите кнопку  на панели инструментов главного окна системы:

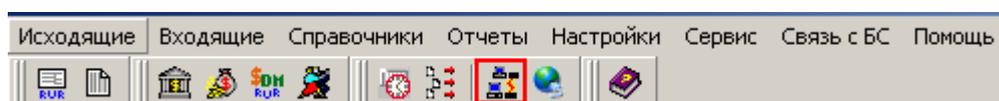


Рис. 2.5 Панель инструментов главного окна подсистемы

13. Дождитесь, когда статус запроса на сертификат изменится на «принят» либо «распознан». Это означает, что запрос принят банком в обработку.

Примечание: Обработка запроса на сертификат в банке занимает до 30-ти минут.

Внимание! При отправке запроса на регенерацию ключей и запроса на перерегистрацию сертификата обратите внимание: Вы должны дождаться ответа на запрос из банка. В противном случае имеющиеся у Вас вновь созданные ключи заменятся на новые, и банк не сможет их распознать. В таком случае Вам придется лично явиться в банк для генерации новых технологических ключей.

14. По окончании обработки документ переходит в статус «зарегистрирован». Появится сообщение:

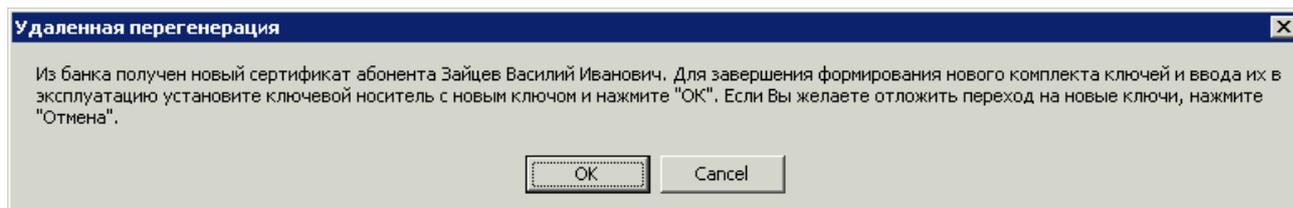


Рис. 2.6 Окно Удаленная регенерация (3)

15. Нажмите кнопку **ОК**.

16. Появится сообщение:

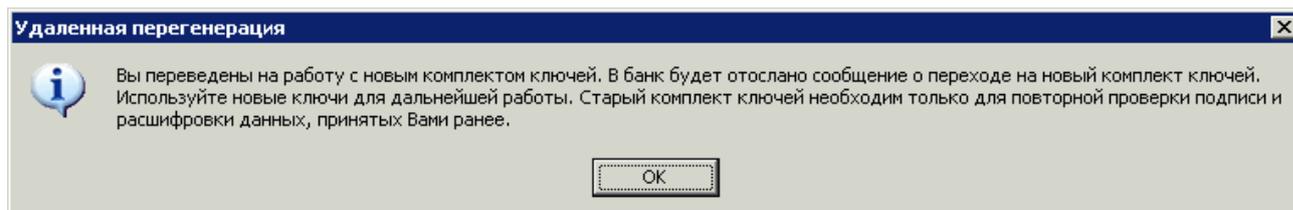


Рис. 2.7 Окно Удаленная регенерация (5)

17. Нажмите кнопку **ОК**. Регенерация завершена.

18. Если добавляется несколько абонентов, то выполните регенерацию для каждого добавляемого абонента.

19. Далее следует распечатать сертификаты абонентов, для которых была пройдена регенерация ключей.

3. Печать сертификата

1. Выполните команды меню **Настройки** → **Криптозащита** → **Список абонентов ЭП**.
2. Откроется окно **Справочник криптографических профилей**.

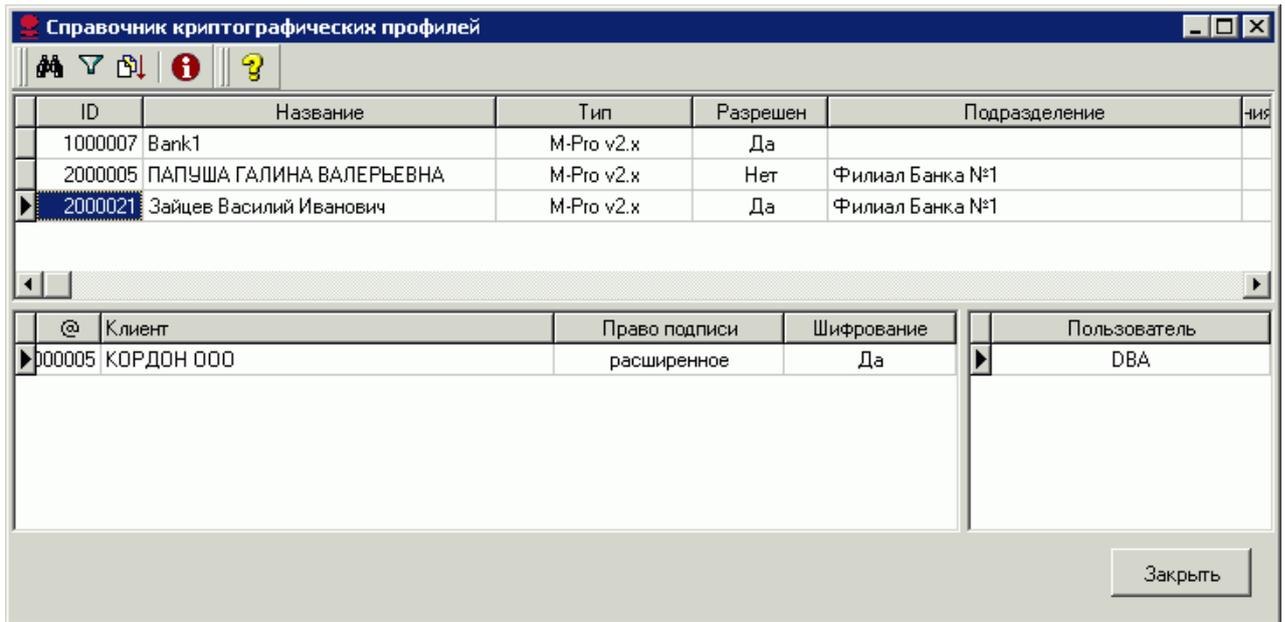


Рис. 3.1 Окно Справочник криптографических профилей

3. Выделите нужный профиль и нажмите клавишу **Enter**.
4. В открывшемся окне **Профиль абонента** перейдите на вкладку **Сертификаты**.

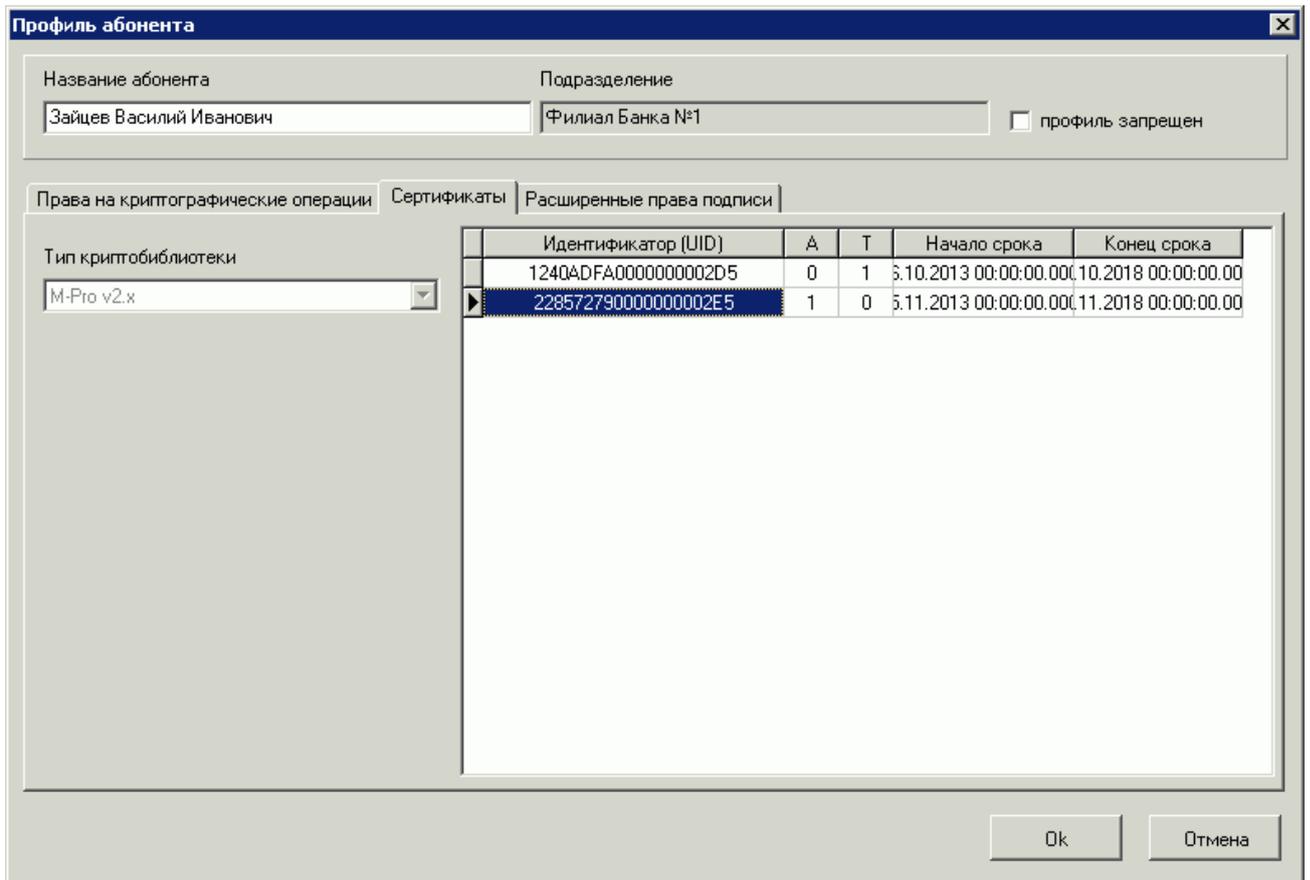


Рис. 3.2 Вкладка Сертификаты окна Профиль абонента



5. В списке сертификатов выделите активный (в столбце **А** указан признак активности **1**). Щелкните правой кнопкой мыши для перехода в контекстное меню. Выберите команду **Просмотр сертификата**. Откроется форма просмотра сертификата.
6. Распечатайте документ в двух экземплярах. Подпишите у руководителя оба экземпляра, поставьте печать организации и предоставьте оба экземпляра в банк.
7. Выполните инструкцию **Печать сертификата** для всех добавленных пользователей.