ООО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, Георгиевский проспект,
дом 5, помещение I, комната 33
Телефон/Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.com
Сайт: http://www.s-terra.com

Программный продукт С-Терра КП
Версия 4.1

Руководство администратора

Инструкция по обновлению и миграции Сервера управления

РЛКЕ.00009-03 90 01

22.07.2015

Содержание

1. Предварительные условия

Для выполнения процедуры **обновления** Сервера управления версии 3.11 до версии 4.1 необходимо обратиться в отдел продаж компании «С-Терра СиЭсПи» по адресу sales@s-terra.com для приобретения «Программного продукта С-Терра КП. Версия 4.1», который поставляется на CD-диске с названием «С-Терра Клиент CP/ST 4.1. Релиз 4.1.14905. С-Терра КП 4.1. Релиз 4.1.14905».

Для выполнения процедуры **переноса** Сервера управления с одного компьютера на другой с сохранением всех настроек Сервера управления, информации об учетных записях всех управляемых устройств, потребуется любой сменный носитель, например, USB-флеш.

2. Сценарий обновления Сервера управления с версии 3.11 до версии 4.1

Для проведения процедуры обновления Сервера управления на одном и том же компьютере выполните следующие шаги.

Шаг 1: Скопируйте каталог с дистрибутивом С-Терра КП версии 4.1 на компьютер с Сервером управления старой версии.

Шаг 2: Зайдите в **Панель управления – Программы и компоненты** и удалите из списка продукт **S-Terra KP, а также FileZilla Server** (Рисунок 1).

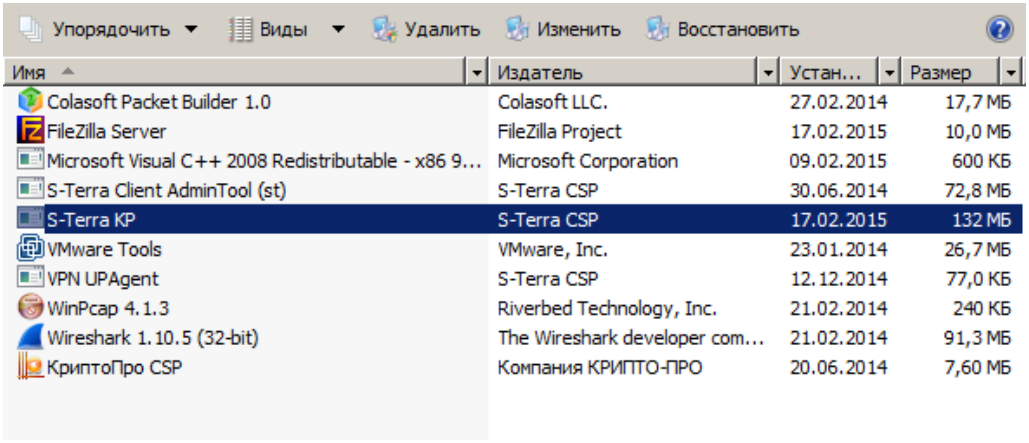

Рисунок 1

В процессе деинсталляции продукта FileZilla Server важно не удалить файл с настройками – об этом предупреждает всплывающее диалоговое окно (Рисунок 2). Необходимо нажать No.

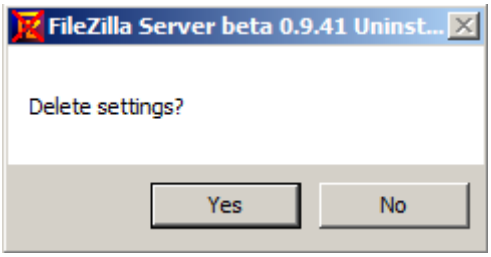

Рисунок 2

Оставшийся компонент, входивший в пакет установки С-Терра КП версии 3.11 (Рисунок 3), удалять необязательно.

Рисунок 3

Шаг 3: Далее перейдите в каталог с дистрибутивом версии 4.1 и запустите setup.exe (Рисунок 4).

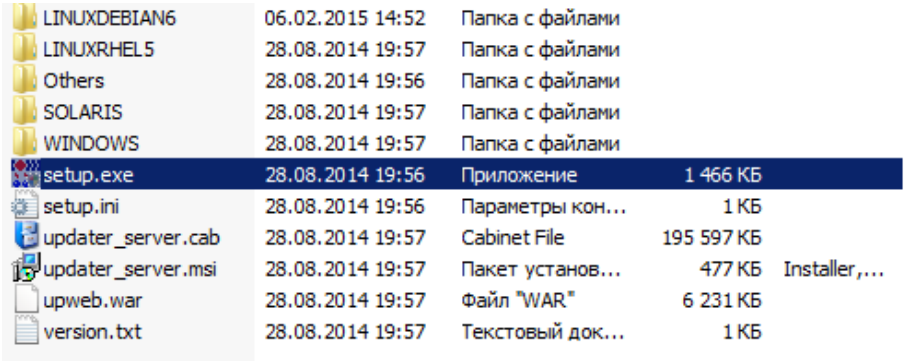

Рисунок 4

Шаг 4: В появившемся окне с запросом на установку необходимых компонент нажмите кнопку Установить (Рисунок 5). Начнется стандартный процесс установки, описанный в разделе 3.1 документа «Программный продукт С-Терра КП. Версия 4.1. Руководство администратора».

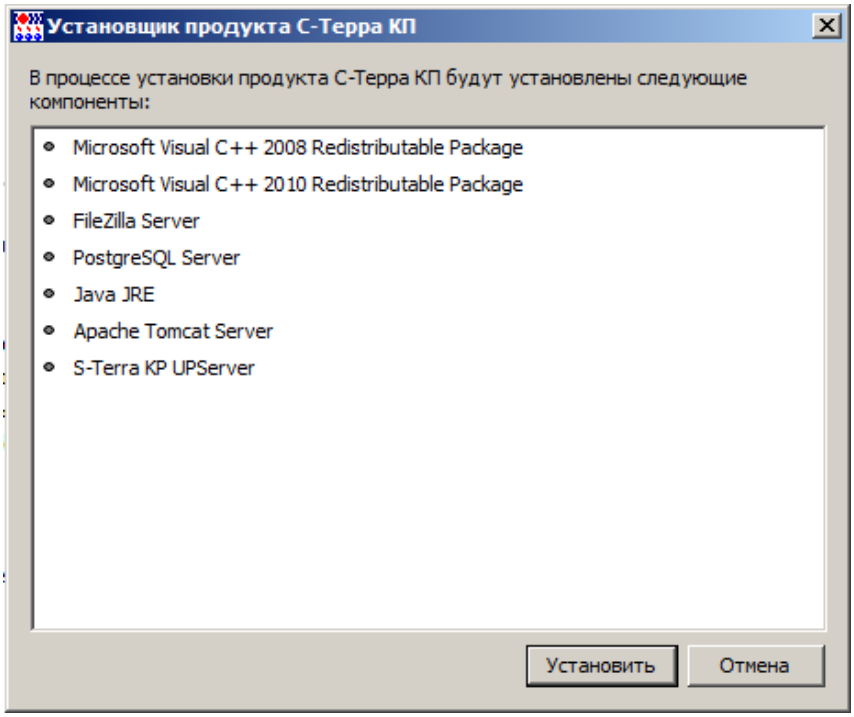

Рисунок 5

В результате установки новой версии сохраняется вся информация о настройках Сервера управления, о сертификатах Сервера управления, все учетные записи об управляемых устройствах. По окончании установки Сервер управления готов к работе.

3. Сценарий переноса Сервера управления версии 4.1 на другой компьютер

3.1. Сбор и сохранение данных Сервера управления

Шаг 1: На компьютере с установленным Сервером управления при помощи утилиты `upmgr` сохраните в файл, например, `C:\backup01.bin`, настройки Сервера управления, СА и рабочий сертификаты, данные о Клиентах управления управляемых устройств, выполнив команду:

```
C:\Program Files\S-Terra KP\upmgr backup -f C:\backup01.bin
```

Сохраняется вся информация, кроме контейнеров с секретными ключами сертификатов Сервера управления и статистической информации (Рисунок 6).

```
c:\Program Files\S-Terra\S-Terra KP>upmgr backup -f C:\backup01.bin
Locking upserver data...

7-Zip 9.20  Copyright (c) 1999-2010 Igor Pavlov  2010-11-18
Scanning

Creating archive C:\backup01.bin

Compressing  authset.ini
Compressing  backup_info.txt
Compressing  certs\cacert.cer
Compressing  certs\passwd.txt
Compressing  certs\workcert.cer
Compressing  clients\client01\desc.txt
Compressing  clients\client01\ftpstate.txt
Compressing  clients\client01\ftp\data\notiflag.txt
Compressing  clients\client01\ftp\data\notifyid.bin
Compressing  clients\client01\passwd_dev.txt
Compressing  clients\client01\state.txt
Compressing  clients\client01\updates\00000000hash1
Compressing  clients\client01\updates\00000000time1
Compressing  clients\client01\updates\00000000\cacert.cer
Compressing  clients\client01\updates\00000000\id.txt
Compressing  clients\client01\updates\00000000\num.txt
Compressing  clients\client01\updates\00000000\settings.txt
Compressing  clients\client01\updates\00000000\setup_product.exe
Compressing  clients\client01\updates\00000000\setup_upagent.exe
Compressing  clients\client01\updates\00000000\start.txt
Compressing  clients\client01\updates\num.txt
Compressing  clients\client01\worked.txt
Compressing  copy_of_upserver.log
Compressing  csettings.txt
Compressing  filezilla.cf
Compressing  regvars.txt
Compressing  ssettings.txt
Compressing  upserver.lic

Everything is Ok
Info: Product data have been backuped successfully to file C:\backup01.bin

c:\Program Files\S-Terra\S-Terra KP>_
```

Рисунок 6

Для переноса всех настроек и контейнеров сертификатов будет использоваться USB-флеш.

Шаг 2: Скопируйте файл `backup01.bin` с настройками Сервера управления на USB-флеш.

Для экспортирования контейнеров сертификатов Сервера управления на USB–флеш перейдите к разделу «Экспорт контейнеров к ГОСТ-сертификатам» либо к разделу «Экспорт контейнеров к RSA-сертификатам».

3.1.1. Экспорт контейнеров к ГОСТ-сертификатам

Шаг 1: Предварительно нужно добавить USB-флеш к списку типов ключевых носителей, распознаваемых «КриптоПро CSP». Для этого вставьте USB-флеш в USB-разъем ПК с Сервером управления и определите логическое имя (букву), под которым он отображается в системе.

Шаг 2: Запустите **CryptoPro CSP** от имени Администратора. Перейдите во вкладку **Hardware**, нажмите кнопку Configurate readers… (Рисунок 7).

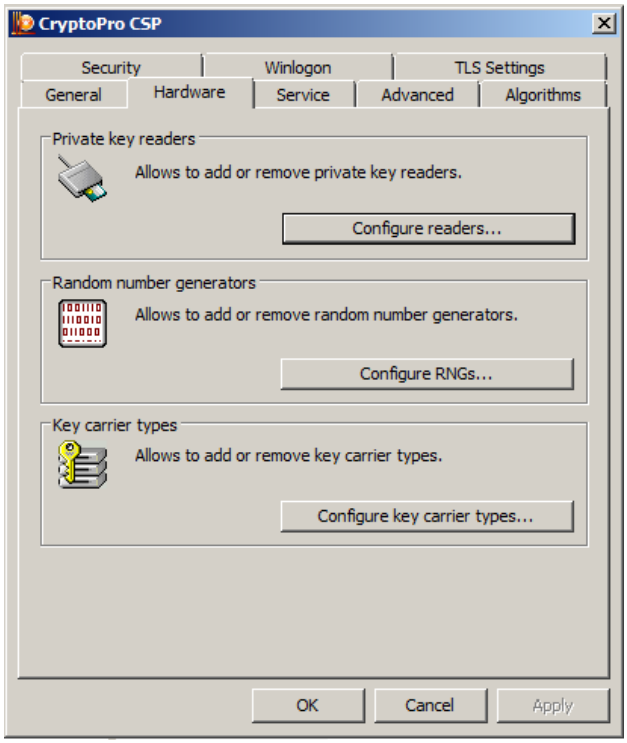

Рисунок 7

Шаг 3: Выберите **All removable media** и нажмите Add… (Рисунок 8).

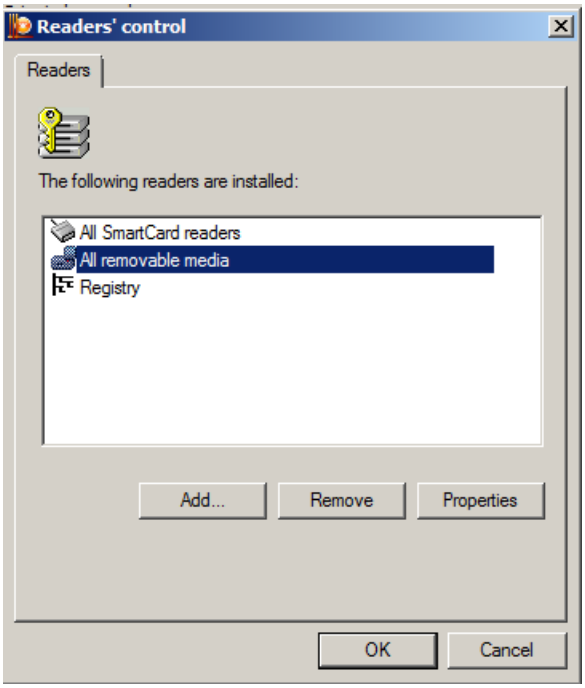

Рисунок 8

Шаг 4: Появится Мастер установки считывателя – **Reader installation wizard**. Нажмите Next > (Рисунок 9).

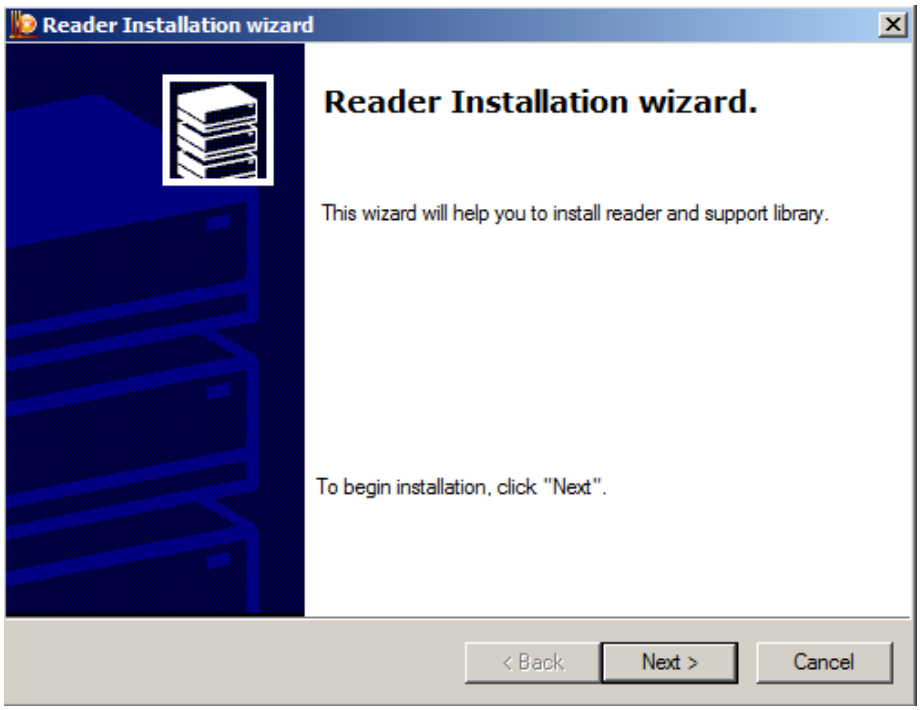

Рисунок 9

Шаг 5: Из списка доступных считывателей выберите устройство (USB-флеш) под необходимой буквой и нажмите Next > (Рисунок 10).

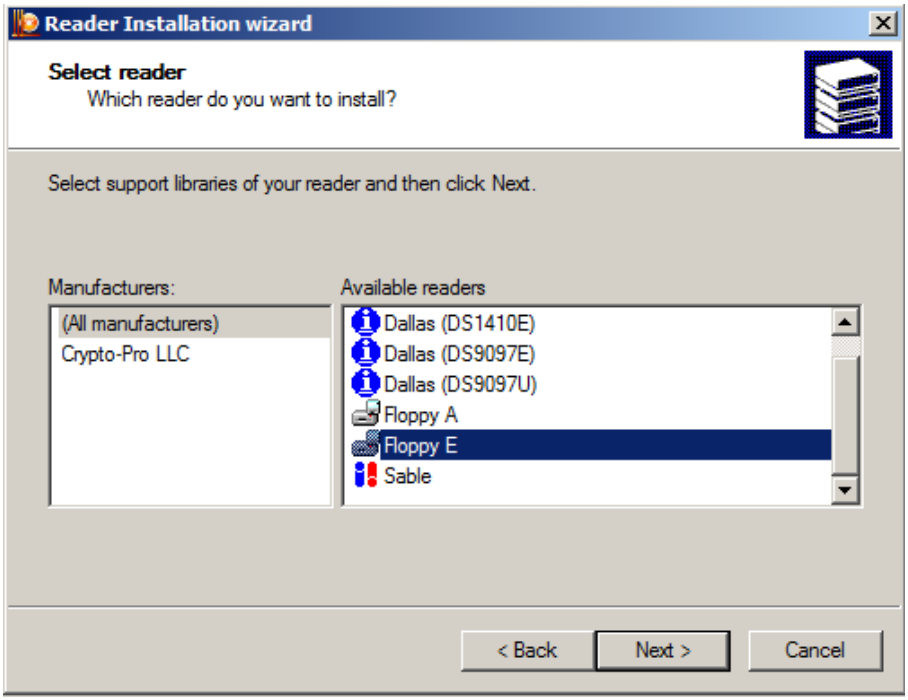

Рисунок 10

Шаг 6: Подтвердите имя считывателя, нажав Next > (Рисунок 11).

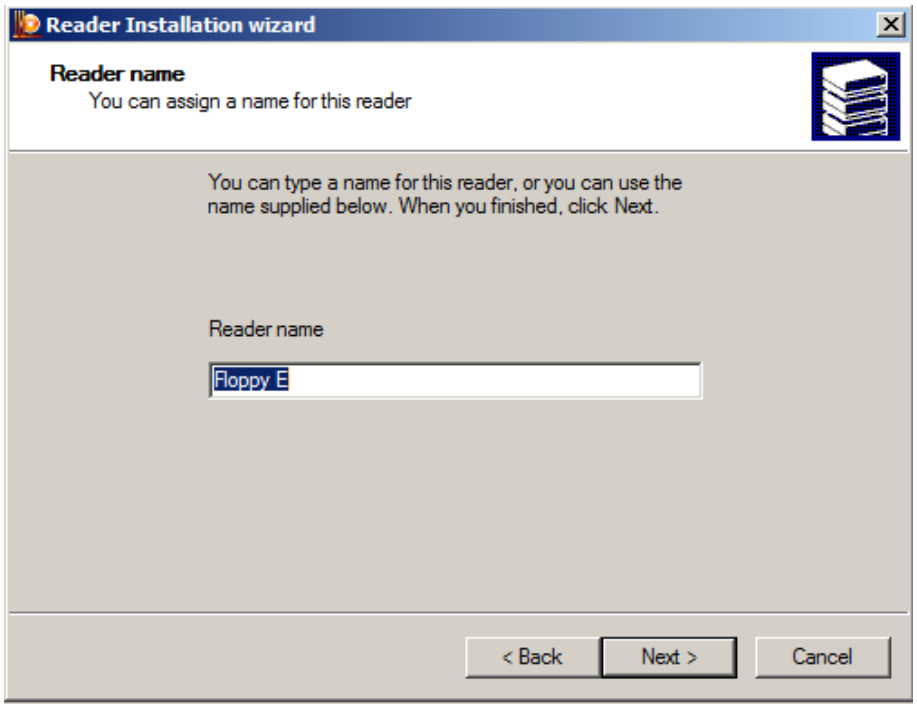

Рисунок 11

Шаг 7: Нажмите Finish и перезагрузите компьютер (Рисунок 12).

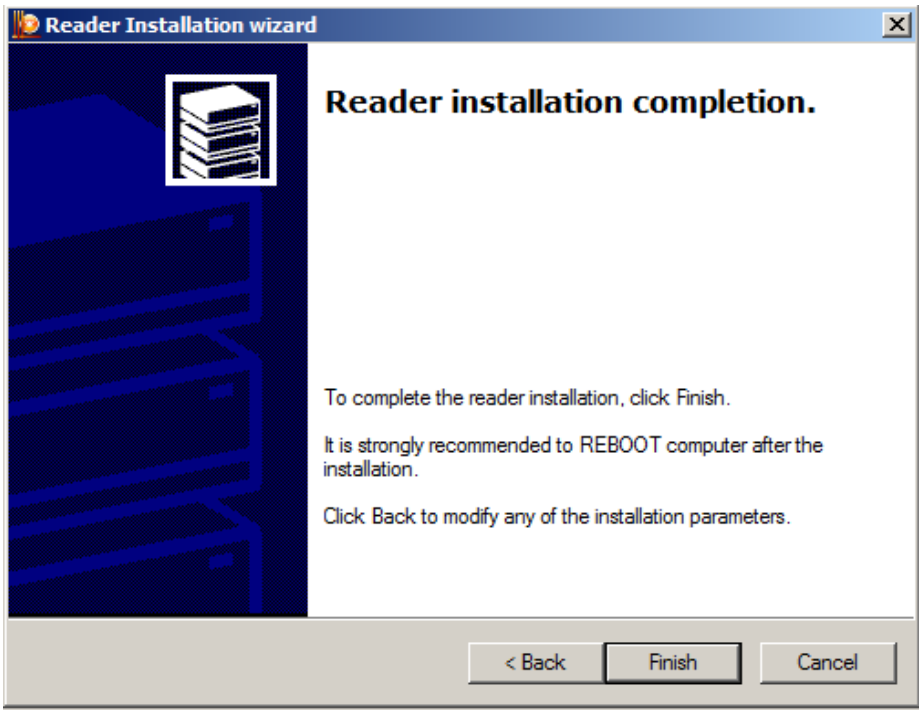

Рисунок 12

Шаг 8: Для копирования контейнеров запустите **CryptoPro CSP,** во вкладке **Service** нажмите кнопку Copy… (Рисунок 13).

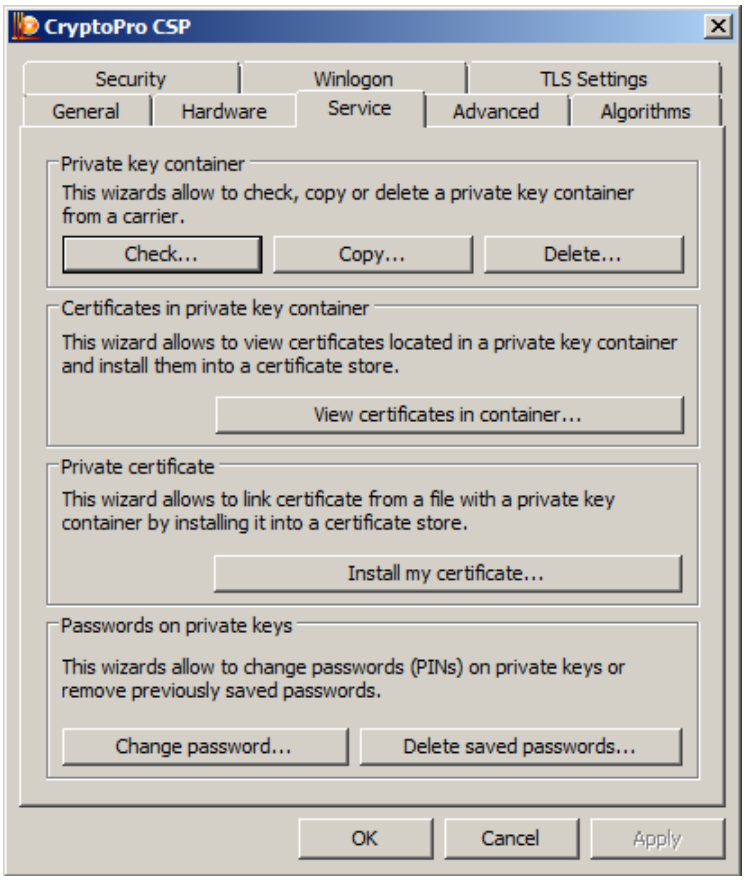

Рисунок 13

Шаг 9: В появившемся окне поставьте переключатель в положение **Computer** и нажмите Browse…(Рисунок 14), выберите необходимый контейнер СА сертификата, размещенный в реестре (Рисунок 15).

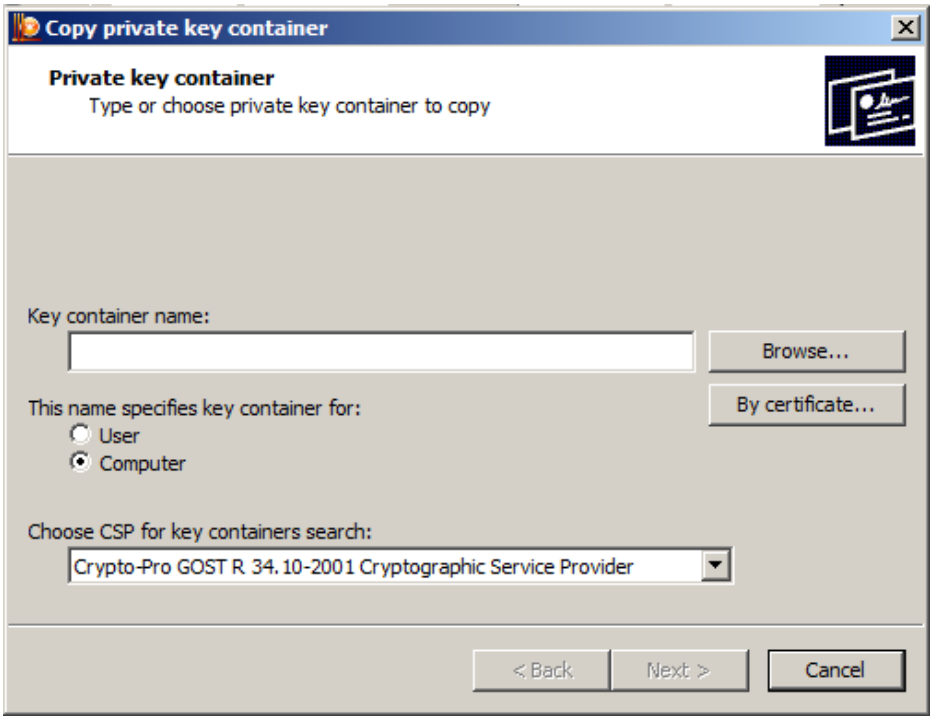

Рисунок 14

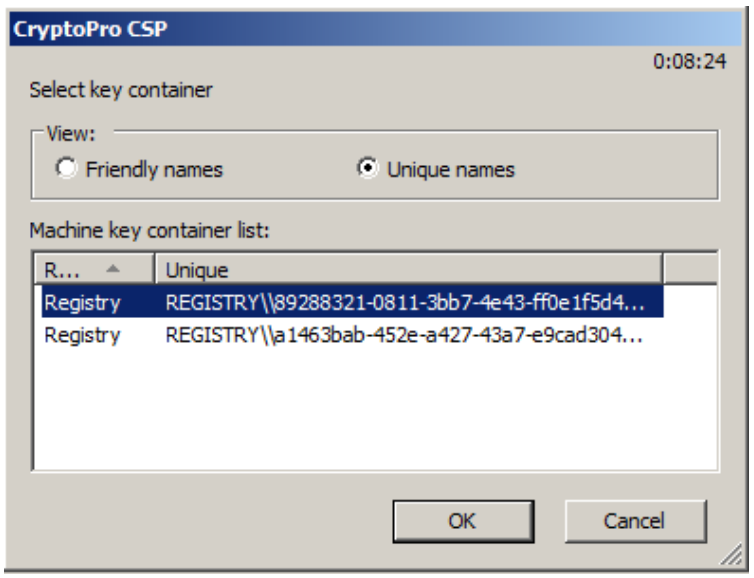

Рисунок 15

Шаг 10: Нажмите кнопку Next > (Рисунок 16).

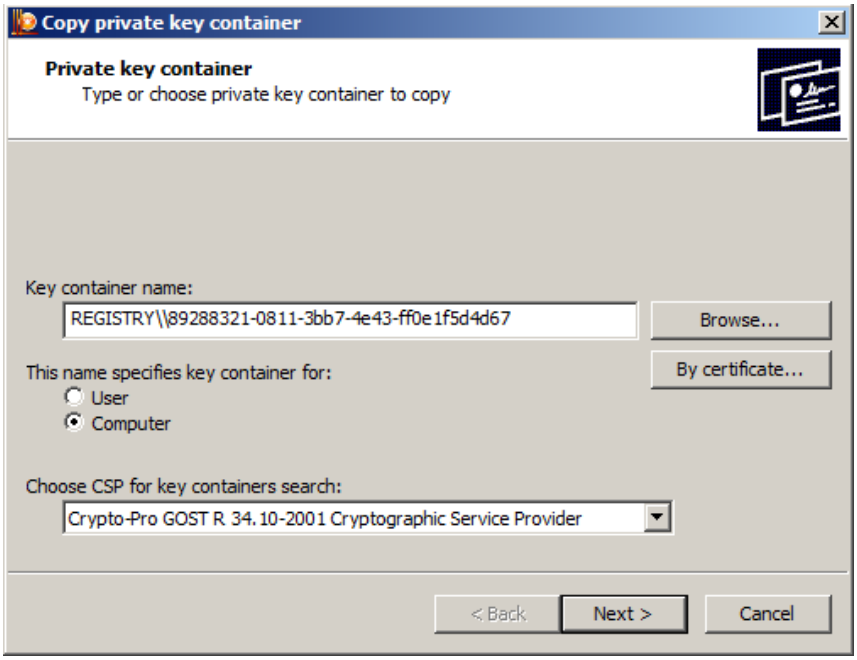

Рисунок 16

Шаг 11 Введите пароль на контейнер с секретным ключом, который задавался при создании СА-сертификата на Сервере управления (Рисунок 17).

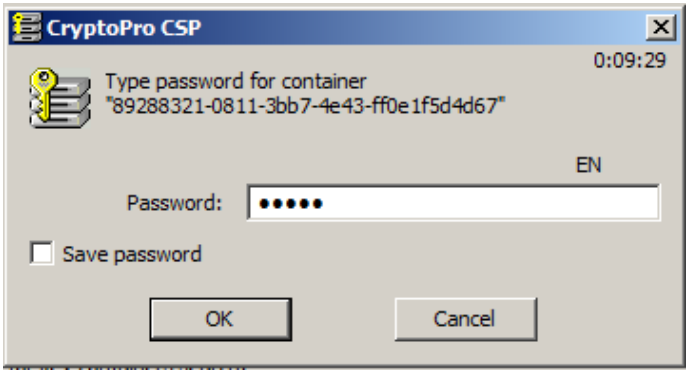

Рисунок 17

Шаг12: В появившемся окне введите имя нового контейнера, в который будет скопирован секретный ключ CA-сертификата, нажмите Finish (Рисунок 18).

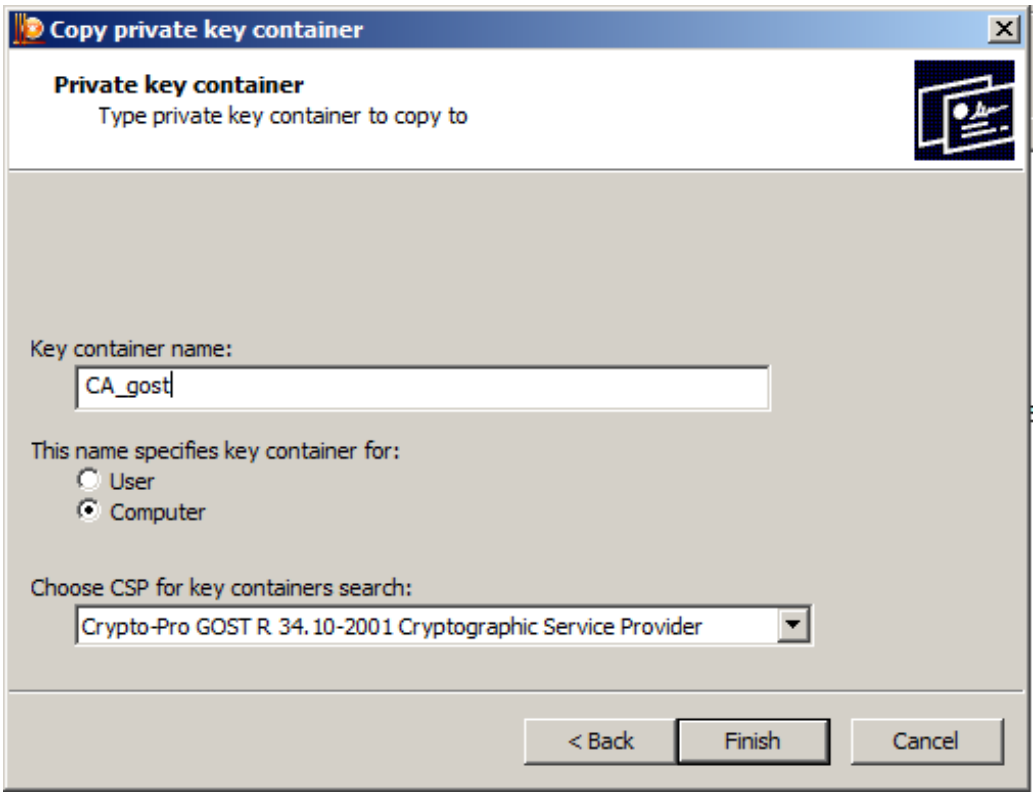

Рисунок 18

Шаг 13: Выберите ключевой носитель для нового контейнера – USB-флеш, нажмите OK (Рисунок 19).

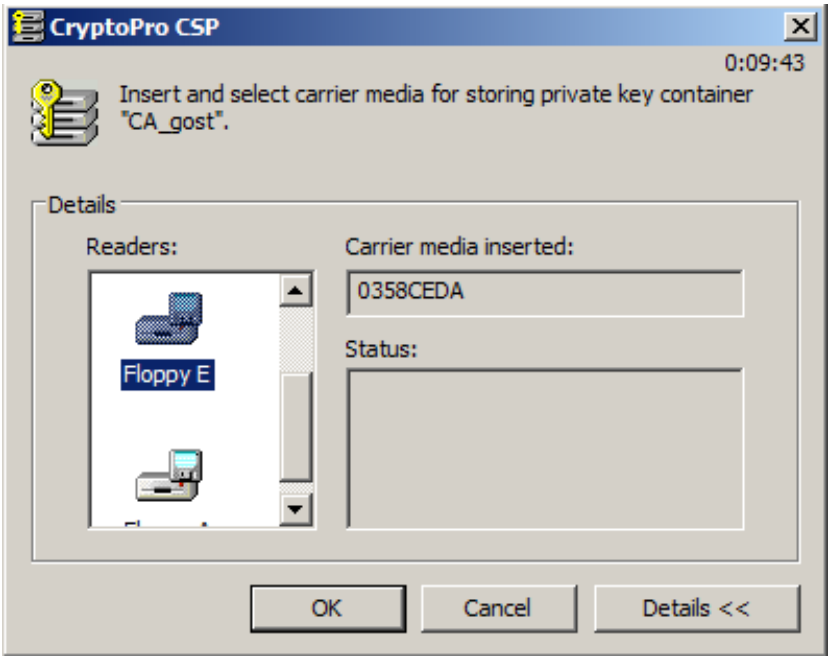

Рисунок 19

Шаг 14: Установите пароль на новый контейнер, нажмите OK (Рисунок 20).

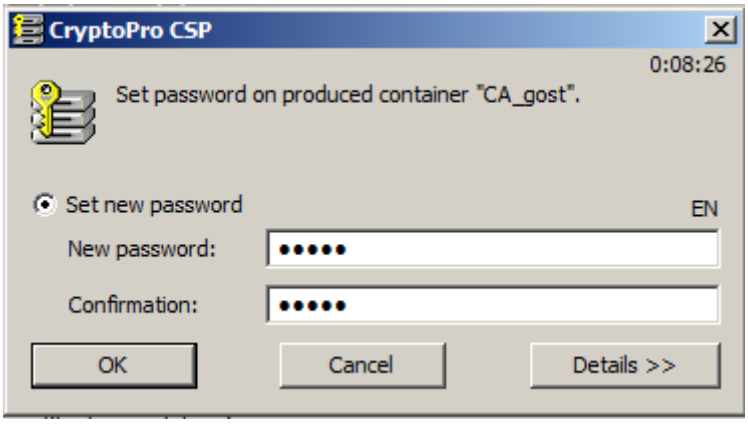

Рисунок 20

Шаг 15: Аналогичным образом скопируйте контейнер с секретным ключом для рабочего сертификата Сервера управления на USB-флеш.

Далее перейдите к разделу «Восстановление данных на новом ПК».

3.1.2. Экспорт контейнеров к RSA-сертификатам

Если на Сервере управления используются сертификаты с ключами на RSA-алгоритме, то для переноса сертификатов с одного Сервера управления на другой экспортируем их вместе с секретными ключами в файл формата `*.pfx`. Для переноса данных будем использовать USB-флеш, предварительно вставленную в USB-разъем.

Шаг 1: На компьютере с исходным Сервером управления из командной строки запустите: `mmc`. Откроется окно консоли (Рисунок 21).

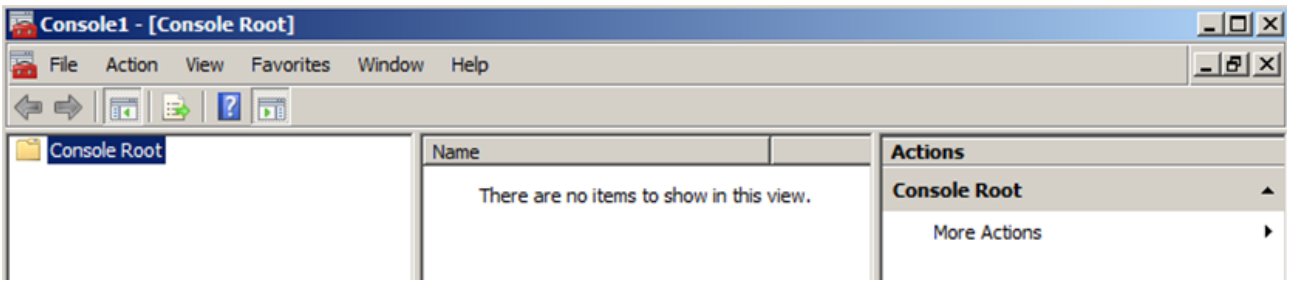

Рисунок 21

Шаг 2: Выберите в меню предложение **File-Add/Remove Snap-in…**(Рисунок 22).

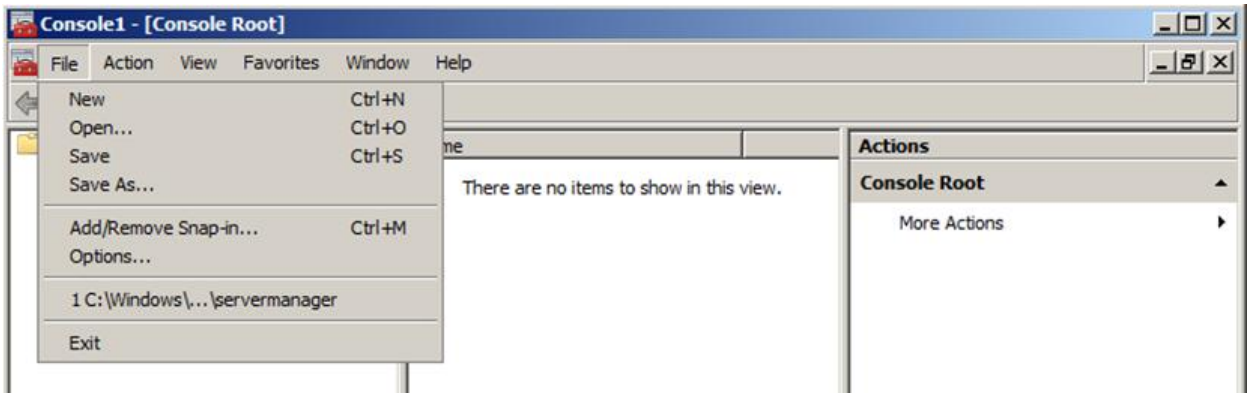

Рисунок 22

Шаг 3: В появившемся окне слева выберите **Certificates** и нажмите Add>, затем OK (Рисунок 23).

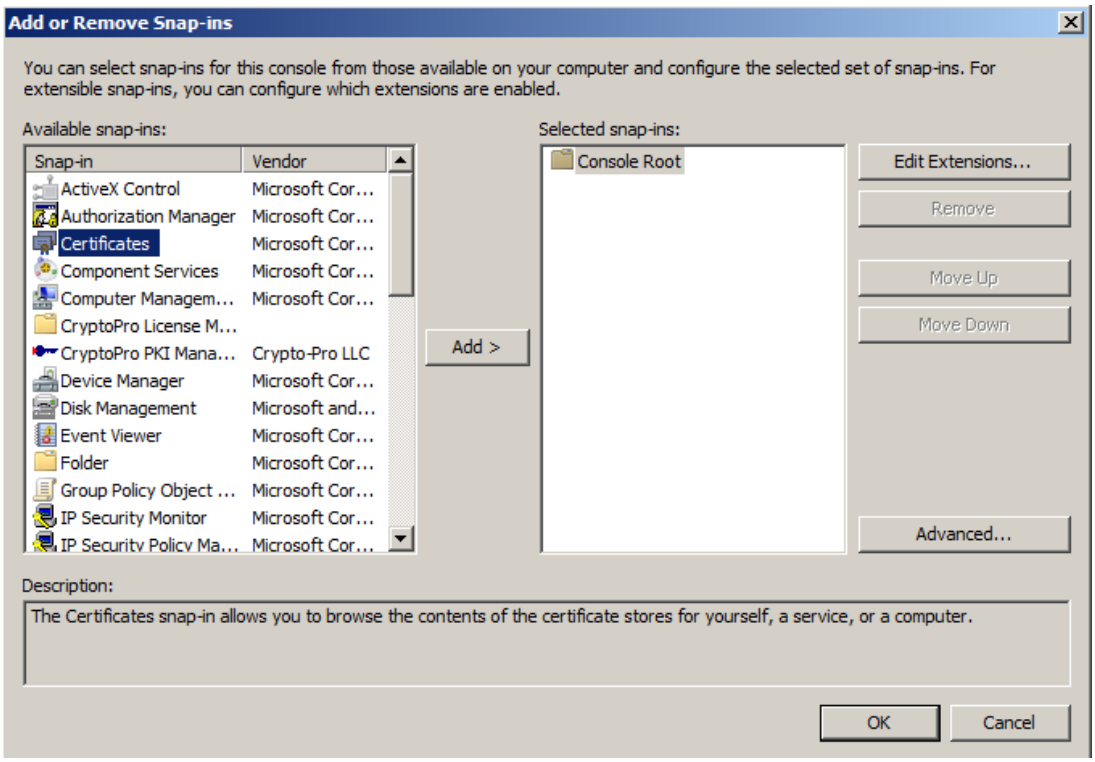

Рисунок 23

Шаг 4: В следующем диалоговом окне поставьте переключатель в положение **Computer account,** нажмите Next > (Рисунок 24).

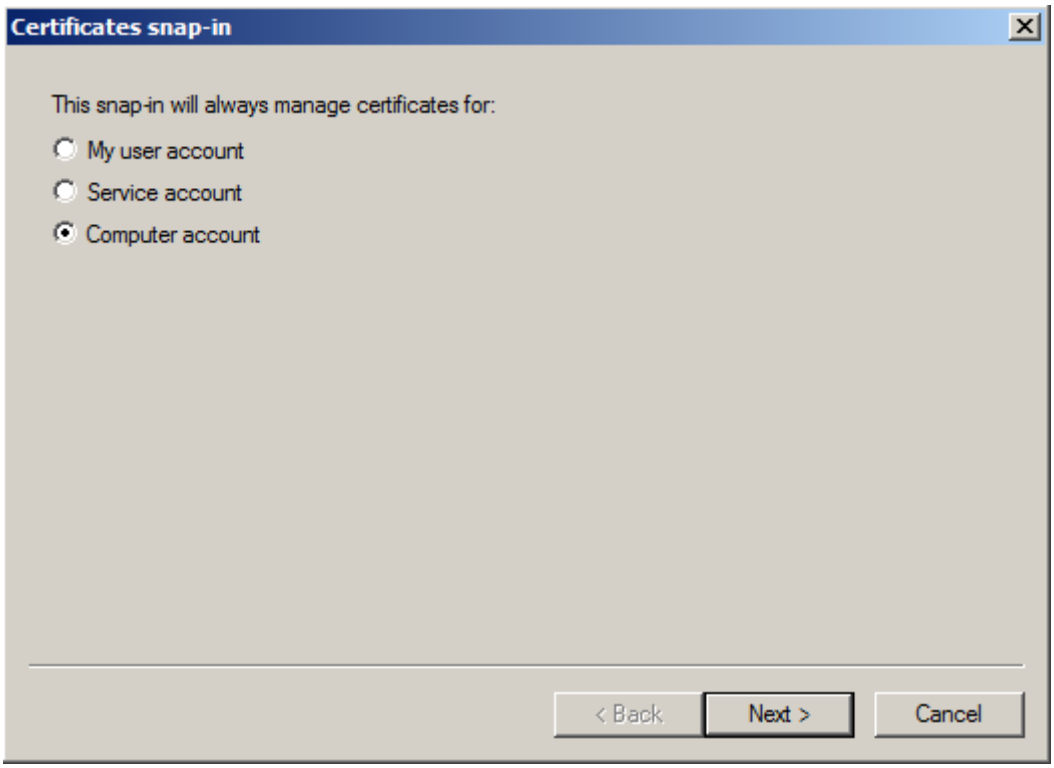

Рисунок 24

Шаг 5: На вкладке **Select Computer** поставьте переключатель в положение **Local computer** и нажмите Finish (Рисунок 25).

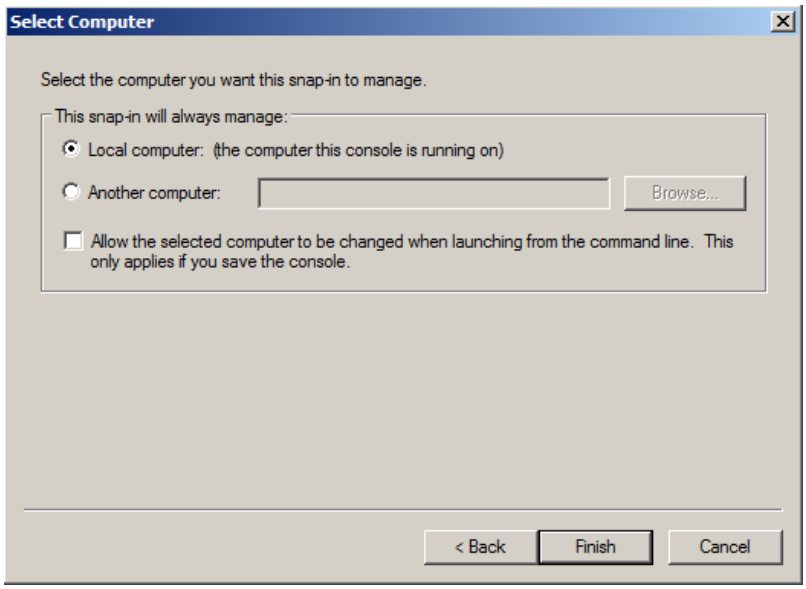

Рисунок 25

Шаг 6: На вкладке **Add or Remove Snap-ins** в правом столбце появляется выбранная оснастка (Certificates). Нажмите OK (Рисунок 26) и перейдите в окно консоли (Рисунок 27).

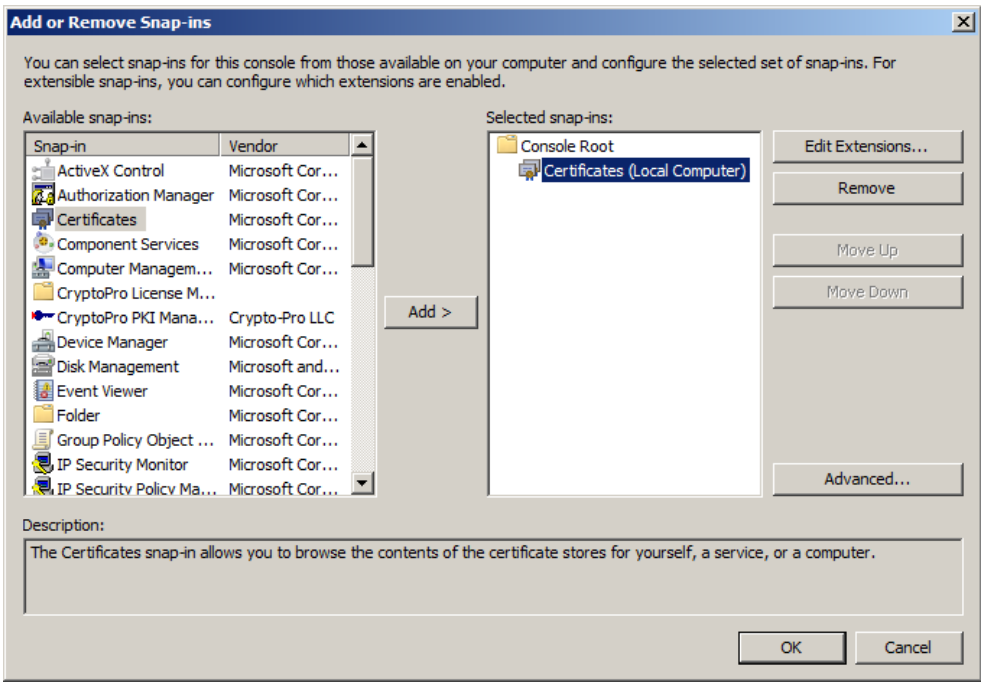

Рисунок 26

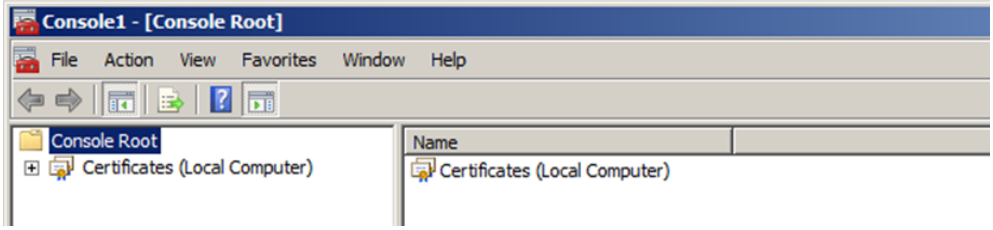

Рисунок 27

Шаг 7: В каталоге **Trusted Root Certification Authorities** выберите каталог **Certificates**, а справа выберите CA сертификат Сервера управления для копирования – **UPServer CA certificate** (Рисунок 28).

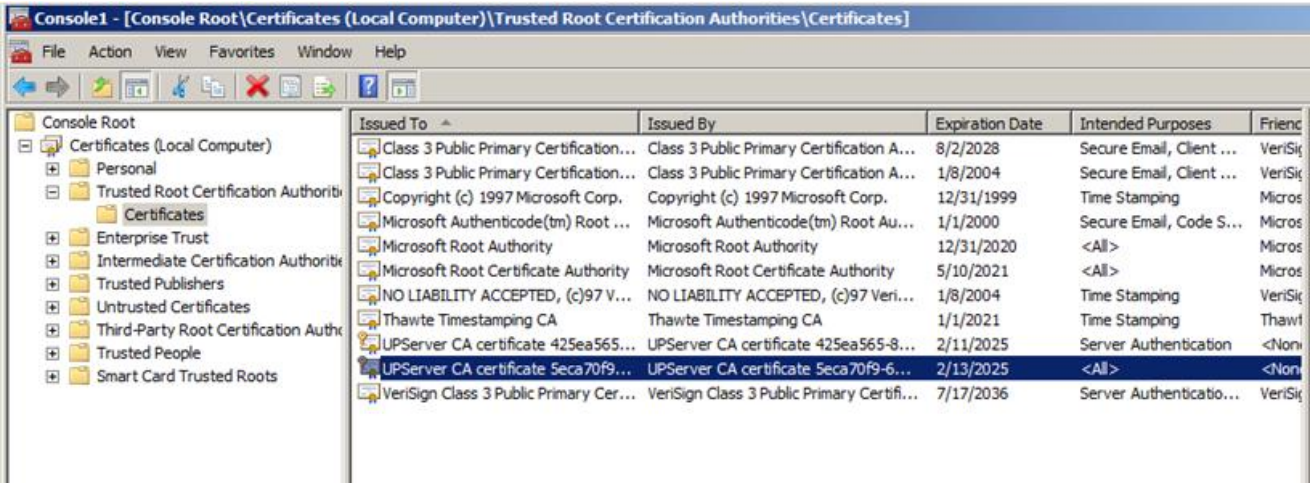

Рисунок 28

Шаг 8: Правой кнопкой мыши нажмите на имени сертификата и из выпадающего меню выберите **All Tasks – Export…** (Рисунок 29).

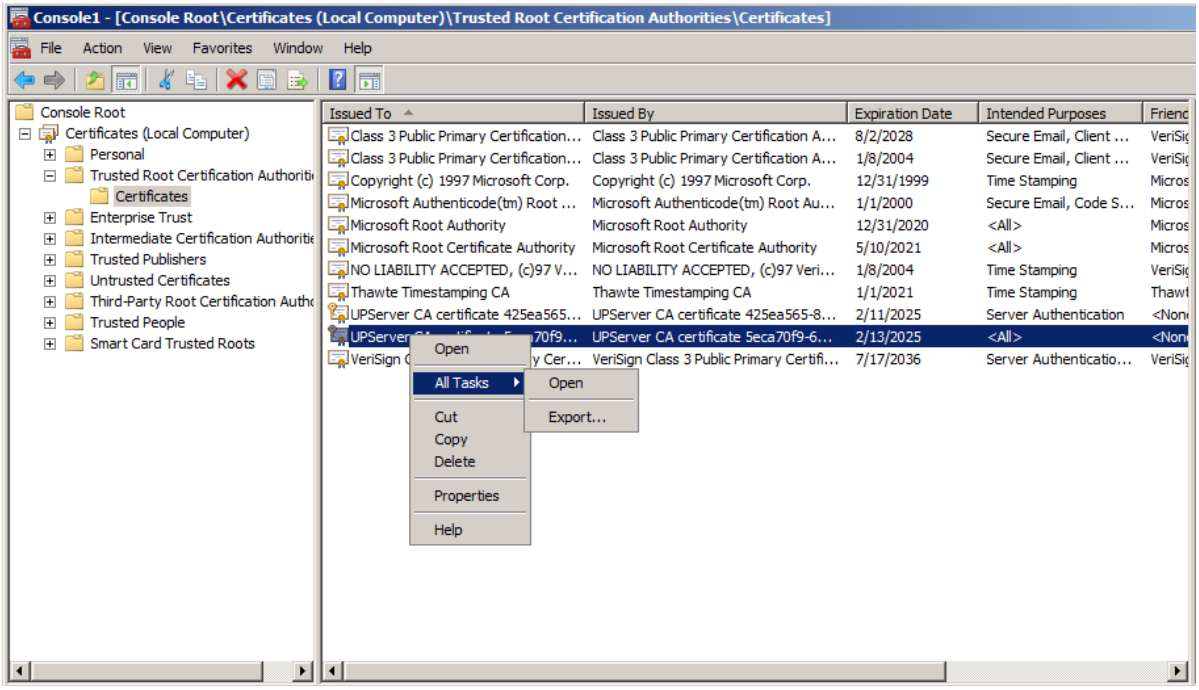

Рисунок 29

Шаг 9: Откроется окно Мастера экспорта сертификатов – **Certificate Export Wizard**, нажмите Next > (Рисунок 30).

Рисунок 30

Шаг 10: Для экспортирования секретного ключа вместе с сертификатом поставьте переключатель в положение **Yes, export the private key,** нажмите Next > (Рисунок 31).

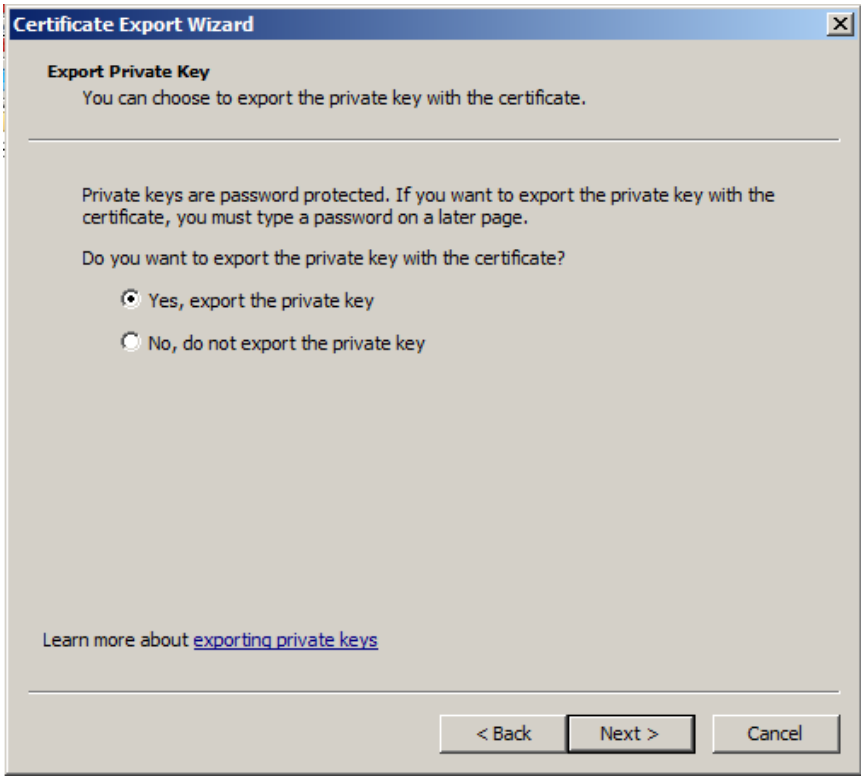

Рисунок 31

Шаг 11: Экспортируйте сертификат и ключ в контейнер формата PKCS#12 (файл формата `.pfx`), нажмите Next > (Рисунок 31).

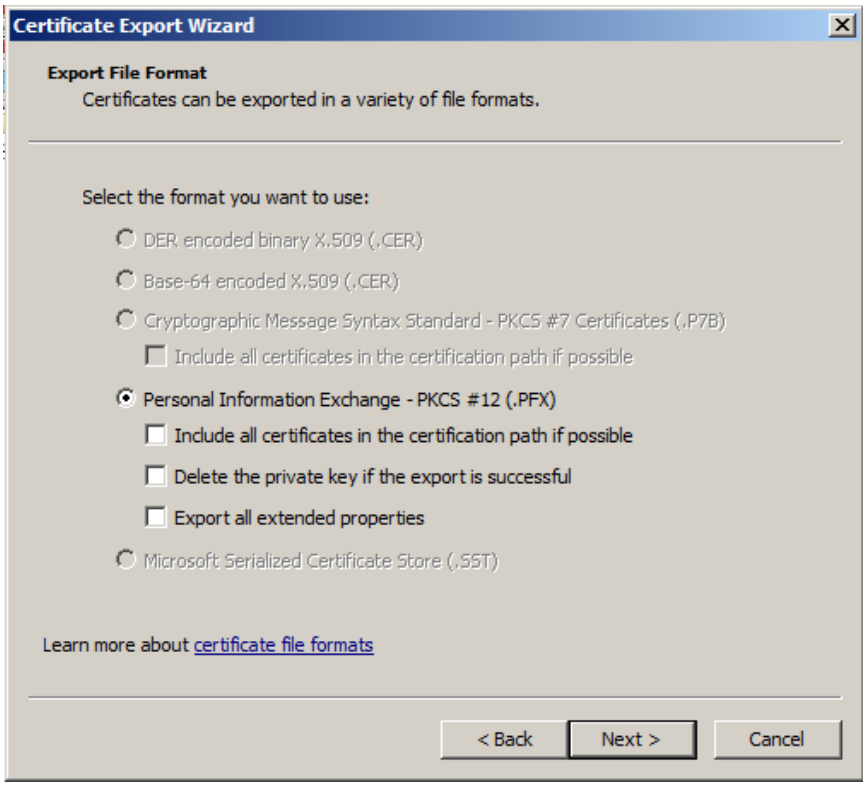

Рисунок 32

Шаг 12: Для защиты контейнера установите пароль и подтвердите его, нажмите Next > (Рисунок 32).

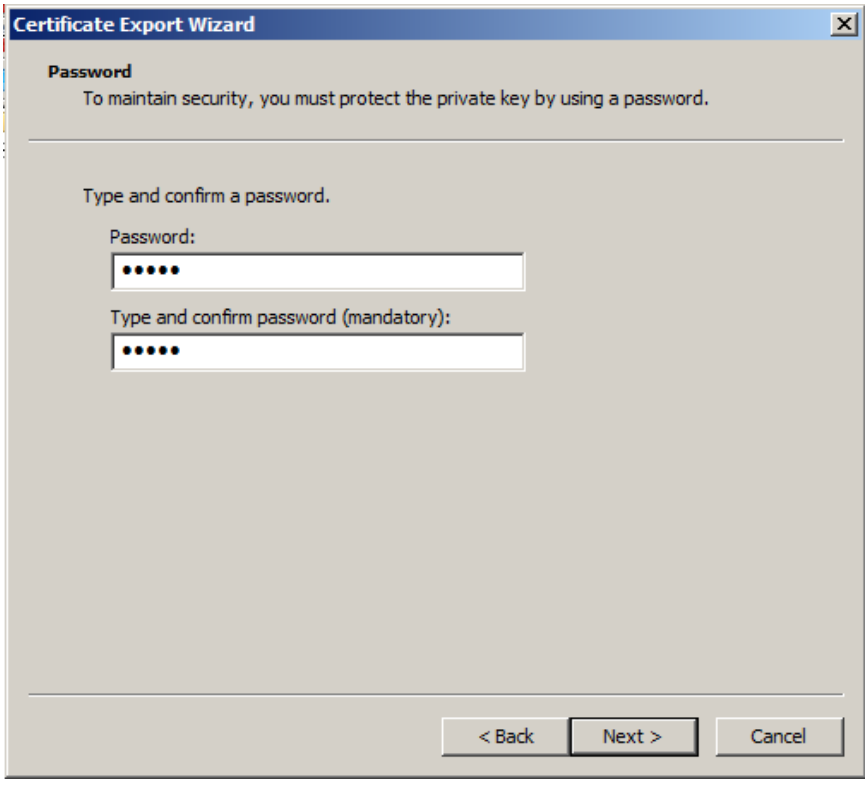

Рисунок 33

Шаг 13: Сохраните контейнер на USB-флеш, указав имя файла, нажмите Save (Рисунок 34).

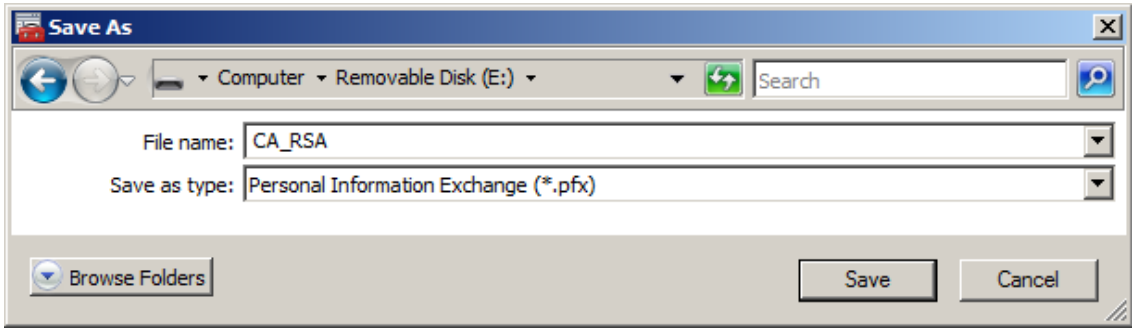

Рисунок 34

Шаг 14: В окне Мастера экспорта сертификатов проверьте правильность отображаемого имени файла, нажмите Next > (Рисунок 35).

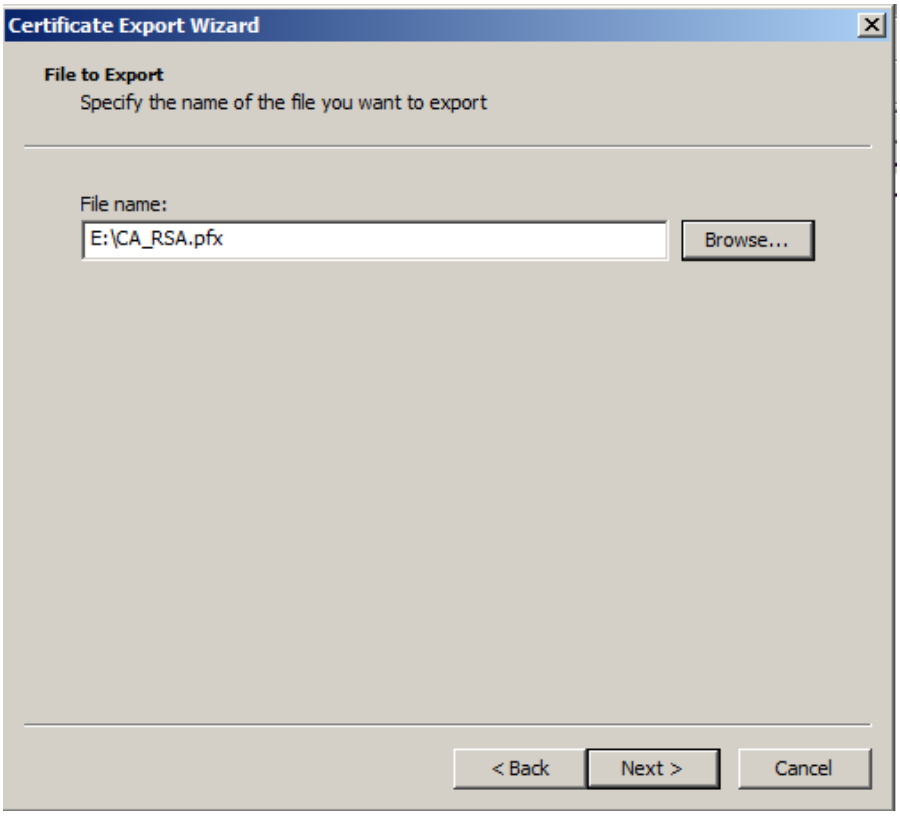

Рисунок 35

Шаг 15: Подтвердите завершение операции, нажав Finish (Рисунок 36). Процедура экспорта CA-сертификата и секретного ключа успешно завершена (Рисунок 37).

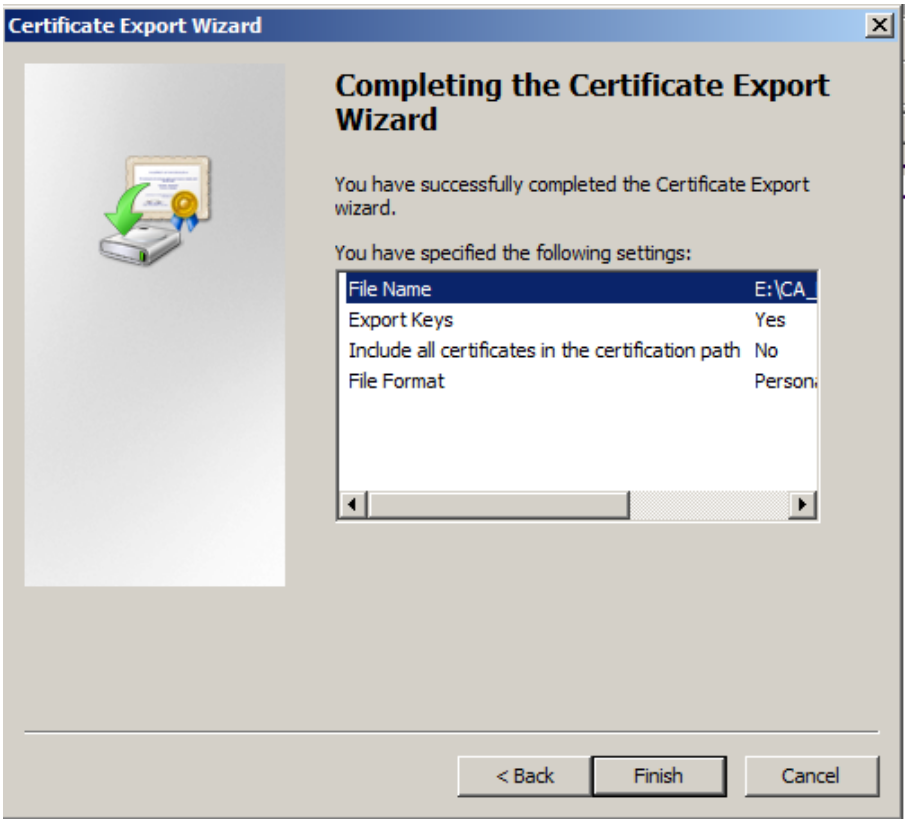

Рисунок 36

Рисунок 37

Процедура переноса рабочего сертификата Сервера управления и секретного ключа к нему аналогична вышеописанной для CA сертификата, однако, путь хранения рабочего сертификата несколько отличается **– Certificates - Personal – Certificates**, поэтому опишем отличающийся Шаг 7.

Шаг 7: Выбираем слева предложение **Certificates** и в выпадающих списках выбираем **Personal - Certificates** (Рисунок 38). Далее в столбце справа выбираем необходимый для копирования сертификат – **UPServer work certificate**.

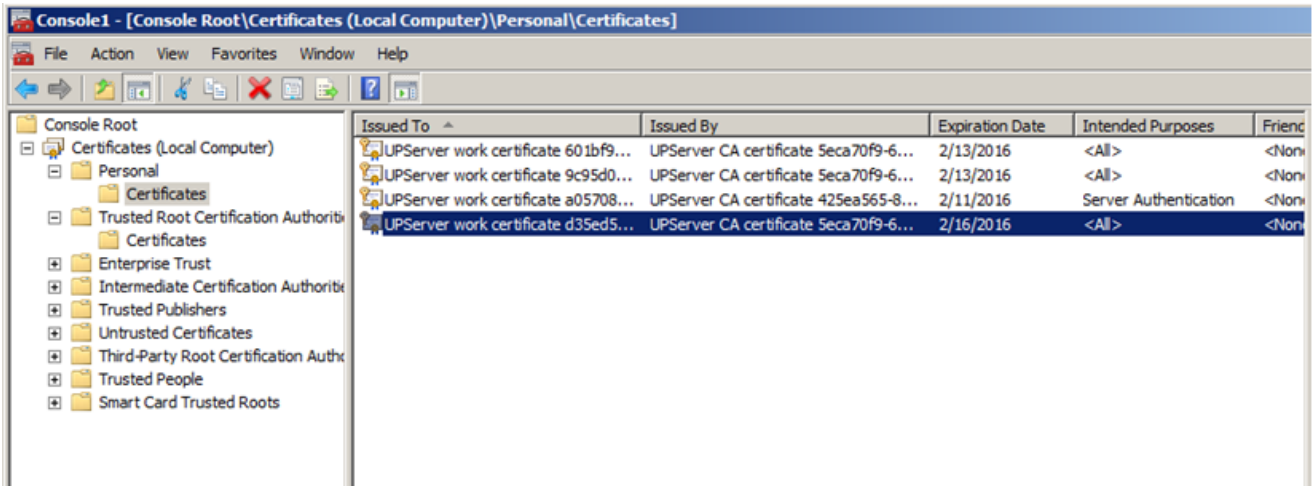

Рисунок 38

Далее перейдите к разделу «Восстановление данных на новом ПК».

3.2. Восстановление данных на новом ПК

На новом ПК с установленной ОС, СКЗИ «КриптоПро CSP 3.6/3.6R2/3.6R4», Сервером управления из состава «Программного продукта С-Терра КП. Версия 4.1», для восстановления всех сохраненных настроек Сервера управления, сертификатов, учетных записей управляемых устройств выполните следующие процедуры.

Шаг 1: Вставьте USB-флеш с сохранеными данными в USB-разъем нового ПК и скопируйте файл `backup01.bin` в любую директорию.

Шаг 2: На новом ПК из консоли запустите команду для восстановления настроек (Рисунок 39), например:

```
C:\Program Files\S-Terra KP\upmgr restore –f C:\backup01.bin
```

После этого данные о клиентах, сертификатах и настройках будут доступны во вкладках Сервера управления.

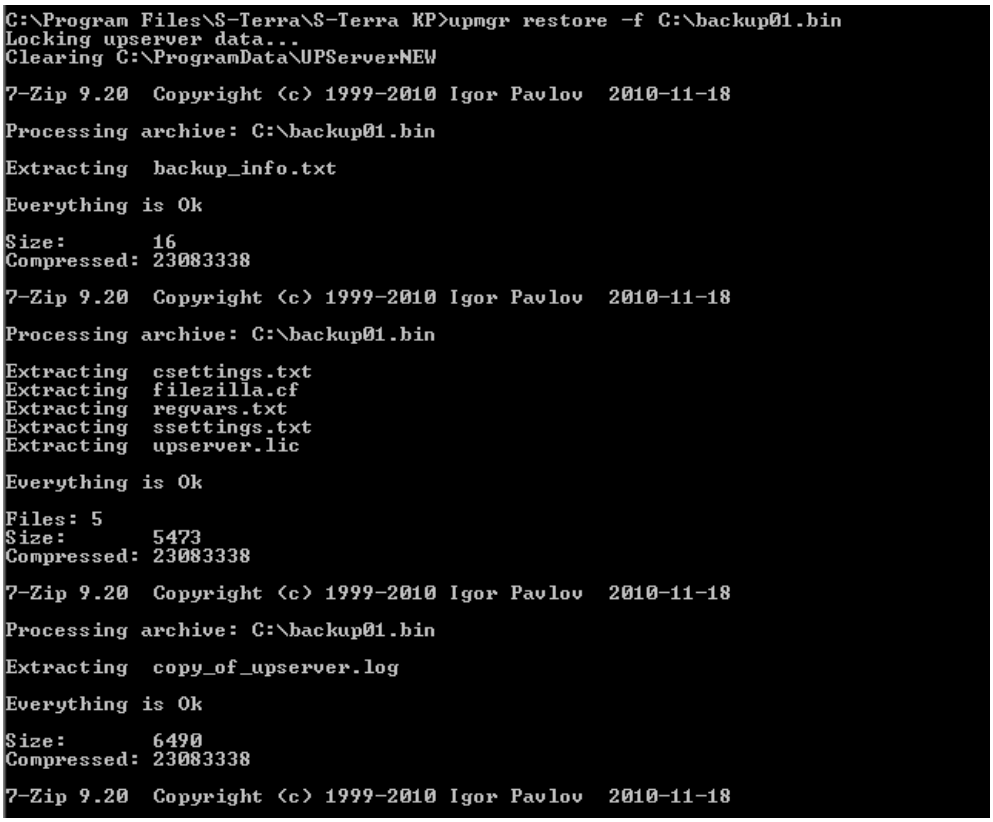

Рисунок 39

Для импортирования контейнеров сертификатов Сервера управления с USB–флеш перейдите к разделу «Импорт контейнеров к ГОСТ-сертификатам» либо к разделу «Импорт контейнеров к RSA-сертификатам».

3.2.1. Импорт контейнеров к ГОСТ-сертификатам

Шаг 1: Скопируйте контейнеры с USB-флеш в реестр нового ПК. Процедура копирования аналогична описанной ранее (шаги 1-14 в разделе «Экспорт контейнеров к ГОСТ-сертификатам»), однако, вместо съемного носителя необходимо выбрать тип носителя – **Registry** (Рисунок 40).

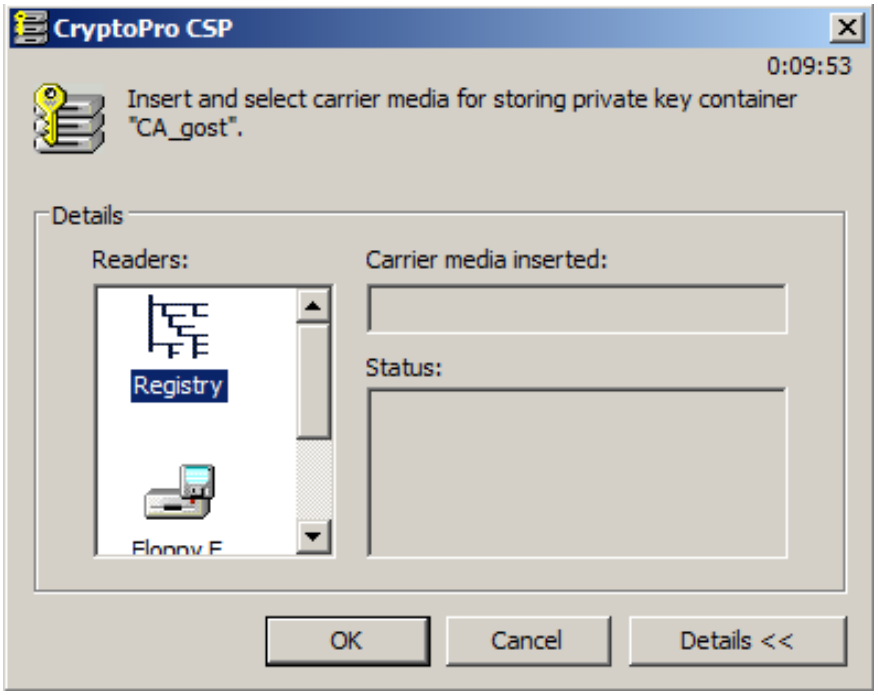

Рисунок 40

Шаг 2: Перейдите на вкладку **CryptoPro CSP – Service – Install my certificate…** (Рисунок 42).

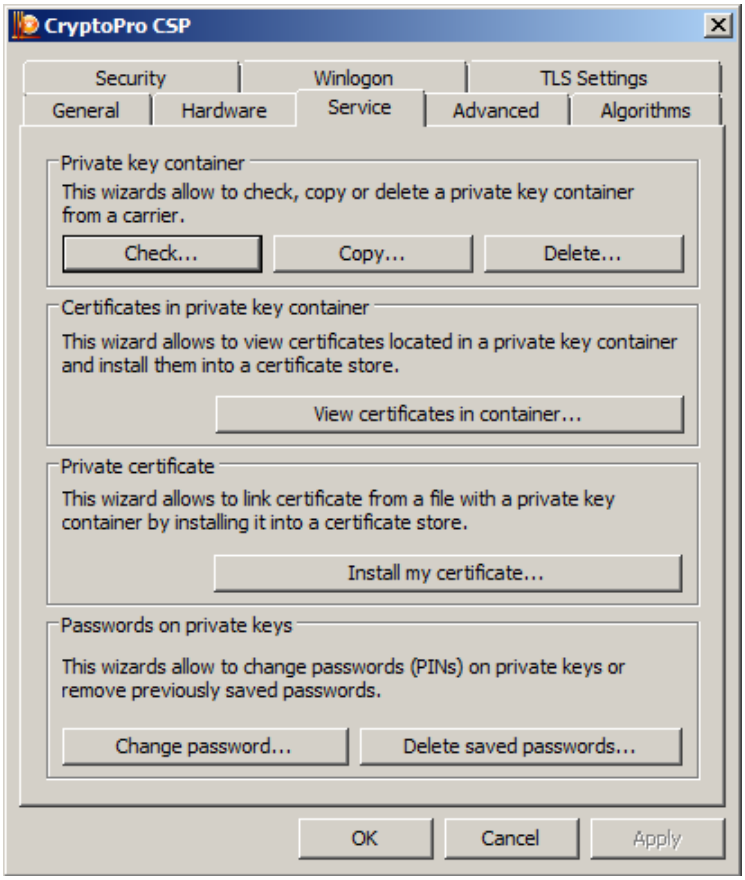

Рисунок 41

Шаг 3: В появившемся окне нажмите кнопку Browse для выбора перенесенных сертификатов (Рисунок 42).

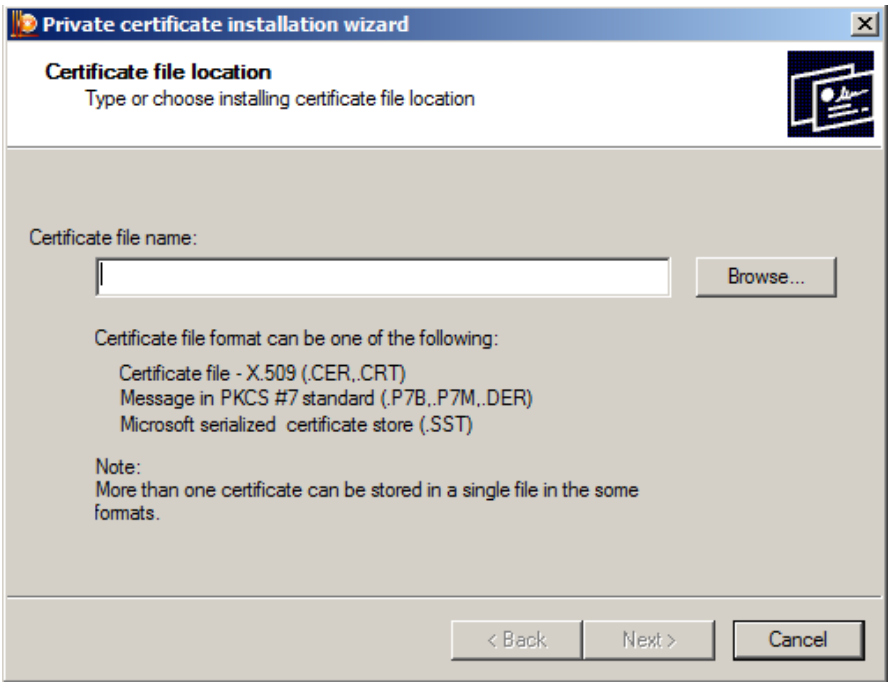

Рисунок 42

Шаг 4: В окне выбора сертификатов выберите путь до перенесенных сертификатов Сервера управления: `C:\ProgramData\UPServer\certs` (Рисунок 43). Выберите CA-сертификат и нажмите кнопку Open.

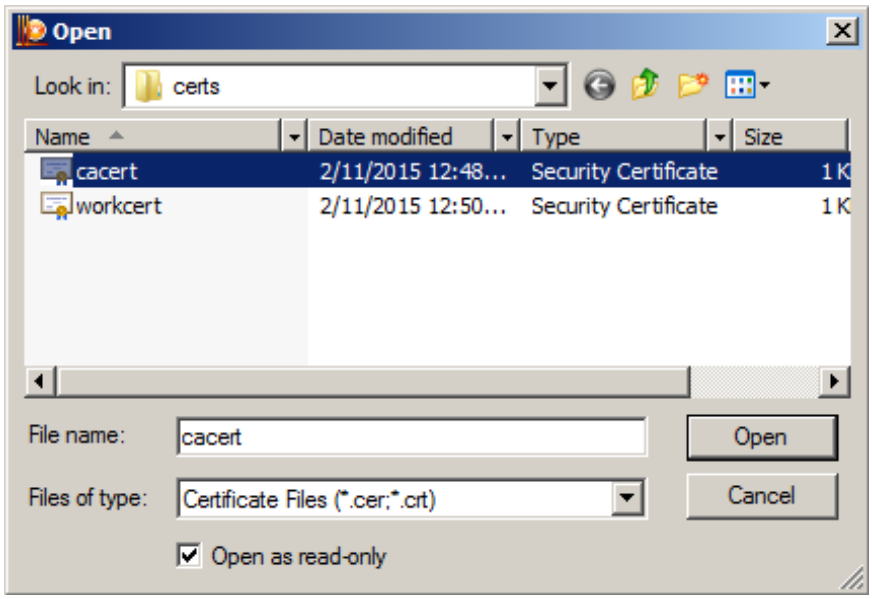

Рисунок 43

Шаг 5: Путь до CA-сертификата будет прописан в окне Мастера установки личного сертификата. Нажмите кнопку Next > (Рисунок 44).

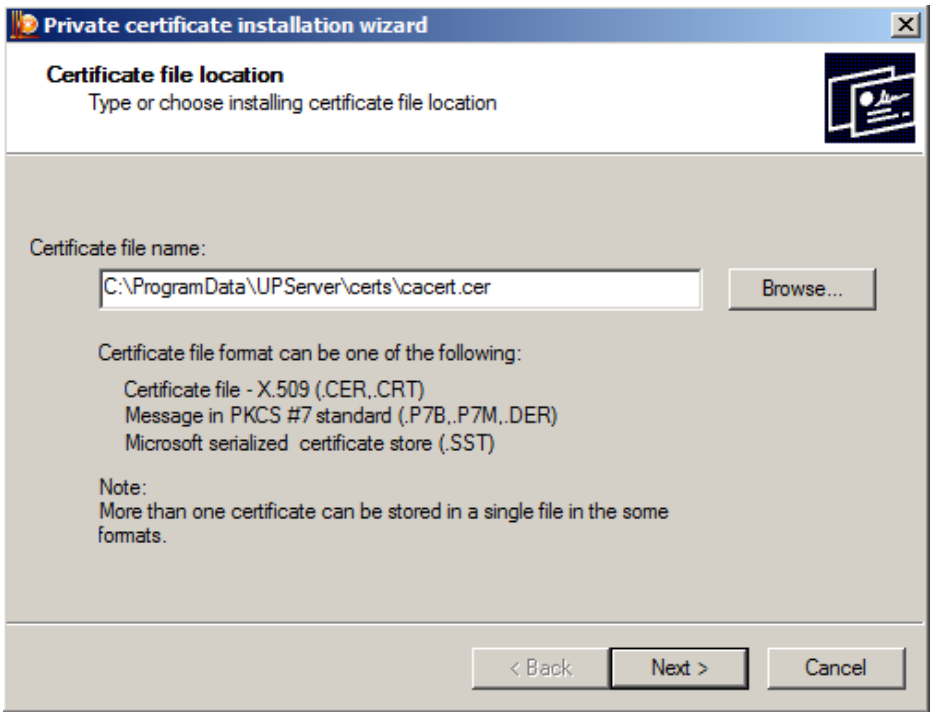

Рисунок 44

Шаг 6: Подтвердите данные о сертификате, нажав Next > (Рисунок 45).

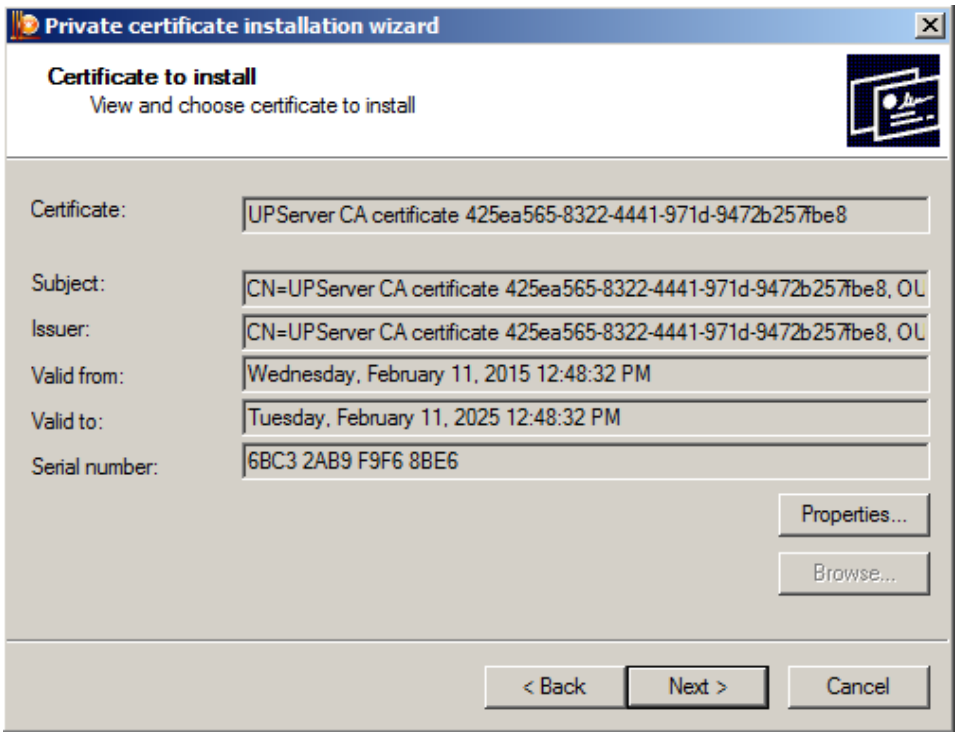

Рисунок 45

Шаг 7: В появившемся окне выбора ключевого контейнера поставьте переключатель в положение **Computer** и нажмите Browse (Рисунок 46).

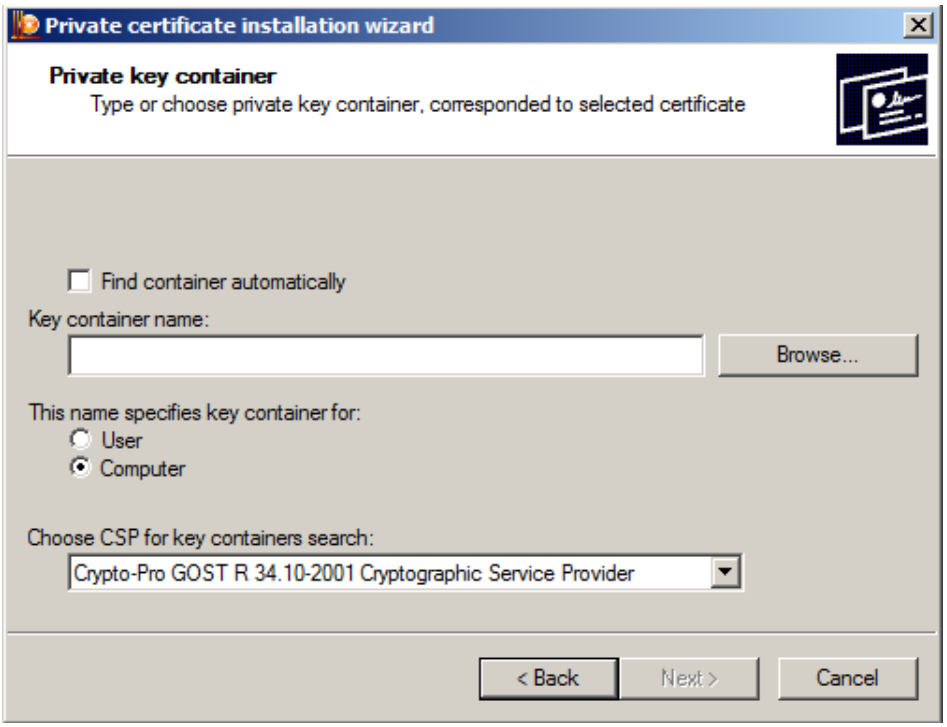

Рисунок 46

Шаг 8: Выберите скопированный ранее в Registry ключевой контейнер для данного сертификата и нажмите OK (Рисунок 47)..

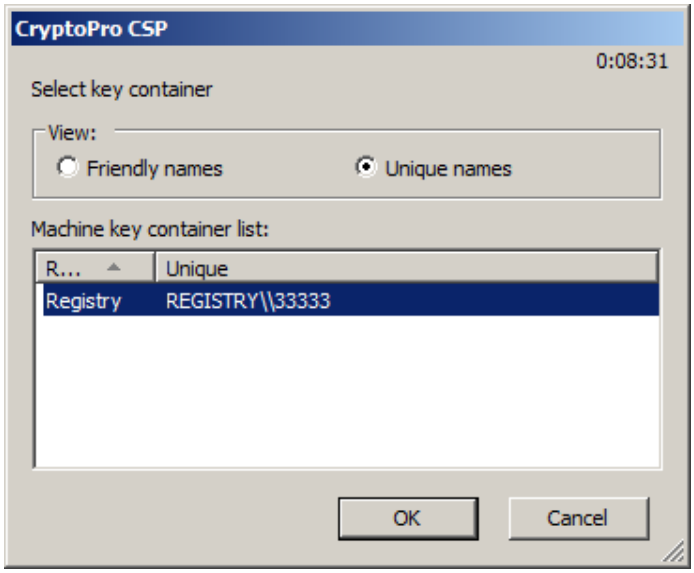

Рисунок 47

Шаг 9: После этого имя контейнера прописывается в окне Мастера установки личного сертификата, нажмите Next (Рисунок 48).

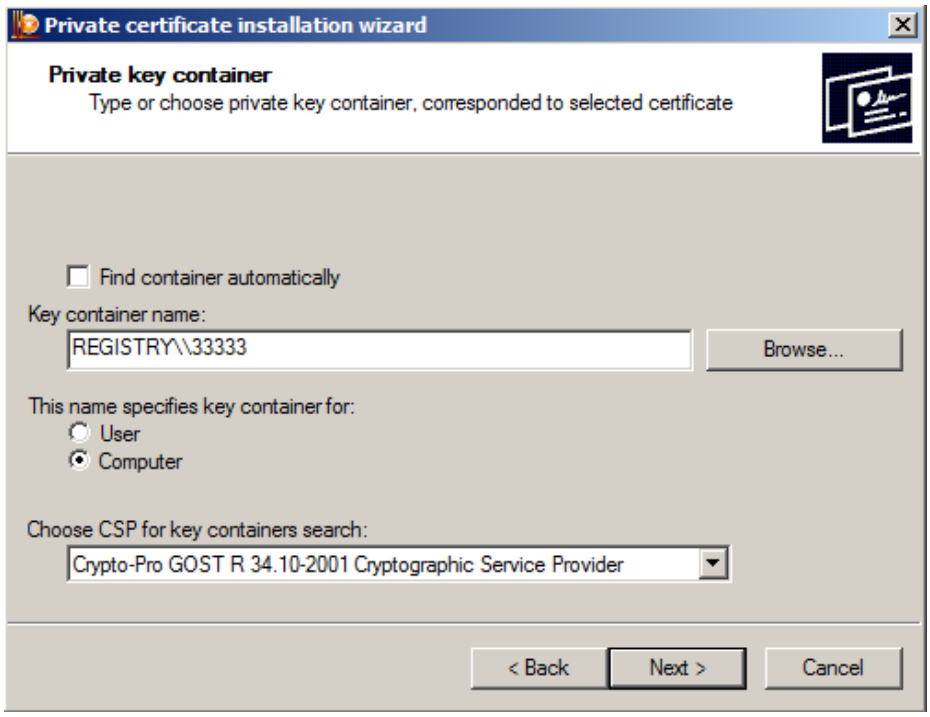

Рисунок 48

Шаг 10: Введите пароль к выбранному контейнеру, нажмите OK. (Рисунок 49)

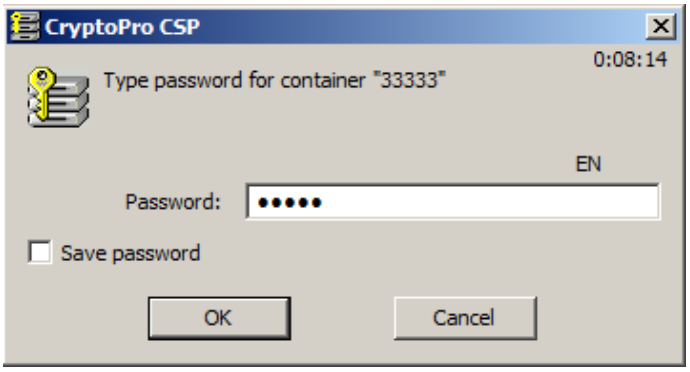

Рисунок 49

Шаг 11: В окне выбора хранилища сертификатов (Рисунок 50) при копировании CA сертификата важно указать папку корневых доверенных центров сертификации. Для этого нажмите Browse… и в появившемся окне выберите **Trusted root Certification Authorities** – OK (Рисунок 51). В следующем окне нажмите Next > (Рисунок 52).

При копировании **рабочего** сертификата следует согласиться с предложенным по умолчанию хранилищем (Personal) и нажать Next >.

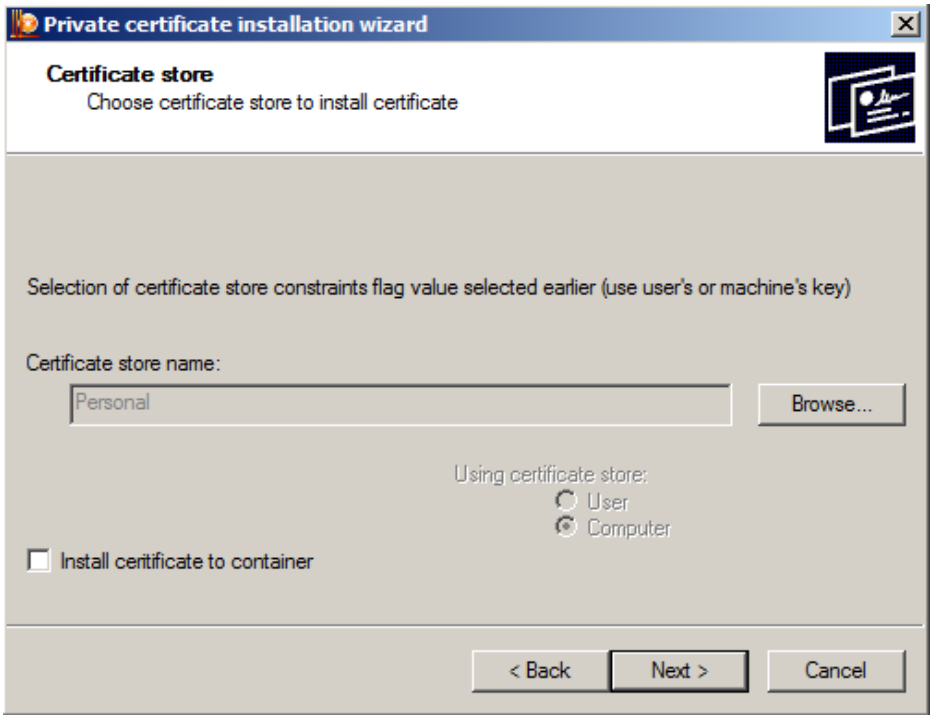

Рисунок 50

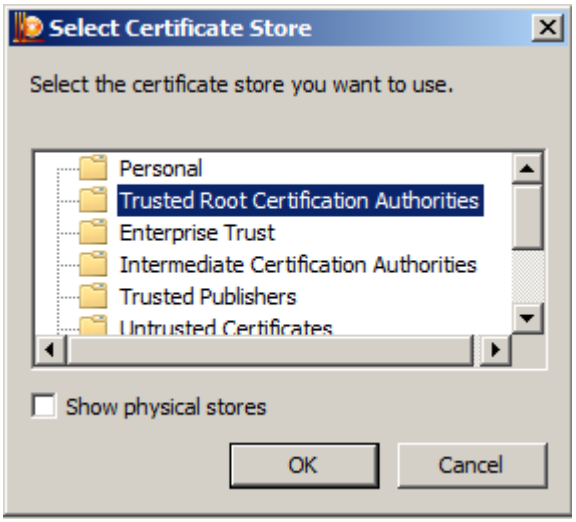

Рисунок 51

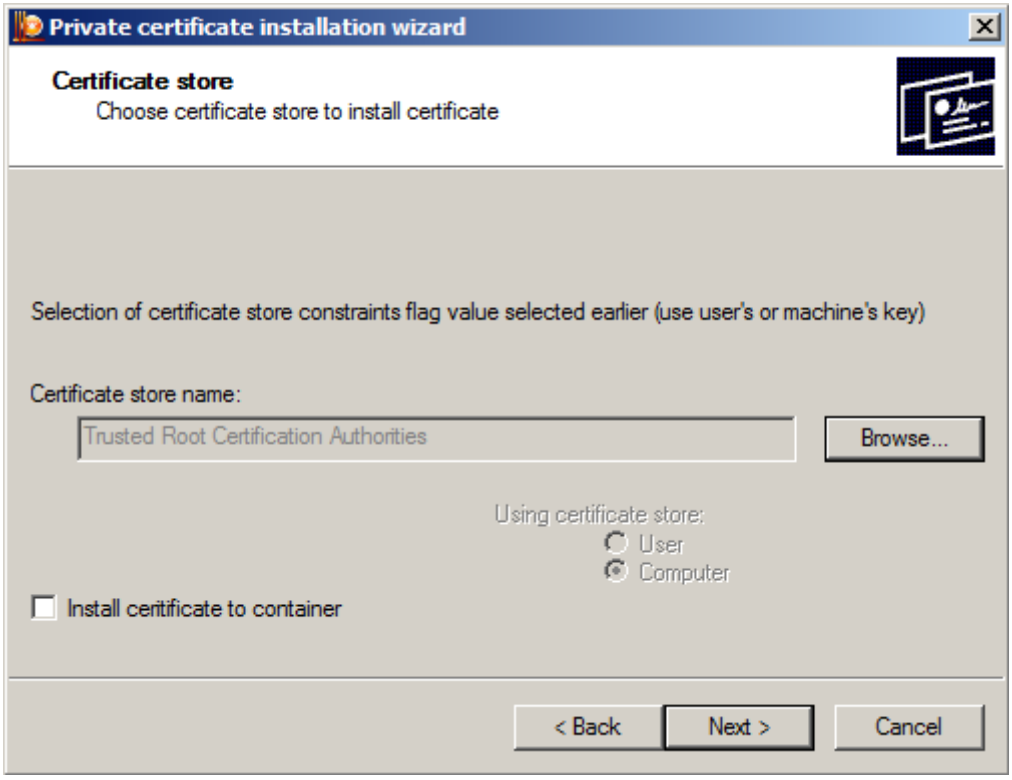

Рисунок 52

Шаг 12: Подтвердите завершение операции - Finish (Рисунок 53).

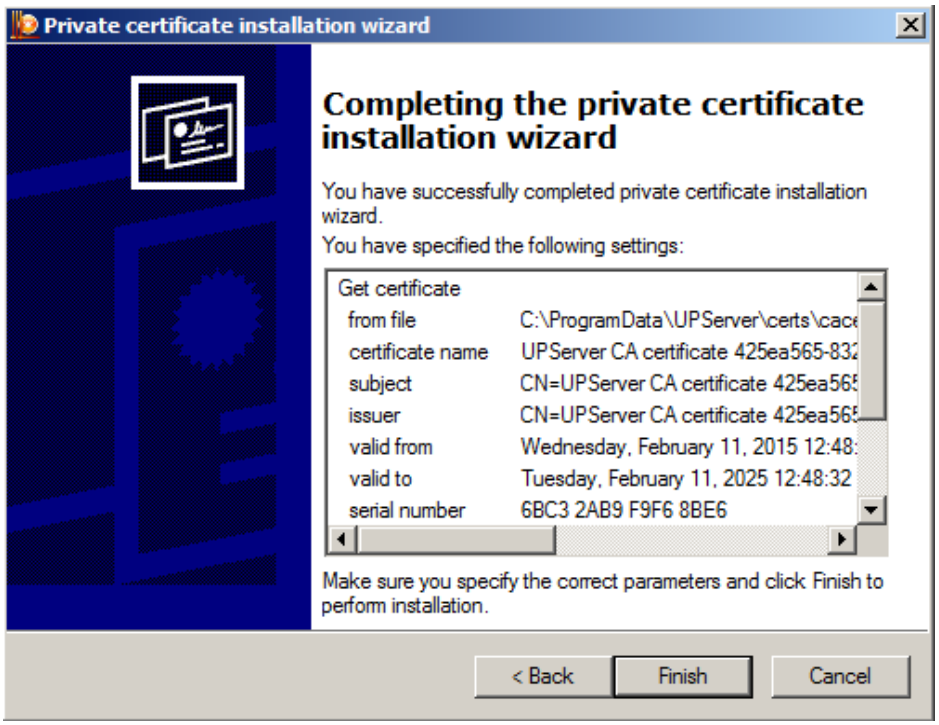

Рисунок 53

Импортирование контейнера и привязка его к CA-сертификату завершена.

Шаг 13: Аналогичным образом импортируйте контейнер к рабочему сертификату и привяжите контейнер к сертификату (шаги 1-12). После запустите консоль Сервера управления и перейдите на вкладку Settings. В области Work certificate нажмите кнопку View… (Рисунок 54).

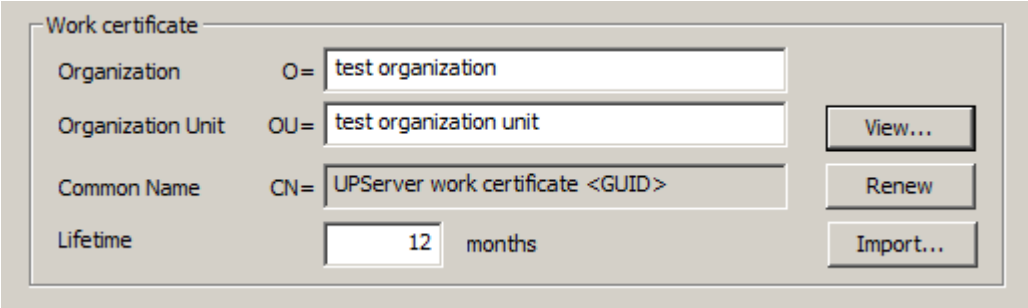

Рисунок 54

Шаг 14: В появившемся окне описания рабочего сертификата введите имя контейнера и пароль к нему, которые были назначены при копировании контейнера с USB-флеш в Реестр (Рисунок 55).

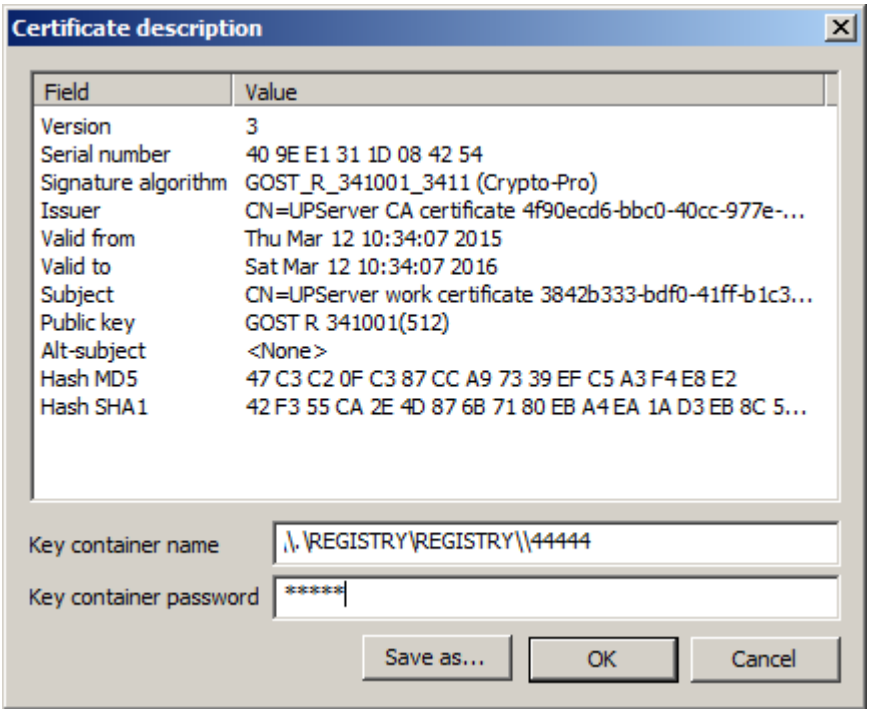

Рисунок 55

Процесс переноса Сервера управления на новый ПК завершен.

3.2.2. Импорт контейнеров к RSA-сертификатам

Шаг 1: На новом ПК с установленным СКЗИ «КриптоПро CSP» и Сервером управления вставьте USB-флеш в USB-разъем, а затем повторите шаги 1-6 включительно раздела 3.1.2 «Экспорт контейнеров к RSA-сертификатам».

Шаг 2: В окне консоли с добавленной оснасткой в левой области выберите **Certificates – Trusted Root Certification Authorities – Certificates**. При этом справа появится список сертификатов, лежащих в указанной директории. Правой кнопкой мыши кликните на пустом месте в этой области и выберите **All Tasks – Import…**(Рисунок 56).

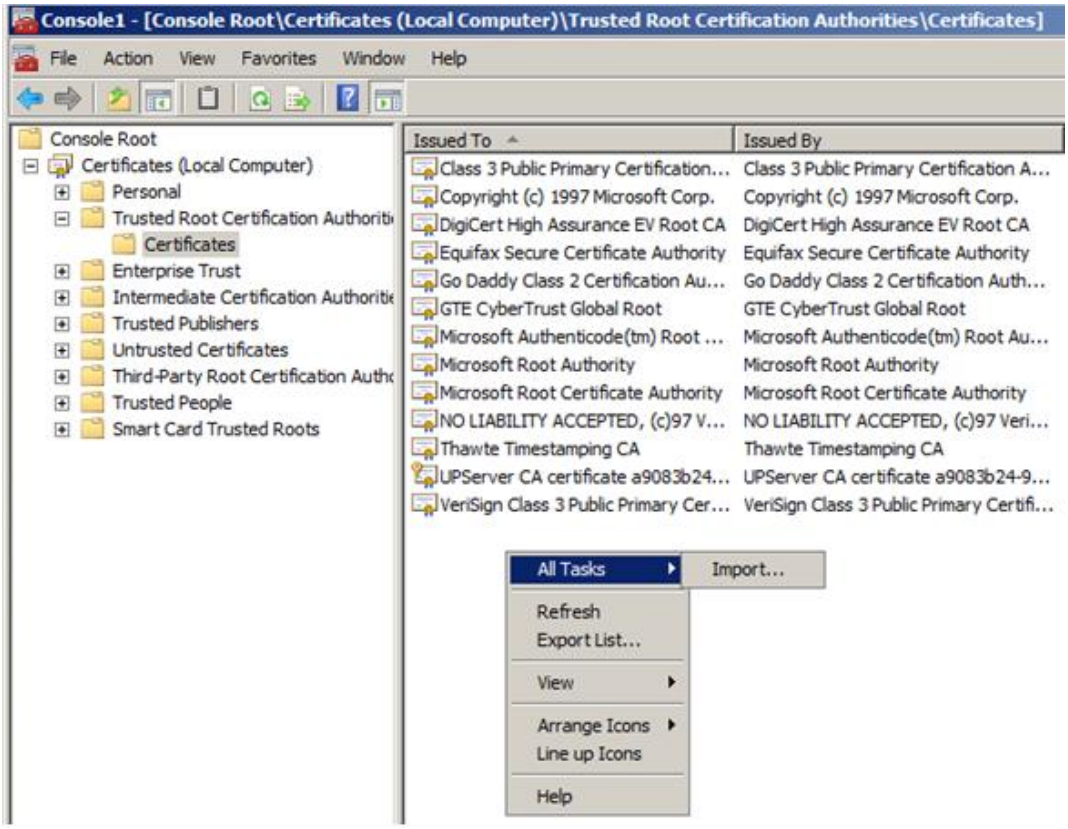

Рисунок 56

Шаг 3: Откроется Мастер импорта сертификатов – **Certificate Import Wizard,** нажмите Next > (Рисунок 57).

Рисунок 57

Шаг 3: В следующем окне нажмите кнопку Browse для выбора переносимого контейнера (Рисунок 58).

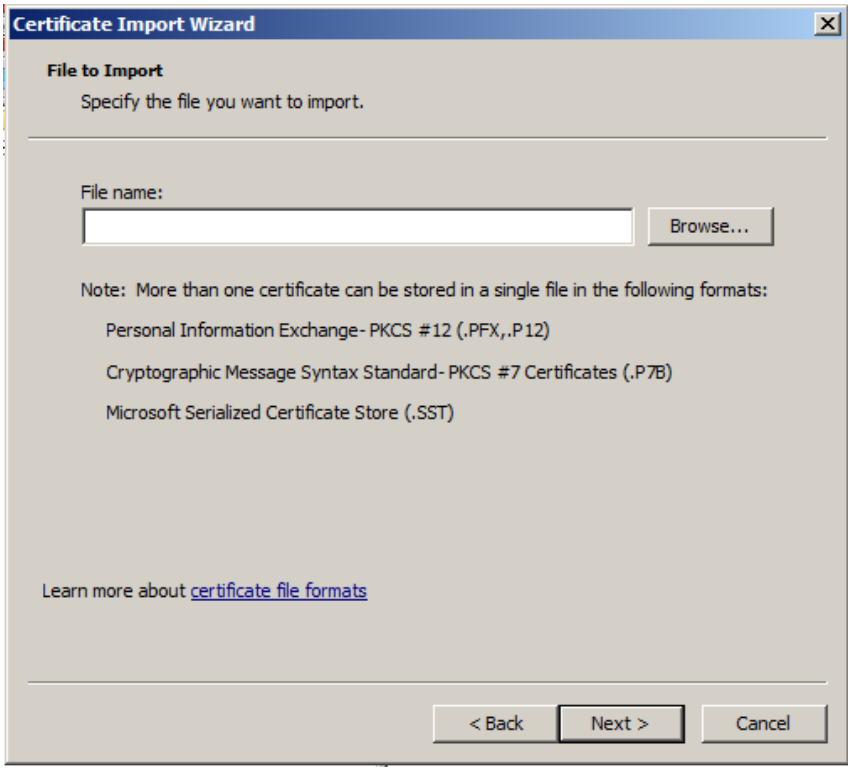

Рисунок 58

Шаг 4: Укажите путь до файла с сертификатом, а также в поле задания формата укажите **Personal Information Exchange** (*.pfx, *.p12), либо **All Files** (*.*) и выберите нужный сертификат. Нажмите кнопку Open (Рисунок 59).

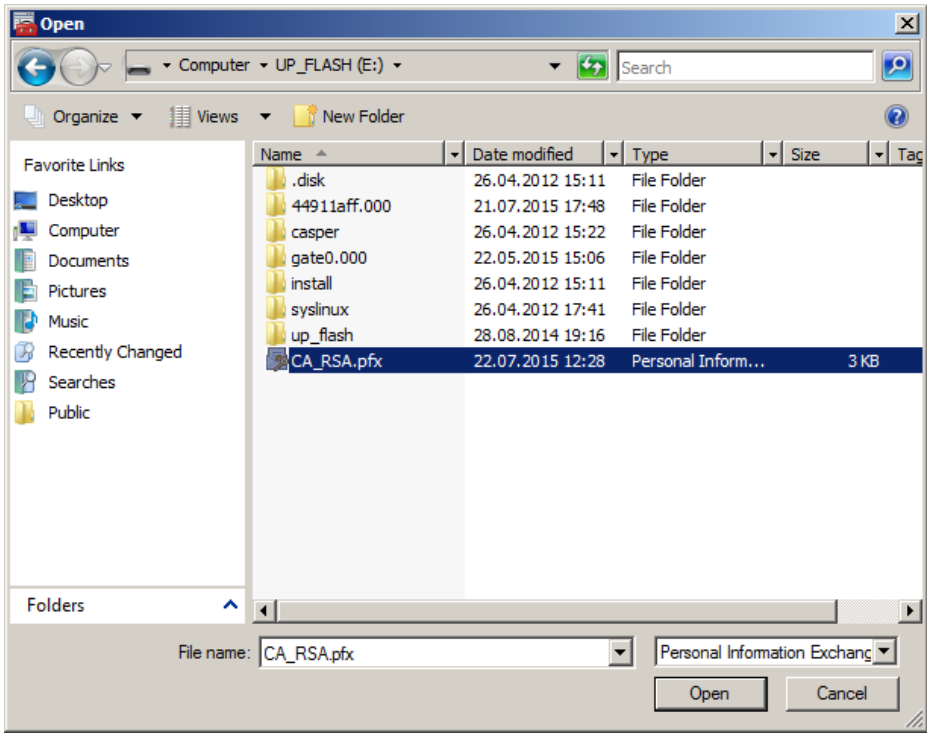

Рисунок 59

Шаг 5: Проверьте правильность указанного имени файла в следующем окне и нажмите Next > (Рисунок 60).

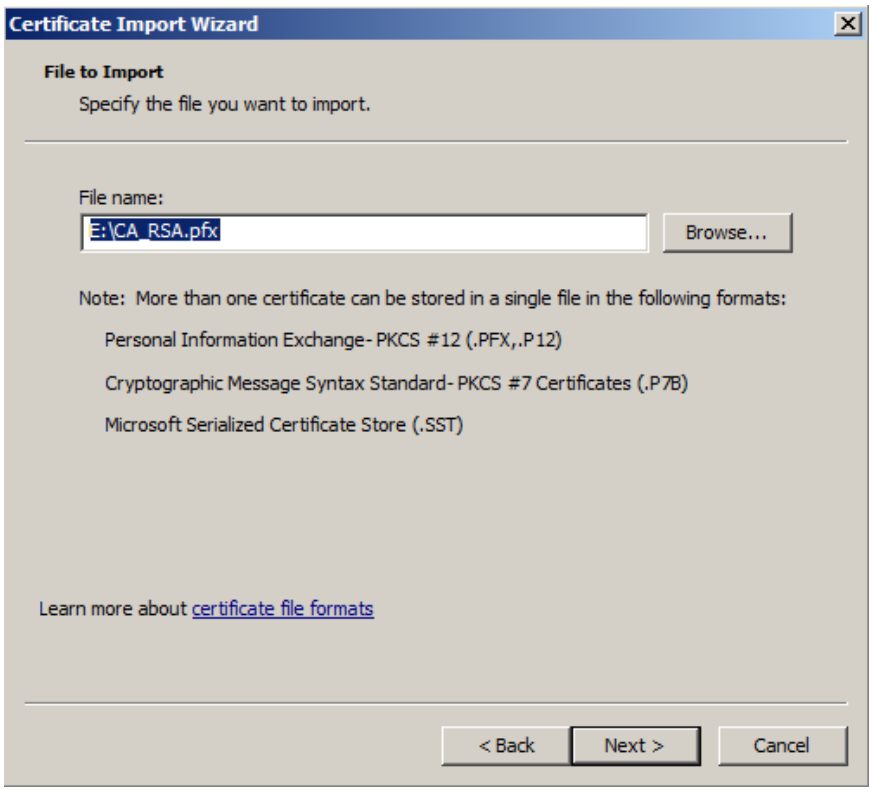

Рисунок 60

Шаг 6: Введите пароль на импортируемый контейнер с сертификатом и ключом, Next > (Рисунок 61).

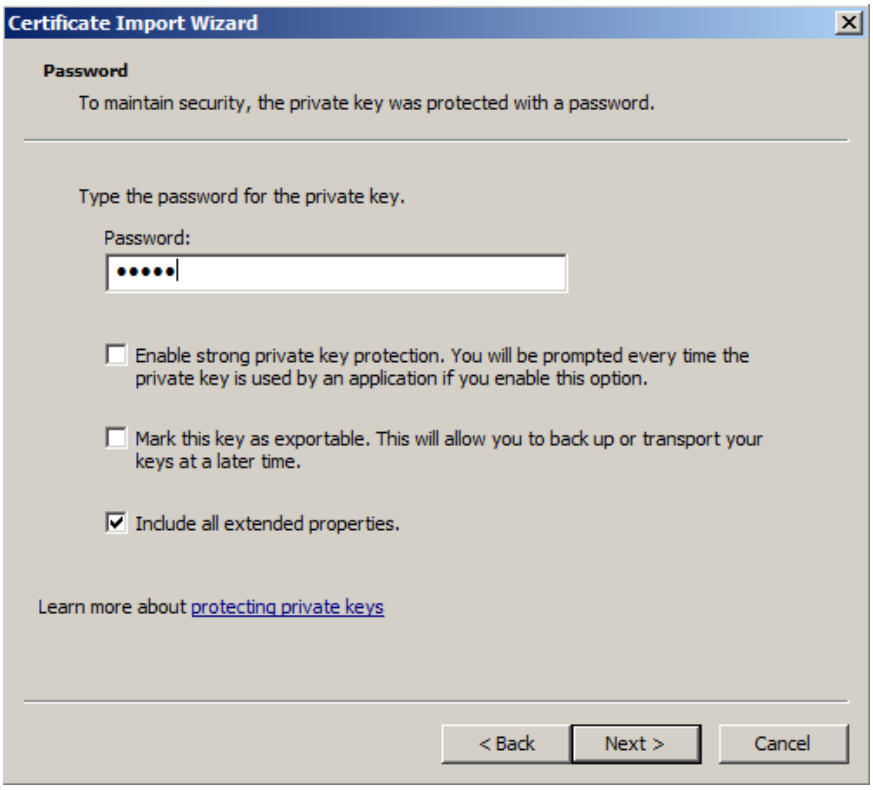

Рисунок 61

Шаг 7: В окне выбора хранилища сертификатов проверьте правильность указанной директории – **Trusted Root Certification Authorities** и нажмите Next > (Рисунок 62).

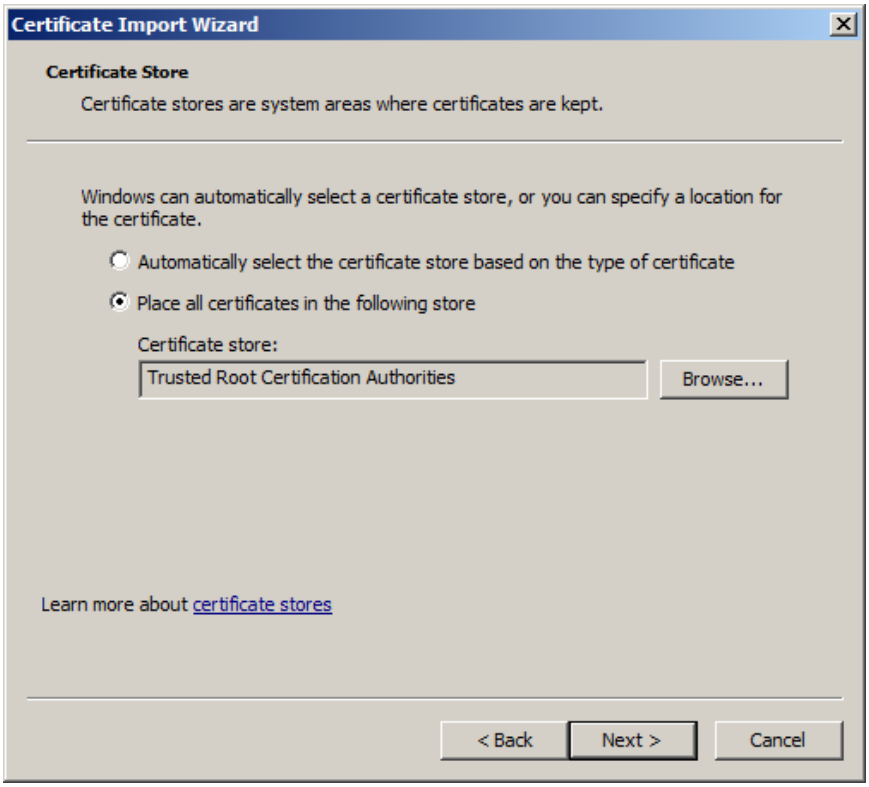

Рисунок 62

Шаг 8: Подтвердите завершение операции импорта, нажав Finish (Рисунок 63).

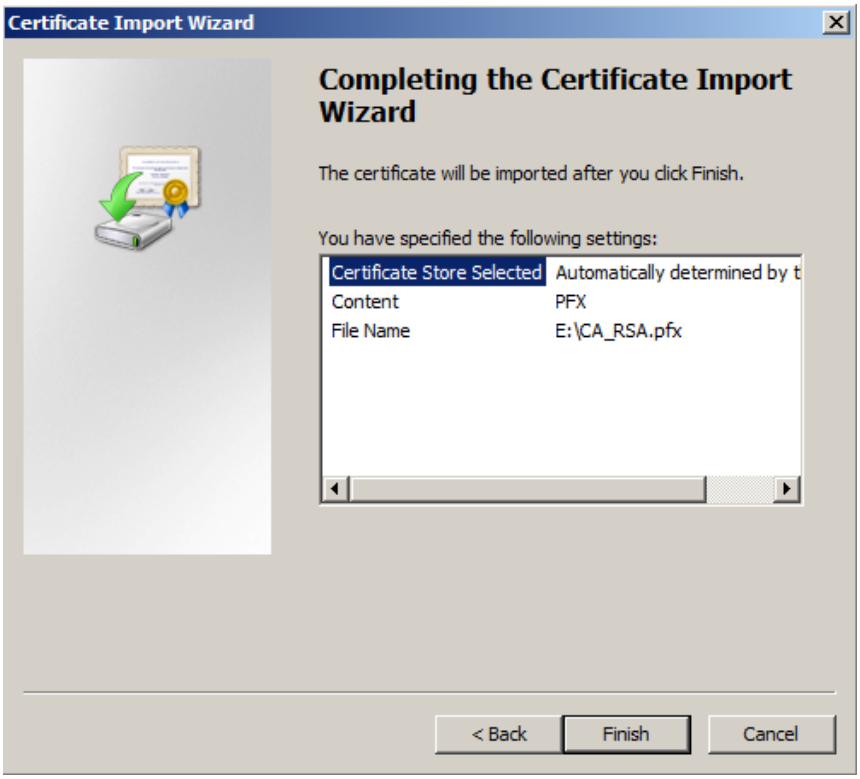

Рисунок 63

Шаг 9: Подтвердите установку CA сертификата в выбранную директорию, нажав Yes (Рисунок 64). Успешное завершение операции (Рисунок 65).

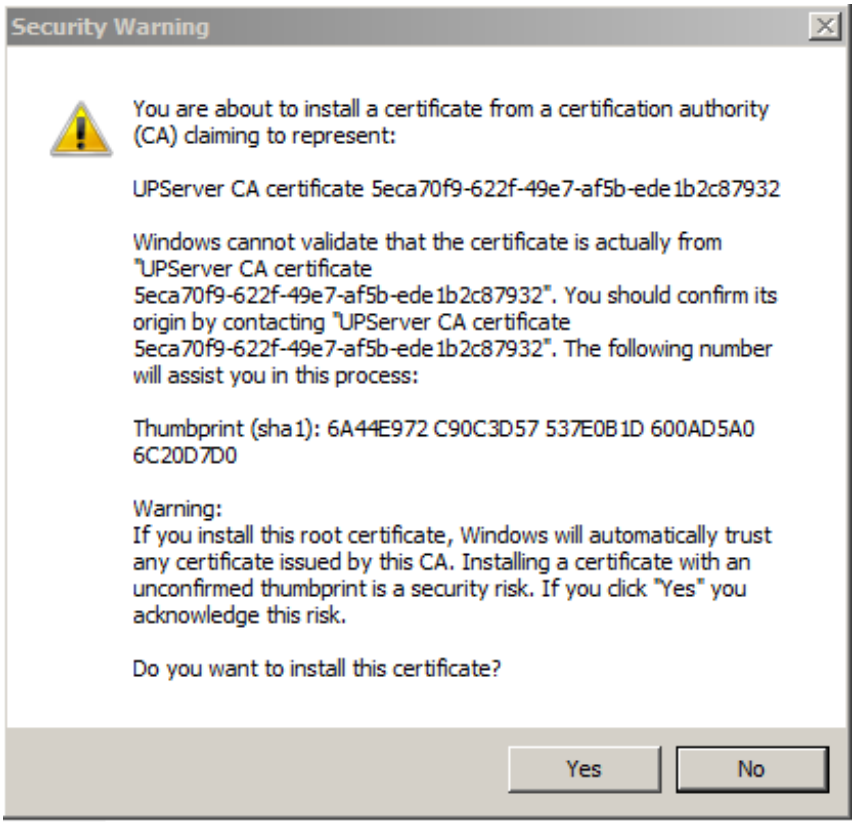

Рисунок 64

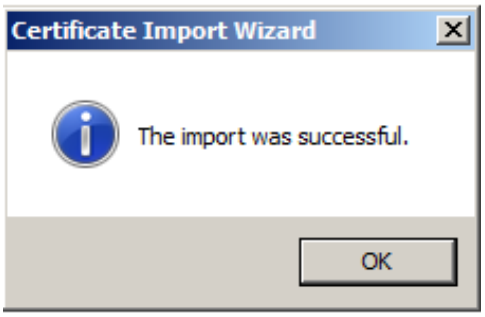

Рисунок 65

Процедура импорта CA-сертификата и секретного ключа завершена.

Процедура переноса рабочего сертификата Сервера управления и секретного ключа к нему аналогична вышеописанной для CA сертификата, однако, путь хранения рабочего сертификата несколько отличается **– Certificates - Personal – Certificates**, поэтому опишем отличающиеся Шаги 2 и 7.

Шаг 2: В окне консоли с добавленной оснасткой в левой области выберите **Certificates – Personal – Certificates**. При этом справа появится список сертификатов, лежащих в указанной директории. Правой кнопкой мыши кликните на пустом месте в этой области и выберите **All Tasks – Import…**(Рисунок 66).

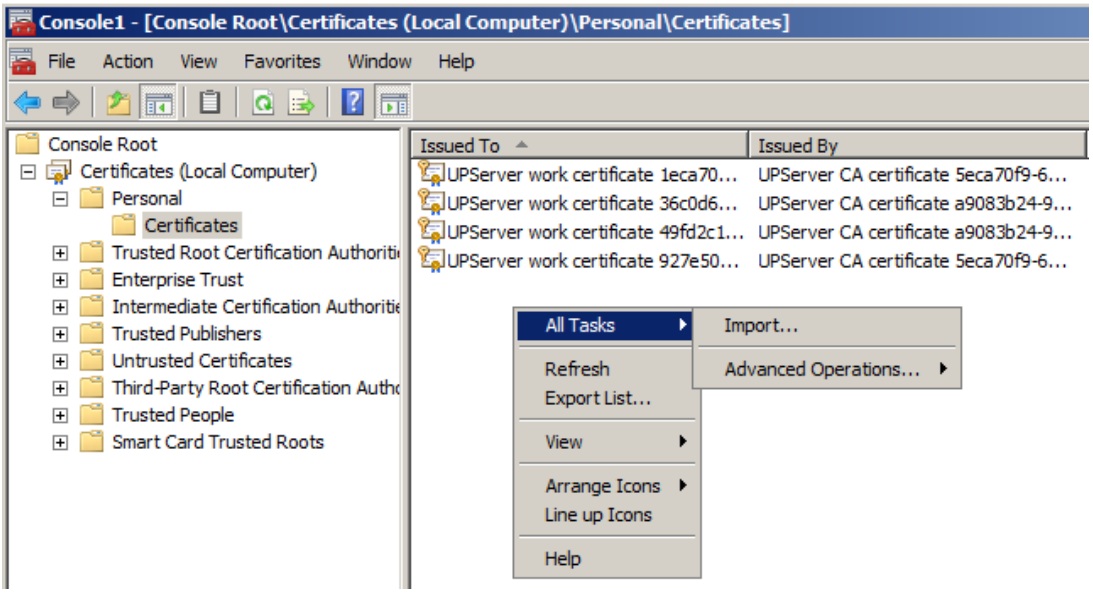

Рисунок 66

Шаг 7: В окне выбора хранилища сертификатов проверьте правильность указанной директории – **Personal** и нажмите Next > (Рисунок 67).

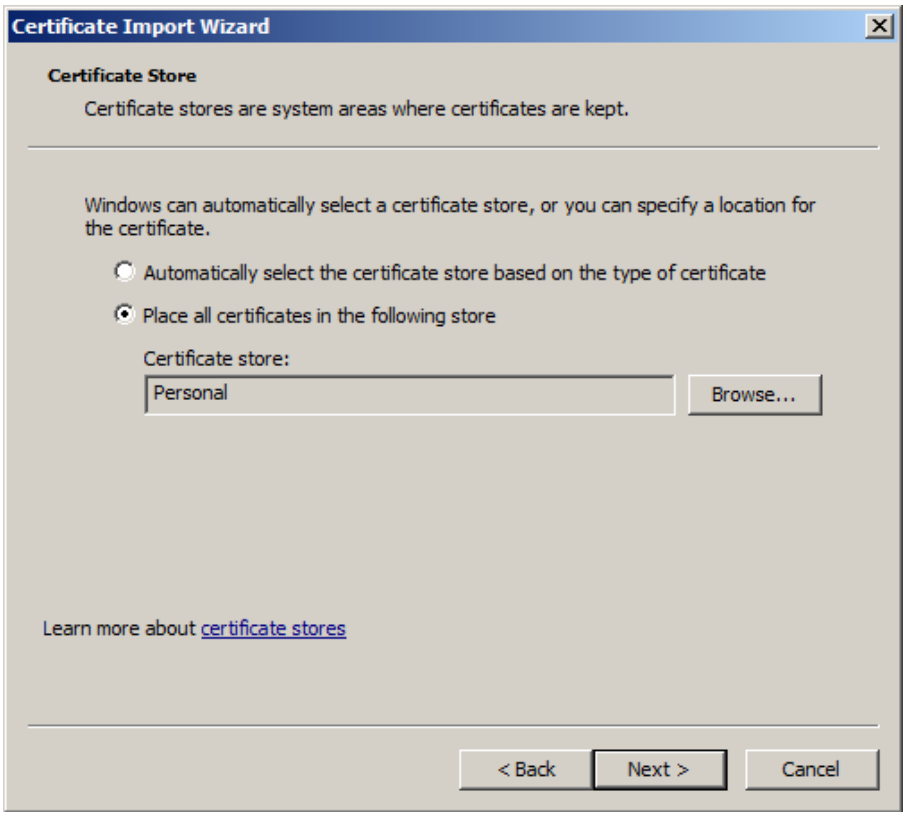

Рисунок 67

Процесс переноса Сервера управления на новый ПК завершен.