



ДБО BS-Client v.3.0
(система «Интернет-Клиент-Банк»)
Подсистема «Интернет-Клиент»
Перегенерация ключей СКЗИ MS Crypto API 2.0

версия от 01.02.2016

Перегенерация ключей СКЗИ MS Crypto API 2.0

1. Общая схема регенерации ключей СКЗИ MS Crypto API 2.0

Процедура регенерации ключа включает в себя несколько этапов:

- Клиент формирует в подсистеме «Интернет-Клиент» (Подсистема) новые секретные ключи, запрос на сертификат и посылает запрос в Банк.
- Банк получает запрос на сертификат и посылает Клиенту сообщение.
- Клиент получает сообщение Банка о получении запроса и продолжает работу в системе «Интернет-Клиент-Банк» (Система) на старых ключах.
- В Банке формируется сертификат, после чего Банк загружает сертификат в Систему.
- Банк регистрирует сертификат и отправляет его клиенту.
- Клиент получает новый сертификат, регистрирует его в Подсистеме.
- Начинается работа с новыми ключами.

2. Создание запроса:

1 этап (генерация ключа и запрос на регистрацию вновь созданного сертификата):

Для того чтобы регенерировать ключ, выполните действия:

- ☞ Войдите в Подсистему.
- ☞ Откройте дерево Сервис.
- ☞ Раскройте ветку Безопасность.
- ☞ Запустите форму Профили.

Перегенерация комплекта ключей

В следующей таблице представлена информация о состоянии ключевых комплектов абонентов, которые Вам доступны. В зависимости от статуса ключевого комплекта с помощью двойного нажатия левой кнопки мыши выполняются следующие действия:

- "в эксплуатации" - переход к форме запроса на регенерацию ключей;
- "необходима первичная регенерация" - переход к форме запроса на регенерацию ключей;
- "необходима плановая регенерация" - переход к форме запроса на регенерацию ключей;
- "принят банком" - запрос на регенерацию обрабатывается банком;
- "получен новый сертификат" - переход к форме получения нового сертификата;
- "получен отказ в регистрации" - просмотр сообщения о причине отказа в регистрации сертификата.

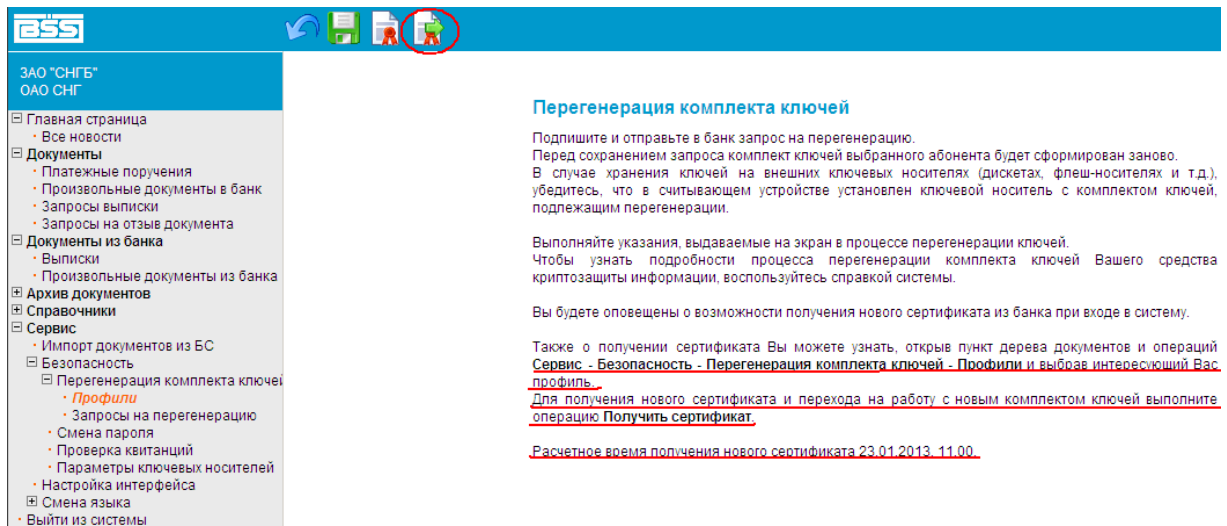
Выберите абонента для регенерации

Абонент	Идентификатор	Криптография	Статус
002 test inet ЭЦП01	7B59C5F9000000000008	Ms Crypto API 2.0	в эксплуатации
002 test 20130108	108FCB08000000000859	Ms Crypto API 2.0	в эксплуатации

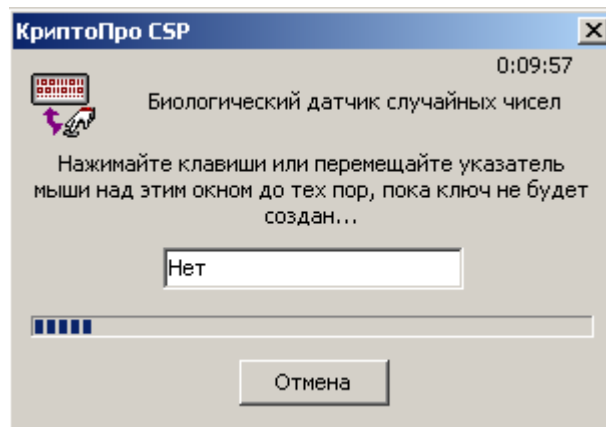
Параметры подписи

Наименование профиля	002 test inet ЭЦП01
Идентификатор	7B59C5F9000000000008
Криптография	Ms Crypto API 2.0
Тип ключа	рабочий
Дата начала срока эксплуатации	29.06.2011
Дата окончания срока эксплуатации	29.09.2013

- ☞ В следующем окне ознакомьтесь с условиями регенерации нажмите кнопку «Отправить документ в банк»

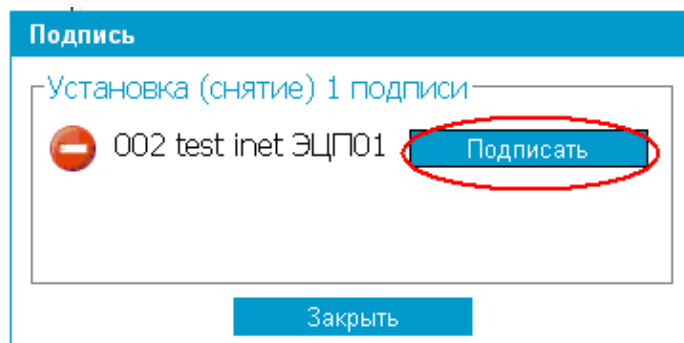


Система предложит вставить ключевой носитель (флешку или eToken, полученный в банке) и создаст в нем новый контейнер с секретными ключами. Во время процедуры создания новых ключей СКЗИ предложит нажимать клавиши или двигать мышью на экране:



После выполнения этой процедуры Вам будет предложено установить пароль на создаваемый носитель (необязательно при использовании флешки, при использовании eToken необходимо ввести действующий пин-код). Нажмите **Ок**.

☞ Подпишите запрос, нажав в данном окне кнопку «Подписать»



Запрос на регистрацию нового сертификата передается в Банк. На экране появится акт. Нет необходимости его распечатывать, можно просто продолжить работу в системе.

Ваш запрос на генерацию нового сертификата поставлен в очередь.
Расчетное время завершения процесса 23.01.2013, 11.00.

Печать

**АКТ
признания открытого ключа (сертификата)
для обмена сообщениями**

" ____ " _____ 20 ____ г.

г. _____

Настоящим Актом признается открытый ключ шифрования, принадлежащий уполномоченному представителю
ОРГАНИЗАЦИИ: 002inet (002 test inet ЭЦП01).

Параметры ключа:

Алгоритм: ГОСТ Р 34.10-2001(1.2.643.2.2.19), Parameters: 3012 0607 2A85 0302 0224 0006 072A 8503 0202 1E01

Текст открытого ключа:

```
0440 A5E1 6773 246E C326 974A 4F1E 7158 56CF
A9C5 36B4 884E F59F 7787 3694 891A 8E94 5428
6D02 F0B1 3333 3925 10D1 6E8D 1F70 CE9E C2D7
29F4 921E 29F4 DCE8 A16F 9231
```

Дополнительные поля открытого ключа (сертификата):

Имя владельца ключей: 002inet

Ключ зарегистрирован и может использоваться для обмена сообщениями.

БАНК

КЛИЕНТ

М.П.

М.П.

☞ Затем необходимо известить администратора системы о намерении перейти на новые ключи по тел.: 39-88-77 или по электронной почте dbo@sngb.ru

☞ Пока новый сертификат не сформирован Банком, Вы продолжаете работать с системой Интернет-Клиент на старых ключах.

3. Обработка ответа банка на запрос:

☞ Откройте дерево **Сервис**.

☞ Раскройте ветку **Безопасность**.

☞ Запустите форму **Профили**.

☞ Найдите сертификат со статусом **«Получен новый сертификат»**, щёлкните по нему левой кнопкой мыши дважды:

БСС

ЗАО "СНГБ"
ОАО СНГ

- Главная страница
 - Все новости
- Документы
 - Платежные поручения
 - Произвольные документы в банк
 - Запросы выписки
 - Запросы на отзыв документа
- Документы из банка
 - Выписки
 - Произвольные документы из банка
- Архив документов
- Справочники
- Сервис
 - Импорт документов из БС
 - Безопасность
 - Перегенерация комплекта ключей
 - Профили
 - Запросы на регенерацию
 - Смена пароля
 - Проверка квитанций
 - Параметры ключевых носителей

Перегенерация комплекта ключей

В следующей таблице представлена информация о состоянии ключевых комплектов абонентов, которые Вам доступны.
В зависимости от статуса ключевого комплекта с помощью двойного нажатия левой кнопки мыши выполняются следующие действия:

- "в эксплуатации" - переход к форме запроса на регенерацию ключей;
- "необходима первичная регенерация" - переход к форме запроса на регенерацию ключей;
- "необходима плановая регенерация" - переход к форме запроса на регенерацию ключей;
- "принят банком" - запрос на регенерацию обрабатывается банком;
- "получен новый сертификат" - переход к форме получения нового сертификата;
- "получен отказ в регистрации" - просмотр сообщения о причине отказа в регистрации сертификата.

Выберите абонента для регенерации

Абонент	Идентификатор	Криптографил	Статус
002 test inet ЭЦП01	7B59C5F9000000000008	Ms Crypto API 2.0	получен новый сертификат
002 test 20130108	108FCB060000000000859	Ms Crypto API 2.0	в эксплуатации

☞ Установите ключевой носитель, и нажмите кнопку **Ок**.

⇒ На экране появится следующее описание **Процесса регенерации секретного ключа**.

Перегенерация комплекта ключей

Из банка получен новый сертификат для абонента "002 test inet ЭЦП01". Для завершения формирования нового комплекта ключей и ввода их в эксплуатацию нажмите кнопку "Продолжить".

Продолжить

☞ Нажмите кнопку **Продолжить**.

⇒ Через непродолжительное время Вы получите сообщение о завершении процедуры регенерации секретного ключа и переводе на новый комплект ключей.

Перегенерация комплекта ключей

Вы переведены на работу с новым комплектом ключей.

☞ Новый сертификат зарегистрирован Банком, Вы можете работать с новым комплектом ключей.