1. ОБЩИЕ ПОЛОЖЕНИЯ

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ

Инфраструктура открытых ключей (Public Key Infrastructure, PKI) предоставляет каркас, состоящий из служб, технологий, протоколов и стандартов, позволяющий развертывать и управлять системой устойчивой информационной безопасности на базе технологии открытых ключей. Основные компоненты инфраструктуры открытого ключа - это цифровые сертификаты, списки отзыва сертификатов (certificate revocation list, CRL) и центры сертификации (certification authority, CA или ЦС). Инфраструктура открытого ключа необходима для реализации решений на основе технологии открытых ключей.

Открытые и закрытые ключи используются при проверке подлинности и для обеспечения конфиденциальности, целостности и невозможности отрицания авторства. Однако сами по себе открытые и закрытые ключи не предоставляют никаких доказательств того, что их пары ключей принадлежат предполагаемому владельцу. А значит, необходим способ достоверно подтвердить личность владельца набора ключей. Для создания системы доверия к наборам ключей в открытых сетях необходимы доверенные учреждения, которые возьмут на себя аутентификацию людей, организаций и компьютеров в сети, предоставляя подтверждение принадлежности открытых и закрытых ключей. Такие доверенные учреждения, называются *центрами сертификации* (certification authority, CA) или *ЦС*. Они однозначно идентифицируют сетевые объекты и предоставляют идентификационные удостоверения, на основе которых участники сетевого обмена проверяют аутентичность объектов сети.

Для установления доверия в инфраструктуре открытых ключей используются электронные удостоверения, которые называются *цифровыми сертификатами* (digital certificates) и выпускаются ЦС. Цифровой сертификат подтверждает, что названный в нем объект является владельцем пары <открытый/закрытый ключи>. При наличии такого свидетельства другие объекты в сети могут быть уверены в принадлежности открытого ключа.

ЦИФРОВЫЕ СЕРТИФИКАТЫ

Цифровые сертификаты служат для идентификации людей, организаций и компьютеров в сети. Сертификаты выпускаются и сертифицируются центрами сертификации. Совместимые со спецификацией PKIX инфраструктуры открытых ключей поддерживают сертификаты промышленного стандарта X.509 v3.

ВЫПУСК СЕРТИФИКАТОВ ЦЕНТРАМИ СЕРТИФИКАЦИИ

Выпущенные ЦС цифровые сертификаты предоставляют доказательства аутентичности объектов в сети. В сертификате содержится информация, идентифицирующая его владельца как объект (иногда называют *субъектом)* в сети. Сертификат также содержит открытый ключ владельца и указывает на выпустивший его ЦС, называемый *издателем* (issuer) сертификата. Сертификат подписывается закрытым ключом ЦС. Для создания этой подписи ЦС вычисляет хэш-код сертификата и шифрует его своим закрытым ключом. Созданная таким образом цифровая подпись включается в сертификат. Проверка целостности сертификата выполняется при помощи хэш-функции и открытого ключа ЦС. Если сертификат поврежден или подменен, его хэш-код не совпадет с хэш-кодом в цифровой подписи ЦС. Сертификат - это открытая, доступная всем информация. Как

правило, сертификаты распространяют через каталоги, общие папки и Web-страницы, а также посредством электронной почты. Распространение сертификатов подразумевает также распространение открытых ключей, ведь сертификаты содержат открытые ключи. Доверие к закрытому ключу владельца сертификата основывается на репутации выпустившего сертификат ЦС и на уверенности в соблюдении им правил выпуска сертификатов.

НАЗНАЧЕНИЯ ПАРЫ КЛЮЧЕЙ

В поле информации открытого ключа субъекта в сертификате X.509 v3 содержатся сведения о криптографических операциях, в которых допускается использовать данную пару ключей. Как правило, системы безопасности на базе открытых ключей поддерживают следующие основные криптографические операции:

- подписание электронных данных для подтверждения их происхождения и целостности;
- проверку подлинности объектов сети;
- шифрование секретного ключа симметричного шифрования для его защиты при передаче и распространении по сети.

Пары открытого и закрытого ключей применяются в технологиях информационной безопасности для выполнения самых различных назначений. Они перечислены в поле расширений. Далее приведены обычные назначения сертификата:

- защищенная почта, обеспечивающая проверку подлинности, конфиденциальность, целостность и невозможность отрицания авторства сообщений;
- безопасная связь через Интернет, обеспечивающая проверку подлинности, целостность и конфиденциальность связи между Web-клиентами и серверами;
- подписание кода, обеспечивающее целостность и невозможность отрицания авторства исполняемого кода при его распространении в Интернете и интрасетях;
- проверка подлинности пользователей ресурсов сети при локальном и удаленном входе в систему;
- проверка подлинности средствами IPSec для клиентов, не использующих протокол Kerberos и общие секретные пароли при связи по протоколам IPSec.

РЕГИСТРАЦИЯ СЕРТИФИКАТОВ

Чтобы получить сертификат в ЦС, пользователи и компьютеры должны подать в центр сертификации заявку на сертификат. Процесс подачи заявки осуществляется посредством специально-созданных Web-страниц. Получив запрос на сертификат, ЦС проверяет, соответствует ли заявитель критериям для выдачи сертификата, и в зависимости от результатов проверки удовлетворяет или отклонят запрос.

СПИСКИ ОТОЗВАННЫХ СЕРТИФИКАТОВ

ЦС публикует *списки отозванных сертификатов* (certificate revocation list, CRL) - списки сертификатов, объявленных недействительными (это происходит, например, когда пользователь сертификата увольняется или когда секретный ключ скомпрометирован). При проверке сертификата программа просматривает списки CRL, чтобы установить, не отозван ли сертификат. В CRL публикуются недействительные сертификаты, которым нельзя доверять. По истечении срока действия сертификат исключается из списка CRL. Для предотвращения фальсификации ЦС подписывает CRL своим закрытым ключом.

ОБНОВЛЕНИЕ СЕРТИФИКАТОВ

По истечении срока действия сертификат становиться недействительным и не подлежит дальнейшему использованию. Однако, сертификаты разрешается выпускать повторно с новыми сроками действия. При этом, процесс обновления заключается в запросе нового сертификата.

УПРАВЛЕНИЕ КЛЮЧАМИ

Управление закрытыми ключами - это важнейшая функция инфраструктуры открытого ключа. Следует неукоснительно обеспечивать безопасность закрытых ключей при их создании, распространении и хранении. Закрытый ключ в руках злоумышленника дискредитирует всю систему безопасности. Перехватив закрытый ключ, злоумышленник сможет заменить его владельца во всех сетевых криптографических операциях с открытым ключом. В зависимости от назначений, скомпрометированный закрытый ключ можно использовать для повреждения сетевых ресурсов, хищения ценной информации или для нанесения вреда репутации.

БЕЗОПАСНОСТЬ ЗАКРЫТЫХ КЛЮЧЕЙ

Владеть закрытым ключом и использовать его должен только его владелец. Поэтому в инфраструктуре открытого ключа закрытые ключи надо хранить в защищенном и недоступном для посторонних месте и, кроме того, обеспечить существование каждого ключа в единственном экземпляре.

СИСТЕМНЫЕ ТРЕБОВАНИЯ ПРИ ЗАКАЗЕ ЦИФРОВОГО СЕРТИФИКАТА

- ОС: Windows 2000 и выше
- Браузер: Internet Explorer 6 и выше (обязательно должны быть включены файлы cookies)

2. ФОРМИРОВАНИЕ ЭЛЕКТРОННОГО ЗАПРОСА НА ВЫПУСК СЕРТИФИКАТА

Генерация пары криптографических ключей осуществляется на стороне пользователя. Процесс генерации ключей может быть выполнен различными способами и зависит от задачи, в которой используются сертификаты. Примерами генерации ключей являются процесс генерации ключей с помощью утилиты openssl или процесс генерации ключей средствами операционной системы MS Windows. Независимо от способа генерации закрытый ключ остается на стороне пользователя, а открытый отсылается в ЦС банка на сертификацию.

Сервер регистрации заявок (http://ca.fuib.com/) позволяет отправлять запросы на цифровой сертификат двумя способами: отправка запроса в формате PKCS#10 и отправка запроса через заполнение формы на web-странице. Для регистрации заявки через Web-страницу, в браузере должна быть включена возможность сохранения cookie и сайт (http://ca.fuib.com/) должен быть добавлен в категорию «доверенные сайты».

Формат PKCS#10 - это стандартизированный формат запроса на выпуск цифрового сертификата, поэтому формирование запроса можно осуществлять любым средством, поддерживающим данный формат.

Электронный запрос на сертификат должен содержать следующие поля, идентифицирующие лицо, ответственное за сертификат:

- Фамилия, имя, отчество;
- Адрес электронной почты;
- Полное юридическое название организации;
- Подразделение организации;
- Город;
- Область/штат;
- Страна/регион.

Заполнение полей осуществляется на английском языке, также допускается использование латинской транслитерации. Все поля в электронной заявке должны быть заполнены.

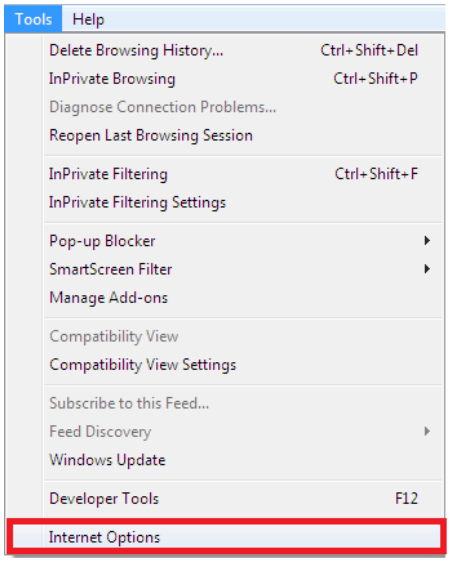
2.1. ФОРМИРОВАНИЕ ЭЛЕКТРОННОГО ЗАПРОСА ЧЕРЕЗ ЗАПОЛНЕНИЕ ФОРМЫ НА WEB-СТРАНИЦЕ

С помощью формы на web-странице можно заказать следующие типы сертификатов:

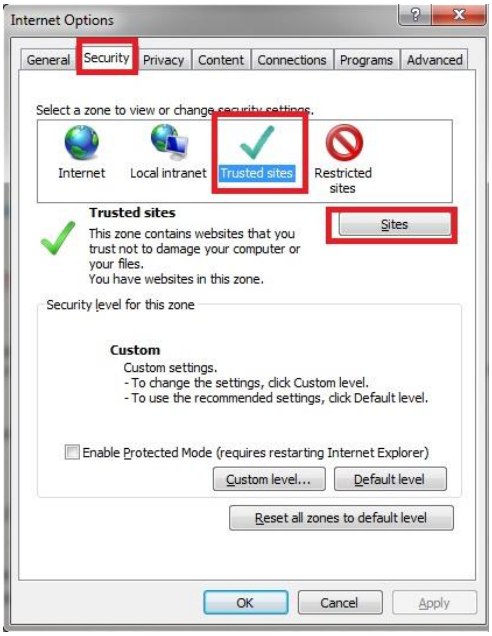
- сертификат для безопасного обмена электронной почтой;
- сертификат для SSL-аутентификации на web-сервере;

Порядок отправки запроса:

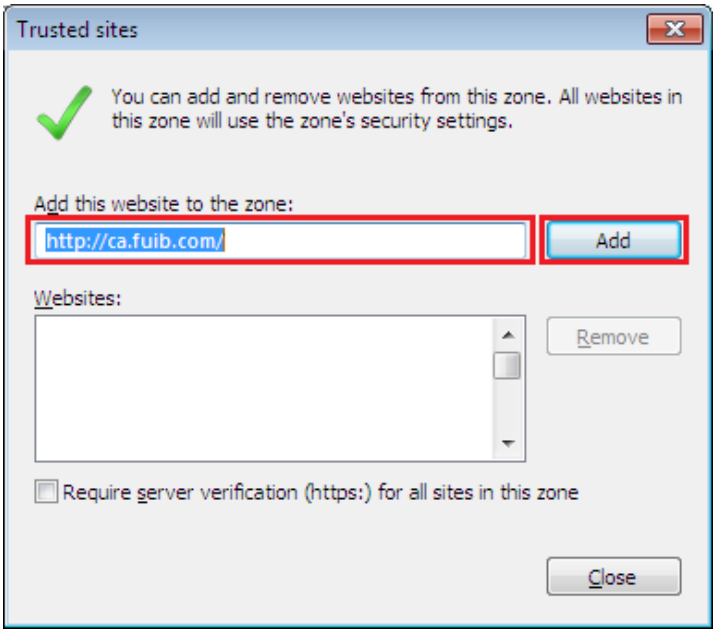
2.1.1. Необходимо добавить сайт **http://ca.fuib.com** в доверенные (данное действие необходимо выполнять на компьютере всего один раз). Для этого, запускаем браузер **Internet Explorer**, и в меню «**Tools**» выбираем **«Internet Options»**.



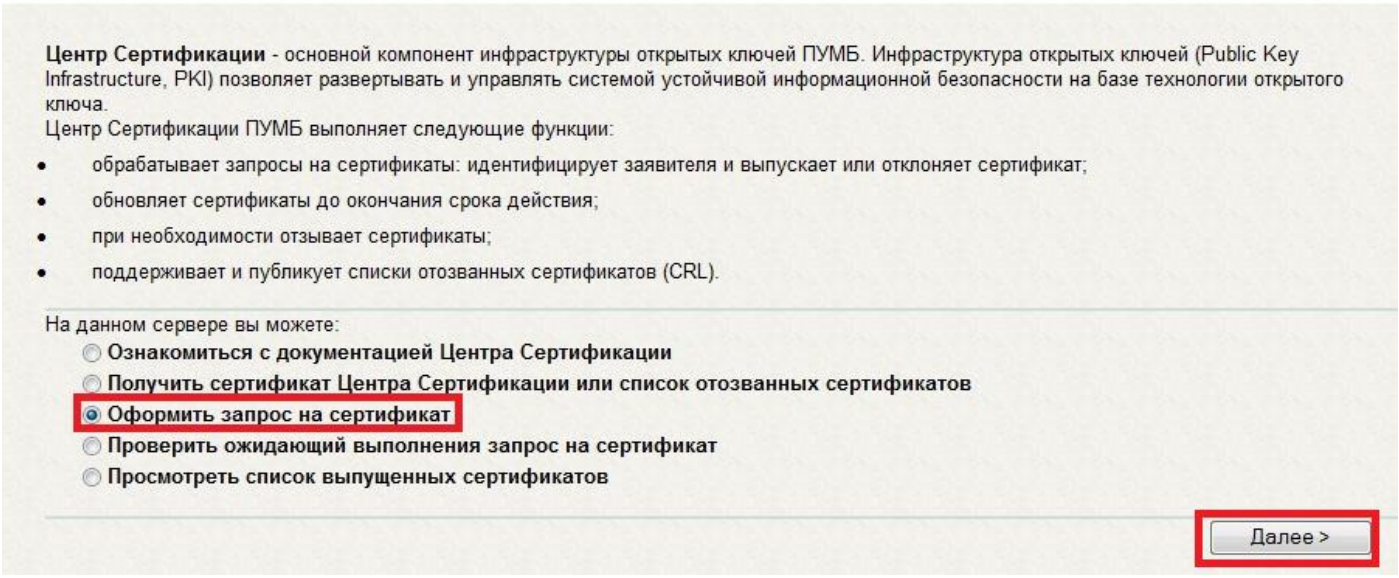
2.1.2. Откоываем вкладку **«Security»** => **«Trusted sites»** и нажимаем на кнопку **«Sites»**.



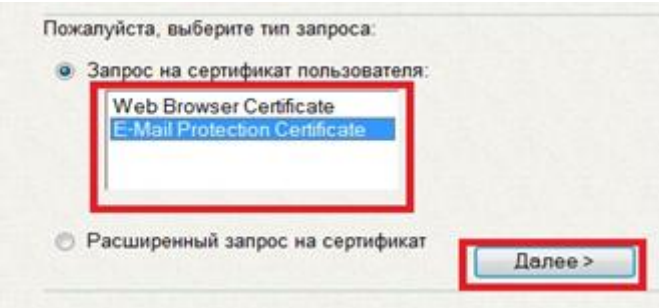
2.1.3. С помощью кнопки **«Add»** добавляем сайт в категорию доверенных **«Trusted sites»**.



2.1.4. На главной странице Центра Сертификации **(http://ca.fuib.com)** выбираем пункт **«Оформить запрос на сертификат»**, и нажимаем на кнопку **«Далее»**.

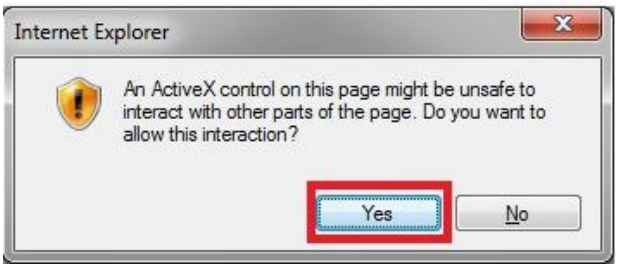


2.1.5. На странице **«Создание запроса на сертификат»** в качестве типа запроса выбираем **«Запрос на сертификат пользователя»**. Выбираем тип запрашиваемого сертификата **(«E-mail Protection Certificate»** или **«Web Browser Certificate»**) и нажимаем на кнопку **«Далее»**.



«E-mail Protection Certificate» - сертификат для обмена защищенной электронной почтой.
«Web Browser Certificate» - сертификат для шифрования передаваемых данных между браузером и сервером.

2.1.6. На вопрос системы «**Разрешить ActiveX на текущей странице?**», выбираем **«Да».**

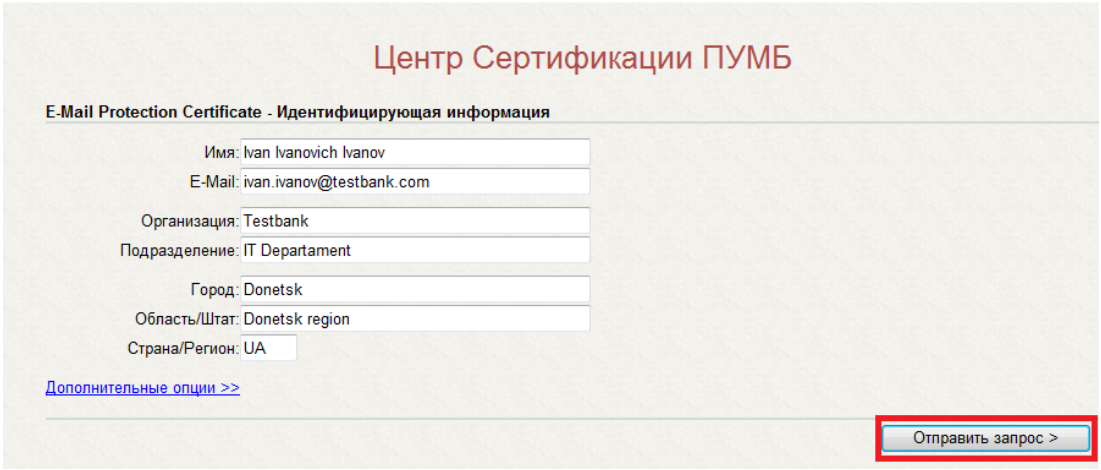


2.1.7. На запрос **«Web Access Confirmation»**, также отвечаем утвердительно («**Да**»).

2.1.8. На следующей странице необходимо ввести информацию, идентифицирующую владельца сертификата. При необходимости, можно изменить некоторые параметры запроса на сертификат, нажав на кнопку **«Дополнительные опции».**

Примечание! *Если заказывается сертификат для работы одной из автоматизированных систем банка (CardGalaxy, BillPayments и т. д.), то необходимо в поле* ***«Имя»*** *(вместо Фамилии, имени и отчества) - указать имя соответствующей автоматизированной системы.*

<u>Пример заполнения формы при заявке “E-mail Protection Certificate”:</u>



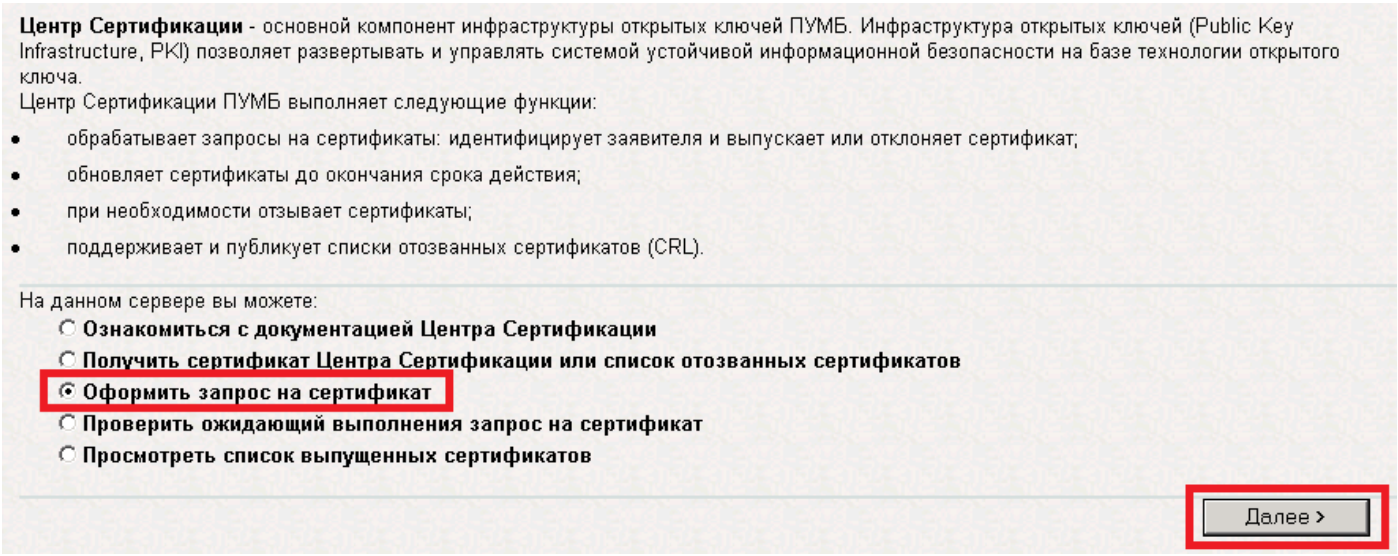
2.1.9. В процессе отправки запроса осуществляется генерация пары ключей. Если процесс генерации ключей и отправка запроса прошли без ошибок, то об этом будет выдано соответствующее сообщение. В случае возникновения ошибки об этом необходимо сообщить в службу поддержки Центра Сертификации (**ca@fuib.com**).

2.2. ФОРМИРОВАНИЕ ЭЛЕКТРОННОГО ЗАПРОСА НА ВЫПУСК СЕРТИФИКАТА В ФОРМАТЕ (PKCS#10)

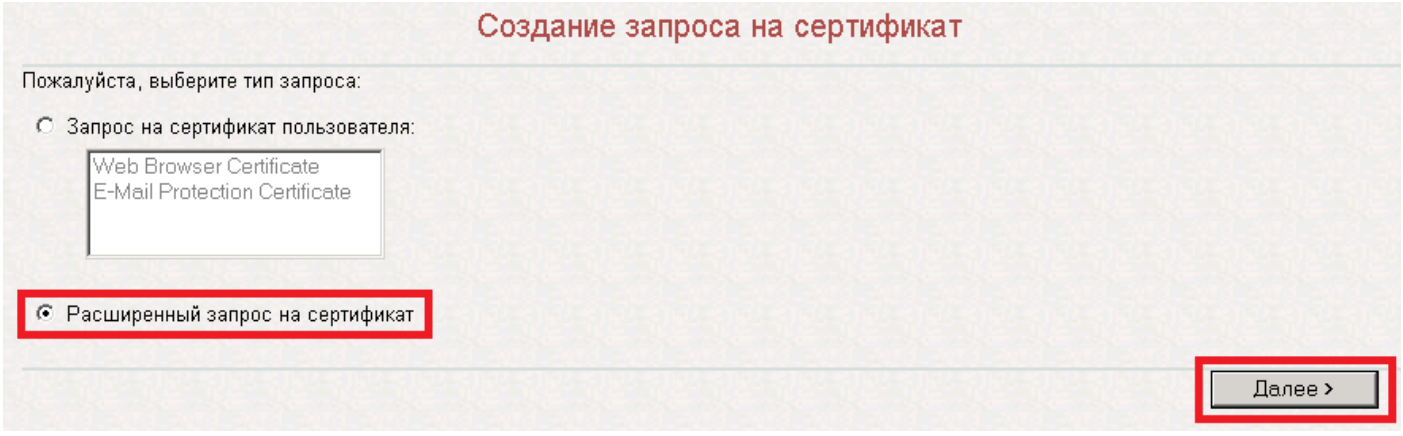
Отправка запроса в формате PKCS#10 предполагает наличие предварительно сформированного файла запроса. Формирование запроса осуществляется с помощью любого средства поддерживающего формат PKCS#10 (например, OpenSSL).

Порядок отправки запроса:

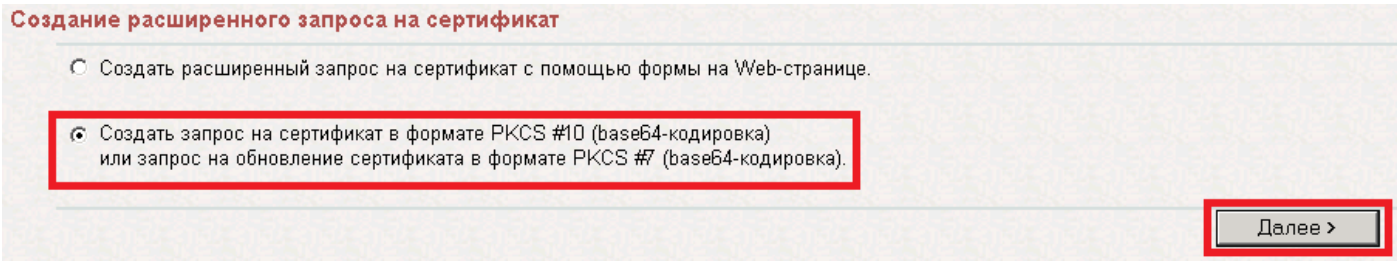
2.2.1 На первой странице Центра Сертификации **(http://ca.fuib.com)** выбираем пункт **«Оформить запрос на сертификат»**, и нажимаем на кнопку **«Далее»**.



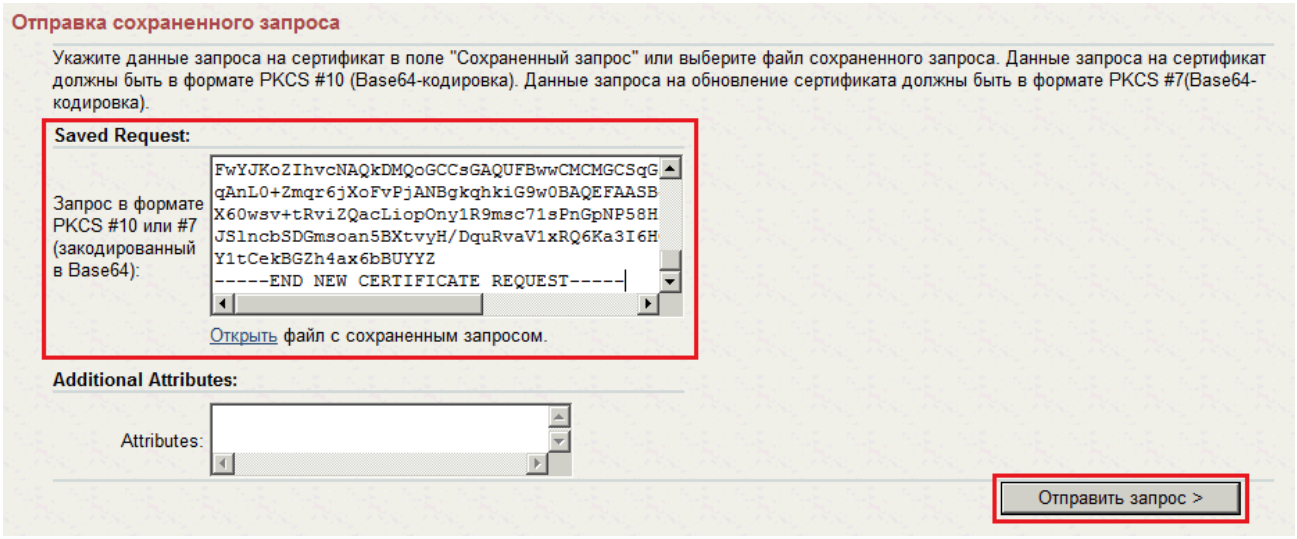
2.2.2 На странице **«Создание запроса на сертификат»** выбираем пункт **«Расширенный запрос на сертификат»** и нажимаем кнопку **«Далее»**.



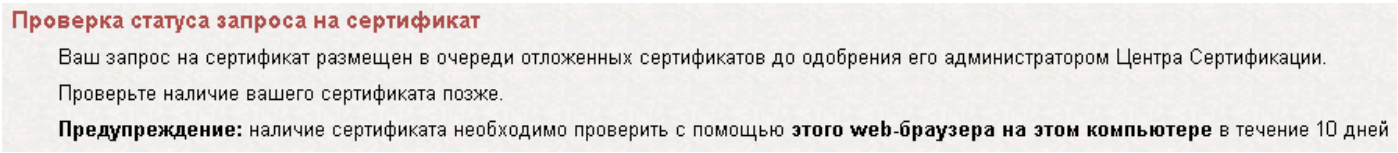
2.2.3 На странице **«Создание расширенного запроса на сертификат»** выбираем пункт **«Создать запрос на сертификат в формате PKCS #10 (base64-кодировка) или запрос на обновление сертификата в формате PKCS #7 (base64-кодировка)**», и нажимаем на кнопку **"Далее"**.



2.2.4. На странице **«Отправка сохраненного запроса»** необходимо указать данные запроса на сертификат в поле **«Сохраненный запрос»** или выбрать файл сохраненного запроса. Данные запроса на сертификат должны быть в формате #PKCS10 (Base64-кодировка). Данные запроса на обновление сертификата должны быть в формате #PKCS7(Base64-кодировка).



2.2.5 После заполнения поля **«Сохраненный запрос»** или открытия файла сохраненного запроса, нажимаем кнопку **«Отправить запрос».** Если запрос отправлен без ошибок, то об этом будет выдано соответствующее сообщение. В случае возникновения ошибки об этом необходимо сообщить в службу поддержки Центра Сертификации (ca@fuib.com).



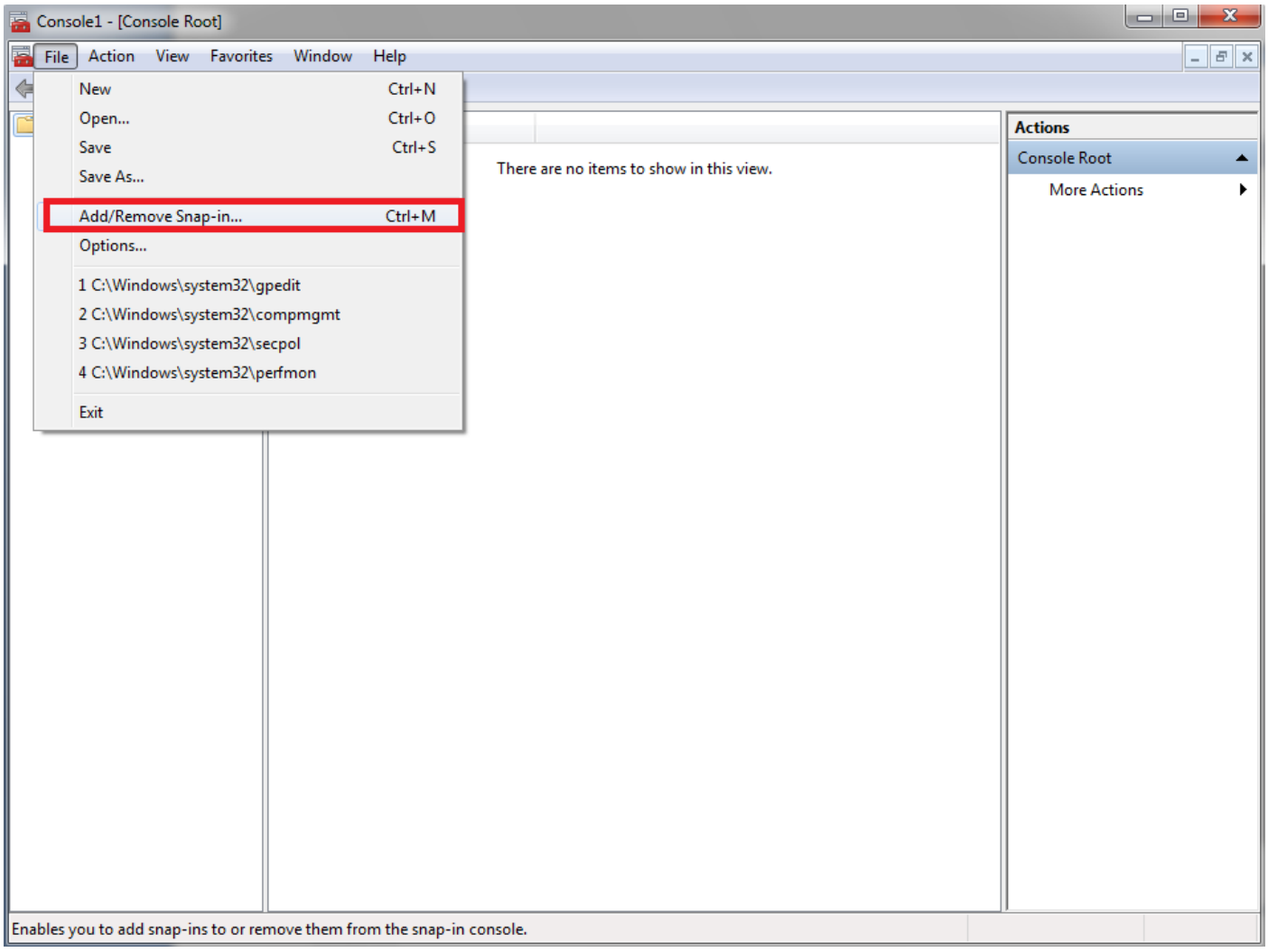
3. ПОЛУЧЕНИЕ ИДЕНТИФИКАТОРА ОТКРЫТОГО КЛЮЧА

3.1. ПОЛУЧЕНИЕ ID-КЛЮЧА СИСТЕМНЫМИ СРЕДСТВАМИ ОС WINDOWS

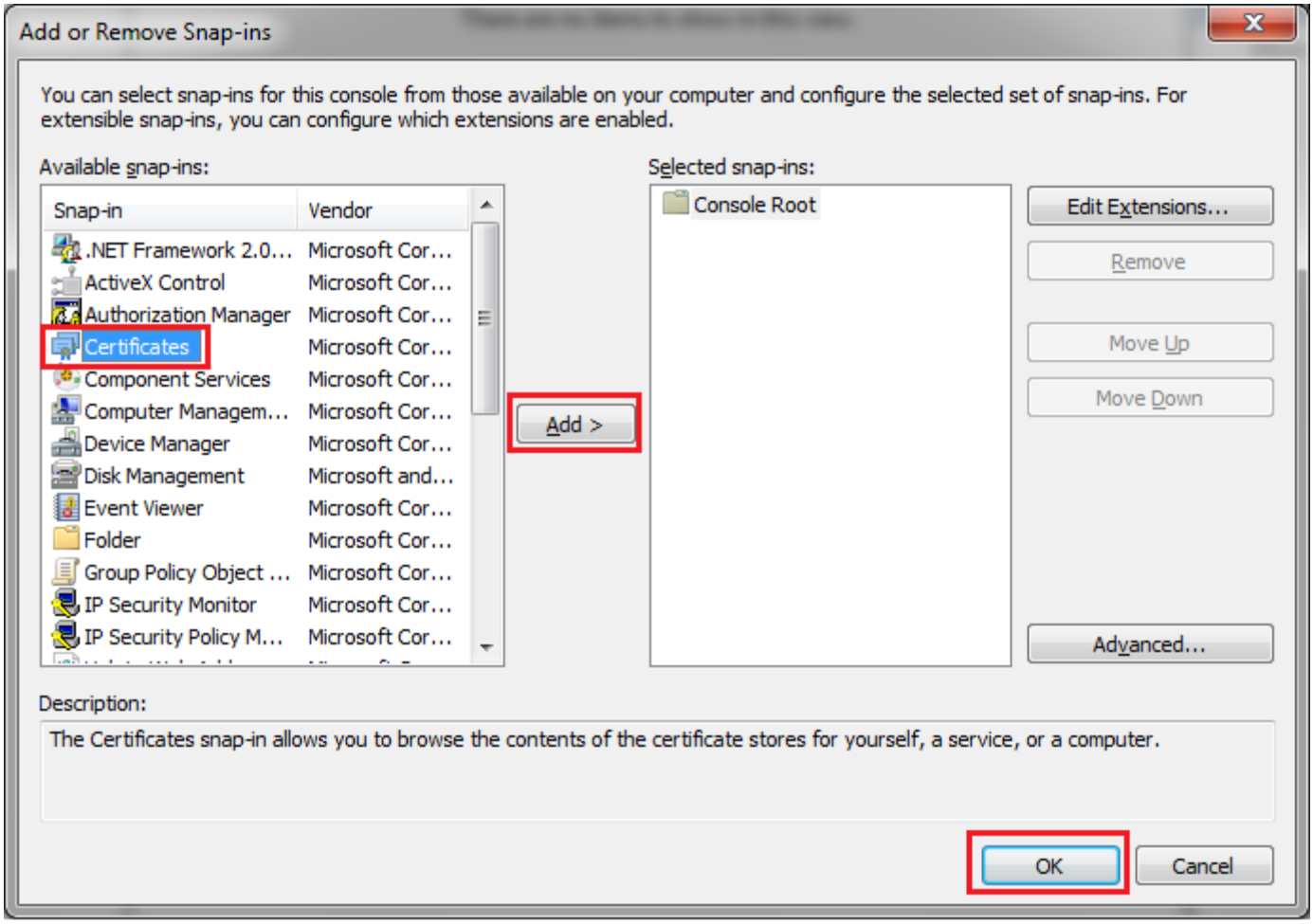
Для получения идентификатора ключа необходимо выполнить следующие действия:

3.1.1 Запускаем программу **«Microsoft Management Console»** (файл **mmc.exe**), входящую в стандартную поставку ОС Windows.

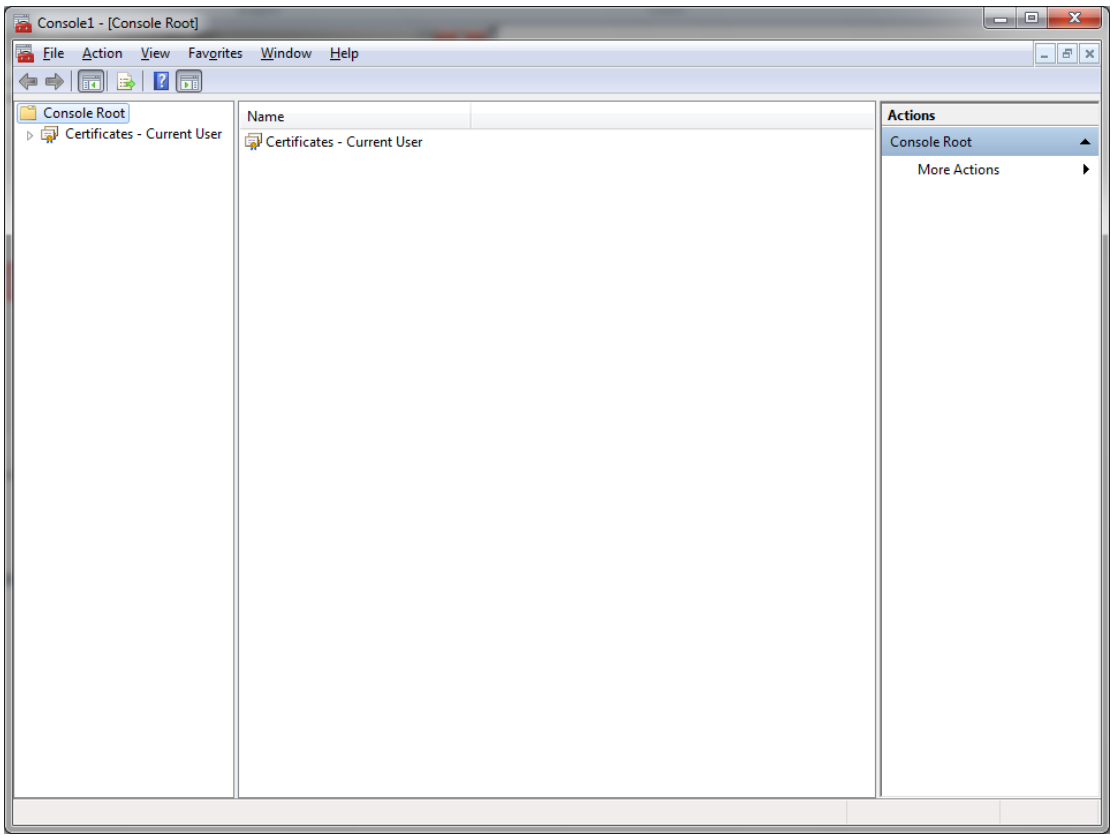
3.1.2 В запустившейся программе, для загрузки оснастки управления сертификатами - выбираем в меню **«File»** пункт **«Add/Remove Snap-in …»**



3.1.3 В появившемся окне **«Add/Remove Snap-in»** - в левом окне находим и выбираем оснастку **«Certificates»** ,затем нажимаем кнопку **«Add»** и подтверждаем выбор нажатием на кнопку **«OK»**.

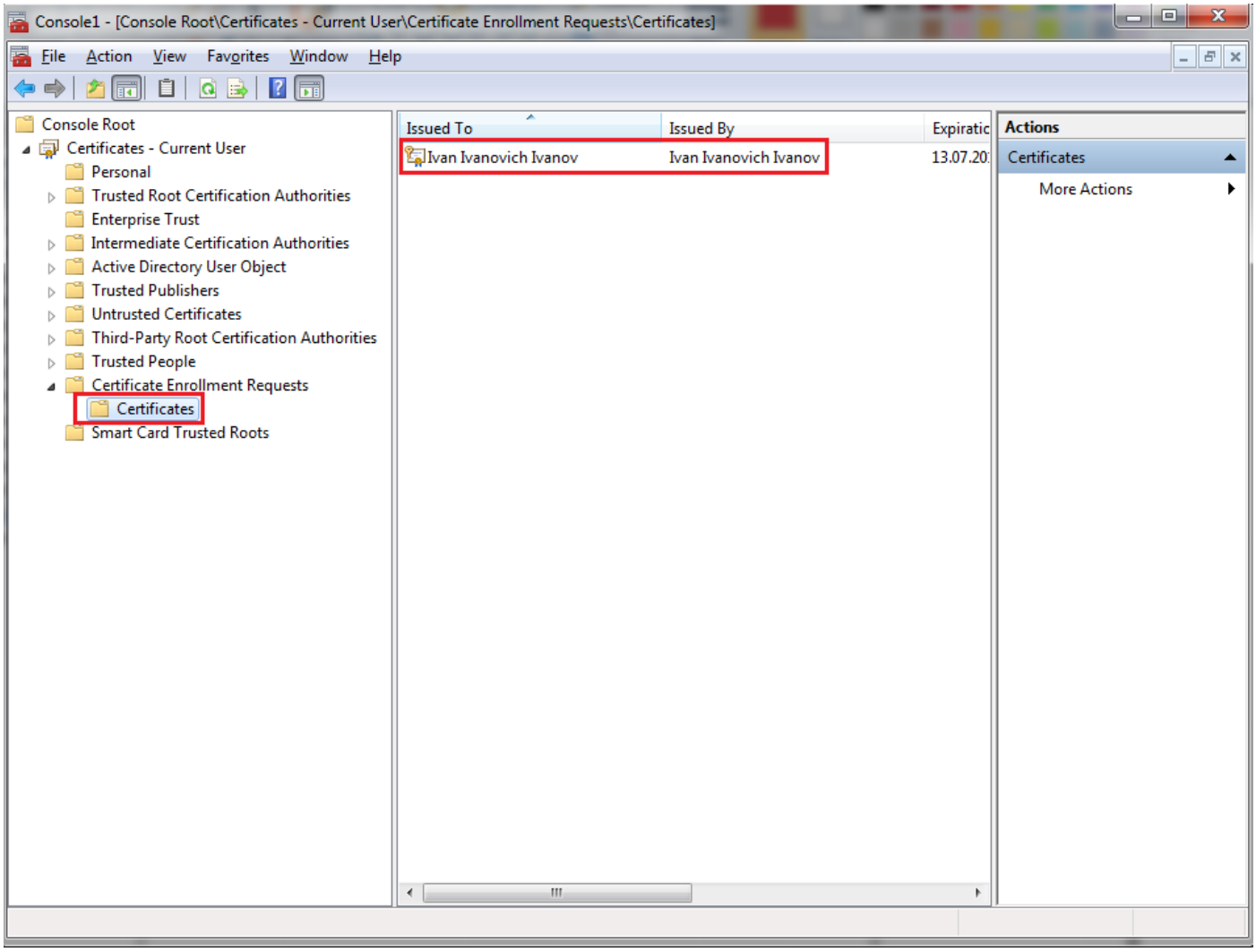


3.1.4 После всех выполненных действий окно **Microsoft Management Console** должно приобрести следующий вид:

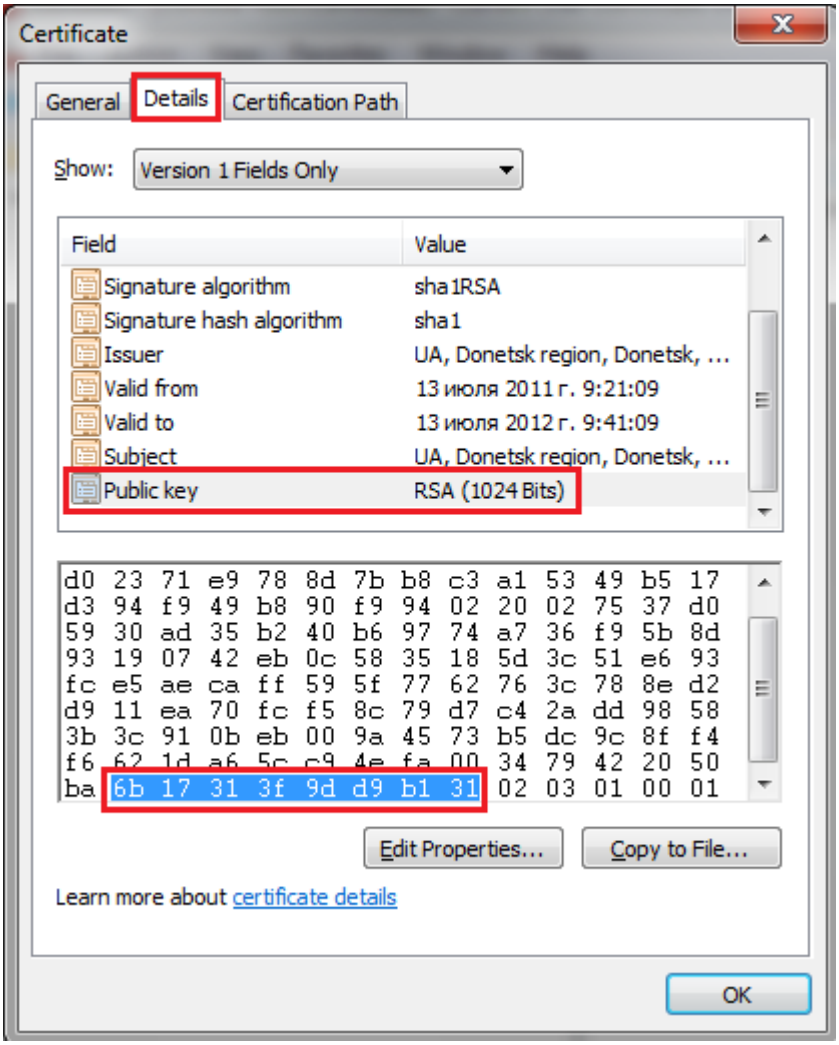


3.1.5 Для получения своего запроса необходимо войти в следующую ветку оснастки **«Certificates»**:

«Certificates - Current User» =>«Certificate Enrollment Requests» => «Certificates» и выбрать нужный запрос. Двойным щелчком мыши вызываем окно свойств запроса.



3.1.6 В окне свойств выбираем закладку **«Details»** и в этой вкладке находим параметр **«Public key»**. В нижнем поле появиться информация об открытом ключе. Для получения идентификатора ключа необходимо отбросить последние 5 байт (**10 символов**) и выписать предыдущие 8 байт (**16 символов в шестнадцатеричной системе исчисления**).



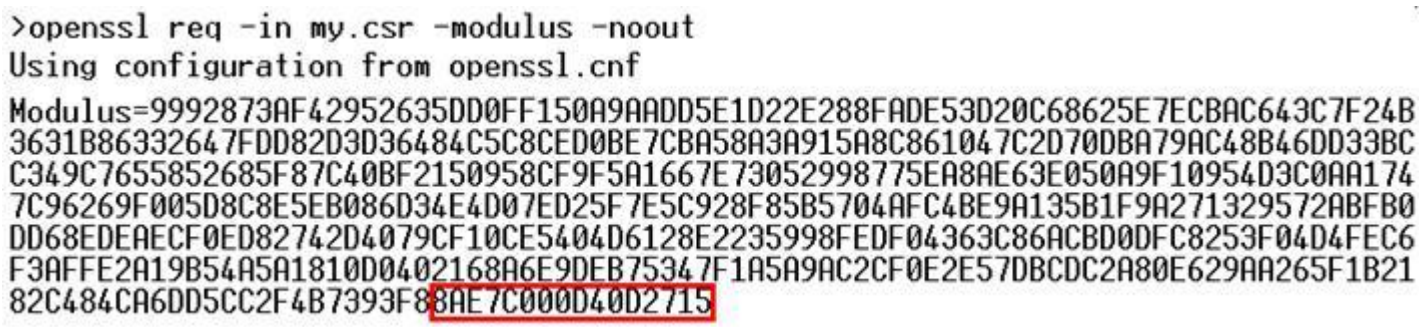
Таким образом, для показанного выше примера ID ключа будет: **«6b 17 31 3f 9d d9 b1 31»**

3.2. ПОЛУЧЕНИЕ ID-КЛЮЧА С ПОМОЩЬЮ УТИЛИТЫ OPENSSL

Для получения идентификатора ключа необходимо выполнить следующие действия:

3.2.1. Выполнить команду: **«openssl req -config "config filename" -in "request filename" -modulus -noout»** или **«openssl rsa -in "private key file" -modulus -noout»**.

"request filename" - это файл с запросом на формирование сертификата в формате PKCS#10.
После выполнения этой команды на экране будет выведен модуль ключа, последние 8 байт (16 символов шестнадцатеричной системы исчисления) и будут идентификатором ключа.



Таким образом, для показанного выше примера ID ключа будет: **«8A E7 C0 00 D4 0D 27 15»**.

4. ПОДТВЕРЖДЕНИЕ ЗАПРОСА НА ВЫПУСК СЕРТИФИКАТА

В процессе отправки электронного запроса в ЦС существует вероятность осуществления злоумышленником атаки типа "человек посередине". В результате чего злоумышленник сможет просматривать и/или изменять передаваемую информацию. Для уменьшения риска, связанного с описанной ситуацией, необходимо отправлять информацию, указанную в электронном запросе на выпуск сертификата, альтернативными путями (например, бумажной почтой или факсимильными сообщениями). В документе, подтверждающем необходимость выпуска сертификата, необходимо указать ту же информацию, которая была указана при формировании электронного запроса:

- "Имя";
- "E-Mail";
- "Организация";
- "Подразделение";
- "Город";
- "Область/Штат";
- "Страна/Регион".

Кроме указанной выше информации, так же необходимо указать **идентификатор открытого ключа (Key ID)**.

Если сертификат заказывается для Банка-Партнера или другой организации, документ, подтверждающий электронный запрос на выпуск сертификата, должен быть оформлен на фирменном бланке, содержать печать и подпись руководителя организации.

После того как документ составлен, его необходимо отправить почтой (допускается факсимильным сообщением) на сотрудника фронт офиса ПУМБ, ответственного за работу с данной организацией.

Подтверждение запроса на сертификат должно попасть к администратору ЦС не позже чем через 15 дней после отправки электронного запроса, иначе в выпуске сертификата будет отказано.

(Пример)

Начальнику Процессингового Центра
Публичного Акционерного Общества «ПУМБ»
Ю.В. Шатровой

Уважаемая Юлия Валериевна!

В связи с необходимостью обмена конфиденциальной информацией, прошу Вас сформировать цифровой сертификат для _____

_____

(цель выпуска сертификата)

и добавить его в базу Центра Сертификации Публичного Акционерного Общества «ПУМБ». Ответственным за цифровой сертификат назначен: _____.

Реквизиты электронного запроса на сертификат:

"Имя":	
"E-Mail":	
"Организация":	
"Подразделение":	
"Город":	
"Область/Штат":	
"Страна/Регион":	
Идентификатор открытого ключа:	

Ф.И.О., должность, дата, подпись, печать.

5. ВЫПУСК СЕРТИФИКАТА

Порядок выпуска цифрового сертификата:

5.1. Документ, подтверждающий запрос на выпуск сертификата, попадает к сотруднику фронт офиса ПУМБ, ответственному за работу с организацией клиента или партнера банка.

5.2. Сотрудник фронт офиса ПУМБ должен проверить наличие договора о предоставлении услуг между банком и организацией, после чего проверить подлинность документа. Если документ подлинный и существуют договорные отношения между банком и организацией, то подтверждение передается на подпись руководителю структурного подразделения.

5.3. Подтверждение, подписанное руководителем структурного подразделения банка, работающего с организацией клиента или партнера, передается администратору ЦС ПУМБ.

5.4. Администратор ЦС ПУМБ проверяет выполнение следующих требований:

- заполнены все поля электронного запроса;
- в подтверждении запроса указана вся информация, описанная в пункте 4;
- информация, указанная в подтверждении, соответствует содержимому электронного запроса;
- идентификатор открытого ключа, указанный в подтверждении, соответствует открытому ключу, содержащемуся в электронном запросе;
- подтверждение запроса содержит печать и подпись руководителя организации, для сотрудника которой выпускается сертификат;
- подтверждение запроса пришло не позже чем через пятнадцать дней, после отправки электронного запроса;
- на документе есть подпись руководителя структурного подразделения ПУМБ, работающего с организацией клиента или партнера.

5.5. Если все требования выполнены, то администратор осуществляет выпуск сертификата.

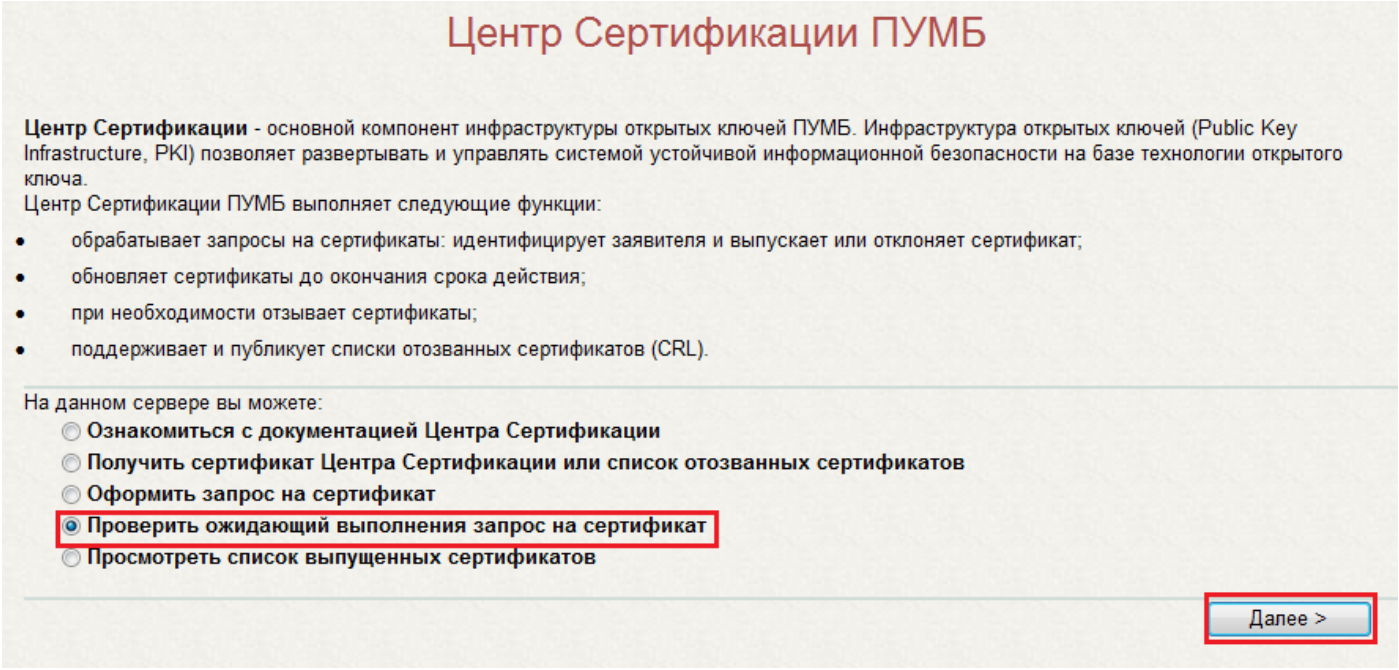
5.6. Выпущенный сертификат заносится в базу сертификатов ЦС ПУМБ.

6. ПОЛУЧЕНИЕ И УСТАНОВКА СЕРТИФИКАТА

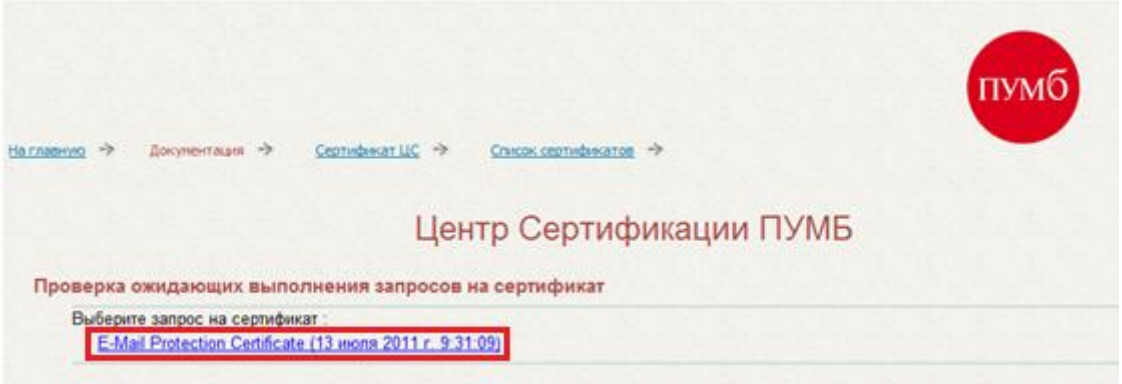
После отправки электронного запроса и подтверждения, пользователь должен сам проверять состояние своего запроса, и в случае если сертификат был выпущен - скачать его к себе на рабочую станцию.

Порядок получения сертификата:

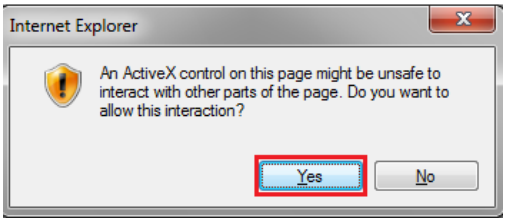
6.1 На первой странице Центра Сертификации **(http://ca.fuib.com)** выбираем пункт **«Проверить ожидающий выполнения запрос на сертификат»**, и нажимаем кнопку **«Далее»**.



6.2. На странице **«Проверка ожидающих выполнения запросов на сертификат»** выбираем интересующий запрос.

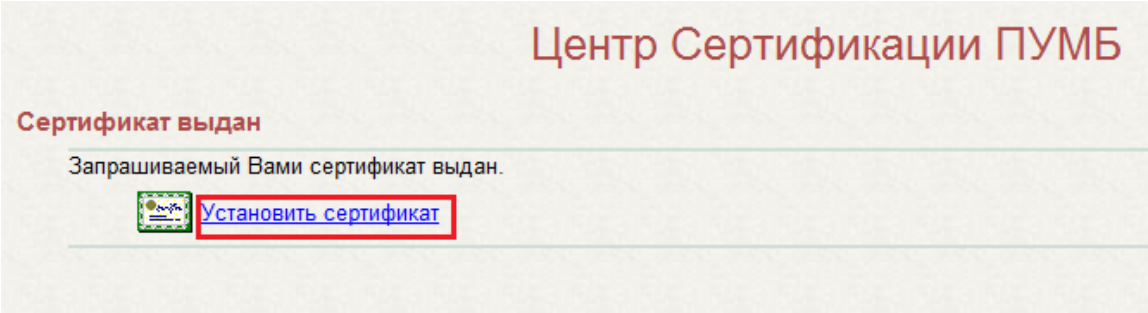


6.3. На запрос использования **ActiveX** - выбираем **«Да»**.



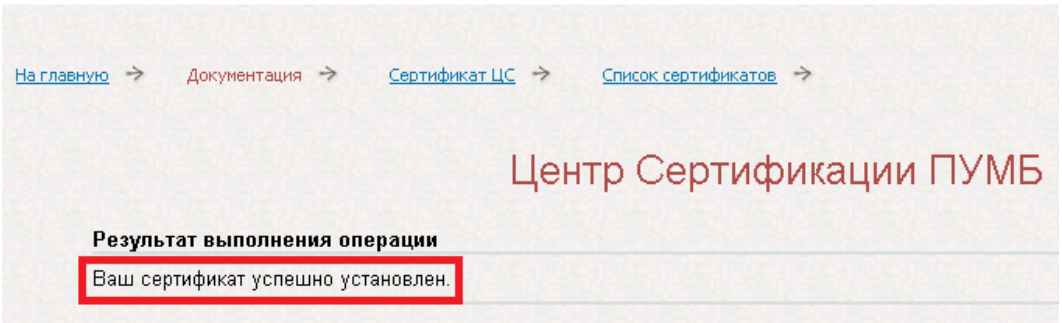
6.4. На вопрос системы **«Разрешить данную операцию?»**, также выбираем **«Да»**.

6.5. Если сертификат был выпущен, то произойдет переход на страницу **«Сертификат выдан»**, на которой можно его установить.



Если после отправки подтверждения электронная заявка на выпуск сертификата долгое время находится в состоянии ожидания, или получено сообщение о том, что в выпуске сертификата отказано - пользователь должен связаться с сотрудником фронт офиса ПУМБ и выяснить причину.

6.6. После установки появится сообщение **«Ваш сертификат успешно установлен».**



7. ОТЗЫВ ЦИФРОВЫХ СЕРТИФИКАТОВ

Отозванный сертификат обозначает то, что секретный ключ, принадлежащий владельцу сертификата, является недействительным. Для того чтобы пользователи могли узнавать, какие сертификаты являются недействительными, ЦС публикует список отозванных сертификатов (**certificate revocation list, CRL**). Список отозванных сертификатов содержит серийный номер сертификата и дату отзыва.

Отзыв сертификата осуществляется в следующих случаях:

- увольнение или перевод на другую должность лица, ответственного за сертификат;
- компрометация секретного ключа;
- невозможность получения доступа к секретному ключу (например, забыт пароль, которым защищен секретный ключ или разрушен носитель, на котором находился секретный ключ).

Отзыв сертификата осуществляется администратором ЦС. Основанием для отзыва является бумажный документ, оформленный в виде заявки. Заявка составляется в свободной форме и должна содержать следующие данные:

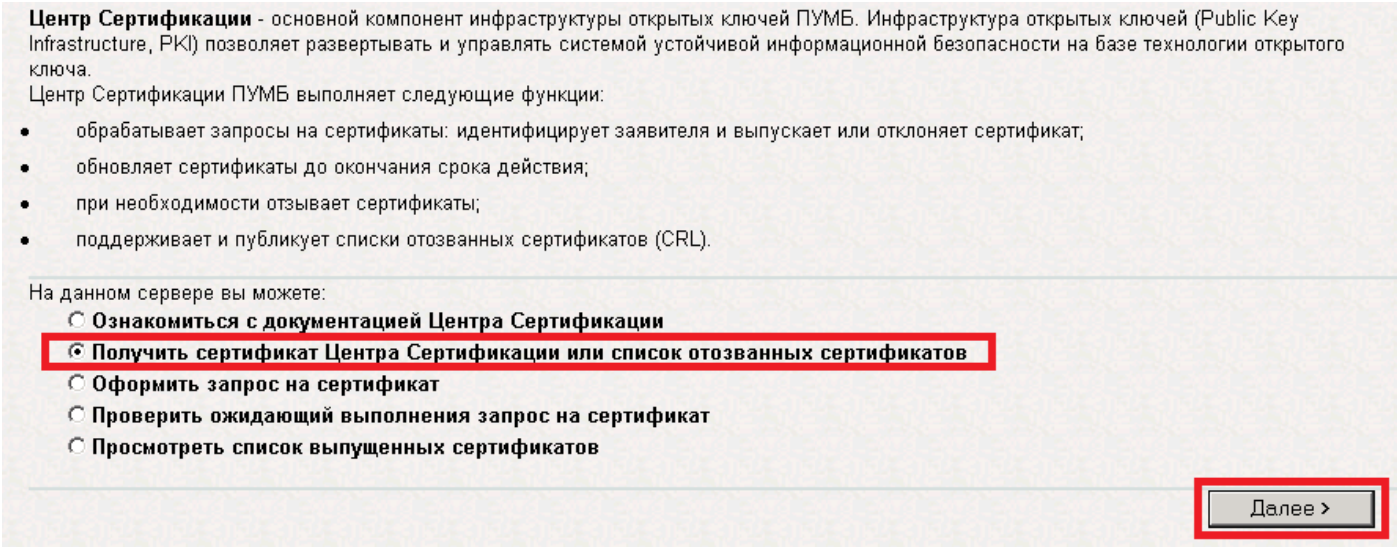
- Фамилия, имя, отчество;
- Адрес электронной почты;
- Полное юридическое название организации;
- Подразделение организации;
- Город;
- Область/штат;
- Страна/регион;
- Серийный номер сертификата;
- Причина отзыва сертификата.

Заявка на отзыв сертификата должна быть заверена подписью руководителя и печатью организации.

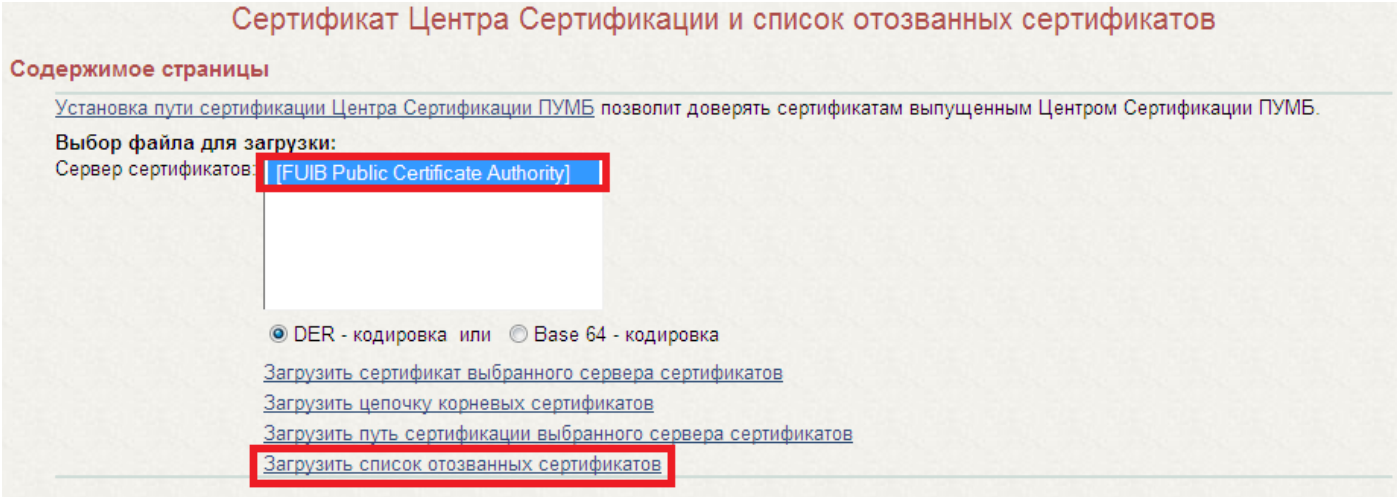
7.1. ПОРЯДОК ПОЛУЧЕНИЯ СПИСКА ОТОЗВАННЫХ СЕРТИФИКАТОВ

Порядок получения списка отозванных сертификатов:

7.1.1. На первой странице сервера регистрации заявок Центра Сертификации (http://ca.fuib.com) выбираем пункт **«Получить сертификат Центра Сертификации или список отозванных сертификатов»**, и нажимаем кнопку **«Далее»**.



7.1.2. В появившейся странице – выбираем **«Сервер сертификации ПУМБ»** и переходим по ссылке **«Загрузить список отозванных сертификатов».**



7.2. ПОРЯДОК ОТЗЫВА СЕРТИФИКАТА

7.2.1. Составляется заявка в (бумажном виде) на отзыв сертификата, согласно требованиям описанным выше.

7.2.2. Заявка на отзыв сертификата отправляется сотруднику фронт офиса ПУМБ, ответственному за работу с организацией клиента или партнера банка.

7.2.3. Сотрудник фронт офиса ПУМБ должен проверить подлинность документа, и если документ подлинный передать его на подпись руководителю структурного подразделения.

7.2.4. После того, как заявка на отзыв заверена руководителем структурного подразделения, работающего с организацией, она передается администратору ЦС, который отзывает сертификат и добавляет его в список отозванных сертификатов.

7.2.5. В случае, когда существуют подозрения о компрометации секретного ключа пользователя, администратор ЦС может сам отозвать сертификат пользователя. В этом случае отзыв может быть осуществлен без наличия заявки.

(Пример)

Начальнику Процессингового Центра
Публичного Акционерного Общества «ПУМБ»
Ю.В. Шатровой

Уважаемая Юлия Валериевна!

В связи с _____,

_____

(причина отзыва сертификата)

прошу Вас отозвать цифровой сертификат и удалить его из базы Центра Сертификации Публичного Акционерного Общества «ПУМБ».

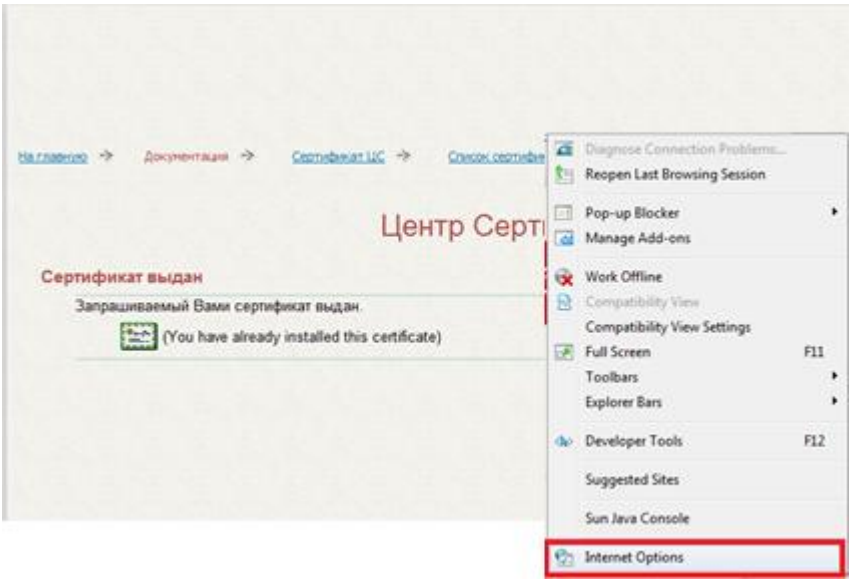
Реквизиты сертификата:

"Имя":	
"E-Mail":	
"Организация":	
"Подразделение":	
"Город":	
"Область/Штат":	
"Страна/Регион":	
Серийный номер сертификата:	

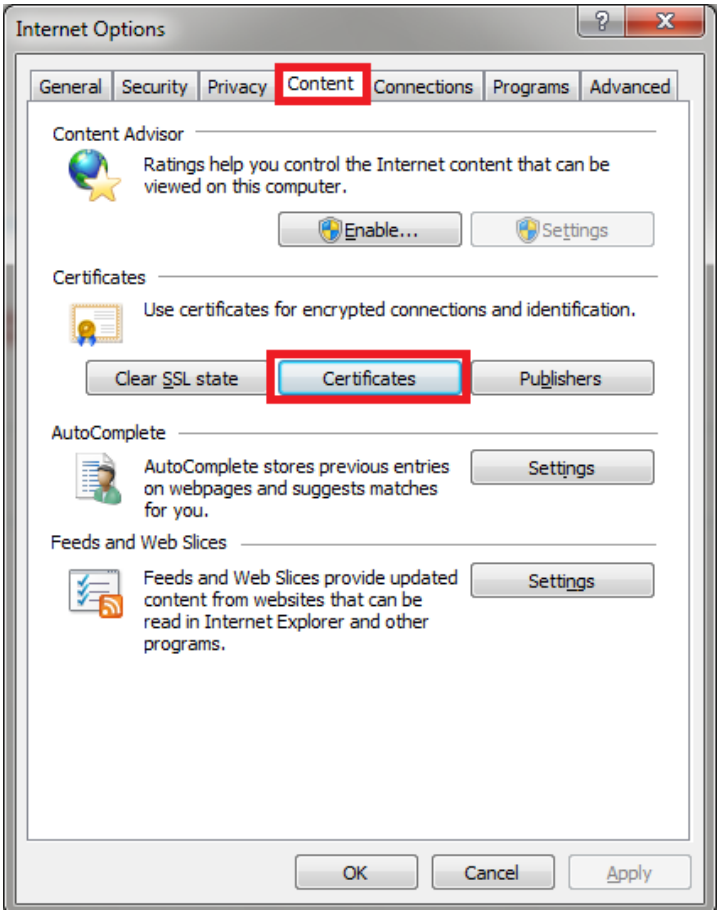
Ф.И.О., должность, дата, подпись, печать

8. ЭКСПОРТ ЦИФРОВОГО СЕРТИФИКАТА В ФАЙЛ

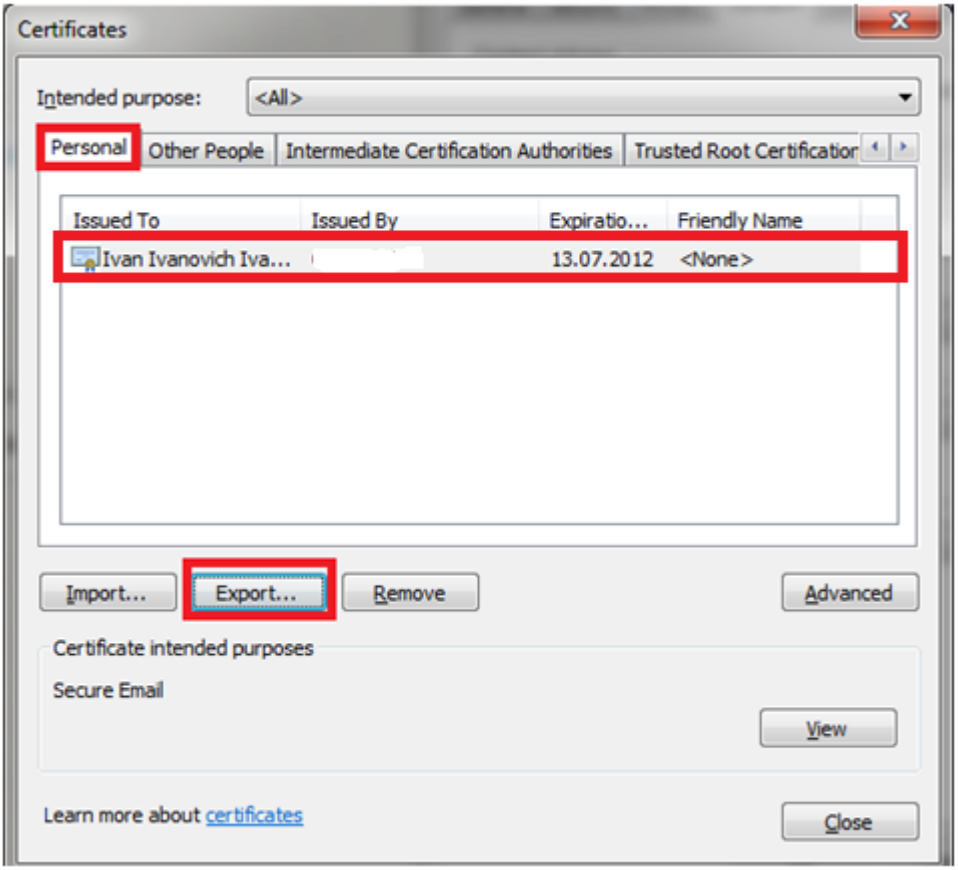
8.1. Запускаем браузер Internet Explorer. В панели инструментов выбираем **«Tools»** => **«Internet Options»**.



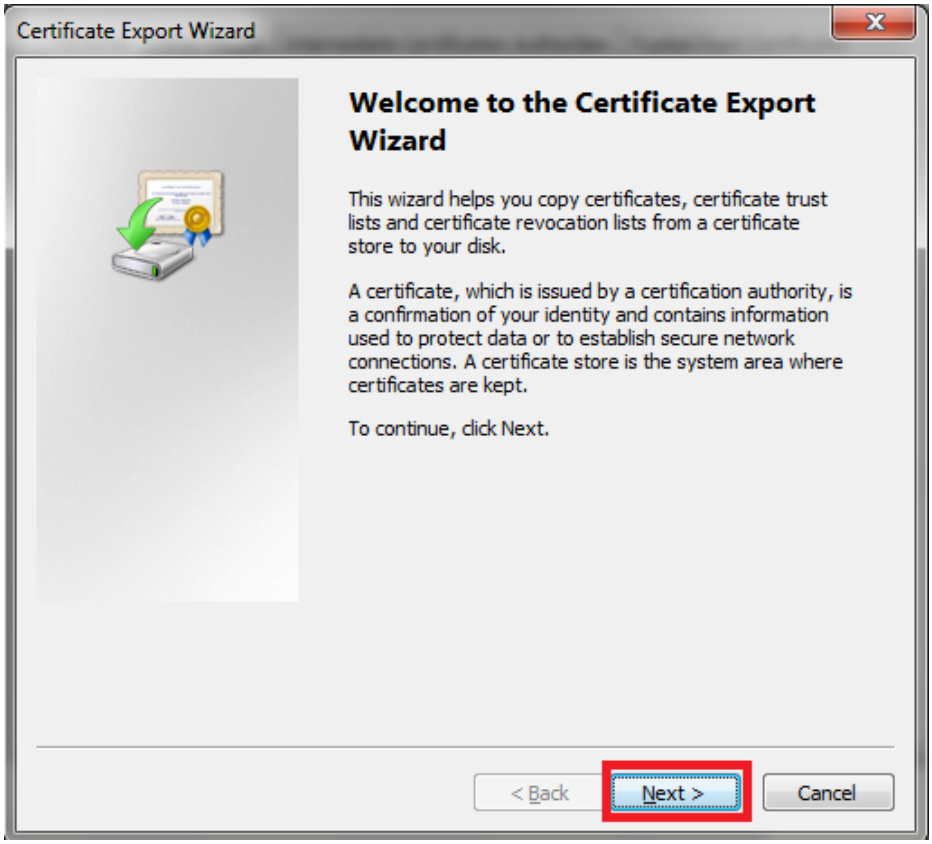
8.2. В окне настроек выбираем закладку **«Content»**, и нажимаем на кнопку **«Certificates…»**, после чего откроется окно управления сертификатами.



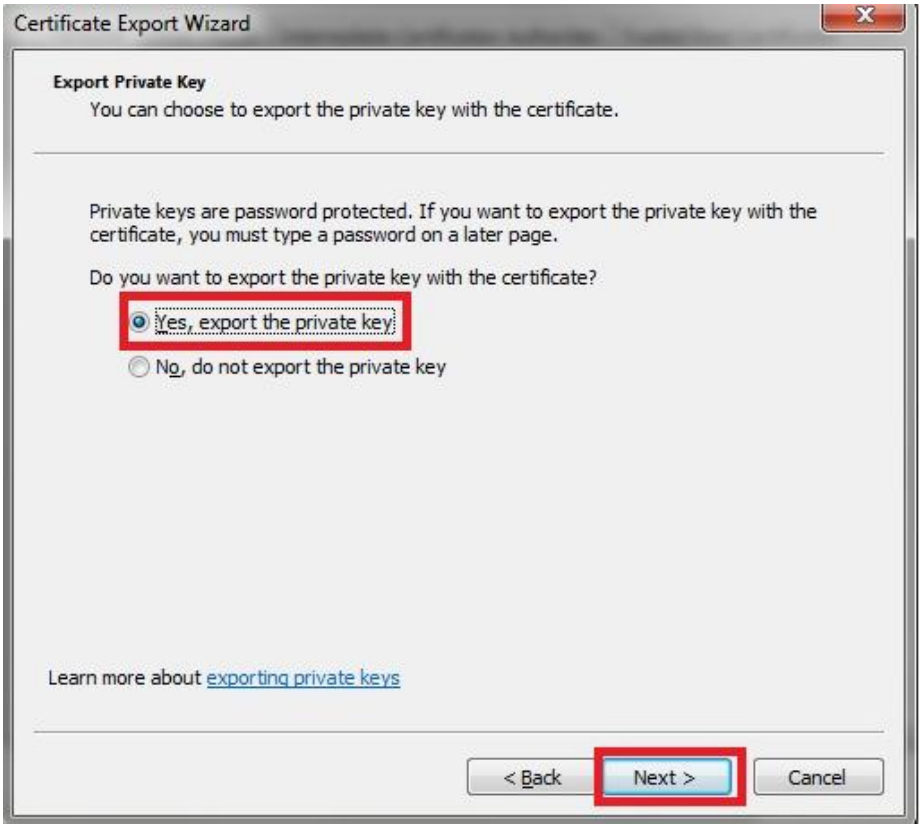
8.3. В окне управления сертификатами выбираем свой сертификат, и нажимаем на кнопку **«Export…»**.



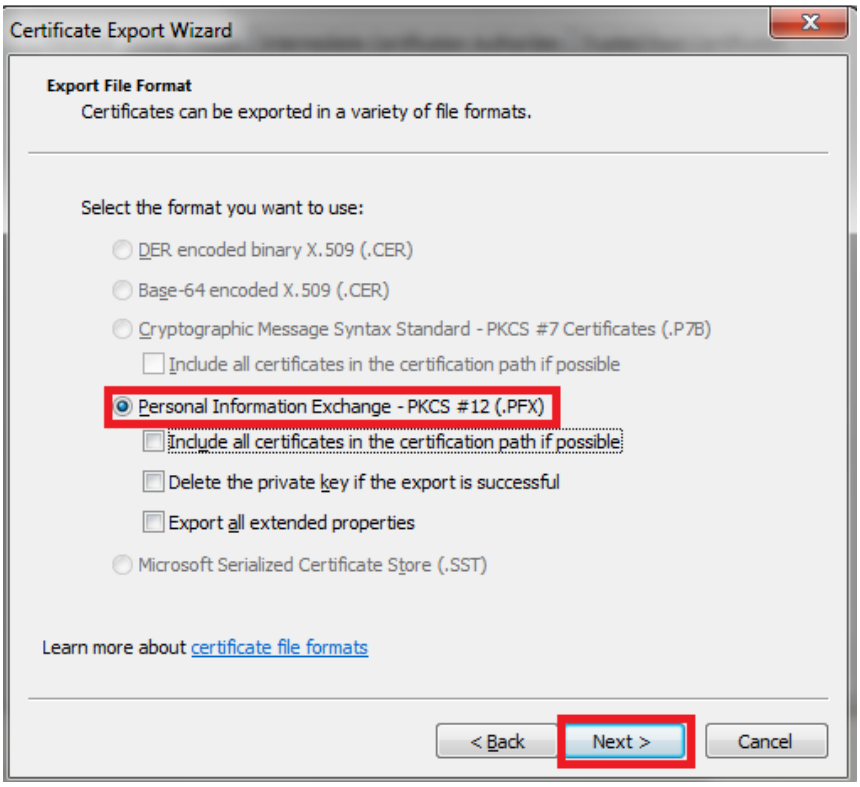
8.4. После того, как запустится мастер экспорта сертификатов, нажимаем на кнопку **«Next»**.



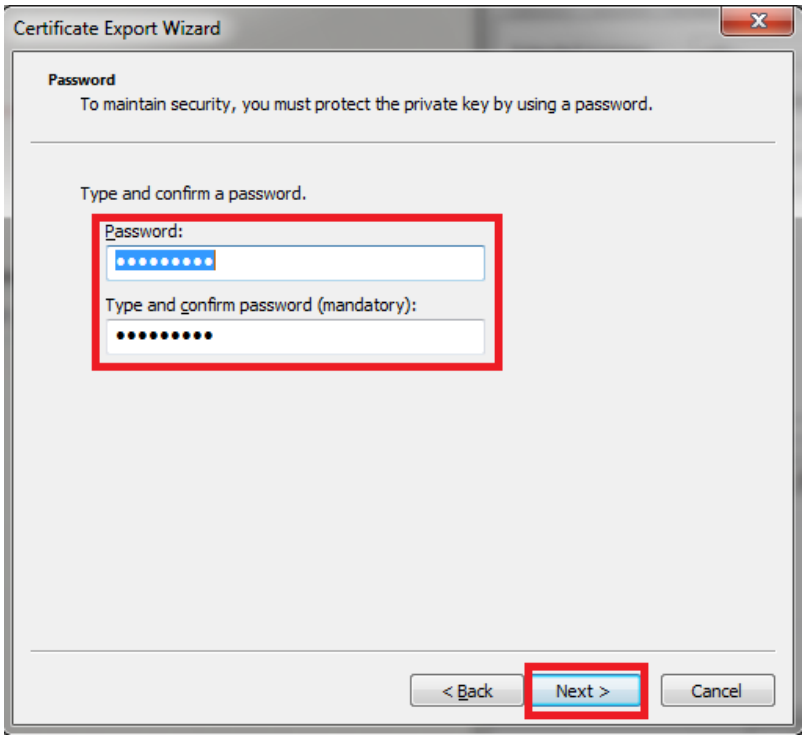
8.5. В первом окне **«Export Private Key»** выбираем пункт **«Yes, export the private key»**, и нажимаем кнопку **«Next»**.



8.6. В окне **«Export File Format»** выбираем **«Personal Information Exchange - PKCS#12 (.PFX)»**, после чего нажимаем на кнопку **«Next»**.

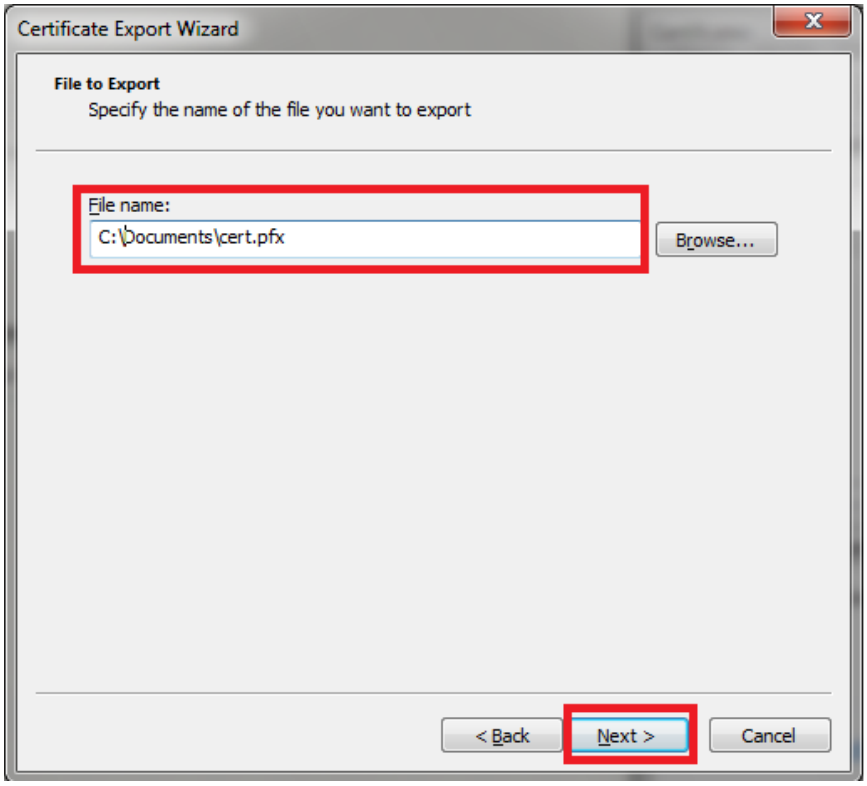


8.7. Вводим пароль, с помощью которого будет защищен секретный ключ**.** После того как пароль введен, нажимаем на кнопку **«Next»**.



После экспорта сертификата, пароль станет единственной защитой закрытого ключа.

8.8. В окне **«File to Export»** вводим имя файла, в котором будет сохранен сертификат и секретный ключ, после чего нажимаем на кнопку **«Next»**.



8.9. Заканчиваем процедуру экспорта **(**нажимаем на кнопку **«Finish»)**. Если операция по экспорту ключа завершилась успешно, об этом будет выдано соответствующее сообщение.