

## Импорт хранилища ключей в формате PKCS#12, содержащего сертификат открытого ключа и личный ключ, в браузер Mozilla Firefox (версия 3.0.19)

Большинство браузеров и почтовых программ придерживается стандарта хранения ключевой пары PKCS#12 (Public-Key Cryptography Standard № 12). Данный стандарт определяет файловый формат, используемый для хранения личного (секретного, закрытого) ключа в сопровождении сертификата открытого ключа. Поскольку в файле PKCS#12 (файле с расширением \*.p12) хранится и сертификат, и личный ключ, с этим файлом необходимо быть столь же осторожными, как и с личным ключом.

1. Пусть, для определённости, личный ключ *JankaKupala\_userkey.pem* и выданный удостоверяющим центром сертификат *JankaKupala\_Certificate.pem* находятся в каталоге *ключи*, который доступен по следующему пути *D:\OpenSSL\openssl\bin\ключи*. Чтобы создать хранилище ключей в формате PKCS#12 выполните команду криптографического пакета программ OpenSSL:

```
openssl pkcs12 -export -in D:\OpenSSL\openssl\bin\ключи\JankaKupala_Certificate.pem  
-inkey D:\OpenSSL\openssl\bin\ключи\JankaKupala_userkey.pem -descert -out  
D:\OpenSSL\openssl\bin\ключи\JankaKupala_Keystore.p12
```

При выполнении команды Вам необходимо ввести пароль к Вашему личному ключу *JankaKupala\_userkey.pem*. Затем требуется создать (ввести и подтвердить) пароль к Вашему хранилищу ключей *JankaKupala\_Keystore.p12*. Требования к сложности пароля такие же, как и к паролю для активации личного ключа (рисунок 1).

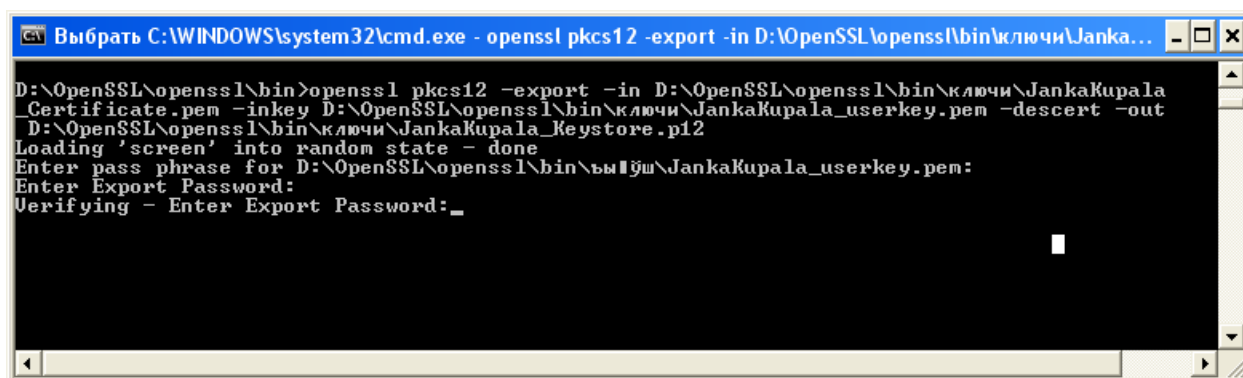


Рисунок 1 – Выполнение команды создания хранилища ключей

Пусть полученное хранилище ключей в формате PKCS#12 *JankaKupala\_Keystore.p12*, также будет находиться в каталоге *ключи*.

2. Сохраните корневой сертификат удостоверяющего центра <http://ca.grid.by/bygca-cacert.der> в каталоге *ключи*.

3. Запустите Firefox.

4. Сначала необходимо импортировать корневой сертификат удостоверяющего центра *bygca-cacert.der* (рисунки 2 – 4).

В меню *Инструменты* выберите пункт *Настройки*. В появившемся окне выберите вкладку *Шифрование*. На вкладке *Шифрование* нажмите кнопку *Просмотр сертификатов* (рисунок 2).

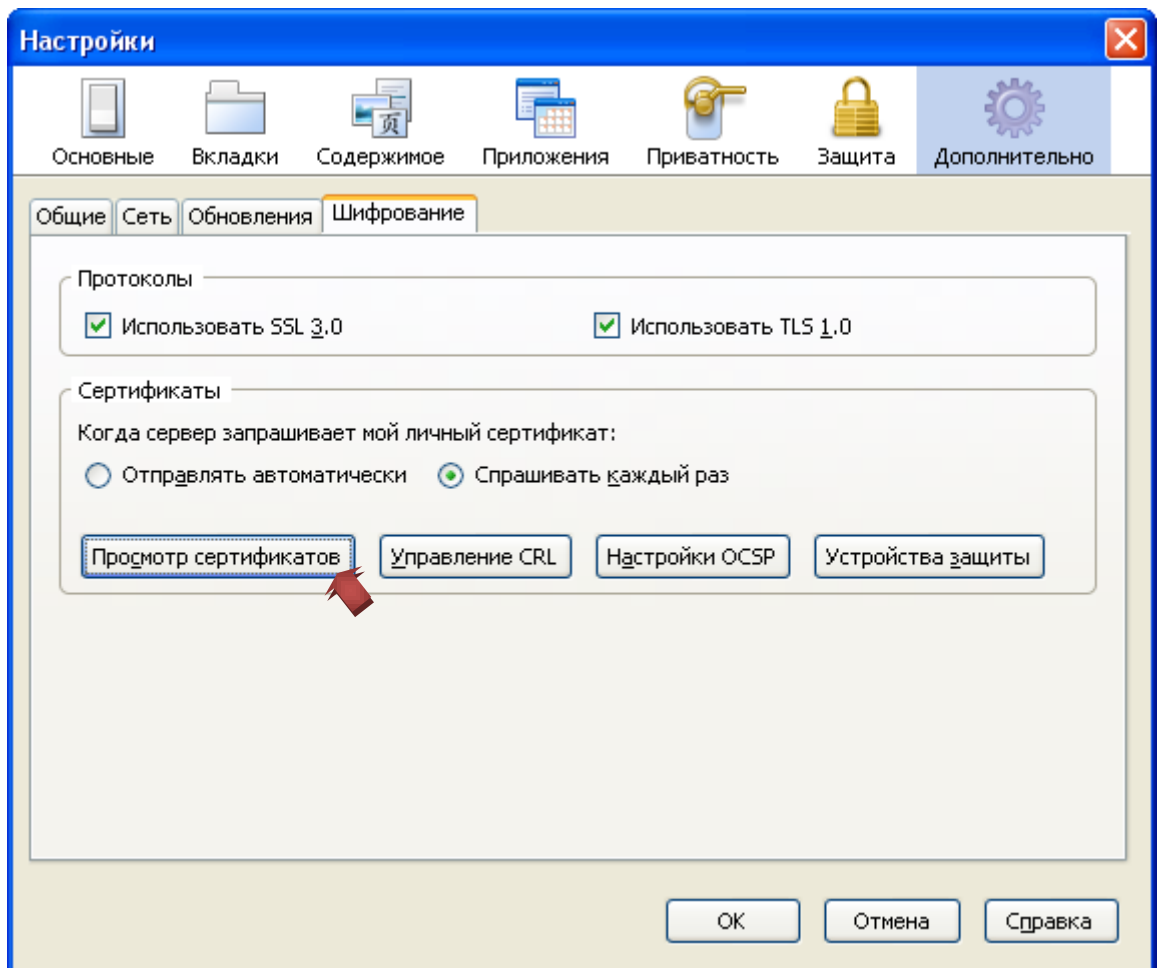


Рисунок 2 – Кнопка *Просмотр сертификатов* на вкладке *Шифрование* в окне *Настройки*

В появившемся окне *Менеджер сертификатов* выберите вкладку *Центры сертификации* (рисунок 3).

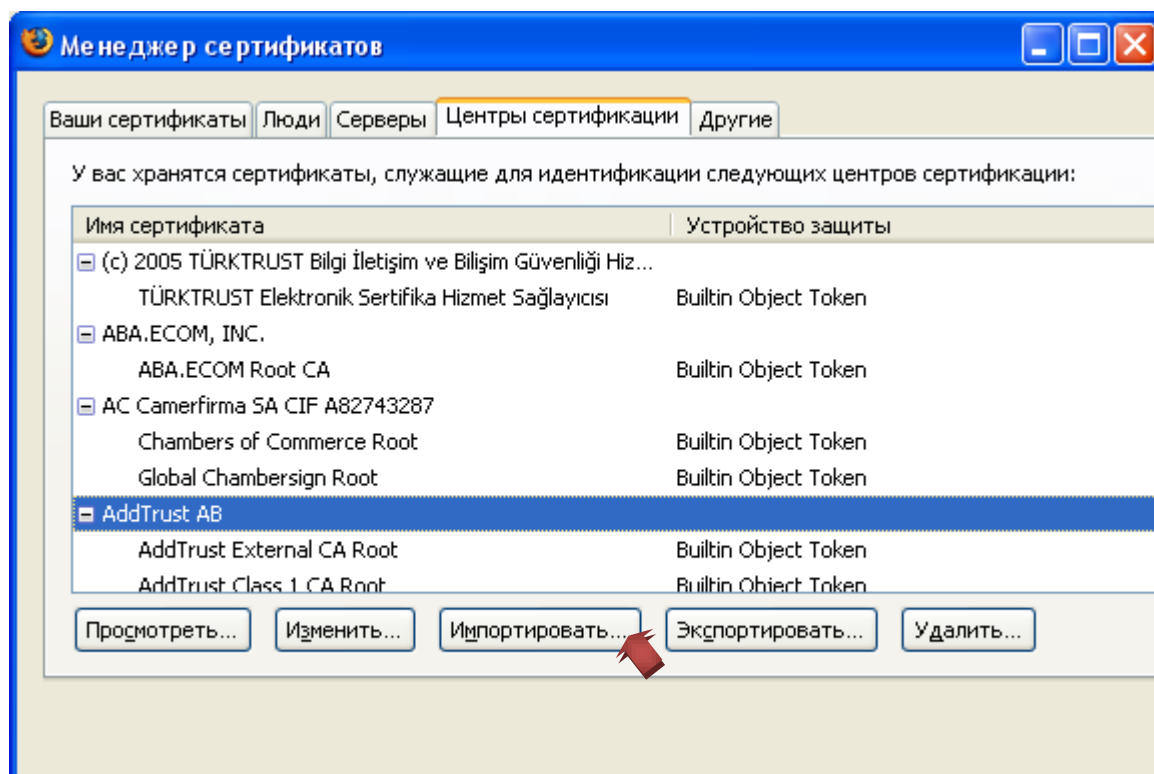


Рисунок 3 – Вкладка *Центры сертификации* в окне *Менеджер сертификатов*

Укажите импортируемый корневой сертификат удостоверяющего центра *bugsa-cacert.der*.

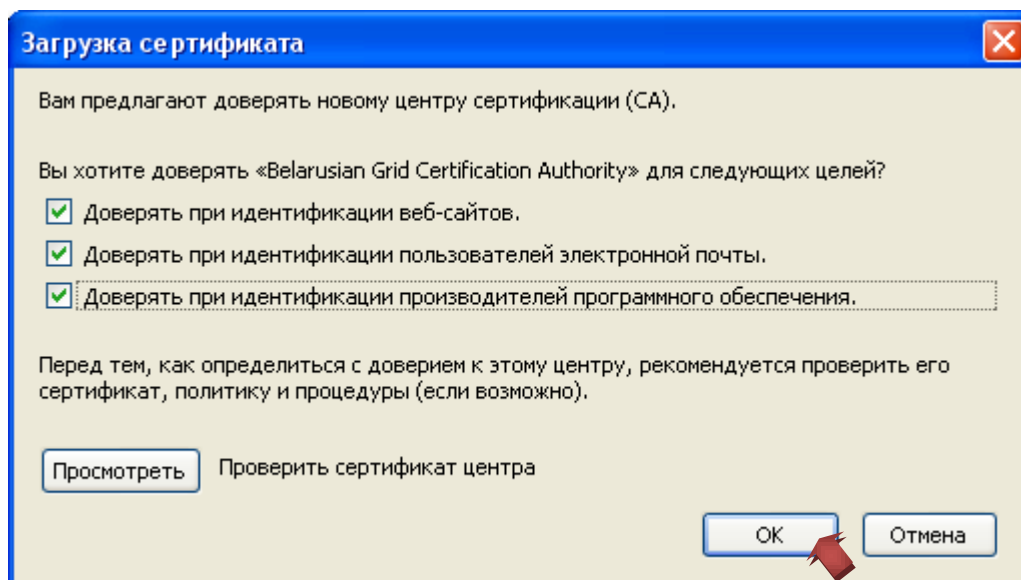


Рисунок 4 – Загрузка корневого сертификата удостоверяющего центра

5. Далее для импорта хранилища ключей в формате PKCS#12 *JankaKupala\_Keystore.p12* (рисунки 5 – 7) необходимо выбрать в меню *Инструменты*

пункт *Настройки*, в появившемся окне выбрать вкладку *Шифрование*, на вкладке *Шифрование* нажать кнопку *Просмотр сертификатов* (рисунок 5).

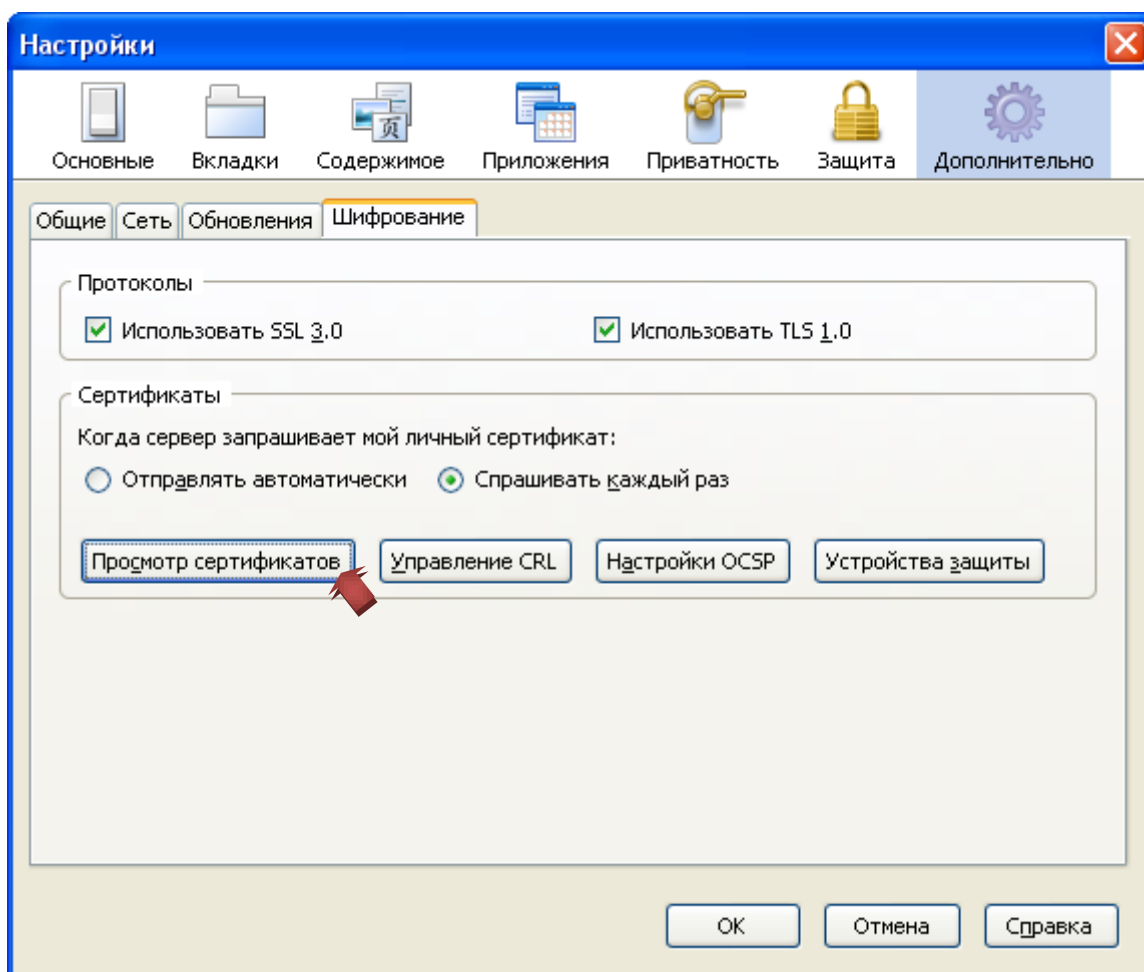


Рисунок 5 – Кнопка *Просмотр сертификатов* на вкладке *Шифрование* в окне *Настройки*

В появившемся окне *Менеджер сертификатов* выберите вкладку *Ваши сертификаты* (рисунок 6).

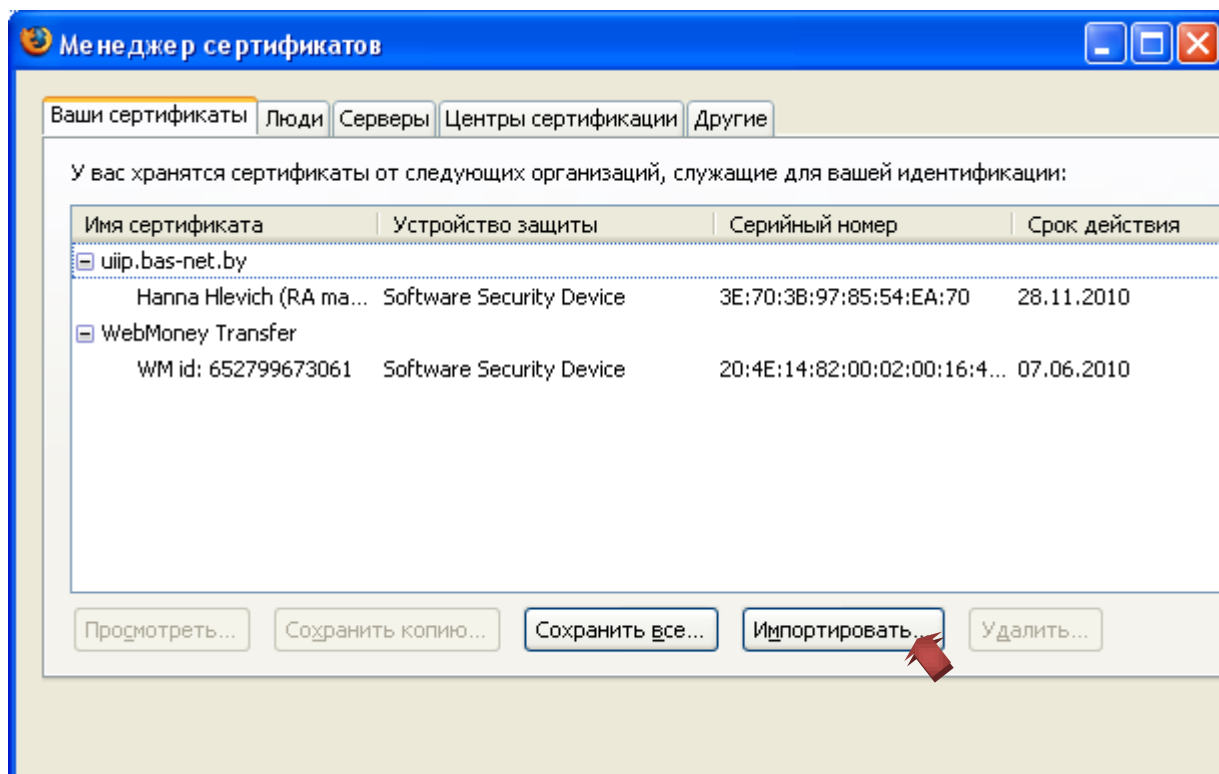


Рисунок 6 – Вкладка *Ваши сертификаты* в окне *Менеджер сертификатов*

Укажите импортируемый файл *JankaKupala\_Keystore.p12*.

Введите пароль к Вашему хранилищу ключей *JankaKupala\_Keystore.p12* (рисунок 7).

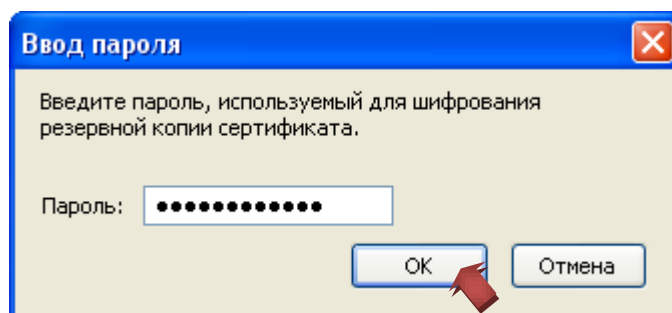


Рисунок 7 – Ввод пароля

6. Для проверки работоспособности импортированного хранилища ключей в формате PKCS#12 перейдите по ссылке <https://jabber.grid.by/test.php>.

При попытке входа на сайт должно появиться окно:

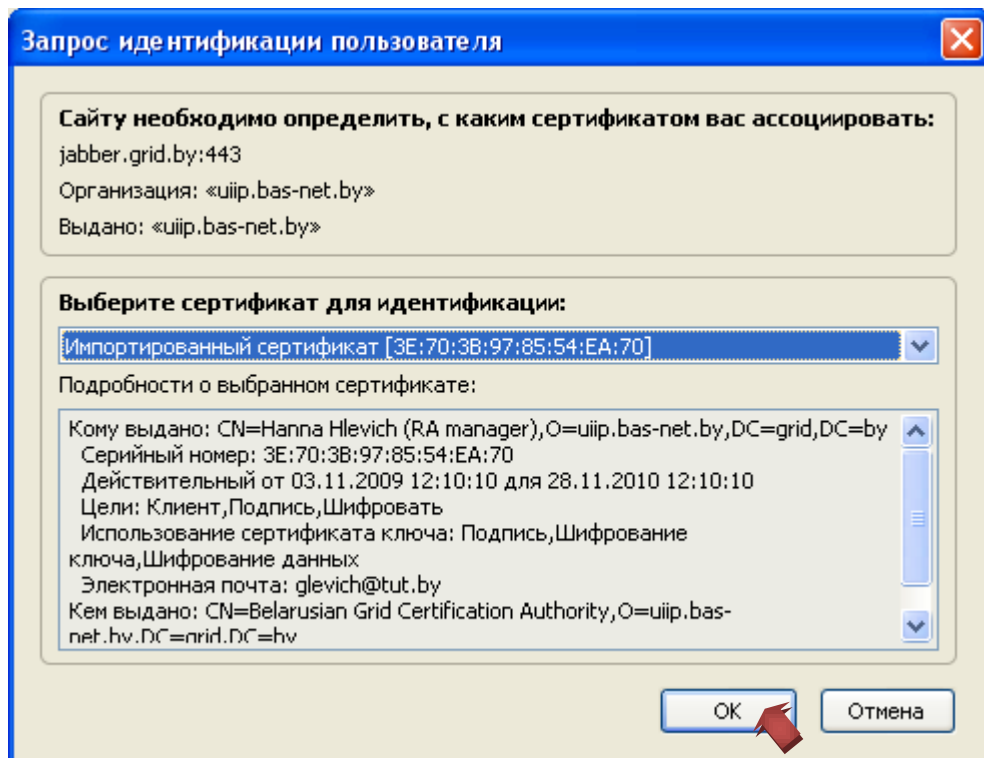


Рисунок 8 – Использование импортированного сертификата

Если импорт хранилища ключей в формате PKCS#12 был произведен успешно, то загрузится страница с базовой информацией о Вашем сертификате, а также ссылки на полезные веб-ресурсы, которыми можно пользоваться только при наличии сертификата:

Проверить сертификат - Mozilla Firefox

Файл Правка Вид Журнал Закладки Инструменты Справка

https://jabber.grid.by/test.php

Самые популярные Начальная страница Лента новостей My Opera Community



Здравствуйте, Hanna Hlevich (RA manager).

Поздравляем, Ваш сертификат действителен.

В таблице приведены некоторые параметры и соответствующие значения Вашего сертификата:

Параметр	Значение
Ваше отличительное имя, как абонента удостоверяющего центра	/DC=by/DC=grid/O=uiip.bas-net.by /CN=Hanna Hlevich (RA manager)
Начало срока действия сертификата	Nov 3 10:10:10 2009 GMT
Окончание срока действия сертификата	Nov 28 10:10:10 2010 GMT
Серийный номер сертификата	3E703B978554EA70
Отличительное имя удостоверяющего центра, который издал сертификат	/DC=by/DC=grid/O=uiip.bas-net.by /CN=Belarusian Grid Certification Authority
Адрес электронной почты, который указан в сертификате и может использоваться удостоверяющим центром для отправки Вам сообщений, связанных с сертификатом	glevich@tut.by

Наличие у Вас действительного сертификата позволяет Вам не только запрашивать доступ к грид-ресурсам в Беларуси и за рубежом, но также

Готово jabber.grid.by

Рисунок 9 – Страница с базовой информацией о сертификате