

UNIZETO



GENERAL
CERTIFICATION AUTHORITY



Руководство пользователя

Exchange Enterprise Edition 2003

Использование сертификатов
в программе Microsoft Exchange 2003
версия 1.2

Содержание

1. ВСТУПЛЕНИЕ	3
2. СОЗДАНИЕ СЕРТИФИКАТОВ.....	3
2.1. СОЗДАНИЕ ЗАЯВКИ НА СЕРТИФИКАТ CSR	3
2.2. СОЗДАНИЕ СЕРТИФИКАТА НА ОСНОВАНИИ СОЗДАННОГО ЗАПРОСА CSR	10
2.3. ПОЛУЧЕНИЕ И ИНСТАЛИРОВАНИЕ СЕРТИФИКАТА НА СЕРВЕРЕ	10
2.4. ПОЛУЧЕНИЕ ПРОМЕЖУТОЧНЫХ СЕРТИФИКАТОВ	17
2.5. ИМПОРТ ПРОМЕЖУТОЧНЫХ СЕРТИФИКАТОВ	18
3. КОНФИГУРАЦИЯ СЕРВЕРА EXCHANGE ДЛЯ СОЕДИНЕНИЙ HTTPS	22
4. ИМПОРТ/ЭКСПОРТ СЕРТИФИКАТОВ СЕРВЕРА	23

1. Вступление

Exchange — это почтовый сервис, предназначенный для системы Windows. Благодаря встроенным механизмам безопасности, при помощи протокола TLS, позволяет создавать шифрованное и авторизованное соединение со вторым сервером SMTP, создавая таким образом безопасный обмен информации. Находящиеся в пакете серверы POP3, NNTP, IMAP, поддерживают также сертификаты x.509, обеспечивая безопасный и авторизованный доступ для клиентов этих серверов. Этот документ содержит инструкцию генерации уникальной пары ключей и CSR для сервера Exchange.

2. Создание сертификатов

2.1. Создание заявки на сертификат CSR

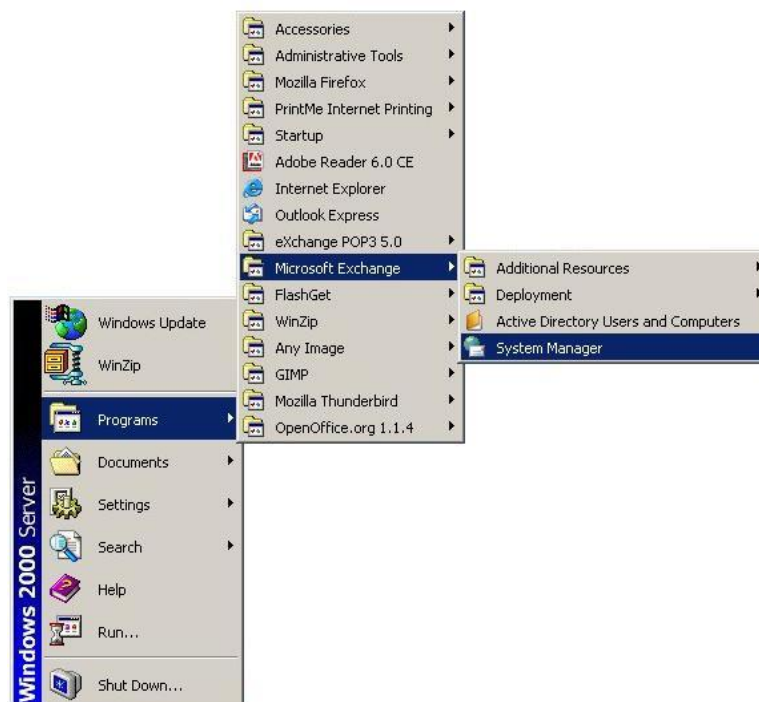
При генерации CSR необходимо ввести следующую информацию:

- **Type a name for a Certificate** – Введите имя создаваемого сертификата, напр.: Сервер SMTP.
- **Organization (O)** – Введите полное название организации/фирмы, например: Delovoj centr Nevskij.
- **Organizational Unit (OU)** – При необходимости можно заполнить это поле, вписывая название отдела, напр.: Otdel Marketinga.
- **Common Name (CN)** – введите полное доменное имя сервера DNS (fqdn) или IP, которое будет использовать пользователь сервера в своей почтовой программе, напр. доменное имя сервера: mail.moyserver.ru.
- **Country (C)** – введите код страны, состоящий из 2 букв (RU). Необходимо использовать код ISO, напр. соответствующий код для России - RU (большие буквы), а не RF.
- **State/Province (ST)** – Введите название области, напр.: Moscow.province Нельзя использовать сокращения.
- **City/Locality (L)** – Введите название города, напр.: Moscow.
- **File Name** – Введите название файла, в котором будет записан запрос на выпуск сертификата, напр.: C:\myreq.csr. Файл с запросом необходимо будет выслать в CERTUM.

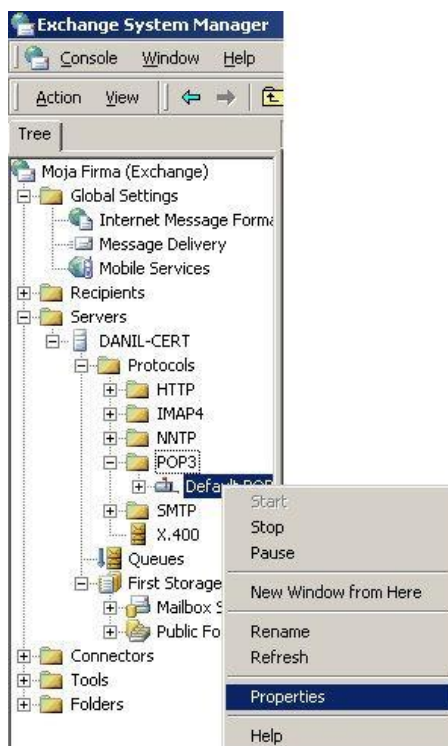
ВНИМАНИЕ: При заполнении вышеуказанных полей не использовать, кириллицу, диакритические и специальные знаки: ^ & _ \$ @ .

Чтобы сгенерировать запрос CSR, который будет отослан в CERTUM, и подписан одним из сертификатов CERTUM, необходимо зарегистрироваться как администратор сервера и запустить **Exchange System Manager**:

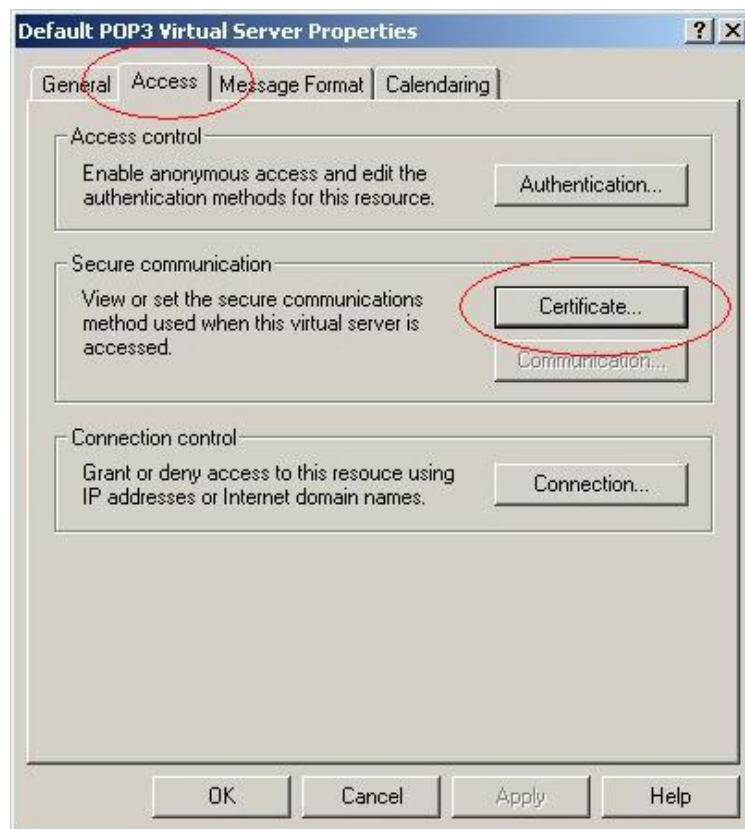
Старт -> Программы -> Microsoft Exchange -> System Manager



Нажимаем правой кнопкой мышки на протокол, для которого хотим ввести передачу данных с защитой **SSL**, после чего выбираем Properties:



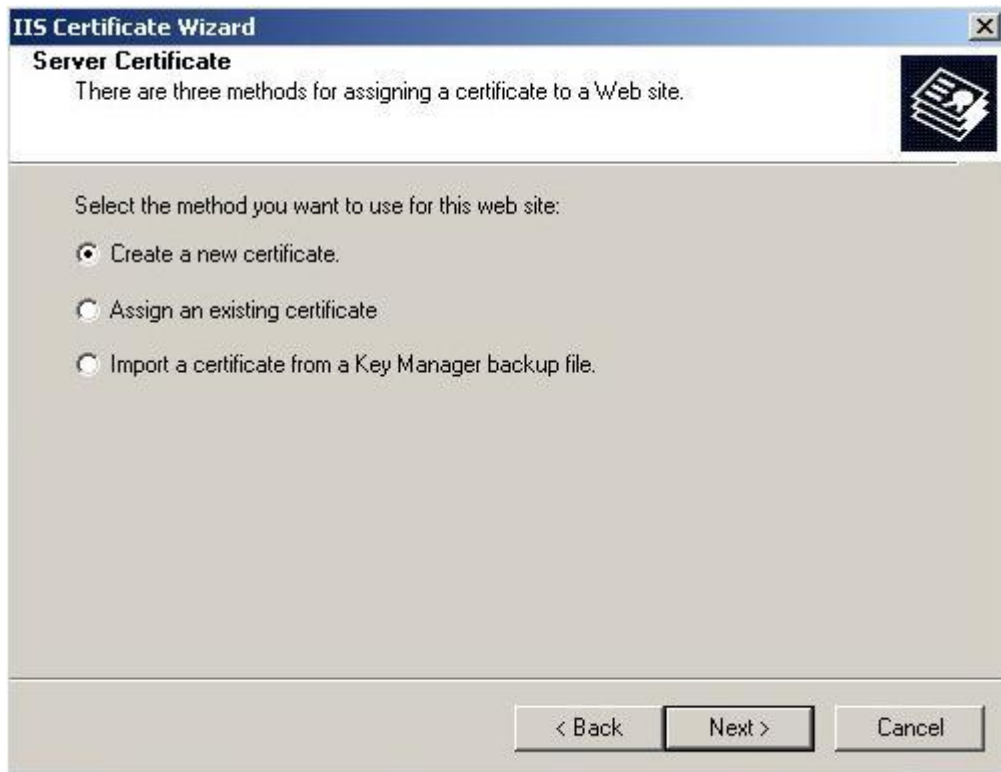
В окне Properties выбираем закладку Access и нажимаем Certificate:



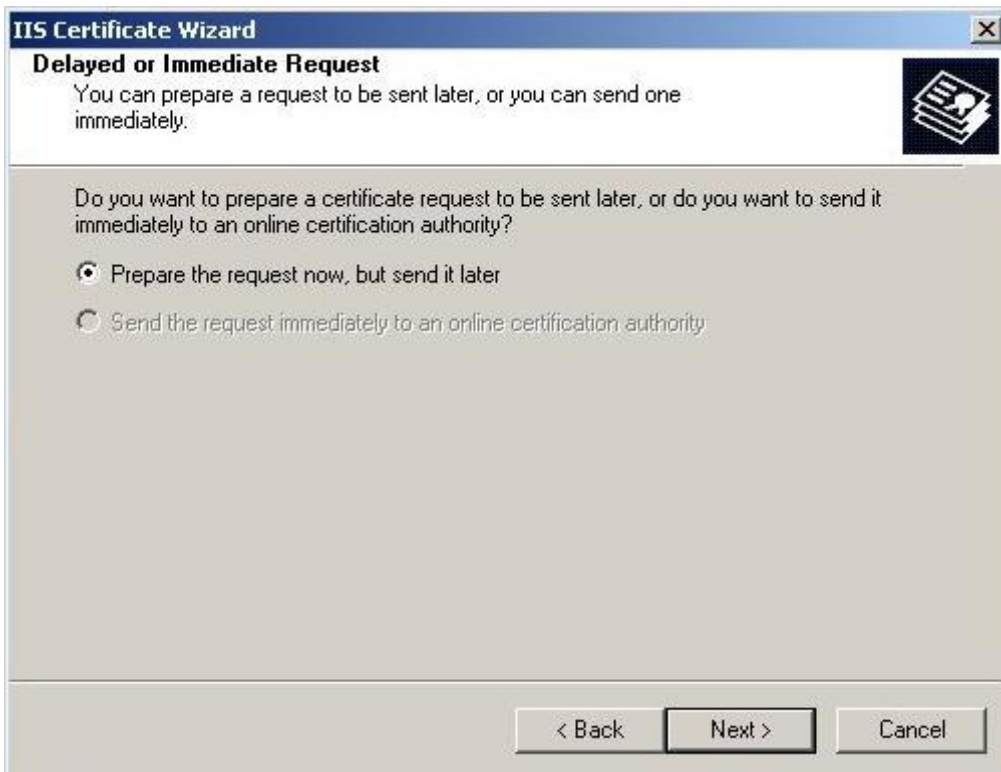
Таким образом запускаем процесс генерации запроса CSR:



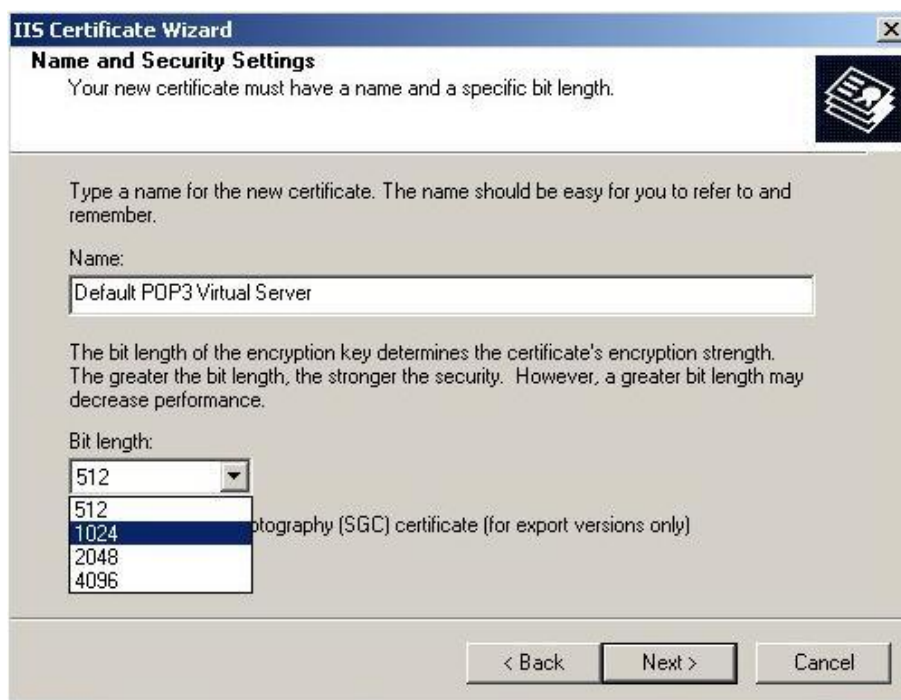
Выбираем опцию Create a new certificate:



Оставляем автоматически установленную опцию:



Вписываем название для нашего Сертификата и выбираем длину ключа (1024 битов - достаточная ёмкость):



The screenshot shows the 'IIS Certificate Wizard' dialog box, specifically the 'Name and Security Settings' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the text says 'Your new certificate must have a name and a specific bit length.' There is a small icon of a certificate on the right. The main area contains instructions: 'Type a name for the new certificate. The name should be easy for you to refer to and remember.' Below this is a 'Name:' label and a text box containing 'Default POP3 Virtual Server'. Another instruction follows: 'The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.' Below this is a 'Bit length:' label and a dropdown menu. The dropdown menu is open, showing options: 512, 512, 1024 (highlighted), 2048, and 4096. To the right of the dropdown, there is a note: '...ography (SGC) certificate (for export versions only)'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Вписываем уникальное название и подразделение фирмы (организации):

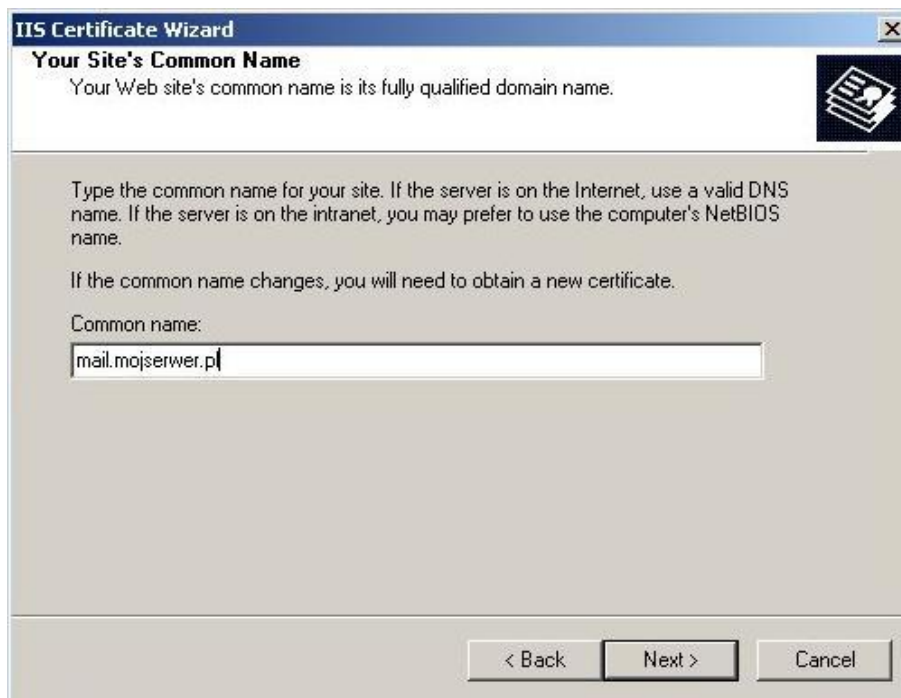
ВНИМАНИЕ: Использование кириллицы, диакритических и специальных знаков %, ^, \$, _ при заполнении этих данных приведет к неправильной генерации сертификата!!!



The screenshot shows the 'IIS Certificate Wizard' dialog box, specifically the 'Organization Information' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the text says 'Your certificate must include information about your organization that distinguishes it from other organizations.' There is a small icon of a certificate on the right. The main area contains instructions: 'Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.' Below this is another instruction: 'For further information, consult certification authority's Web site.' Below these are two labels: 'Organization:' and 'Organizational unit:'. Each label is followed by a dropdown menu. The 'Organization:' dropdown contains 'Moja Firma'. The 'Organizational unit:' dropdown contains 'Oddzial w Moja Firma'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

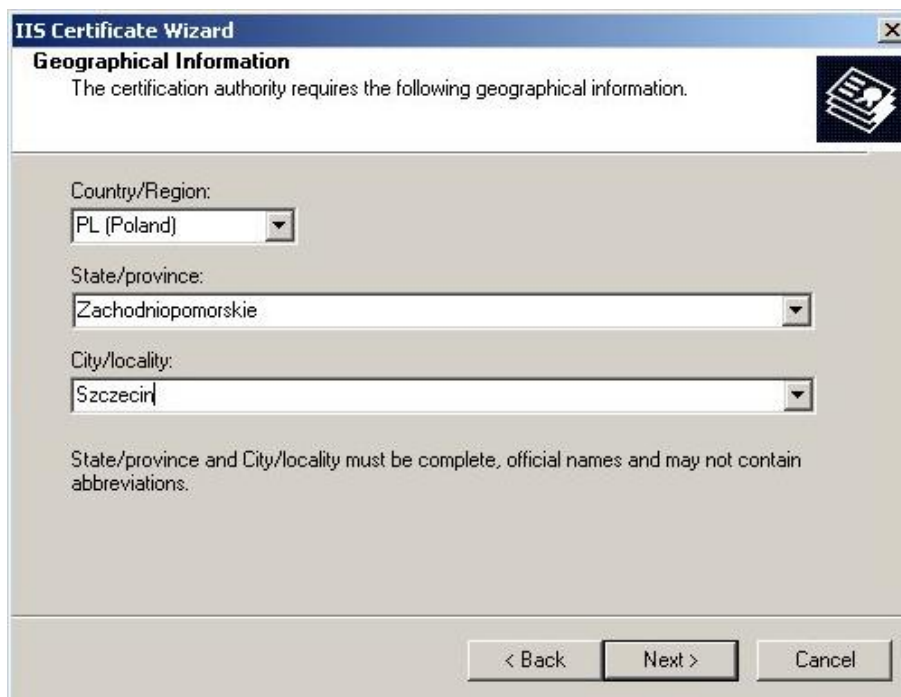
Вписываем полное название своего сервера (Common Name):

ВНИМАНИЕ: Это очень важное поле и здесь необходимо записать полное доменное имя DNS (fqdn) или IP сервера напр.: mail.mojsrwer.pl (пользователь сервера должен ввести этот адрес в своей программе)



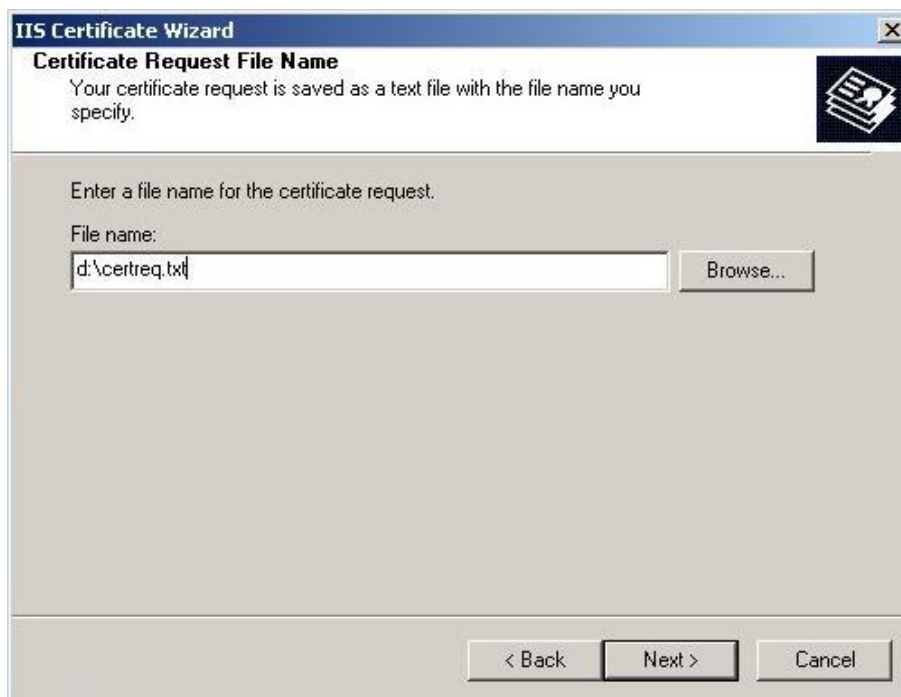
The screenshot shows the 'IIS Certificate Wizard' dialog box, specifically the 'Your Site's Common Name' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the text says 'Your Site's Common Name' and 'Your Web site's common name is its fully qualified domain name.' There is a small icon of a certificate on the right. The main area contains instructions: 'Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name. If the common name changes, you will need to obtain a new certificate.' Below this, there is a label 'Common name:' followed by a text input field containing 'mail.mojsrwer.pl'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

В завершении вписываем географические данные, касающиеся нашего сертификата..:

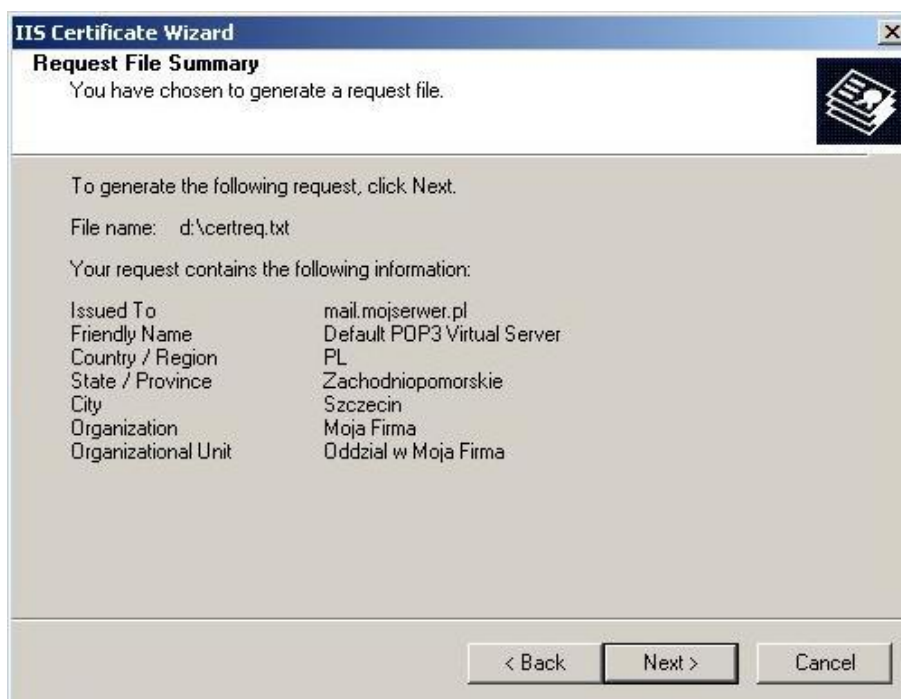


The screenshot shows the 'IIS Certificate Wizard' dialog box, specifically the 'Geographical Information' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the text says 'Geographical Information' and 'The certification authority requires the following geographical information.' There is a small icon of a certificate on the right. The main area contains three dropdown menus: 'Country/Region:' with 'PL (Poland)' selected, 'State/province:' with 'Zachodniopomorskie' selected, and 'City/locality:' with 'Szczecin' selected. Below these, there is a note: 'State/province and City/locality must be complete, official names and may not contain abbreviations.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

... и вписываем имя файла, в котором будет записан наш сертификат:



В завершении проверяем данные, которые мы записали в сертификате. При необходимости возвращаемся назад (нажимая на back) и корректируем неправильно заполненные поля:



Программа создания сертификатов сообщит о правильной генерации запроса CSR (кроме запроса в реестрах уже находится также персональный ключ):



2.2. Создание сертификата на основании созданного запроса CSR

Сгенерированный нами запрос будет выглядеть подобным образом как указано ниже:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDMCCApkCAQAwgZoxGzAZBgNVBAMTEmRsdWJhY3oudW5pemV0by5wbDEhMB8G
A1UECxMYRHpYwWgT2Nocm9ueSBJbmZvcmlhY2ppMRswGQYDVQQKEhJVbml6ZXRv
IFNwLiB6IG8uby4xETAPBgNVBAClTCFN6Y3plY2luMRswGQYDVQQIEhJaYWNob2Ru
aW9wb21vcnNraWUxYzA1BGMoEKBCCyZF1kHodsWW
0ZF54FrTZhyKwYqfghiHO5duLfJSBqb/PTzovZH9qXUtxl+zQIhcJnA4Z/jKyWHG1
X7LUlC9u2bas/vWwQZWYvxeqNMW4RZ+LU9Qqm9b/YD2qtOZ2qwIDAQABOIBUzAa
BgorBgEEAYI3DQIDMQwWCjUuMC4yMTk1LjIwNQYKkYyBBAGCNwIBDjEnMCUwDgYD
VR0PAQH/BAQDAgTwmBMGA1UdJQMMMAoGCCsGAQUFBwMBMIH9BgorBgEEAYI3DQIC
MYHuMIHrAgEBH1oATQBpAGMAcGvAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEA
bgBuAGUAbAAgAEMAcb5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkA
ZAB1AHIDgYkAXxNuAz6gcBaZUdef8WQ2PAroKMW8sprcKv7QD2encz6/Wct9DZ5C
kGynLGy0f+Lff7ViSDJqXyWaj68ddqgXyAqIilF63kivPTiC6yxLaNX65v3cnKFx
4UrUrGXZtub7M7/NuxSipOW0Vv7yCHganypxDyRzp6IhulEnL4APEH4AAAAAAAAA
ADANBgbkqhkiG9w0BAQUFAAOBgQAsTG3Hu00fFzNTekFo/fb3tKsmuS/1rCCB5sQK
iNpWGZ8Z8+TmqBB0Tuz4FPTkeSqLpWv1ORfmxMKPIu10dC3QwRP2E//oMPnaU807
IJIDwn2VZ7qQ/h0KcWoWSPmvt7J0KKshdGgAF7P6AYc7W4yA9B9nPeYEzQRW0t4D
YBApPQ==
-----END NEW CERTIFICATE REQUEST-----
```

Имея созданный запрос, необходимо заполнить заявку и вклеить CSR напр. на сайте CERTUM (ank-pki.certum.ru -> Предложение -> выбрать, который сертификат хотим купить и на сайте выбрать Купить сертификат).

Появится окно с информацией о документах, необходимых для окончания процесса получения сертификата. Для продолжения процесса покупки необходимо выбрать Купить.

Купить сертификат Enterprise SSL с периодом действительности (1 год)

Запрос сертификата

В нижеследующее поле вставьте запрос сертификата (CSR)*.

Запрос сертификата можно сгенерировать:

- пользуясь генератором, представленным на сайте CERTUM,
- на сервере домена, для которого хотите получить сертификат.

```
fj
+VdemsApGUbQ5zdwKhQxCd6KMC6NoQUY/62saRsiivFiFNZ9IL5I92D0/G8CK
/Ah
xX7nLr7nu3xUhSiqzllbv783tBYaQ4IjWFXW/AqkrryHVX4NIQcLceS4AN6i/UJ
G
J5uwbsbm3jNrYNH2pqDPPrTpwZHj8dKeqNz5cmH8CAmItB9GXbc0DeiG1w2Q
QScKH
fiPRJgPlofpx0hKfyw+PE/GuFIMQ/rbsh0NNpRePagP/IwXdvN2rDva2BpuFeY
B0
-----END CERTIFICATE REQUEST-----
```

Адрес e-mail

E-mail*:

mojadres@mail.ru

Верификация домена

Выберите email адрес, на который будет отправлена ссылка. При переходе по ссылке Вы, тем самым, подтвердите, что имеете доступ к аккаунту, указанному в CSR запросе. Ниже находится список доступных для администратора аккаунтов. Выберете адрес к которому имеете доступ.

Верификация e-mail*:

admin@domain.ru

На этом шаге происходит верификация прав доступа к серверу, доступному в домене, указанном в CSR запросе. Можете выбрать один из двух методов верификации: используя вставку META tag в содержании главной страницы или сохранив сгенерированный файл в корневой папке сервера, доступного под доменным именем, указанным в CSR запросе.

Верификация домена*:

Запиши файл HTML

Заявление

ПЕРЕД ПОДАЧЕЙ ЗАЯВКИ НА ВЫПУСК СЕРТИФИКАТА, ЕГО ПОДТВЕРЖДЕНИЯ ИЛИ ИСПОЛЬЗОВАНИЯ ДЛЯ ПЕРВОЙ ПОДПИСИ – ВЫ ДОЛЖНЫ ПРОЧИТАТЬ ТЕКСТ НАСТОЯЩЕГО ЗАЯВЛЕНИЯ. ЕСЛИ ВЫ НЕ СОГЛАСНЫ С УСЛОВИЯМИ НАСТОЯЩЕГО ЗАЯВЛЕНИЯ, НЕ ПОДАВАЙТЕ ЗАЯВКУ НА ВЫПУСК СЕРТИФИКАТА, НЕ ПОДТВЕРЖДАЙТЕ И НЕ ИСПОЛЬЗУЙТЕ ЕГО.

Заявление является обязательным с момента подачи заявки на выпуск сертификата до CERTUM – Открытого Удостоверяющего Центра. Подавая заявку на выпуск сертификата, Вы требуете от выдающего органа рассмотреть заявку и выпустить сертификат:

Подтверждаю заявление*

* - обязательное поле

Заказываю

Входим на сайт, вставляем ID и нажимая Далее активируем сертификат:

Инсталляционное ID сертификата: f00d56ad1edb4fd3d00bbe237fbe9772d65ab0cf

Введите ID на сайте:

<https://www.certum.eu/ru/install/>

Коллектив ANK и Certum

SSL@ank-pki.ru

Входим на сайт, вклеиваем ID и, нажимая Далее, активируем сертификат:

Инсталлирование сертификата

Впишите ID инсталляции сертификата, который Вы получили в сообщении e-mail от CERTUM:

Внимание!

В случае сертификатов e-mail инсталляция подписи должна происходить на том же самом компьютере и с помощью того же самого браузера, который Вы использовали указывая адрес e-mail.

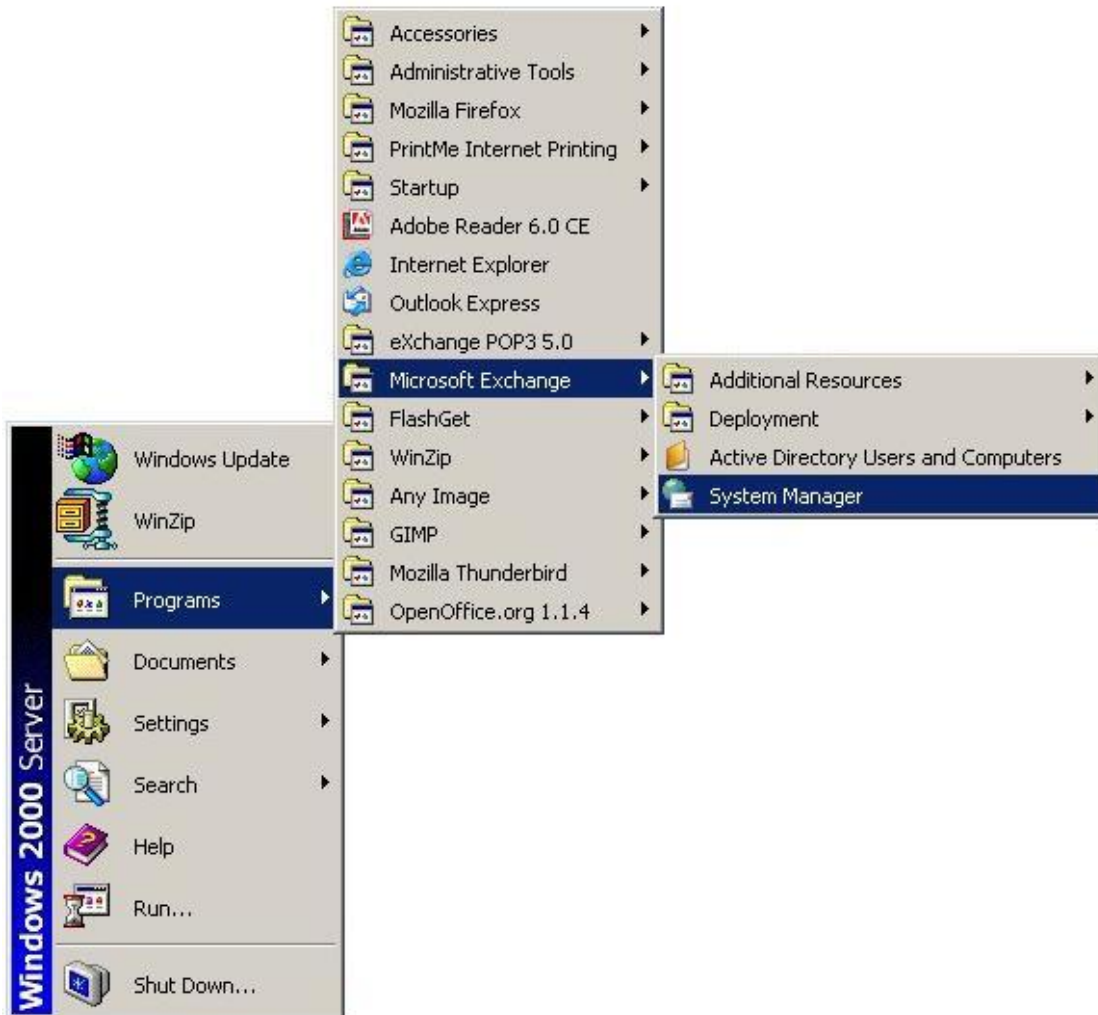
Для интересующего нас сертификата выбираем опцию Записать в текстовом или Записать в бинарном виде:

Инсталлирование сертификата

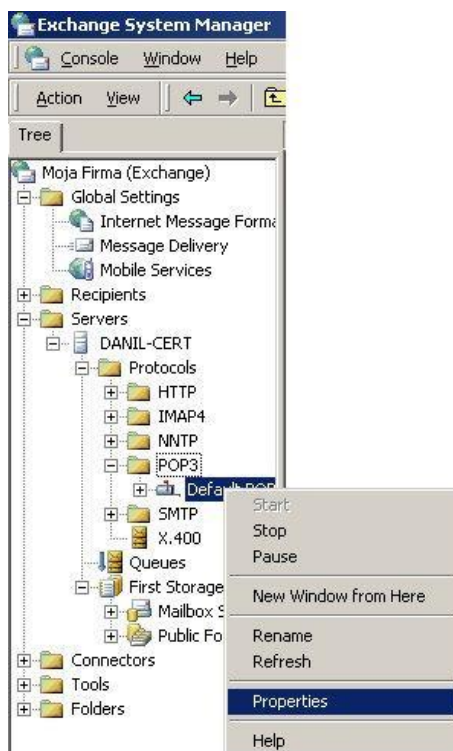
Enterprise SSL	действителен до: 30.04.2010
Субъект: exampledomain.ru Email: root.mydomain@gmail.com Номер: 0x493DC	
<input type="button" value="Записать бинарно"/>	<input type="button" value="Записать текстово"/>

Для инсталляции сертификата на сервере необходимо зарегистрироваться как администратор сервера и запустить **Exchange System Manager**:

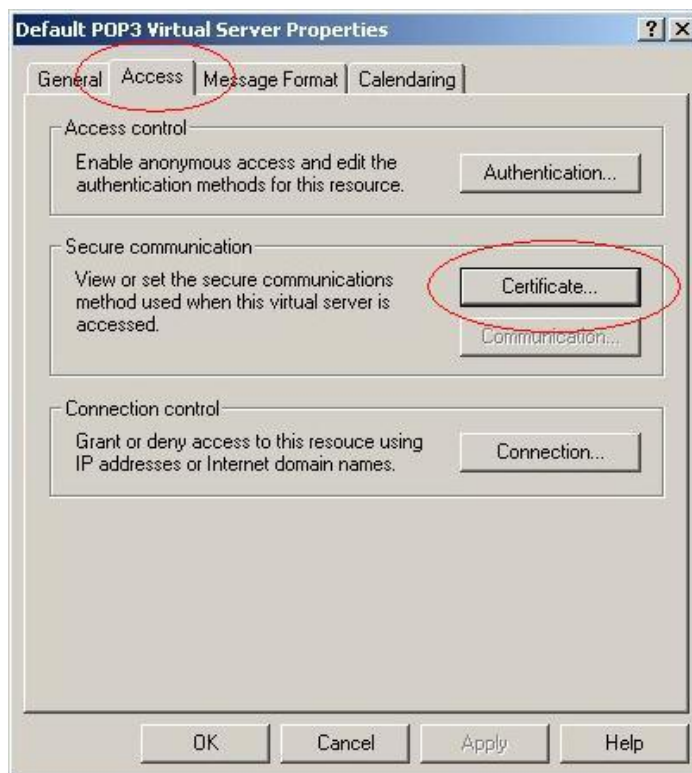
Старт -> Программы -> Microsoft Exchange -> System Manager



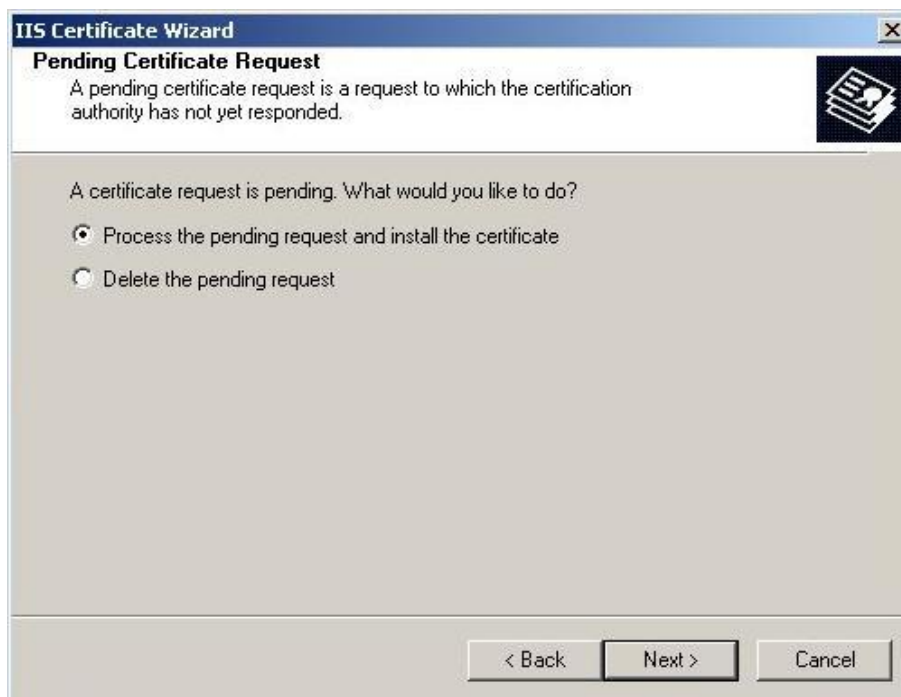
Нажимаем правой клавишей мышки на протокол, для которого хотим ввести передачу данных с защитой, после этого выбираем Properties:



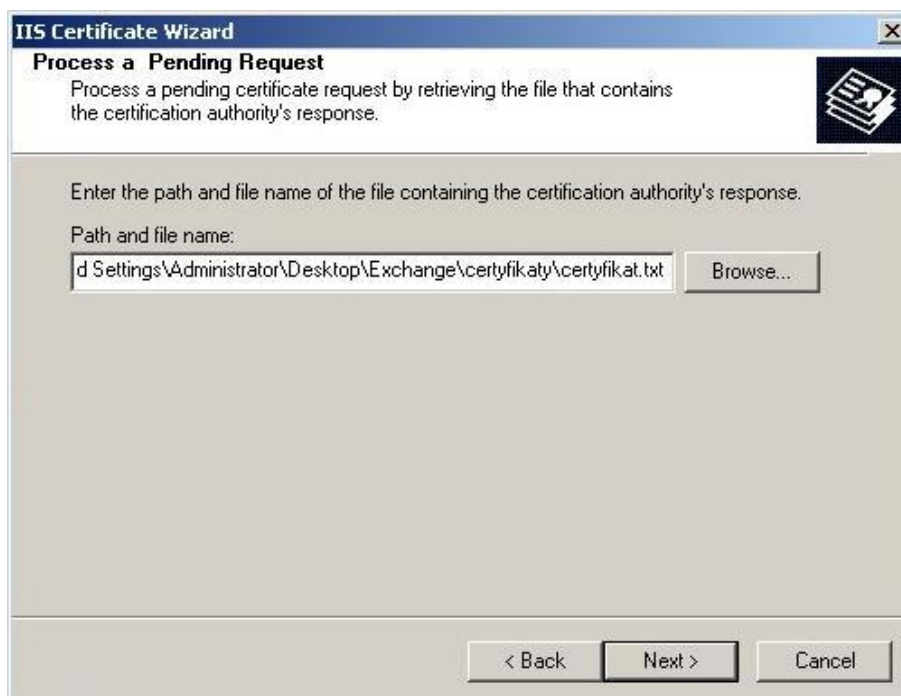
В окне Properties выбираем закладку Access нажимаем на Сертификат:



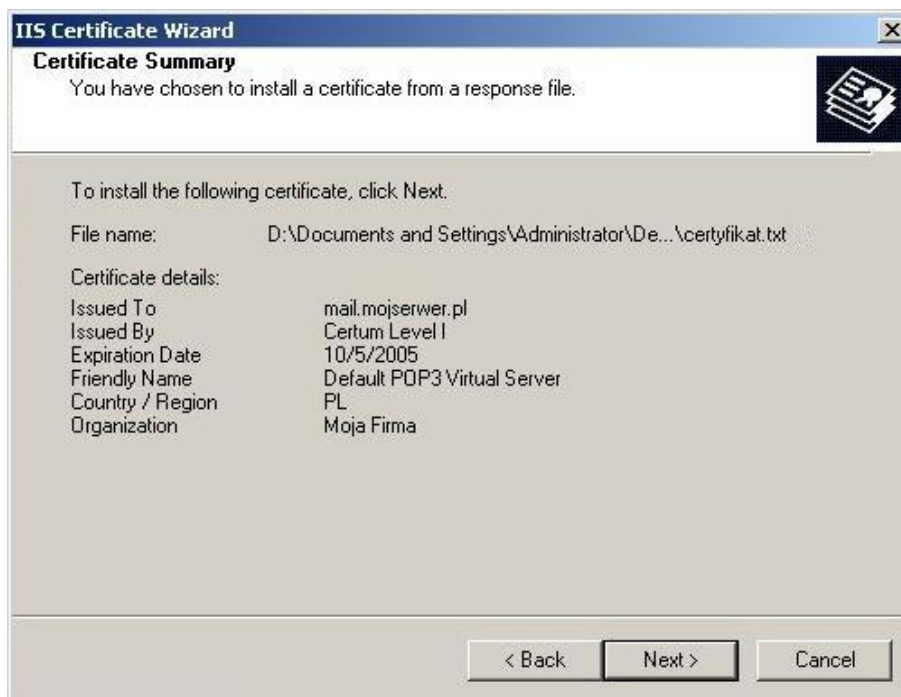
Выбираем Process the pending request and install the certificate:



Указываем название файла, в котором мы записали сертификат для сервера:



Будут указаны данные сервера, которые записаны в сертификате.



Программа сообщит о завершении процесса инсталляции сертификата на сервере:



2.4. Получение промежуточных сертификатов

Чтобы получить Сертификат Certum CA или промежуточные сертификаты необходимо войти на сайт ank-pki.certum.ru в раздел Обслуживание сертификатов → Корневые сертификаты и ключи. После выбора сертификата необходимо выбрать опцию Сертификат для серверов WWW.

Главный ключ центра – Certum CA	
Серийный номер:	10020
Действителен от:	Jun 11 10:46:39 2002 GMT
Действителен до:	Jun 11 10:46:39 2027 GMT
Сертификат для браузеров	<input type="button" value="Инсталлировать"/>
Сертификат для серверов WWW и SSL / TLS	<input type="button" value="Инсталлировать"/>
Сертификат для сетевого оборудования	<input type="button" value="Инсталлировать"/>

[ВЕРХ](#)

Появится интересующий нас сертификат, который выбираем мышкой, вставляем в файл и записываем.

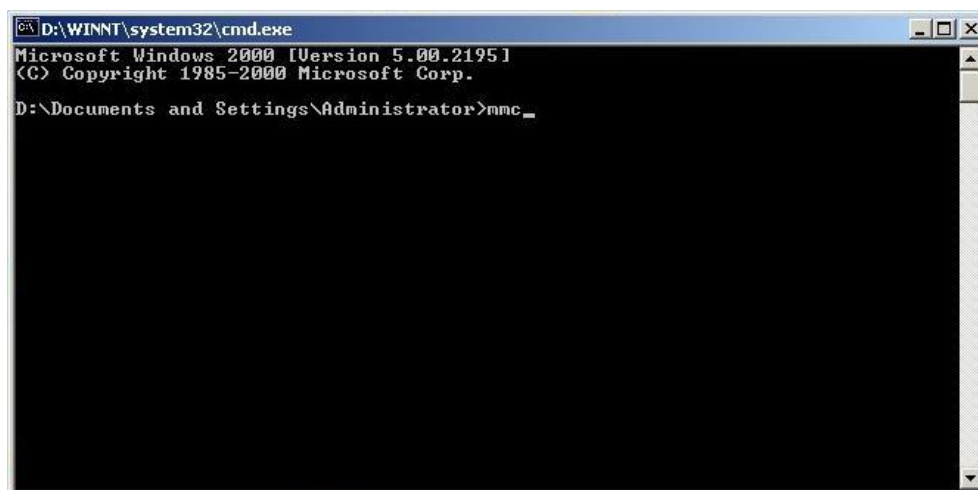
ВНИМАНИЕ: Чтобы вклеить в файл сертификата, представленного на сайте необходимо скопировать фрагмент текста начиная с текста "--BEGIN CERTIFICATE --" до "--END CERTIFICATE--" (вместе с линиями!!!), используя для этого текстовый редактор, напр. Notepad и мышку. **Не следует использовать для этой операции Word, или какой-нибудь другой текстовый редактор!**

В случае получения промежуточных сертификатов, выбираем со списка интересующий нас сертификат, напр. CERTUM Level IV (Сертификаты Level IV следует получить в случае, когда уже имеем сертификат типа Trusted, сертификат III уровня следует получить в ситуации, когда имеем сертификат типа Enterprise / Wildcard, сертификат II уровня следует получить, когда имеем в наличии сертификат типа Commercial; для сертификатов типа Private – сертификат I класса). Последующая часть процесса (запись в файл) происходит также как и для сертификата Certum CA.

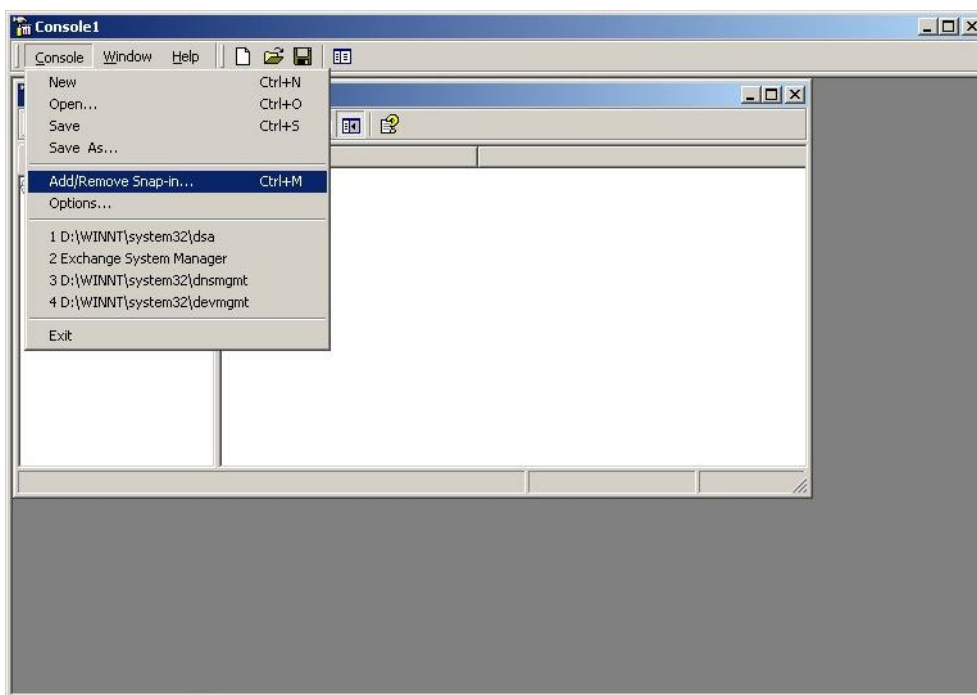
2.5. Импорт промежуточных сертификатов

Необходимо создать специальную консоль для администрирования и управления сертификатами, находящимися в базе сертификатов компьютера (стандартный визард Windows соединяется с реестрами определенного пользователя), если же консоль была уже создана раньше, тогда она доступна в меню Административные инструменты.

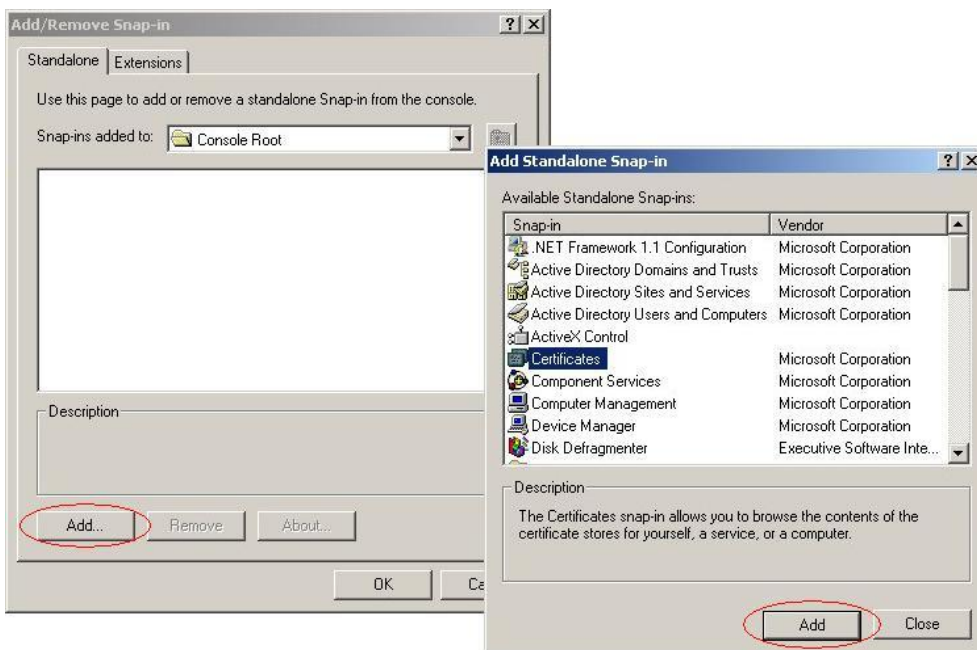
Для этого создание консоли запускаем с командной строки вписывая **mmc:**



В открытой консоли выбираем с верхнего меню опцию Добавить/Удалить оснастку или выбираем комбинацию клавиш ctrl + M:



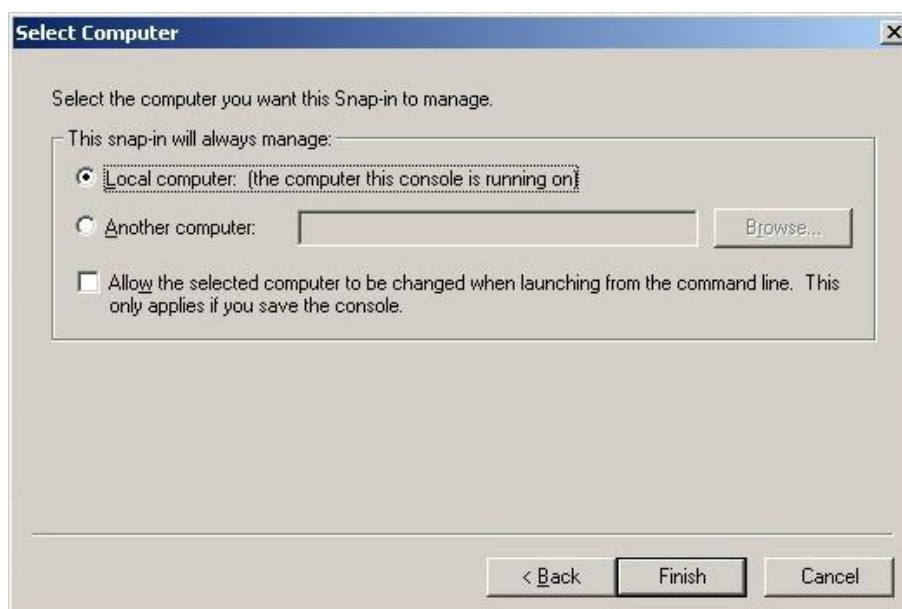
Выбираем опцию Добавить, после этого оснастку Сертификаты:



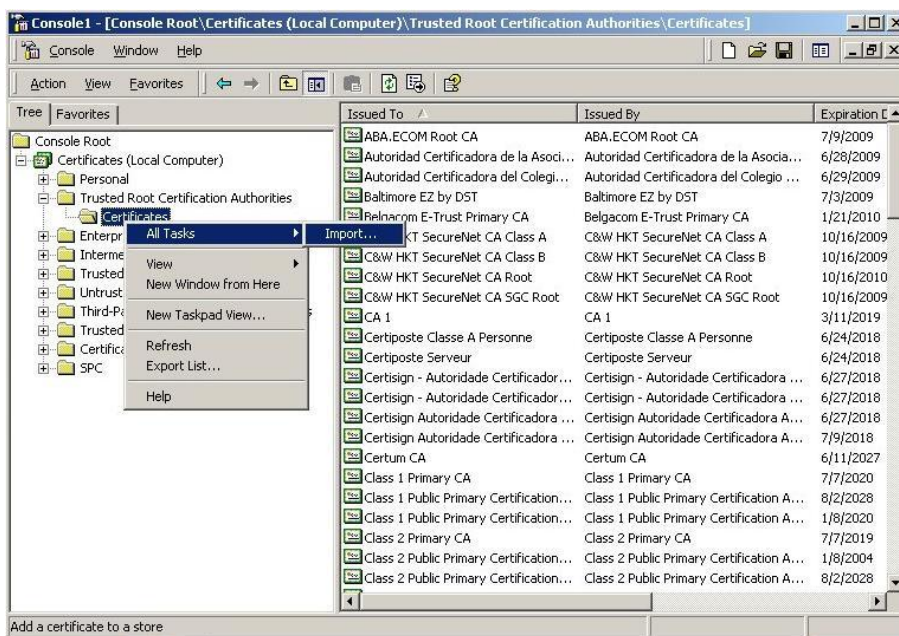
Выбираем опцию Учетная запись компьютера:



Оставляем автоматически установленную позицию (если операция относится к локальному компьютеру):



Входим в консоль – опция *Сертификаты* имеет сейчас второстепенную опцию – после ее открытия переходим по указанным опциям (**Главные доверенные удостоверяющие центры, Промежуточные удостоверяющие центры, Главные удостоверяющие центры других фирм**) и добавляем промежуточные сертификаты (лучше всего добавлять все сертификаты - Certum CA и Certum Level I-IV для всех баз данных; практически достаточно добавить промежуточные сертификаты в базу *Промежуточные удостоверяющие центры*). Главный сертификат (Certum CA) и промежуточные сертификаты (Level I-IV) можно скачать с сайта: ankpki.certum.ru в раздел Обслуживание сертификатов → Корневые сертификаты и ключи



Нажимая правой клавишей мышки на каталоги Сертификаты отдельных баз выбираем опцию Все задачи -> Импорт – здесь уже появляется знакомый визард

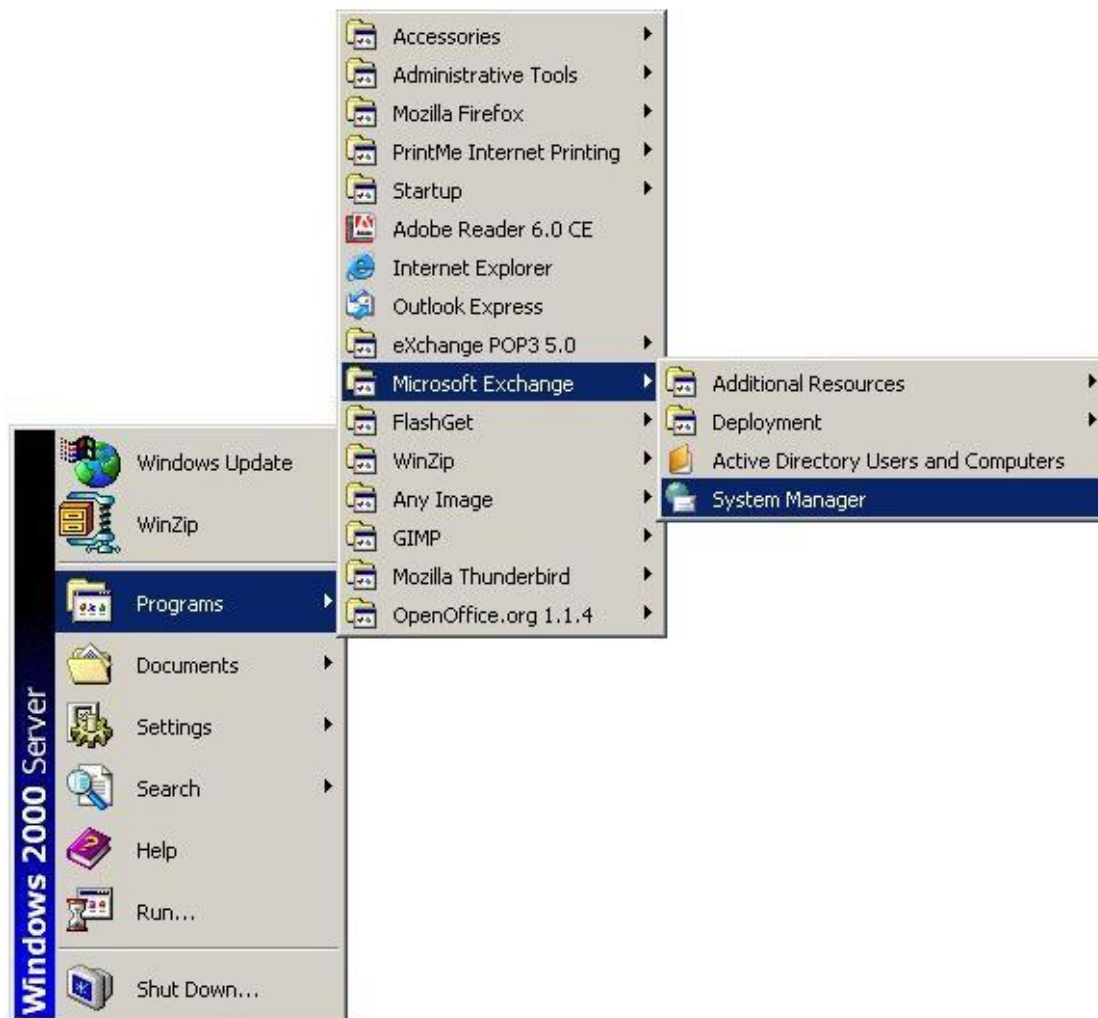
После окончания импорта сервер необходимо перезагрузить.

После импортирования сертификата в указанные папки Exchange извлекает информацию, которая позволяет пользователю построить полный путь сертификации (вместе с сертификатом Certum CA, находящимся в базе программы клиента).

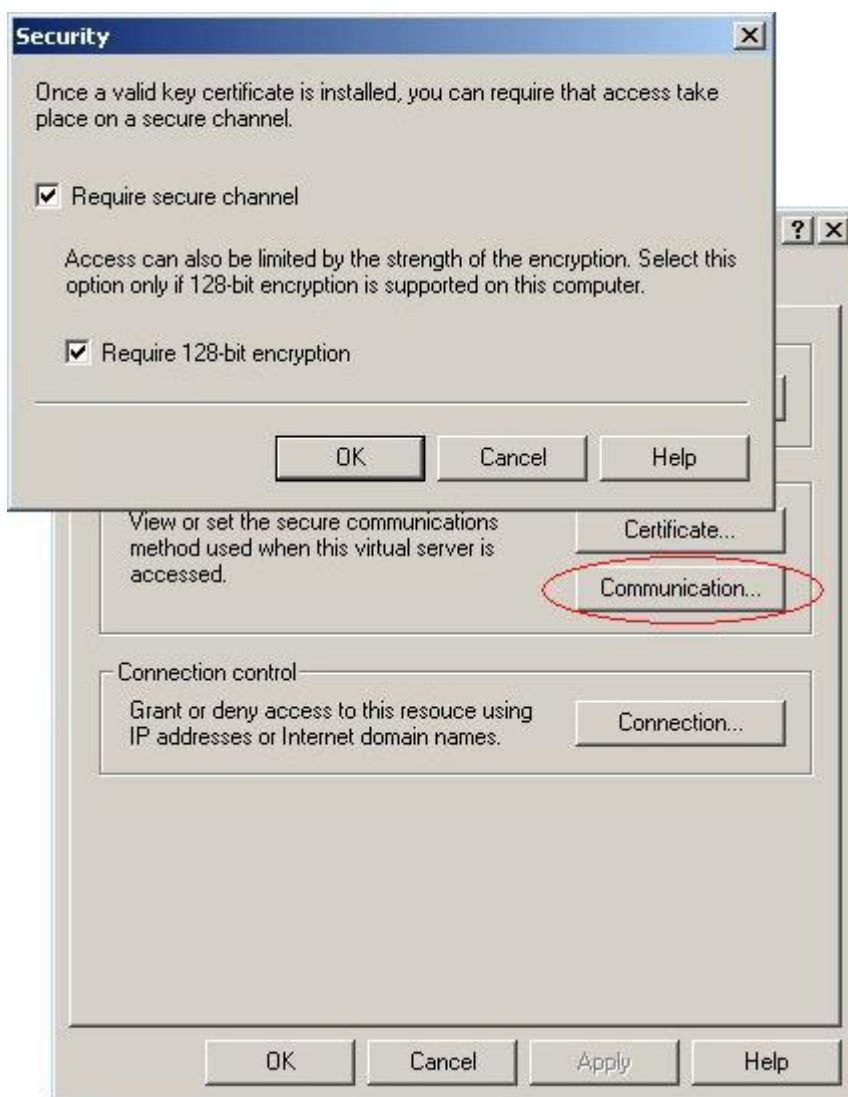
3. Конфигурация сервера Exchange для соединений https

Для того, чтобы наш сервер обслуживал шифрование соединения, необходимо зарегистрироваться как администратор сервера и запустить **Exchange System Manager**:

Старт -> Программы-> Microsoft Exchange -> System Manager



С окна Свойства выбираем закладку Access нажимаем на Communication и отмечаем опцию Require secure channel и Require 128-bit encryption:



4. Импорт/Экспорт сертификатов сервера

Для импорта/экспорта сертификата сервера (вместе с персональным ключом) необходимо создание специальной консоли для администрирования и управления сертификатами, помещенными в базе сертификатов компьютера (стандартный визард Windows соединяется с реестрами определенного пользователя), если же консоль была создана раньше, тогда она будет доступна в меню Административных инструментов в панели Управления (смотрите пункт выше).

С целью импортирования сертификата сервера после запуска консоли переходим к опции Personal и в меню Action -> Все задачи указываем команду Импорт... появится окно программы импортирования сертификата. В программе необходимо выполнить следующие действия:

- Указать файл с копией ключа и сертификата (в формате *.pfx)

- Ввести пароль для персонального ключа и выбрать опцию Обозначить ключ как импортированный
- Закрывать программу

С целью экспортирования сертификата сервера после запуска консоли переходим к опции Personal и выбираем сертификат, для которого хотим создать копию. Для этого в меню Action -> Все задачи указываем команду Экспорт... появится окно программы экспортирования сертификата. В программе необходимо выполнить следующие действия:

- Указать опцию Экспорт с ключом персональным
- НЕ указывать опцию Удалить ключ персональный после удачного экспорта
- Ввести пароль, который будет защищать экспортированный персональный ключ
- Ввести имя файла, в который будет записана запасная копия
- Закрывать программу