



AS-ClientBank

Руководство по установке

Прилагаемые данные	2
Системные требования.....	3
Установка системы	4
Установка программы.....	4
Установка сертификата банка	4
Настройка системы	5
Создание конфигурации системы	5
Первый вход в систему.....	6
Ввод реквизитов клиента	6
Создание пользователей	6
Первый вход пользователя в систему.....	7
Проверка связи.....	8
Пароль смены ключей	9
Получение сертификата	10
1. Генерация пары (секретного и открытого) ключей.....	10
2. Отправка в банк запроса на сертификат (открытого ключа)	11
3. Проверка статуса запроса на сертификат.....	12
Вход пользователя в систему после получения сертификата	13

Прилагаемые данные

1. Инсталляционный пакет программы
2. Файл сертификата банка: имеет расширение .cer.
3. Файл начальных данных программы: "CBInit.txt"
4. Руководство по установке

Системные требования

Система **AS-ClientBank** использует криптографическую библиотеку, которая доступна начиная с версии Internet Explorer 5.5. По этой причине в процессе инсталляции первым делом проверяется версия программы Internet Explorer, установленной на Вашем компьютере и в случае необходимости предлагается установить необходимую версию.

Дополнительные минимальные требования для установки системы **AS-ClientBank**:

1. Pentium 200 Mhz, 64 Mb RAM
2. Операционная система:
 - Microsoft Windows XP
 - Microsoft Windows 2000 Service Pack 1
 - Microsoft Windows NT4.0 Service Pack 6
 - Microsoft Windows 98
 - Microsoft Windows Millennium Edition.
3. Средства связи с Web-сервером банка (в зависимости от того как предоставляет банк услугу это может быть модем или доступ в Интернет).



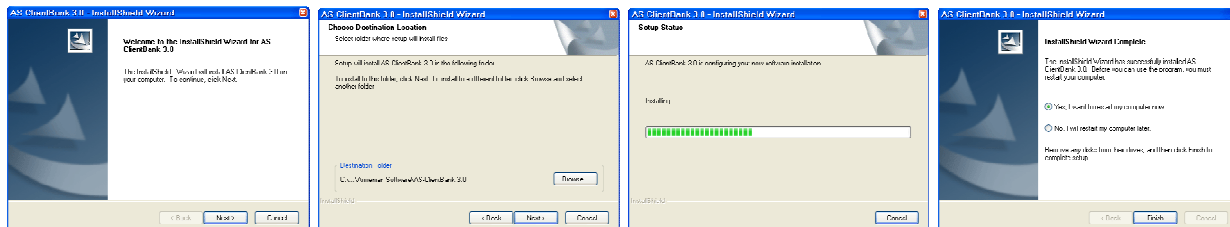
Внимание: При запуске система **AS-ClientBank** автоматически меняет следующие опции Региональных Стандартов Панели Управления

1. Разделитель компонентов даты: "/"
2. Краткий формат даты: "dd/мм/yy"
3. Разделитель целой и дробной части: "." (точка)
4. Разделитель групп разрядов: "," (запятая)

Установка системы

Установка программы

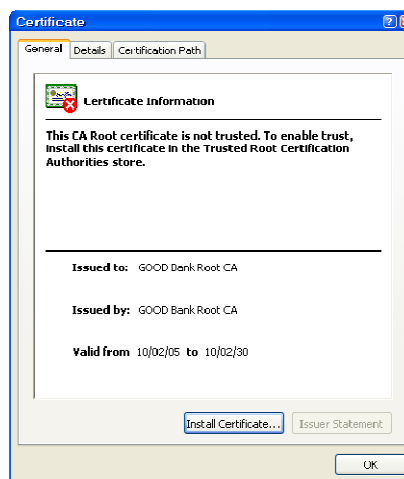
Для установки системы запустите setup.exe (находится в каталоге ASClientBank, прилагаемого компакт-диска) и далее следуйте инструкциям:



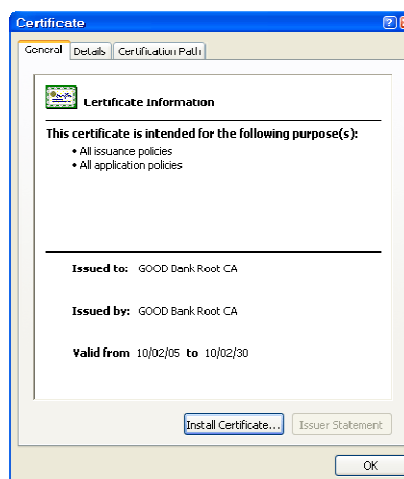
Установка сертификата банка

Для установки сертификата банка необходимо выполнить следующие шаги:

1. Открыть файл сертификата (файл с расширением .cer), из открывшегося окна выбрать "Install Certificate" ("Установить сертификат") и далее следовать инструкциям по умолчанию.



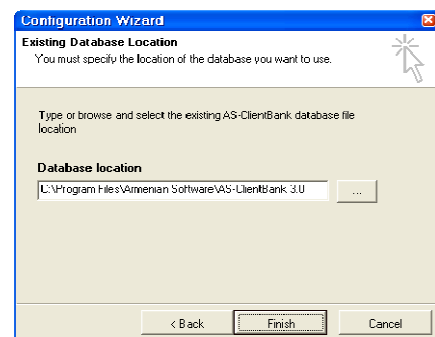
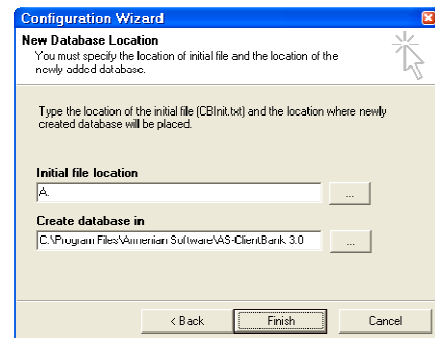
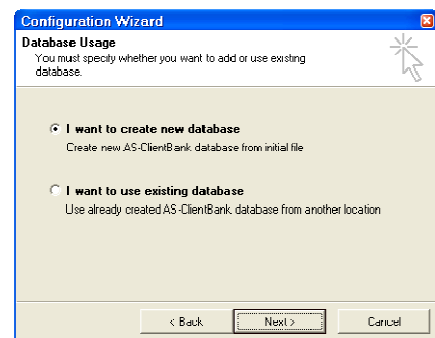
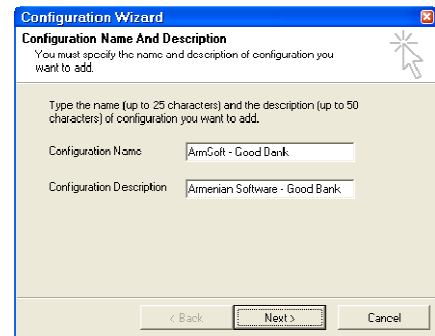
2. В случае удачного завершения действий выдается сообщение. При повторном запуске файла сертификата на экране появится окно следующего вида:



Создание конфигурации системы

При первом запуске системы предлагается создать новую конфигурацию. Конфигурация системы создается с помощью мастера конфигураций (Configuration Wizard) и состоит из следующих шагов:

1. На первом шаге заполняются поля наименования и описания конфигурации. Эти поля носят информативный характер.
2. Необходимо отметить создается ли новая база данных (при первом запуске) или используется (в случае сетевого эксплуатирования на остальных станциях) уже созданная.
3. При создании базы данных необходимо ввести или выбрать путь к файлу с начальными данными (прилагаемый файл "CBInit.txt") а также путь, где должен быть создан файл базы данных. Для завершения необходимо нажать "Finish".
4. При использовании существующей базы данных необходимо указать путь к файлу этой базы и нажать "Finish".



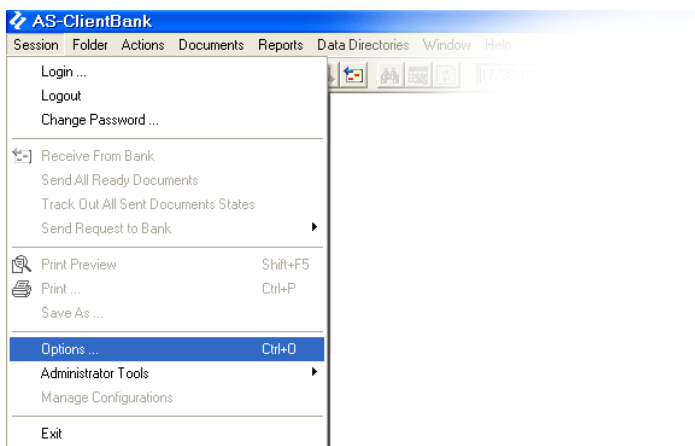
Первый вход в систему

При установке системы создается пользователь с административными привилегиями, именем "ADMIN" и пустым паролем. Для входа в систему остается лишь нажать "OK".

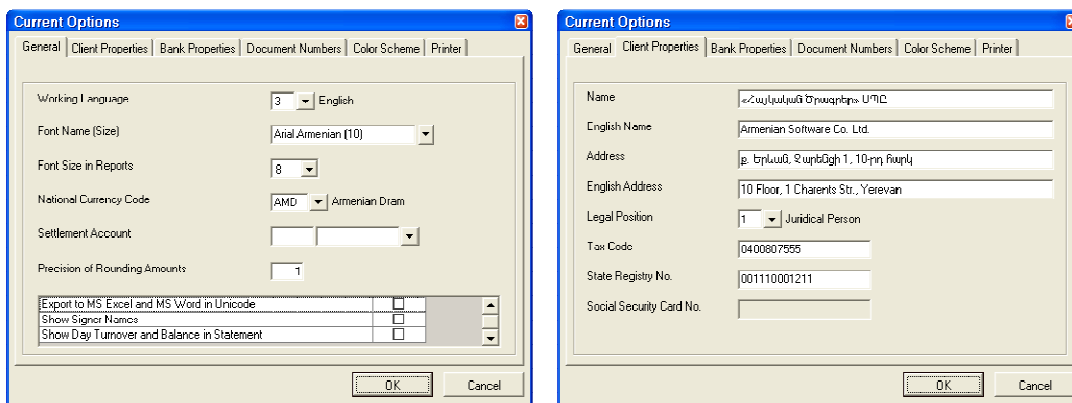


Ввод реквизитов клиента

При эксплуатации системы, например при создании платежных поручений реквизиты клиента автоматически заполняются в соответствующих полях документа. Поэтому желательно при первом же входе в систему заполнить эти данные. Для ввода реквизитов клиента необходимо выбрать пункт "Options" из меню "Session" или нажать "Ctrl+O".



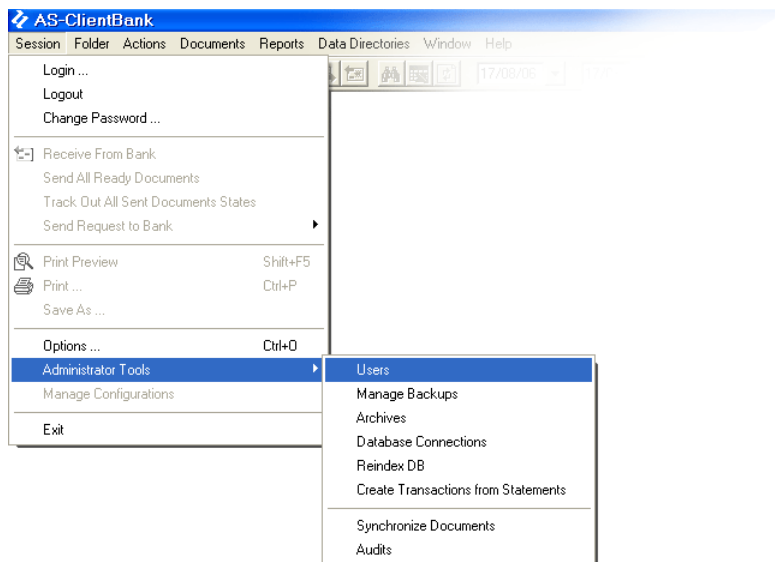
В открывшемся окне "Current Options" необходимо выбрать закладку "Client Properties" и ввести реквизиты. Окно "Current Options" также используется для настройки параметров системы, таких как, например, расчетный счет по умолчанию (поле "Settlement Account" из закладки "General"), язык (поле "Working Language" из закладки "General") и т.д.



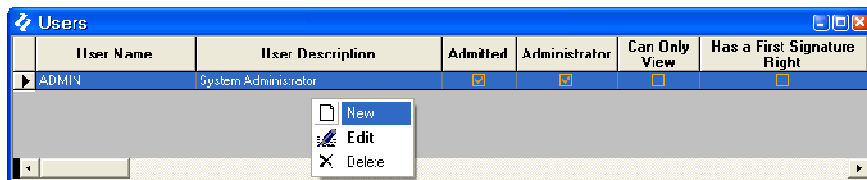
После внесения изменений необходимо нажать "OK". Если значение одного из полей введено неправильно, то система выдаст соответствующее сообщение.

Создание пользователей

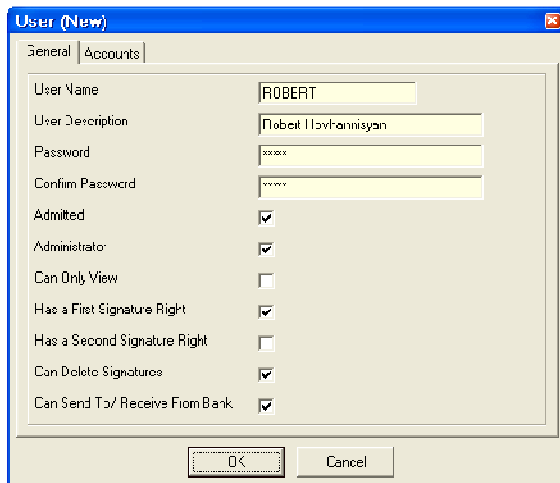
После установки системы необходимо создать пользователей системы со своими привилегиями (например, первой электронной цифровой подписи, второй и т.д.). Желательно иметь одного пользователя с административными привилегиями, а созданному по умолчанию пользователю "ADMIN" запретить вход в систему. Для создания пользователей необходимо выбрать пункт "Users" из подменю "Administrator Tools" меню "Session".



В открывшемся окне "Users" отображается список пользователей системы. Для создания пользователя необходимо из контекстного меню (или меню "Action") выбрать пункт "New".



В открывшемся окне "User" необходимо ввести данные пользователя, его привилегия (например, имеете администратор, право первой подписи, право второй подписи и т.д.) а также доступ к разным счетам клиента (из закладки "Accounts") и нажать "OK".



Для пользователей с привилегиями "Has a First Signature Right" (право первой подписи), "Has a Second Signature Right" (право второй подписи) и "Can Send To/Receive From Bank" (право обмена информацией с банком) поле описания пользователя ("User Description") будет использовано в качестве имени сертификата (ключа). Следовательно, в этом поле необходимо ввести имя и фамилию пользователя.



Внимание: Имена и фамилии пользователей с правом первой цифровой и/или второй цифровой подписи должны быть согласованы с банком. Банк принимает электронные документы посланные клиентом только в том случае, если первая и вторая подписи поставлены согласованными с банком пользователями.

Первый вход пользователя в систему

После того, как пользователи системы созданы, каждый пользователь может начать пользоваться системой, введя свое имя и начальный пароль.

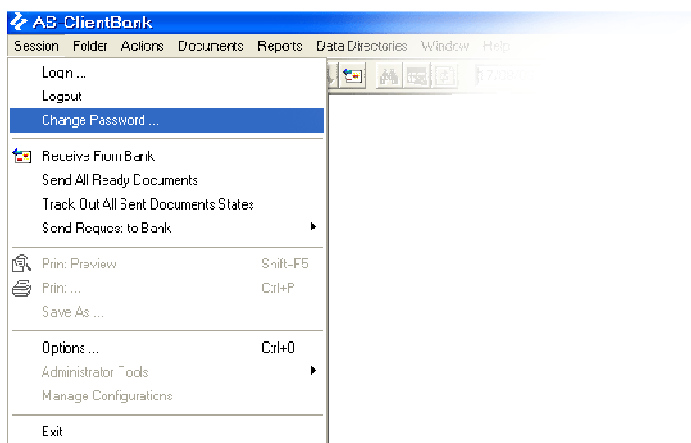


Если пользователю присвоено одно из следующих привилегий: право первой подписи, право второй подписи, право на обмен информацией с банком, то при входе система сообщит об отсутствии секретного ключа у пользователя (т.к. все вышеперечисленные привилегии требуют наличия сертификата с секретным ключом).

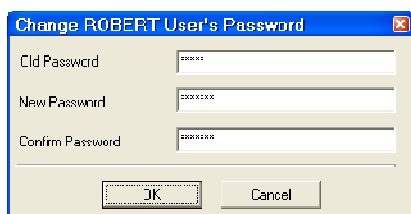


О том, как создать секретный ключ, послать в банк запрос на сертификат и получить сертификат смотрите ниже.

После входа пользователя в систему, он может изменить свой пароль. Для этого необходимо выбрать пункт "Change Password" из меню "Session":

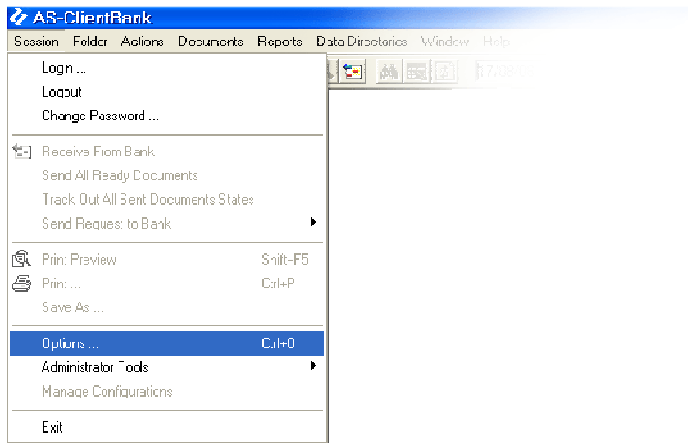


В открытом окне необходимо ввести текущий пароль, и два раза новый пароль, а затем нажать "OK".

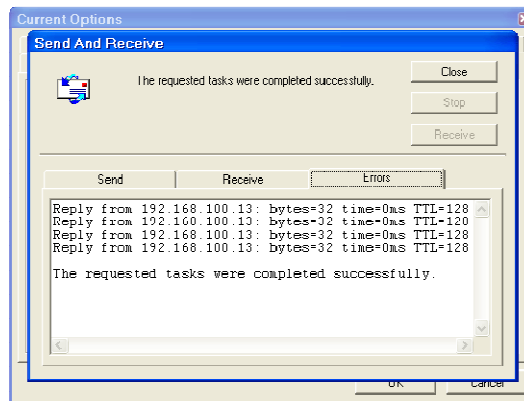
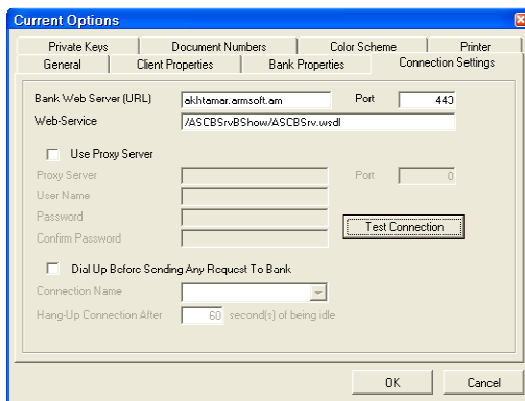


Проверка связи

Следующим важным шагом перед началом эксплуатации является проверка наличия связи с банком. Для этого необходимо выбрать пункт "Options" из меню "Session".



Из открывшегося окна "Current Options" необходимо выбрать закладку "Connection Settings" и нажать кнопку "Test Connection". При наличии связи система выдаст соответствующее сообщение.



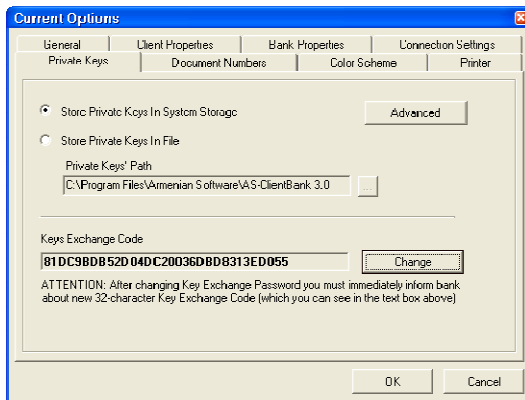
Если тест завершился неудачно, то причинами могут быть:

- отсутствие связи Интернет связи,
- настройки прокси сервера,
- сертификат банка не установлен

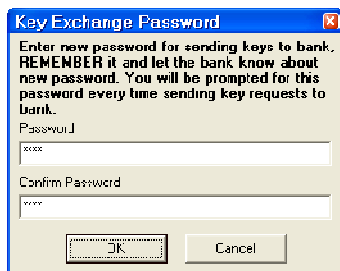
Пароль смены ключей

Перед тем как пользователи системы смогут послать запросы на сертификат (открытые ключи) в банк администратор системы должен назначить пароль смены ключей.

Для назначения пароля смены ключей администратором системы, необходимо выбрать пункт "Options" из меню "Session". Из открывшегося окна "Current Options" необходимо выбрать закладку "Private Keys" и нажать "Change".



В открывшемся окне необходимо ввести пароль смены ключей и нажать "OK".



Пароль смены ключей нигде не хранится и, следовательно, администратор должен запомнить его (как каждый пользователь помнит свой пароль входа в систему). Этот пароль используется каждый раз при смене ключей, т.е. при отправке запроса на сертификат (открытого ключа) в банк и при получении созданного в банке сертификата (заверенного банком открытого ключа).

После ввода пароля смены ключей система на его основании генерирует *код смены ключей*, который отображается в поле "Keys Exchange Code" (в закладке "Private Keys" открытого окна "Current Options").

Код смены ключей представляет собой последовательность из 32 символов, которая с помощью специальных преобразований (алгоритма MD5-hash) получается из *пароля смены ключей*, причем имея этот код невозможно получить начальный пароль.



Внимание: После изменения пароля смены ключей, сгенерированный *код смены ключей* должен быть согласован с банком. Банк принимает запрос на сертификат только в том случае, если ему известен код смены ключей.

Получение сертификата

Для обмена информацией с банком и/или цифровой подписи электронных документов пользователю необходимо иметь свой сертификат с секретным ключом. Этот сертификат используется банком для идентификации пользователя.

По этой причине каждый пользователь, имеющий хотя бы одну из привилегий подписи или право обмена информацией с банком, должен сгенерировать пару (секретный и открытый) ключей и отправить запрос на сертификат (открытый ключ) в банк. На основе этого запроса банк создает для пользователя сертификат (заверенный банком открытый ключ). После того, как пользователь получит свой сертификат, он может ставить подписи и/или обмениваться информацией с банком.

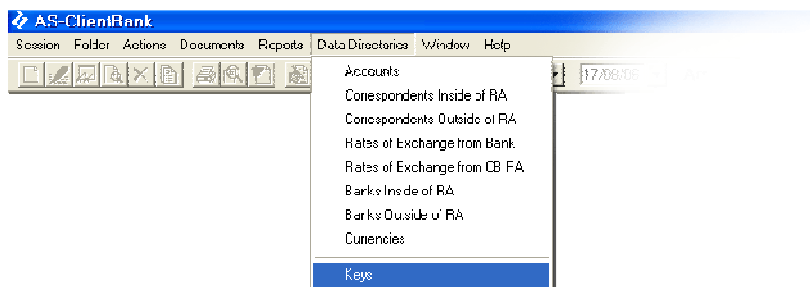
Итак, для получения сертификата пользователю необходимо:

1. сгенерировать пару (секретный и открытый) ключей и запрос на сертификат,
2. отправить запроса на сертификат (открытый ключ) в банк,
3. получить сертификат (заверенный банком открытый ключ).

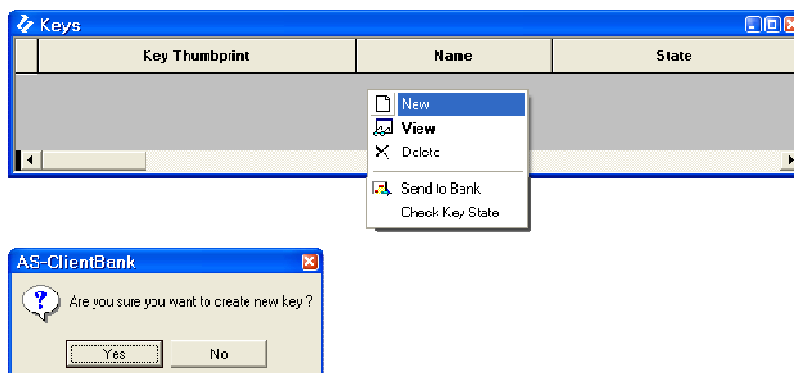
1. Генерация пары (секретного и открытого) ключей

Для того чтобы сгенерировать пару ключей необходимо:

1. Выбрать пункт "Keys" из меню "Data Directories"



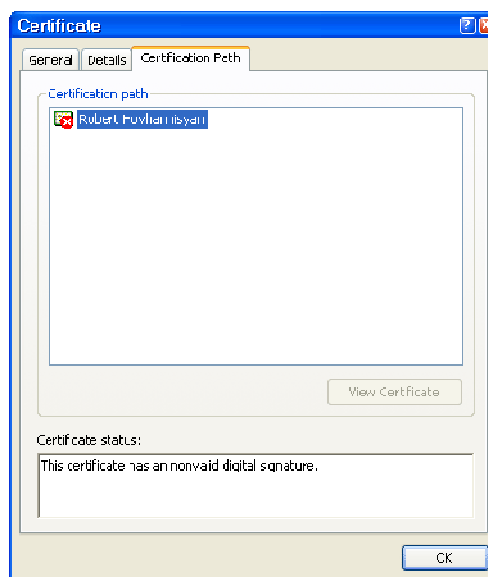
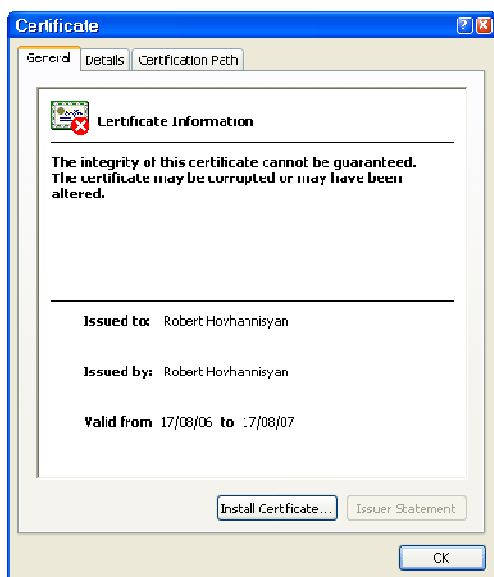
2. Из открытого окна "Keys", где отображается список сертификатов, необходимо выбрать пункт "New" контекстного меню и подтвердить генерацию.



Если генерация успешно завершилась, то система выдаст соответствующее сообщение, а в списке сертификатов добавится соответствующая новая строка со статусом "Created" (статус отображается в колонке "State" списка "Keys").



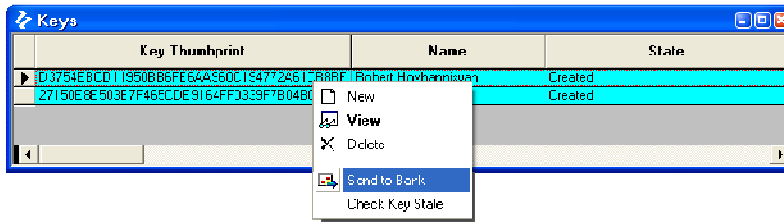
Для просмотра нового сгенерированного ключа необходимо выбрать пункт "View" контекстного меню списка сертификатов, при этом отобразится окно следующего вида:



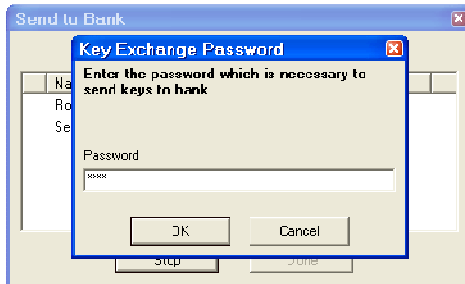
2. Отправка в банк запроса на сертификат (открытого ключа)

После того как пара ключей сгенерирована, она еще не готова к использованию для подписи и обмена информацией с банком. Необходимо отправить запрос на сертификат (открытый ключ) в банк для заверения. Для этого необходимо:

1. выбрать пункт "Keys" из меню "Data Directories".
2. в открытом списке "Keys" отметить (с помощью клавиши "Insert") тот, или те сертификаты, которые необходимо отправить в банк.
3. выбрать пункт "Send to Bank" из контекстного меню открытого списка "Keys".



4. в отображенном окне "Key Exchange Password" ввести пароль смены ключей



5. Если пароль смены ключей был правильно введен, отмеченные запросы на сертификат будут отправлены в банк.

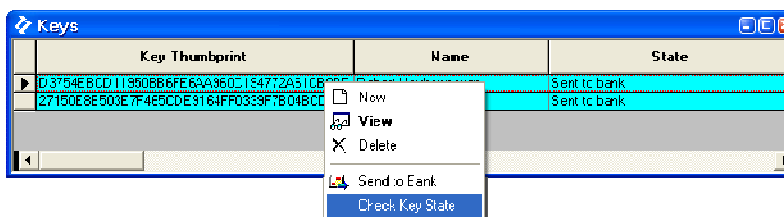


После того как запросы на сертификаты были отправлены в банк, в списке "Keys" сертификатов значение колонки статуса ("State") соответствующих строк изменится на "Send To Bank".

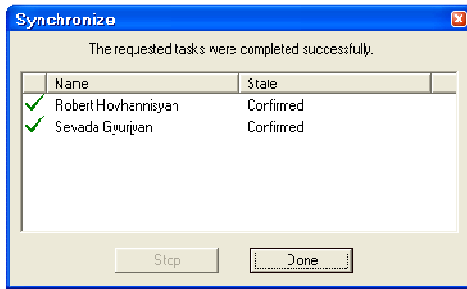
3. Проверка статуса запроса на сертификат

Для проверки статуса отправленного запроса на сертификат необходимо:

1. выбрать пункт "Keys" из меню "Data Directories";
2. в открытом списке "Keys" отметить (с помощью клавиши "Insert") тот, или те сертификаты, статусы которых необходимо проверить;
3. выбрать пункт "Check Key State" из контекстного меню открытого списка "Keys";



4. в отображенном окне "Key Exchange Password" ввести пароль смены ключей;
5. если пароль смены ключей был правильно введен, статусы отмеченных запросов на сертификат будут проверены. А в случае, если банк заверил эти запросы, созданные на их основании сертификаты будут получены.



После проверки статуса запроса, в списке сертификатов значение колонки статуса ("State") соответствующих строк изменится на "Confirmed"(заверен банком) или "Refused"(отклонен банком). Если запрос на сертификат был заверен банком, то изменятся также значения колонок "Valid From" и "Valid To" - период времени, когда данный сертификат считается действительным (имеющим силу) и может быть использован для подписи и обмена информацией с банком.

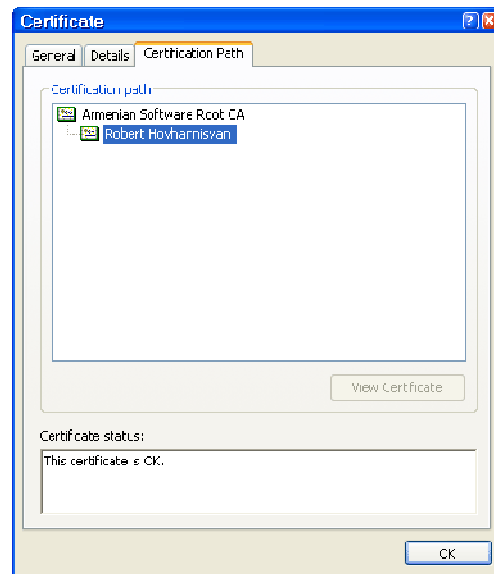
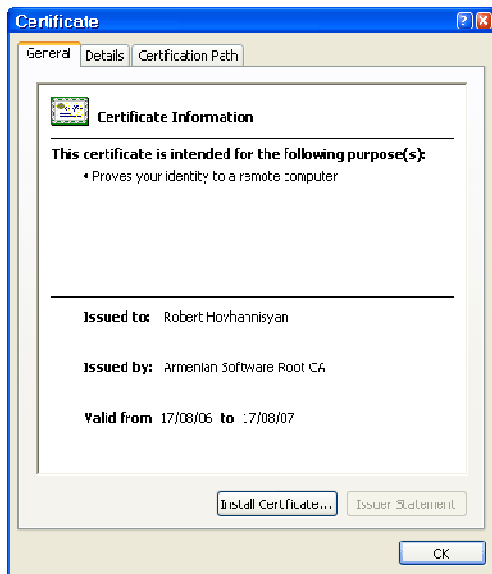


Внимание: Заверенный банком сертификат действителен в течение одного года с момента заверения. По истечении срока действия сертификата необходимо выполнить шаги, описанные выше в разделе "Получение сертификата".



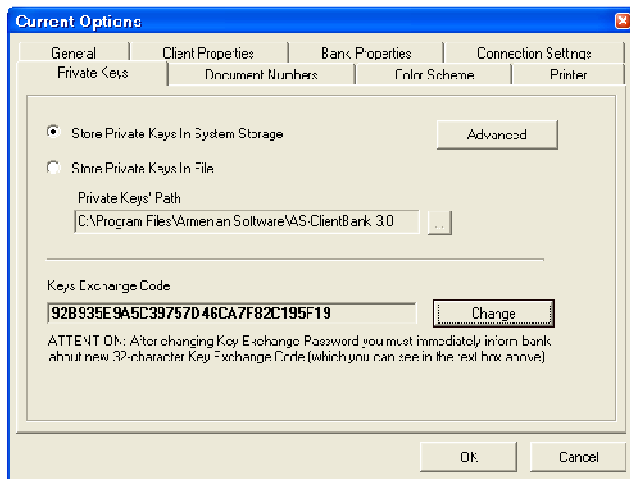
Внимание: После отправки запроса на сертификат в банк, отпечаток (Thumbprint) отправленного запроса должен быть сообщен банку. Банк заверит запрос на сертификат только в том случае, если клиент согласует с ним отпечатки отправленных запросов. Отпечаток запроса на сертификат отображается в колонке "Key Thumbprint" списка ключей (пункт "Keys" меню "Data Directories").

Для просмотра заверенного банком сертификата необходимо выбрать пункт "View" контекстного меню списка сертификатов, при этом отобразится окно следующего вида:



Вход пользователя в систему после получения сертификата

По умолчанию сертификат и секретный ключ пользователя запоминаются в хранилище сертификатов Windows. Настройки хранилища можно изменить из вкладыша "Private Keys" окна "Current Options".



При желании пользователь может изменить хранилище, выбрав "Store Private Keys In File" (запомнить секретный ключ в файле) и указать путь, где секретный ключ должен храниться. После изменения этого параметра, при следующем входе система сообщит о том, что ключ будет сохранен в файле по указанному пути.



Если путь находится на внешнем носителе, то система предложит установить носитель для последующего сохранения секретного ключа.