www.rapida.ru

# Часть 3. Общие Технические требования.

# Раздел 1. Использование сертификатов

| | |
|---|---|
| Код документа: | EXT.2.03.05.00002.004 |
| Версия: | 004 |
| Статус: | Действующий |
| Дата: | 01.06.2017 |

# Оглавление

## История изменений документа

| Версия | Дата | Внесенные изменения |
|---|---|---|
| 1.01 | 18.11.2011 | Начальная версия<br>(замена устаревшего документа) |
| 1.02 | 21.11.2011 | Добавлен раздел:<br>Формирование сертификата формата PKSC12 |
| 1.03 | 24.11.2011 | Обновлен пункт о месте хранения файла Акта признания открытого ключа |
| 004 | 01.06.2017 | Внесены правки в соответствии с реорганизацией 28 апреля 2017 КИВИ Банк (АО) в форме присоединения к нему ООО НКО «Рапида». Изменена структура и нумерация документа Внесены уточняющие правки по всему тексту. |

## Общие положения

Для получения Участнику Системы доступа к КИВИ Банк (АО) (далее Банк) в рамках взаимодействия с платежными и служебными сервисами Рапида (далее Система) необходимо разрешение Системы – сертификат доступа (безопасности). В Системе используется несколько видов сертификатов.

# 1. Виды сертификатов

## *1.1. Основной сертификат*

Основной сертификат открытого ключа Участника (далее просто сертификат) используется для передачи запросов со стороны Участника на сервера Системы при использовании собственного программного обеспечения Участника и/или при использовании программы АРМ «Платежи и Переводы».

Для работы Участнику выдается как минимум два вида основного сертификата.

- «Тестовый» сертификат - предназначен для «тестового» режима работы. Тестовый - режим обучения, в котором можно делать все доступные операции, которые не несут никаких финансовых или других обязательств сторон. Тестовый сертификат может быть получен Участником и до заключения договора при проведении технологического тестирования. Тестовый сертификат может быть далее использован Участником для целей тестирования обновлений протокольных решений и/или обучения сотрудников.

Тестовый сертификат НЕ может быть переведен в «рабочий» режим

- «Рабочий» - предоставляется после заключения договора и окончания этапа тестирования со стороны Участника для доступа в Рабочий режим работы. Рабочий режим - режим, в котором манипуляции запросами приводят к реальным финансовым обязательствам/требованиям сторон или реальным записям в Системе. Например, формирование шаблонов платежей для их дальнейшего использования.

## *1.2. Сертификат для доступа к АРМ «Кабинет Агента»*

Указанный сертификат:

- Устанавливается на ПК, с которых необходим доступ к информационному АРМу Системы.
- Не влияет на возможность/невозможность проведения платежей.
- Не может быть идентичным сертификату 1.1.
- Не имеет режима работы в тестовом режиме. Выдается только после заключения договора. (Тестовый сертификат отсутствует.)

## 2. Порядок и сроки получения сертификатов

Сертификаты выдаются:

А) для начала работы с системой;

Б) при истечении срока действия;

В) при компрометации секретного ключа.

Сертификаты выдаются в течение одних рабочих суток. Запрос, пришедший во второй половине рабочего дня, может быть принят обработке не ранее первой половины следующего рабочего дня.

При замене сертификата запрос от Участника должен генерироваться не менее чем за 2 рабочих дня до истечения срока действующего сертификата. В последний день действуют оба сертификата.

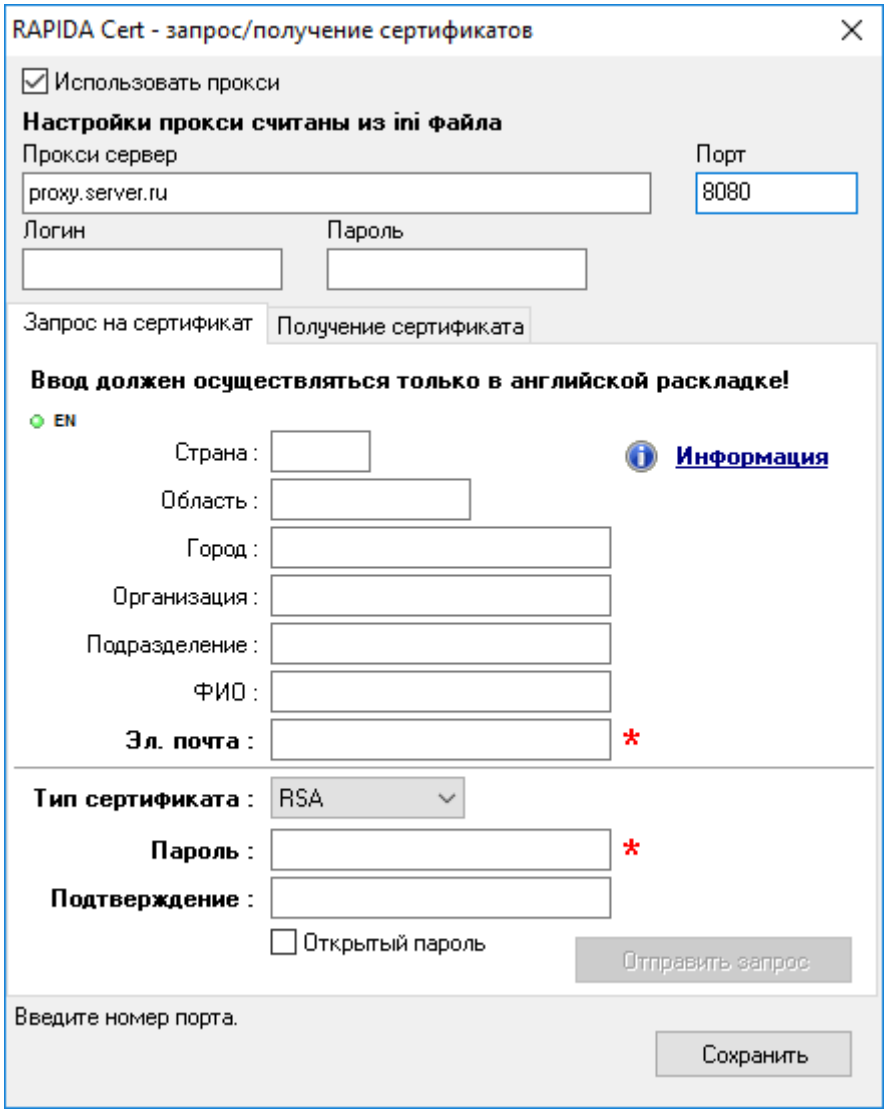
При компрометации секретного ключа доступ к системе блокируется по запросу заинтересованной стороны.

# 3. Алгоритм получения и установки сертификата 1.1.

Уполномоченным сотрудником Участника генерируется запрос на сертификат. Запрос может быть создан с использованием программного обеспечения Системы и с помощью стороннего программного обеспечения.

## *3.1. Использование программы RAPIDA Cert*

1) Скачать по адресу http://soft.rapida.ru/crt АРМ для работы с сертификатами и установить его.
2) При использовании прокси-сервера для соединения с Интернет необходимо задать настройки сервера. В основном окне необходимо заполнить все поля. Допустимо использовать только латинские (английские) символы.




3) В том же окне необходимо выбрать Тип сертификата RSA или ГОСТ, при выборе RSA- ввести пароль для закрытого ключа (английскими буквами и **не более 16 символов**). Этот пароль

рекомендуется записать и сохранить в надежном месте (сейф и т.п.). Пароль известен только Участнику и не известен Системе(Банку).

4) Отправить запрос на сертификат в Систему, нажав на соответствующую кнопку. После отправки запроса на сертификат необходимо вывести на печать 2 экземпляра «Акта признания открытого ключа» по установленному образцу (после генерации запроса файл Акта ***<ваш E-mail>*.rtf** находится или в папке с установленной программой …**RapidaCert\<ваш E-mail>**) или в папке пользователя (возможный путь:**%USERPROFILE%\Local Settings\Application Data\RapidaCert\<ваш E-mail>**).

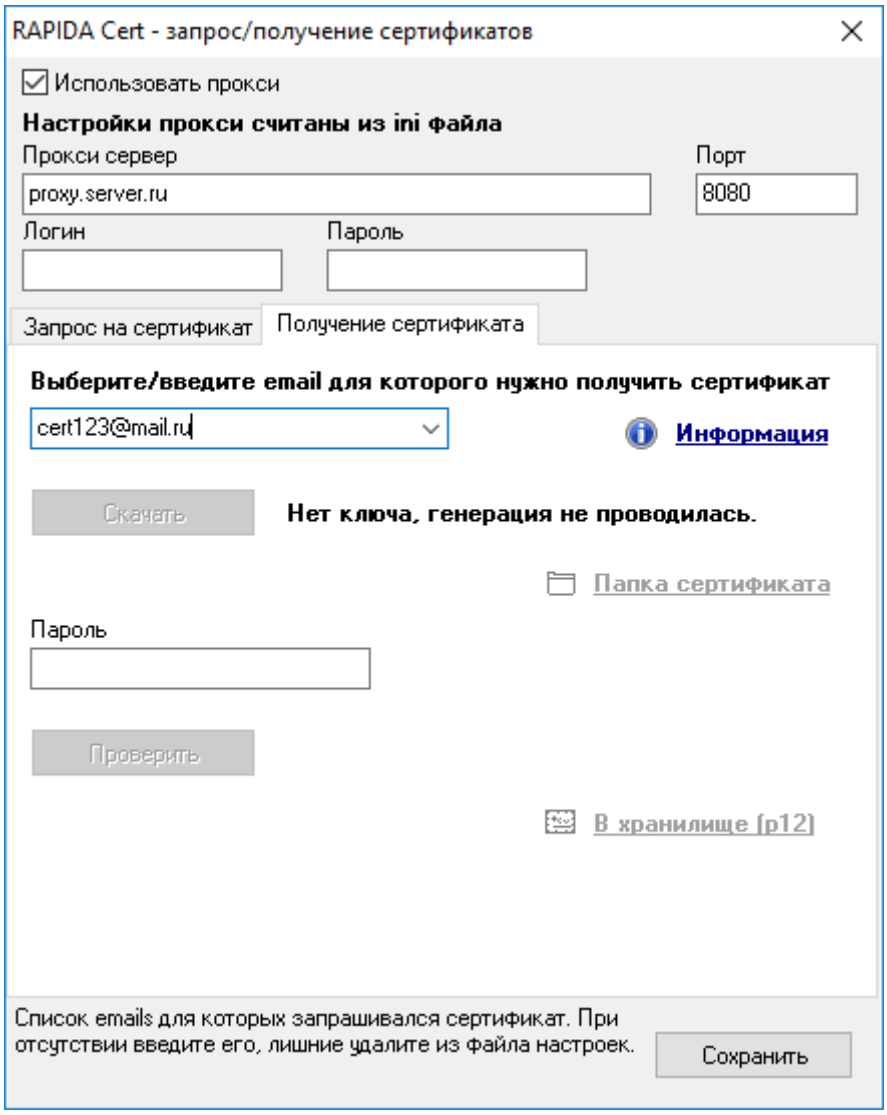
Путь может зависеть от версии Windows и способа ее установки. Акт подписывается руководителем организации, заверяется печатью и в двух экземплярах направляется в Банк. Далее свяжитесь с курирующим менеджером – проинформируйте о факте создания запроса. Программу можно закрыть.

Письмо–уведомление, посылаемое по электронной почте курирующему менеджеру в Банке, о выдаче сертификата должно иметь следующий вид:

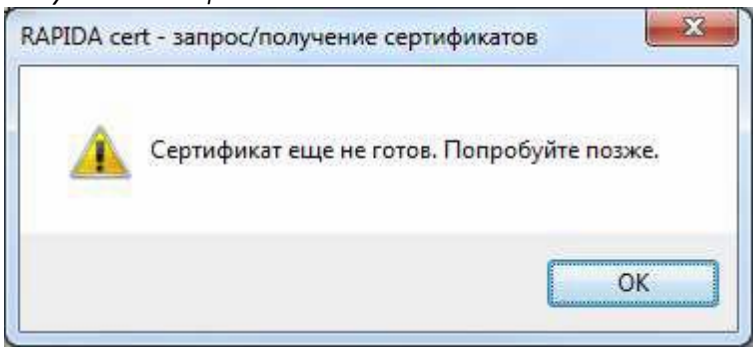
- название организации, запросившей сертификат;
- название точки, запросившей сертификат;
- адрес электронной почты, указанный в запросе на сертификат;
- режим использования сертификата: тестовый или рабочий.

3) Менеджер информирует о готовности сертификата. Дождитесь уведомления от Системы о выдаче сертификата.

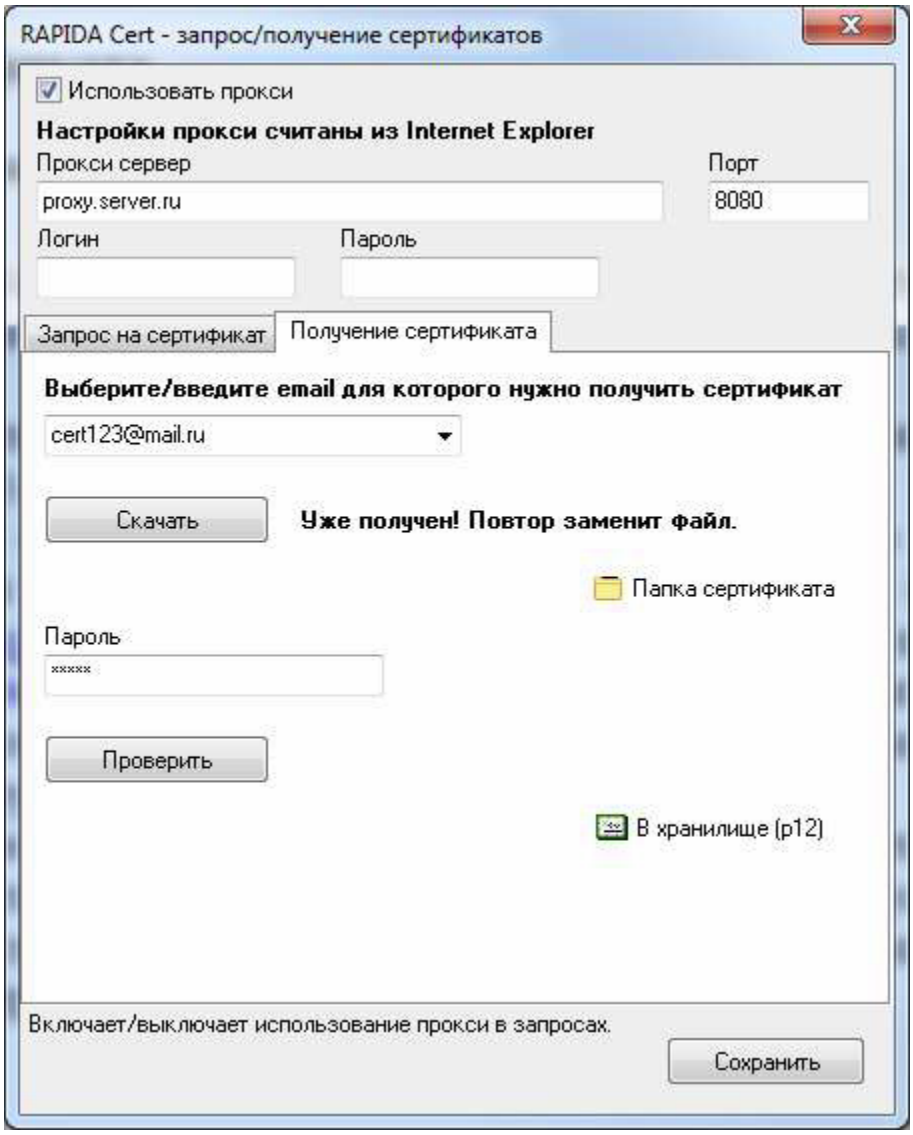
4) Как только менеджер Банка сообщает о готовности сертификата, еще рез запускаем программу и переходим на закладку "Получение сертификата". Получаем сертификат, нажав кнопку «Скачать».




*До получения сообщения о готовности сертификата от курирующего менеджера нажимать на кнопку «Скачать» не имеет смысла. Если сертификат не готов Участник получит сообщение вида:*




5) Если это необходимо, то чтобы добавить сертификат в хранилище, необходимо преобразовать его в формат p12 (PKCS12). Для этого можно воспользоваться встроенной в АРМ функцией "В хранилище (p12)". Для преобразования необходимо ввести известный Участнику пароль закрытого ключа.




Также смотри раздел: 6. Формирование сертификата формата PKSC12

## *3.2. Получение сертификата через АРМ «Платежи и переводы»*

Файлы с сертификатами находятся в папке
**..[Каталог программы]\Data\Key**.

Каталог программы – это каталог, в котором установлена программа. При выполнении установки «по умолчанию», каталог программы зависит от версии, разрядности и способа установки системы Windows.

Например:
**C:\Program Files\Rapida\PaymMaster\Data\Key**

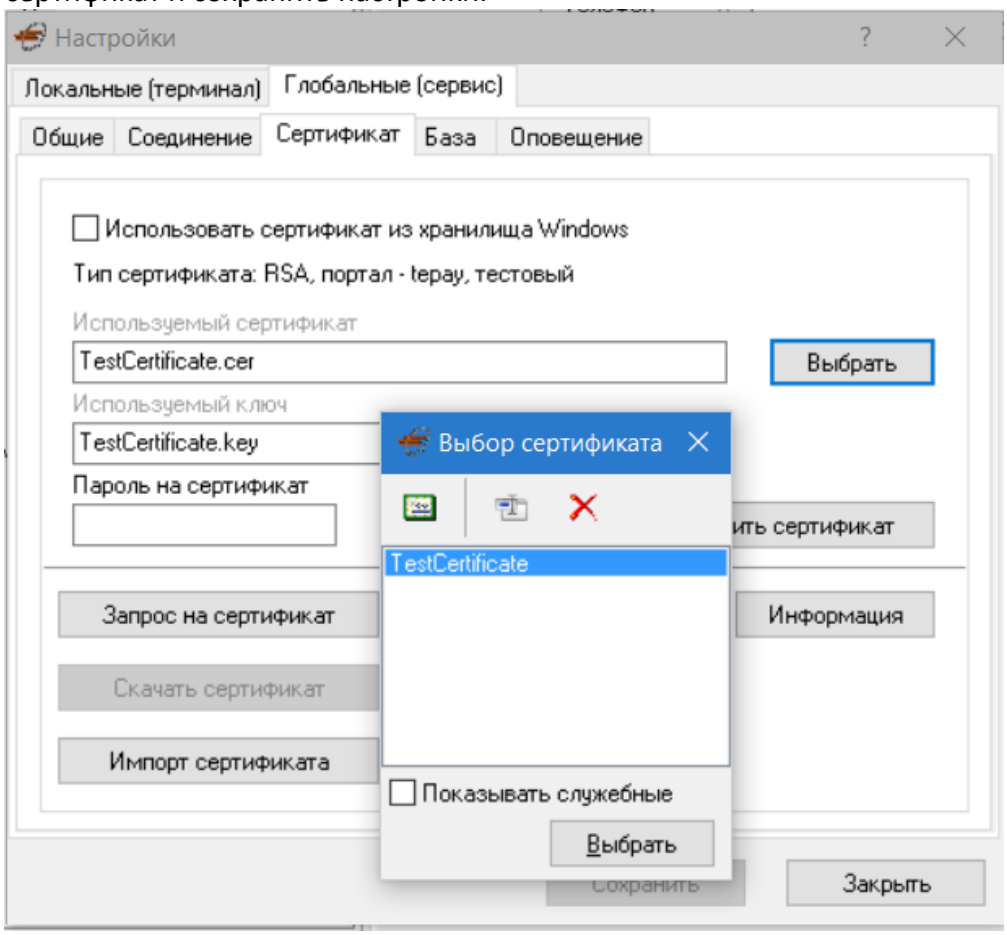
Основными файлами являются:
**Certificate.cer** - рабочий файл сертификата,
**Certificate.key** – рабочий файл ключа.
***Если сертификат необходимо получить впервые, то этих файлов в папке нет.***

**Request.cer, Request.key** – файл сертификата и ключа для получения рабочего сертификата от Банка. Данные файлы должны обновляться не реже одного раза в год. Обновления скачиваются с сайта https://soft.rapida.ru.

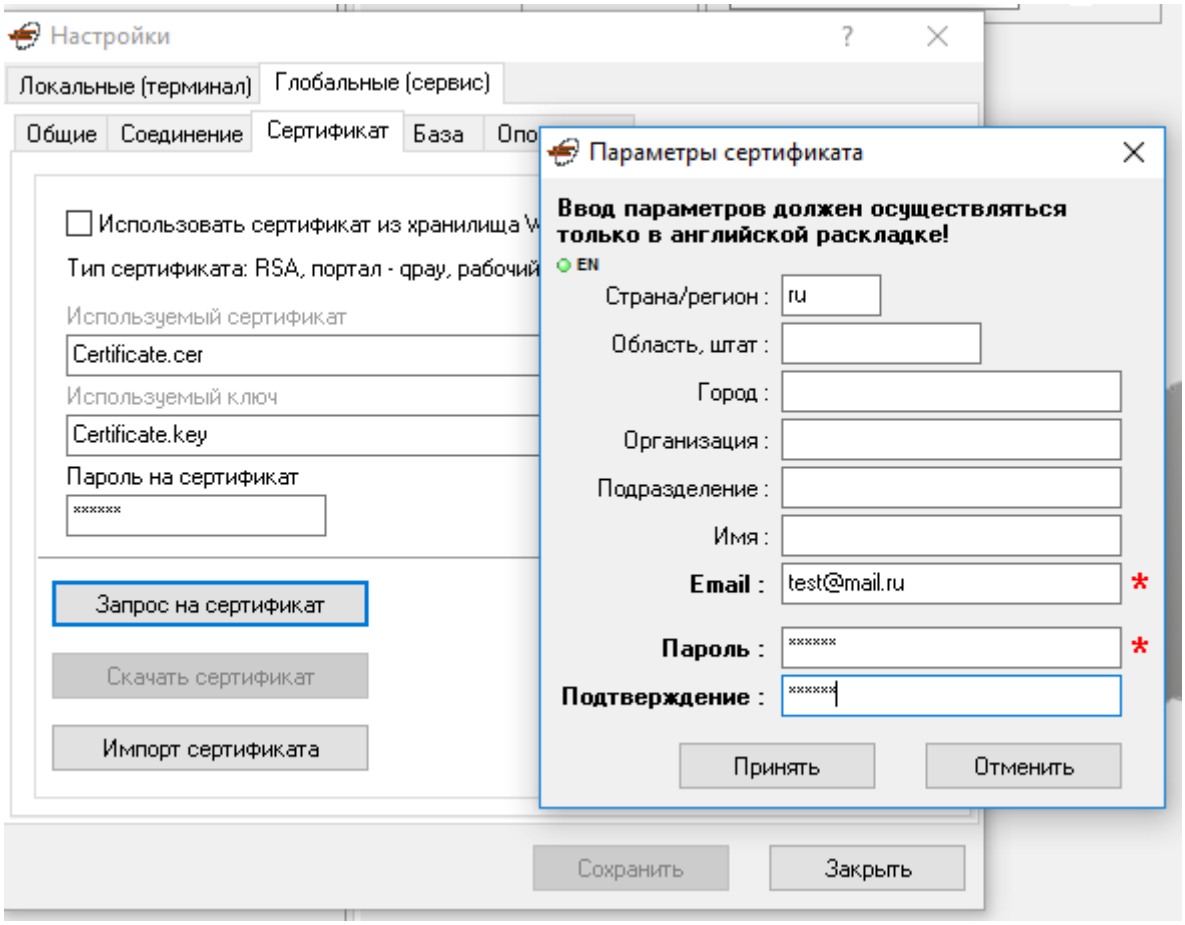
**Внимание!** Через данное ПО генерируются только RSA сертификаты. Но использоваться могут и выпущенные на алгоритме ГОСТ. Запрос сертификатов с алгоритмом ГОСТ в этом случае осуществляется через ПО RapidaCert.

1) Найти в меню **Действия/Настройки/Глобальные (сервис)/Сертификат**
2) Нажимаем кнопку **«Выбрать»** и вид сертификата **Certificate.**

На той же странице настроек можно выбрать и проверить другой полученный сертификат и сохранить настройки.



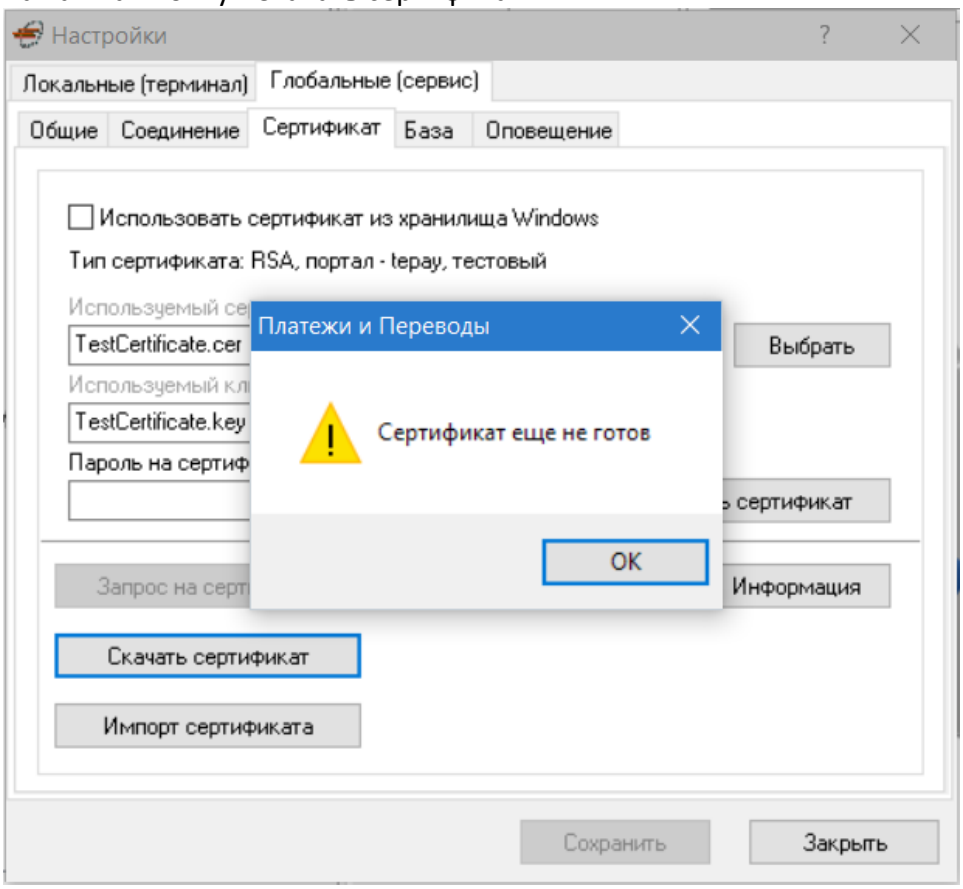

3) Далее генерируем запрос на сертификат. Для этого заполняем обязательные поля и отправляем запрос




Запрос автоматически отправляется в Систему.

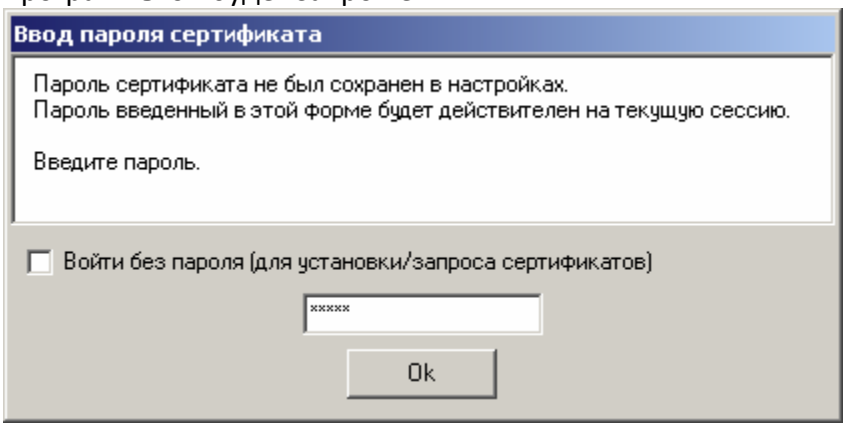
4) После отправки запроса на сертификат свяжитесь с курирующим менеджером.
5) Письмо–уведомление, посылаемое по электронной почте курирующему менеджеру в Банке, о выдаче сертификата должно иметь следующий вид:
   - название организации, запросившей сертификат;
   - название точки, запросившей сертификат;
   - адрес электронной почты, указанный в запросе на сертификат;
   - режим использования сертификата: тестовый или рабочий;

Проверить готовность сертификата до истечения положенного времени можно, нажав на кнопку «Скачать сертификат».




6) При успешном запросе формируется файл приватного ключа Certificate.key и дается возможность скачать сам сертификат.
7) Скачиваем сертификат - файл с именем Certificate.cer.

Если пароль сертификата не сохранен (пустой при сохранении), то при старте программы он будет запрошен.




Вводится он один раз на сессию (время работы программы), т.е. при перезапуске программы пароль сбрасывается, и его придется вводить еще раз. При работе нескольких клиентов, работающих с общей программой, пароль вводится только один раз, первым подключившимся клиентом.

# 4. Алгоритм получения и установки сертификата 1.2

Сертификат для доступа к «Кабинету Агента» выдается без специального программного обеспечения на стороне Участника.

Последовательность действий

1) Участник информирует по электронной почте курирующего менеджера в Банке о необходимости выдать сертификат.
2) Банк выпускает сертификат и отправляет двумя письмами на адрес, указанный Участником. В одном письме содержится сертификат, в другом – пароль. Письма приходят на один адрес электронной почты.

Дополнительно в письме приходит подробная инструкция по установке сертификата в систему.

# 5. Замена сертификата

## *5.1. Причины замены сертификатов*

Одна из характеристик сертификата – срок действия. Сертификат всегда выпускается с ограниченным сроком действия, который равен, как правило, двум годам для сертификата 1.1 и одному году для сертификата 1.2.

При истечении срока действия сертификата, прием платежей (либо доступ к иному ресурсу Системы) полностью БЛОКИРУЕТСЯ.

Еще одной особенностью сертификата является то, что он является основным идентифицирующим Участника механизмом и обеспечивает доступ к финансам Участника. И если секретный ключ становится доступным кому-то постороннему (это факт компрометации секретного ключа). О факте компрометации или о подозрении на компрометацию необходимо незамедлительно сообщить своему курирующему менеджеру.

И в первом и во втором случае порядок действий почти одинаков – сделать запрос на новый сертификат, дождаться сертификата, получить и установить сертификат.

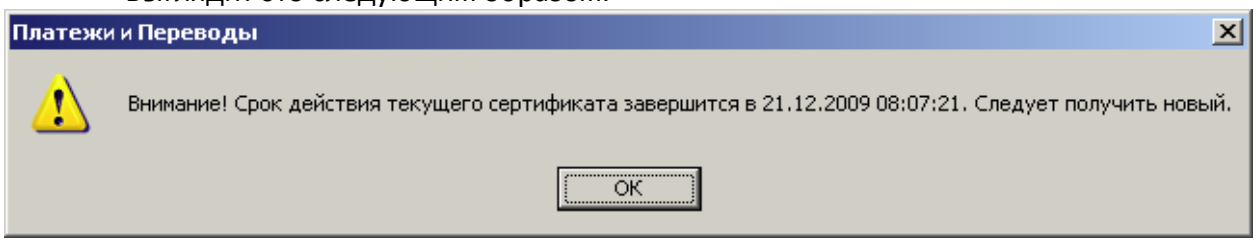
Однако в случае с компрометацией необходимо сразу оповестить Банк о таком факте с целью блокировки старого сертификата.

## *5.2. Оповещение о сроке действия сертификата и порядок замены*

### 5.2.1. АРМ «Платежи и Переводы»

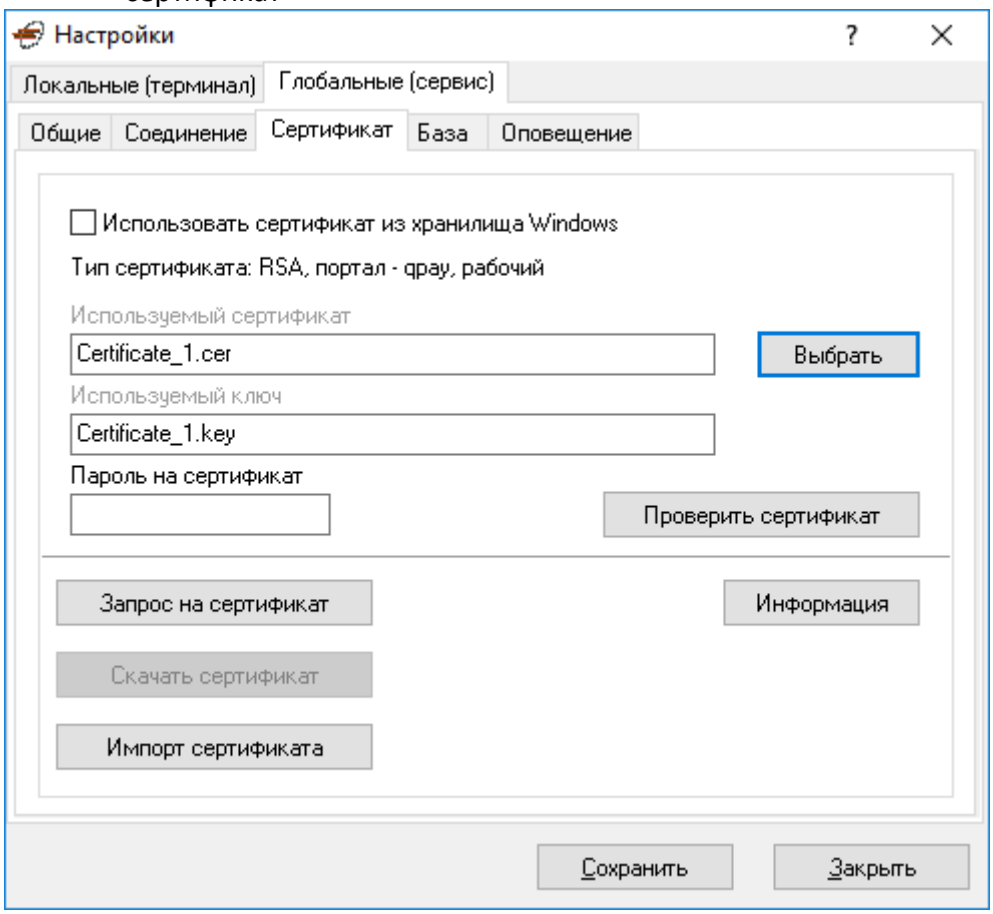
При работе с АРМ «Платежи и Переводы», процедура контроля срока действия весьма проста - если срок действия сертификата заканчивается, то предупреждения о необходимости получения нового сертификата начнутся за 6 дней до истечения срока действия.

Выглядит это следующим образом:




1) Для замены сертификата сначала необходимо переименовать файлы в папке с сертификатами. Это делается вручную средствами операционной системы. Новые имена файлов должны быть такими: Certificate_1.cer, Certificate_1.key). Файлы сертификатов находятся по адресу:
**..[Каталог программы]\Data\Key**.

2) В настройках программы (найти в меню **Действия/Настройки/Глобальные (сервис)/Сертификат**) необходимо переименовать ранее установленный сертификат




3) Сохранить изменения и перезапустить программу.

На замену сертификата отводится 2 рабочих дня.
Получение нового сертификата описано в соответствующем разделе.
После получения нового сертификата необходимо выбрать его как действующий.

После перенастройки и проверки работоспособности необходимо удалить из каталога с сертификатами файлы **Certificate_1.cer, Certificate_1.key –** они больше не понадобятся.

### 5.2.2. Другие системы

Контроль за сроком действия сертификатов должен осуществляться на стороне Участника.

Порядок замены определяется Администратором безопасности на стороне Участника.

Установка в систему производится аналогично процедуре установке новых сертификатов.

# 6. Формирование сертификата формата PKSC12

Если полученный ранее сертификат необходимо преобразовать к формату PKSC12, то для этих целей можно воспользоваться свободно распространяемой утилитой OpenSSL.

Формат командной строки:

```
$openssl pkcs12 -export -in Certificate.cer -inkey Certificate.key -out
Certificate.p12 -passin pass:PASSWORD -passout pass:PASSWORD
```

где PASSWORD - пароль к закрытому ключу установленный Участником и известный только ему.

Установка сертификата в хранилище операционной системы производится согласно документации к данной операционной системе.

## Примечания

При использовании на стороне Участника для формирования запросов программного продукта OpenSSL, необходимо использовать версии данного продукта, начиная с 0.9.6c и заканчивая 0.9.8k. В других версиях использовать при установке параметр: OPENSSL_ENABLE_UNSAFE_LEGACY_SESSION_RENEGOTATION