Инструкция по получению SSL-сертификата

(Версия 1.0)

Оглавление

Глава 1

Введение

Данный документ описывает процедуру получения серверного SSL-сертификата (англ. Secure Sockets Layer — протокол защищённых сокетов). Серверный SSL-сертификат используется для подтверждения подлинности сайта банка при подключении к нему клиента. Его использование позволяет помешать злоумышленнику подменить сайт банка и таким образом получить конфиденциальную информацию о клиенте. Чаще всего SSL применяется для защищенного обмена данными между Web-браузерами и Web-серверами. Основное назначение протокола защиты состоит в следующем:

- Аутентификация сервера, гарантирующая пользователям, что они попали именно на тот узел Web, который хотели посетить;
- Подтверждение легитимности компании и её юридического адреса;
- Создание защищенного SSL-сертификатом канала, благодаря которому информация может передаваться между клиентом и сервером в закодированном виде, с целью предотвращения искажения данных во время пересылки.

В системе iBank 2 UA в рамках Сервера Приложения работает вспомогательный Web-сервер с поддержкой протокола SSL, который загружает в Web-браузер клиента HTML-страницы, Java-апплеты и конфигурационные файлы. Для работы вспомогательного Web-сервера необходим SSL-сертификат. При промышленной эксплуатации системы SSL-сертификат необходимо получать у одного из мировых Сертификационных Центров — организации, которая удостоверяет подлинность информации, указанной в серверном SSL-сертификате.

SSL-сертификат можно получить в одном из Сертификационных Центров: VeriSign, Inc. (http://www.verisign.com/), THAWTE (http://www.thawte.com/home.html) и др. Ниже описана процедура получения серверного SSL-сертификата у РБК (http://ssl.rbc.ru/) – представителя компании THAWTE в России, странах СНГ и Балтии. SSL-сертификат можно получить и у украинских дистрибьютеров компании THAWTE, например здесь http://ssl.kravchuk.biz/.

При опытной эксплуатации допустимо использование самозаверенного сертификата (сертификат, который банк выдает самому себе). Подробно процесс генерирования самозаверенного SSL-сертификата описан в документе ***Установка системы iBank 2 UA под ОС Windows/Unix***.

Глава 2

Получение SSL-сертификата у РБК

Получение сертификата включает в себя следующие шаги:

1. Создание хранилища секретных ключей;
2. Генерация запроса на получение SSL-сертификата;
3. Регистрация на сайте РБК (если банк уже зарегистрирован, то данный шаг не нужен);
4. Оформление запроса на получение сертификата;
5. Документальное оформление сертификата;
6. Импорт электронного SSL-сертификата.

Создание хранилища ключей

Создание хранилища секретных ключей производится с помощью утилиты `keytool.exe`, входящей в состав дистрибутива системы iBank 2 UA. Выполните следующую команду:

```
%ibank_home%\jre\bin\keytool -genkey -alias ibank -keyalg RSA ⟹
⟹ -keysize 1024 -keystore %ibank_home%\conf\.sslkeystore -validity 730
```

Ответьте на задаваемые вопросы. Здесь `%ibank_home%` – каталог, в котором установлен Сервер Приложения. Ниже приведен пример подобного диалога:

```
What is your first and last name?
[Unknown]: ibank.bankname.ua

What is the name of your organizational unit?
[Unknown]: IT Department

What is the name of your organization?
[Unknown]: Bankname

What is the name of your City or Locality?
[Unknown]: Dnepropetrovsk

What is the name of your State or Province?
[Unknown]: UA

What is the two-letter country code for this unit?
[Unknown]: UA

Is <CN=ibank.bankname.com.ua, OU=IT Department, O=Bankname, L=Dnepropetrovsk,
ST=UA, C=UA> correct?
[no]: yes
```

В результате в каталоге `%ibank_home%\conf` будет создан файл с хранилищем ключей `.sslkeystore`

Внимание!

Запишите в надежном месте пароль к хранилищу ключей и сделайте резервную копию хранилища. При потере пароля или ключа процедуру его получения придется повторять заново (из соображений безопасности THAWTE не позволяет повторной генерации сертификатов), включая оплату нового сертификата.

Генерация запроса на получение сертификата

Следующим шагом является создание запроса на получение SSL-сертификата. Данный запрос генерируется утилитой `keytool.exe` и сохраняется в файле `.csr`. Для генерации CSR-файла выполните следующую команду:

```
%ibank_home%\jre\bin\keytool -certreq -alias ibank -file ⟹

⟹ %ibank_home%\certreq.csr -keystore %ibank_home%\conf\.sslkeystore
```

Утилита запросит пароль (по умолчанию `changeit`). В результате в каталоге `%ibank_home%\` будет сформирован файл `certreq.csr`. Содержимое этого файла необходимо отправить в Сертификационный Центр.

Регистрация на сайте РБК

Для получения сертификата, заверенного компанией THAWTE, необходимо зарегистрироваться на сайте РБК (представителя компании THAWTE в России, странах СНГ и Балтии). Для этого выполните следующие действия:

1. Откройте в веб-браузере страницу по следующей ссылке:
   http://ssl.rbc.ru/cgi-bin/Enter.cgi?PERS_CLICK=1
   Нажмите на кнопку **зарегистрироваться** (см. рис. 2.1).

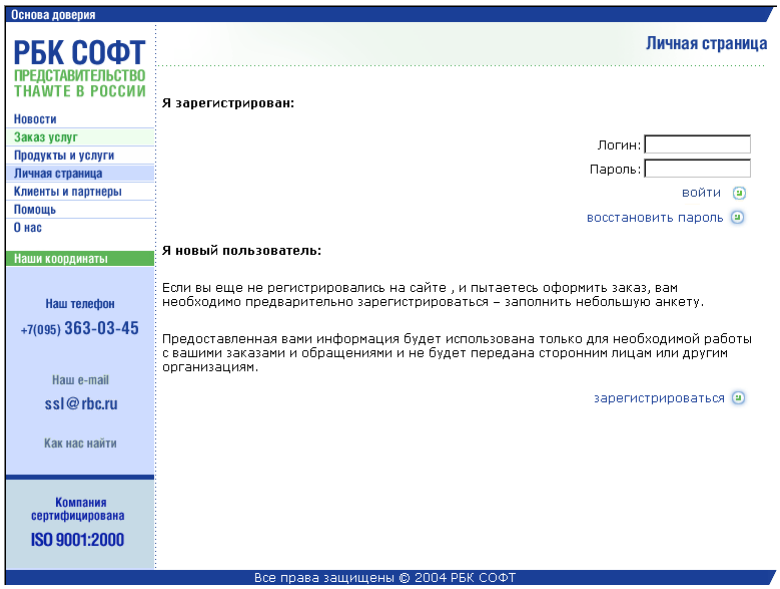

Рис. 2.1. Вход на личную страницу пользователя

2. **Шаг 1.** Введите логин и пароль на доступ к личной странице, подтверждение пароля и нажмите **далее**.
3. **Шаг 2.** На следующей странице (см. рис. 2.2) введите сведения о представителях организации, для которой будет получен сертификат. В форму **Административный контакт** введите информацию о руководителе организации, в форму **Технический контакт** — информацию об IT специалисте, занимающемся вопросом получения сертификата, в форму **Лицо, подписывающее документы** — информацию о представителе организации, который будет подписывать документы в процессе получения сертификата.
4. **Шаг 3.** Введите сведения об организации[1]. Вводимые сведения должны совпадать с указанными в свидетельстве о государственной регистрации юридического лица. Также название компании должно соответствовать указанному в базе данных регистратора домена.
5. **Шаг 4.** На этом этапе можно просмотреть условия договора о выдаче SSL-сертификата по соответствующей ссылке. После этого регистрация пользователя на сайте РБК завершена и можно оформить запрос на получение сертификата.

Оформление запроса на получение сертификата

Для формирования запроса на получение сертификата выполните следующие действия:

1. Войдите на личную страницу, используя логин и пароль, введенные на этапе регистрации.
2. В левой части окна выберите пункт **Продукты и услуги**.
3. Выберите пункт **Стандартный сертификат** и нажмите на кнопку **заказ**.
4. На открывшейся странице (см. рис. 2.3) введите данные о сертификате:
   - В списке **Тип сертификата** выберите **Стандартный сертификат**.
   - Введите доменное имя своего сайта.
   - Укажите количество дополнительных лицензий 0.

[1] В анкете указаны наименования банковских реквизитов, действующих в пределах Российской Федерации. Необходимо ввести соответствующие данные украинских банковских реквизитов.

Рис. 2.2. Ввод информации о представителях организации

- Выберите срок действия сертификата (1 или 2 года).
- В списке **Тип сервера** выберите **Tomcat**.
- В поле CSR скопируйте содержимое файла запроса на получение SSL-сертификата (файл `%ibank_home%\certreq.csr`). Содержимое необходимо копировать полностью, включая начальную и конечную строки.

5. На следующей странице можно ознакомиться с условиями договора на услуги, предоставляемые РБК. Для окончательной регистрации запроса нажмите кнопку **принять**.

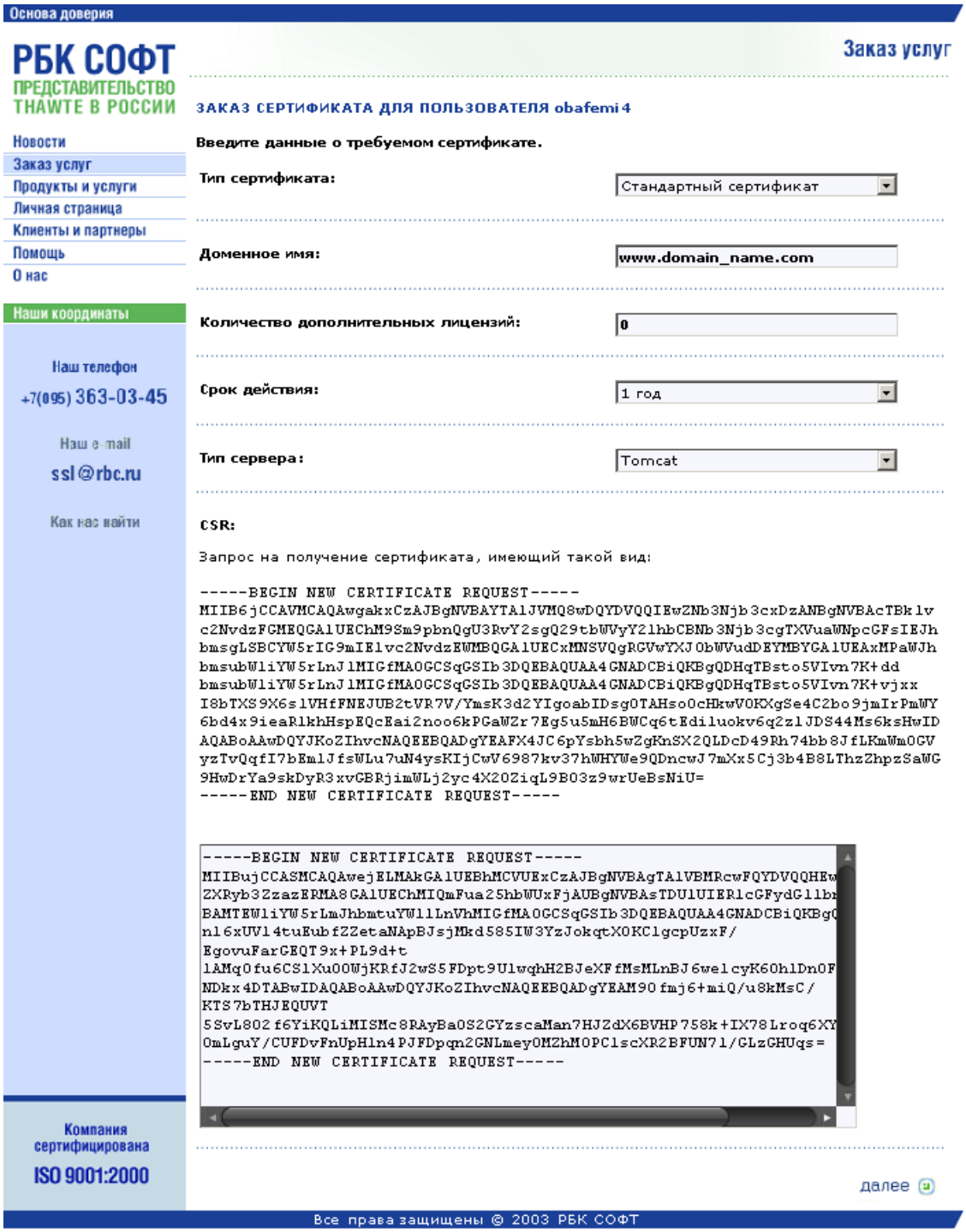

Рис. 2.3. Заказ сертификата

Документальное оформление сертификата

После оформления запроса на получения сертификата необходимо будет предоставить следующие документы:

1. Регистрационные документы[2] — нотариально заверенная копия свидетельства о государственной регистрации юридического лица и нотариально заверенная копия справки о постановке на учет плательщика налогов в Государственной Налоговой Инспекции.
2. Счет за оплату услуг выдачи сертификата — выставляется после проверки подлинности предоставленных регистрационных документов.

SSL-сертификат предоставляется в электронном виде на личной странице организации.

Внимание:
Во избежание недоразумений относительно необходимых документов, следует перед созданием заявки на получение сертификата обратиться по электронному адресу ssl@rbc.ru за актуальной информацией.

Импорт SSL-сертификата

После получения электронного SSL-сертификата его необходимо импортировать в хранилище сертификатов следующей командой:

```
%ibank_home%\jre\bin\keytool -import -trustcacerts -alias ibank -file ⟹
⟹ ibank.cer -keystore %ibank_home%\conf\.sslkeystore
```

Здесь `ibank.cer` — файл с сертификатом, полученный из сертификационного центра.

После импорта SSL-сертификата в хранилище он становится доступным для использования клиентами, подключающимися к банковскому серверу.

[2] документы должны быть заверены нотариально не более 2-х месяцев назад

Глава 3

Продление срока действия SSL-сертификата

Выдаваемый сертификат имеет свой срок действия (1 или 2 года), по истечении которого его необходимо продлевать.

Для продления срока действия SSL-сертификата необходимо обращаться непосредственно на сайт компании THAWTE.
Перейдите по ссылке http://www.thawte.com/ssl-digital-certificates/renew-ssl-certificates/. На открывшейся странице (см. рис. 3.2) в списке видов сертификатов выберите **SSL Web Server Certificates**. На новой странице введите в поля **Order number** (номер) и **Password** (пароль) информацию, полученную при выдаче сертификата и нажмите кнопку **Submit** (подтвердить) (см. рис. 3.1).

Рис. 3.1. Ввод номера и пароля

В дальнейшем введите срок, на который будет продлено действие сертификата, информацию о количестве дополнительных лицензий (0), серверном ПО (Tomcat), информацию о способе оплаты и контактную информацию. После ввода запросу будет присвоен номер, который необходимо записать и в дальнейшем использовать для аутентификации.

После завершения регистрации запроса компания THAWTE может затребовать документы, аналогичные предоставляемым на этапе выдачи сертификата. После их проверки новый сертификат будет доступен в электронном виде по адресу http://www.thawte.com/cgi/server/status.exe.

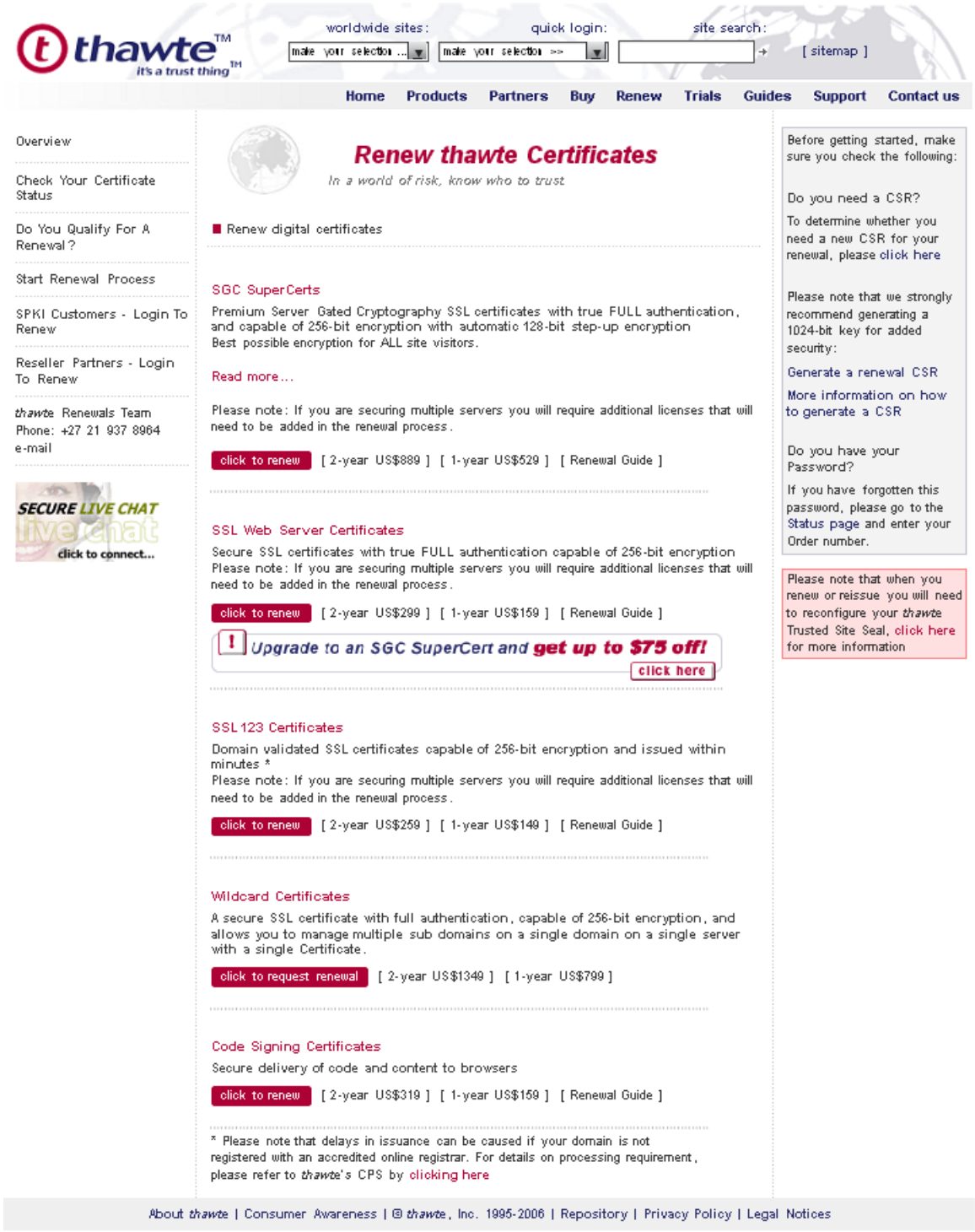

Рис. 3.2. Вход на страницу продления сертификата

Глава 4

Источники дополнительной информации

С дополнительной информацией по данной тематике можно ознакомиться в документах:

- ***Общая информация о системе iBank 2 UA***
- ***Выбор аппаратного и программного обеспечения для работы системы iBank 2 UA***
- ***Установка системы iBank 2 UA под ОС Windows/Unix***
- ***Типичные проблемы при работе с системой iBank 2 UA. Решения***
- ***Механизмы безопасности в системе iBank 2 UA***

Примечание:
Со всеми предложениями и пожеланиями по документации обращайтесь по электронному адресу support@bifit.com.ua