

Инструкция по получению SSL-сертификата

(Версия 1.0)

Оглавление

1 Введение	2
2 Получение SSL-сертификата у РБК	3
Создание хранилища ключей	3
Генерация запроса на получение сертификата	4
Регистрация на сайте РБК	4
Оформление запроса на получение сертификата	5
Документальное оформление сертификата	8
Импорт SSL-сертификата	8
3 Продление срока действия SSL-сертификата	9
4 Источники дополнительной информации	11

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 ТНАВТЕ 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 ТНАВТЕ, необходимо зарегистрироваться на сайте РБК (представителя компании ТНАВТЕ 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

- Шаг 1.** Введите логин и пароль на доступ к личной странице, подтверждение пароля и нажмите далее.
- 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.
- Шаг 3.** Введите сведения об организации¹. Вводимые сведения должны совпадать с указанными в свидетельстве о государственной регистрации юридического лица. Также название компании должно соответствовать указанному в базе данных регистратора домена.
- 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:

- Войдите на личную страницу, используя логин и пароль, введенные на этапе регистрации.
- В левой части окна выберите пункт **Продукты и услуги**.
- Выберите пункт **Стандартный сертификат** и нажмите на кнопку **заказ**.
- 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.

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

Основа доверия

РБК СОФТ
ПРЕДСТАВИТЕЛЬСТВО
ТНAWTE В РОССИИ

Личная страница

Шаг 1 Шаг 2 Шаг 3 Шаг 4

Просим вас при заполнении анкеты использовать данные, которые в случае необходимости могут быть подтверждены документально.

Административный контакт

ФИО (на русском): Пример: <i>Богданов Сергей Александрович</i>	<input type="text" value="Богданов Сергей Александрович"/>
ФИО (на английском): Пример: <i>Bogdanov Sergey Aleksandrovich</i>	<input type="text" value="Bogdanov Sergey Aleksandrovich"/>
Должность (на русском):	<input type="text" value="Генеральный директор"/>
Должность (на английском):	<input type="text" value="Director -general"/>
E-mail: Несколько адресов указываются через ";", или ";"; Пример: <i>ivanov@ivanov.ru</i>	<input type="text" value="ivanov@ivanov.ru"/>
Телефон: (с обязательным указанием международного кода и кода города). Пример: +7 095 1234567	<input type="text" value="+7 095 1234567"/>

Технический контакт

ФИО (на русском): Пример: <i>Королев Александр Александрович</i>	<input type="text" value="Ольга Лисицина"/>
ФИО (на английском): Пример: <i>Korolev Aleksandr Aleksandrovich</i>	<input type="text" value="Olga Lisitsina"/>
Должность (на русском):	<input type="text" value="Менеджер по работе с клиентами"/>
Должность (на английском):	<input type="text" value="Account manager"/>
E-mail: Несколько адресов указываются через ";", или ";"; Пример: <i>ivanov@ivanov.ru</i>	<input type="text" value="rodina@rbc.ru"/>
Телефон: (с обязательным указанием международного кода и кода города). Пример: +7 095 1234567	<input type="text" value="+7 (095) 363-0309"/>

Лицо, подписывающее документы

ФИО (на русском): Пример: <i>Королев Александр Александрович</i>	<input type="text" value="юлев Александр Александрович"/>
ФИО (на английском): Пример: <i>Korolev Aleksandr Aleksandrovich</i>	<input type="text" value="Korolev Aleksandr Aleksandrovich"/>
Должность (на русском):	<input type="text" value="Бухгалтер"/>
Должность (на английском):	<input type="text" value="Chief accountant"/>
E-mail: Несколько адресов указываются через ";", или ";"; Пример: <i>ivanov@ivanov.ru</i>	<input type="text" value="ivanov@ivanov.ru"/>
Телефон: (с обязательным указанием международного кода и кода города). Пример: +7 095 1234567	<input type="text" value="+7 095 1234567"/>
Основание: Пример: <i>Устав организации</i>	<input type="text" value="Устав организации"/>

Компания
сертифицирована
ISO 9001:2000

далее


Все права защищены © 2003 РБК СОФТ

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.

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

Основа доверия
Заказ услуг



РБК СОФТ
ПРЕДСТАВИТЕЛЬСТВО
ТНАОУТЕ В РОССИИ

ЗАКАЗ СЕРТИФИКАТА ДЛЯ ПОЛЬЗОВАТЕЛЯ obafemi 4

Введите данные о требуемом сертификате.

Тип сертификата:

Доменное имя:

Количество дополнительных лицензий:

Срок действия:

Тип сервера:

CSR:

Запрос на получение сертификата, имеющий такой вид:

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB6jCCAVMCAQAwaGakxCzAJBgNVBAYTA1JVMQ8wDQYDVQQIEwZMb3Njb3cxZzAMBgNVBAcTBk1v
c2NvdzFCMEQCA1UEChM9Sm9pbmQgU3RvY2sgQ29tbWVvY21hbCENb3Njb3cgTXVuaWNpcGFsIEJh
bmsqLSECYW5rIG9mIElvc2NvdzEWMBCQA1UECXMNSVQgRGVwYXJObWVudDEYMBYGA1UEAxMPaWJh
bmsubWliYW5rLnJlMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDHqTBsto5VIvn7K+dd
bmsubWliYW5rLnJlMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDHqTBsto5VIvn7K+dd
I8bTXS9X6s1VHfFNEJUE2tVR7V/YmsK3d2YIgoabIDsg0TAHso0cHrwVORXgSe4C2bo9jmIrxPmWY
6bd4x9ieaRlkhHspEQcEai2noo6kPGaWZr7Eg5u5mH6BWCq6tEdiluokv6q2z1JDS44Ms6ksHwID
AQBoAAwDQYJKoZIhvcNAQEEBQADgYEAfX4JC6pYsbh5w2gKnSX2QLDcD49Rh74bb8JfLkMwOCV
yzTvQqfI7bEmlJfsWLu7uN4ysKIjCwV6987kv37hWHYWe9QDncwJ7mXx5Cj3b4B8LThzZhpzSaWC
9HwDrYa9skDyR3xvGBRjimWlj2yc4X202iqL9B03z9wrUeBsNiU=
-----END NEW CERTIFICATE REQUEST-----

```

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBujCCASMQAwejELMAkCA1UEBhMCVUExCzAJBgNVBAGTA1VBMRCwFQYDVQQHEwZlbnVvY21hbCENb3Njb3cgTXVuaWNpcGFsIEJh
BAMTEWliYW5rLnJlMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQ
n16xUV14tuEubfZZetaNAPBjsjMkd585Iw3YzJokqtXORClgcpUzxF/
EgovuFarCEQT9x+PL9d+t
lAMq0fu6CS1Xu00WjKRfJ2wS5FDpt9UlwqhH2BJeXFfMsMLnBJ6welcyK60h1DnOF
NDkx4DTABwIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAAM90fmj6+miQ/u8kMsC/
KTS7bTHJEQUVT
5SvL802f6YiKQLiMISMc8R&yBa0S2CYzscaman7HJZdX6BVHP758k+IX78Lroq6XY
OmLguY/CUFdvFnUpHln4PJFDpqn2GNLmey0M2hMOPClscXR2BFUN71/GLzGHUqs=
-----END NEW CERTIFICATE REQUEST-----

```

Компания
сертифицирована
ISO 9001:2000

далее

Все права защищены © 2003 РБК СОФТ

Рис. 2.3. Заказ сертификата

Документальное оформление сертификата

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

1. Регистрационные документы² — 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.

²документы 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](#)).



■ enter the order number and password for renewal

order number : (i.e. USABCD12)

password :

(only if you have protected your certificate with a password)

[lost password?](#)

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>.

The screenshot shows the Thawte website's renewal page for SSL certificates. The header includes the Thawte logo, navigation links (Home, Products, Partners, Buy, Renew, Trials, Guides, Support, Contact us), and utility links (worldwide sites, quick login, site search, sitemap). The main content area is titled "Renew thawte Certificates" and lists various certificate types with their features and renewal options. A sidebar on the left contains links for certificate status, renewal process, and contact information. A right sidebar provides additional instructions and a warning about reissues.

thawte™
it's a trust thing™

worldwide sites: [make your selection ...] quick login: [make your selection >>] site search: [] [sitemap]

Home Products Partners Buy Renew Trials Guides Support Contact us

Renew thawte Certificates
In a world of risk, know who to trust

■ Renew digital certificates

SGC SuperCerts
Premium Server Gated Cryptography SSL certificates with true FULL authentication, and capable of 256-bit encryption with automatic 128-bit step-up encryption. Best possible encryption for ALL site visitors.
[Read more...](#)
Please note: If you are securing multiple servers you will require additional licenses that will need to be added in the renewal process.
[click to renew](#) [2-year US\$889] [1-year US\$529] [Renewal Guide]

SSL Web Server Certificates
Secure SSL certificates with true FULL authentication capable of 256-bit encryption. Please note: If you are securing multiple servers you will require additional licenses that will need to be added in the renewal process.
[click to renew](#) [2-year US\$299] [1-year US\$159] [Renewal Guide]

Upgrade to an SGC SuperCert and get up to \$75 off!
[click here](#)

SSL 123 Certificates
Domain validated SSL certificates capable of 256-bit encryption and issued within minutes*. Please note: If you are securing multiple servers you will require additional licenses that will need to be added in the renewal process.
[click to renew](#) [2-year US\$259] [1-year US\$149] [Renewal Guide]

Wildcard Certificates
A secure SSL certificate with full authentication, capable of 256-bit encryption, and allows you to manage multiple sub domains on a single domain on a single server with a single Certificate.
[click to request renewal](#) [2-year US\$1349] [1-year US\$799]

Code Signing Certificates
Secure delivery of code and content to browsers
[click to renew](#) [2-year US\$319] [1-year US\$159] [Renewal Guide]

* Please note that delays in issuance can be caused if your domain is not registered with an accredited online registrar. For details on processing requirement, please refer to thawte's CPS by [clicking here](#)

Before getting started, make sure you check the following:

Do you need a CSR?
To determine whether you need a new CSR for your renewal, please [click here](#)

Please note that we strongly recommend generating a 1024-bit key for added security:
[Generate a renewal CSR](#)
More information on how to generate a CSR

Do you have your Password?
If you have forgotten this password, please go to the [Status page](#) and enter your Order number.

Please note that when you renew or reissue you will need to reconfigure your [thawte Trusted Site Seal](#), [click here](#) for more information

[thawte Renewals Team](#)
Phone: +27 21 937 8964
e-mail

SECURE LIVE CHAT
live chat
[click to connect...](#)

About thawte | Consumer Awareness | @ thawte, Inc. 1995-2006 | Repository | Privacy Policy | Legal Notices

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
