

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 резервному копированию и восстановлению Сервера управления

РЛКЕ.00009-03 90 01

17.04.2015

Содержание

1. Резервное копирование данных Сервера управления.....	3
1.1. Экспорт контейнеров к ГОСТ-сертификатам.....	5
2. Восстановление Сервера управления.....	12
2.1. Импорт контейнеров к ГОСТ-сертификатам.....	12

1. Резервное копирование 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 1).

```
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\00000000cacert.cer
Compressing clients\client01\updates\00000000id.txt
Compressing clients\client01\updates\00000000num.txt
Compressing clients\client01\updates\00000000settings.txt
Compressing clients\client01\updates\00000000setup_product.exe
Compressing clients\client01\updates\00000000setup_upagent.exe
Compressing clients\client01\updates\00000000start.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 backedup successfully to file C:\backup01.bin
c:\Program Files\S-Terra\S-Terra KP>
```

Рисунок 1



Подробное описание использования утилиты `upmgr.exe` приведено в разделе «Управление с использованием командной строки» [Руководства администратора C-Терра КП](#).

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

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

Кроме описанных выше шагов, можно задать выполнение резервного копирования, например, через Task Scheduler с определенным интервалом сохранения копий в указанную директорию. Для этого предварительно создается файл `backup.bat` следующего содержания:

```
@set todaysdate=%date:~10,4%_%date:~4,2%_%date:~7,2%  
"C:\Program Files (x86)\S-Terra\S-Terra КР\upmgr.exe" backup -f  
c:\backup\%todaysdate%
```

После этого выполнить Server Manager – Configuration – Task Scheduler – Create Task, задать имя и расписание задачи, во вкладке Action прописать путь до файла backup.bat.

В результате резервное копирование данных Сервера управления будет производиться с определенной частотой и записываться в zip-файлы с датой в имени в директорию C:\backup.

Для экспортирования контейнеров сертификатов Сервера управления на USB-флеш перейдите к разделу [«Экспорт контейнеров к ГОСТ-сертификатам»](#).

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 **Configure readers...** (Рисунок 2).

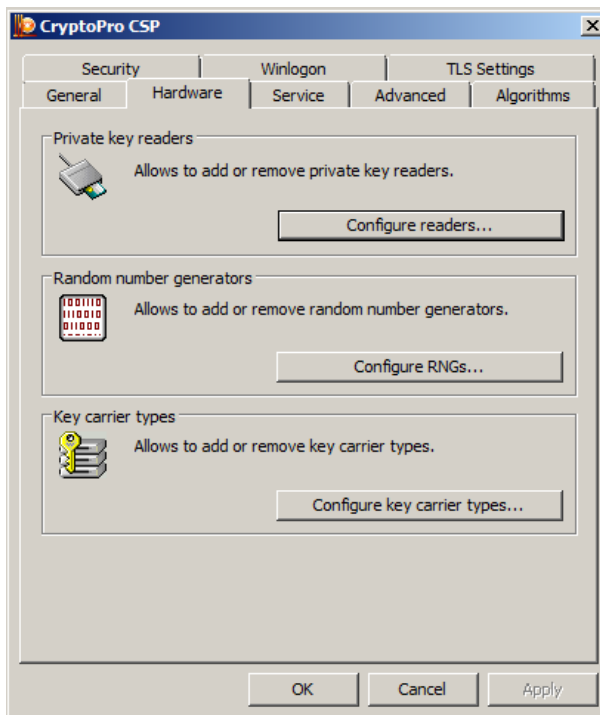


Рисунок 2

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

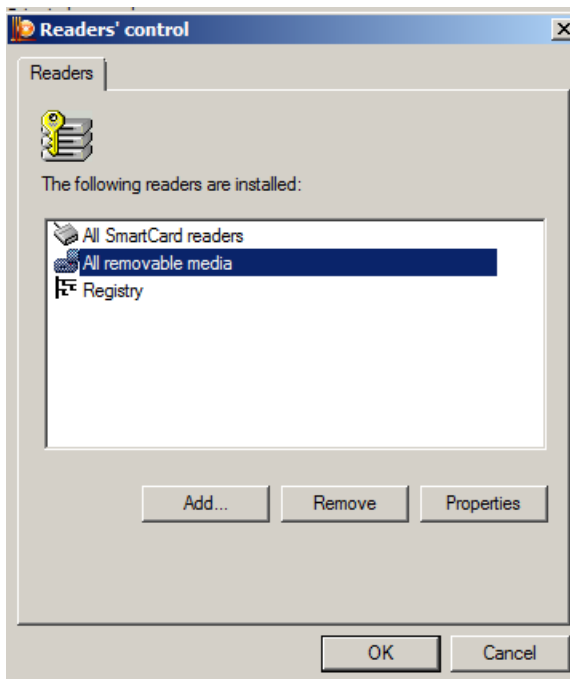


Рисунок 3

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

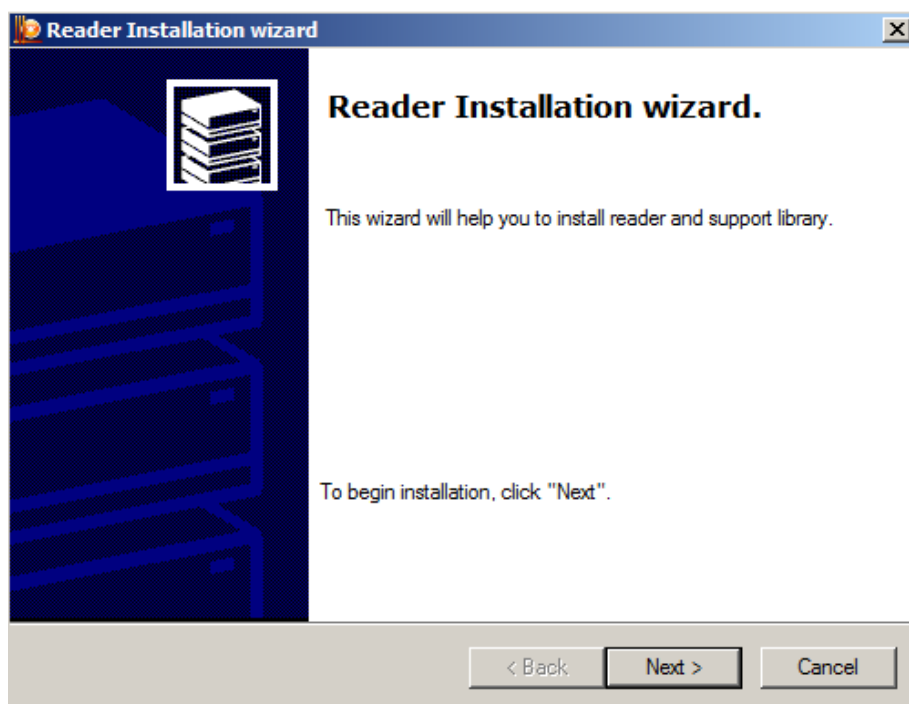


Рисунок 4

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

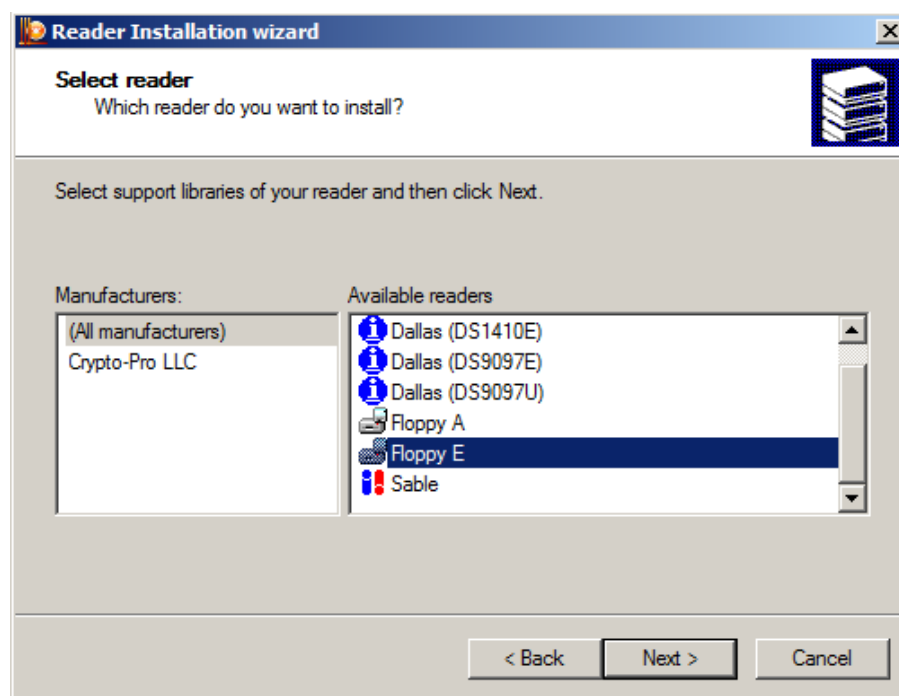


Рисунок 5

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

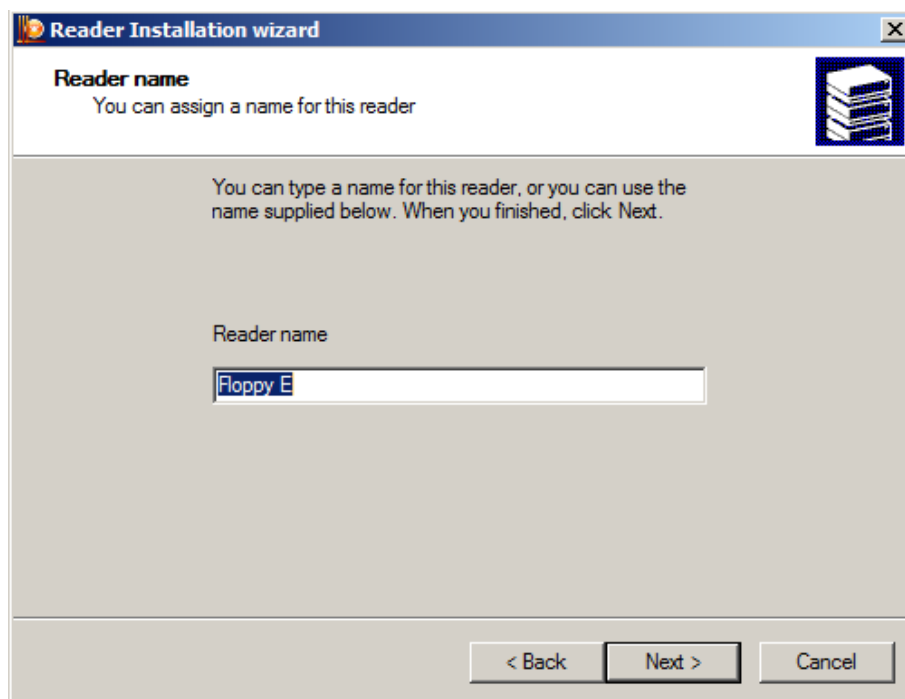


Рисунок 6

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

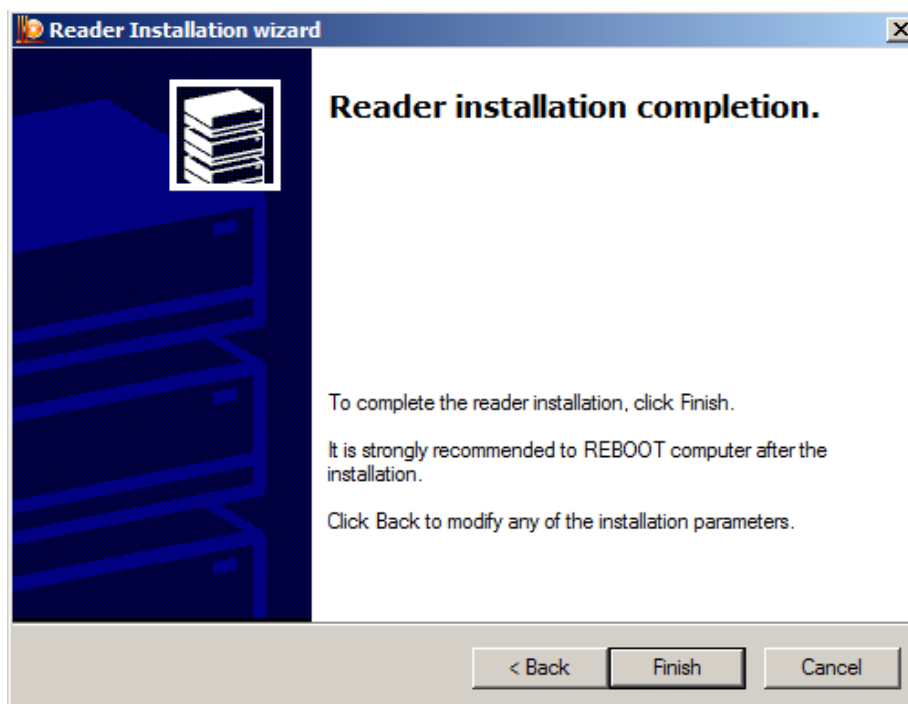


Рисунок 7

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

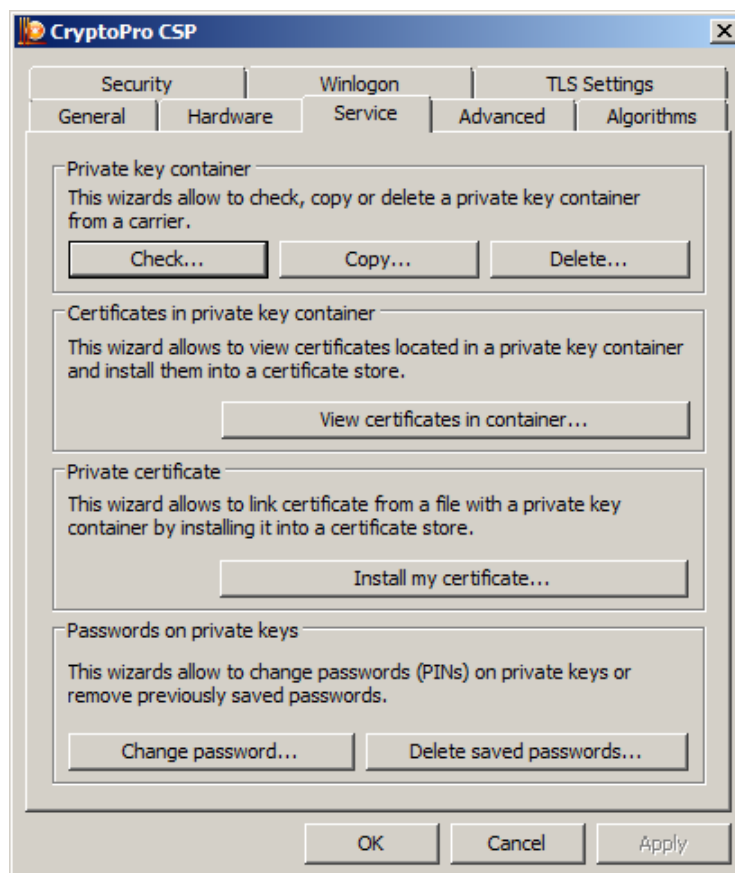


Рисунок 8

Шаг 9: В появившемся окне поставьте переключатель в положение **Computer** и нажмите **Browse...** (Рисунок 9), выберите необходимый контейнер CA сертификата, размещенный в реестре (Рисунок 10).

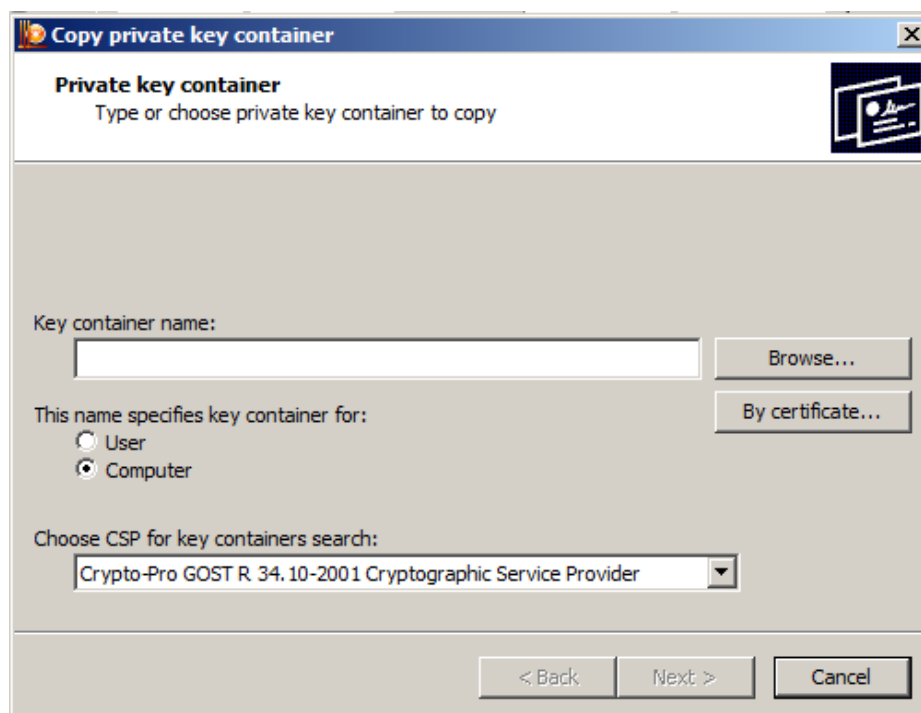


Рисунок 9

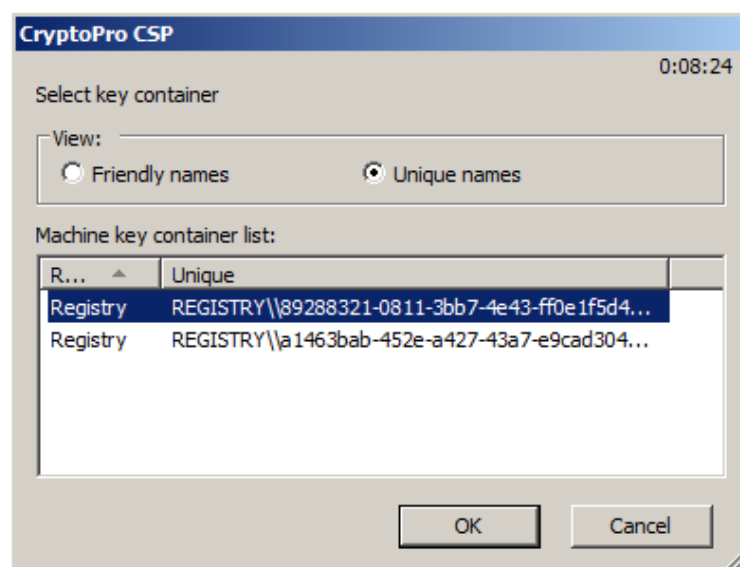


Рисунок 10

Шаг 10: Нажмите кнопку **Next >** (Рисунок 11).

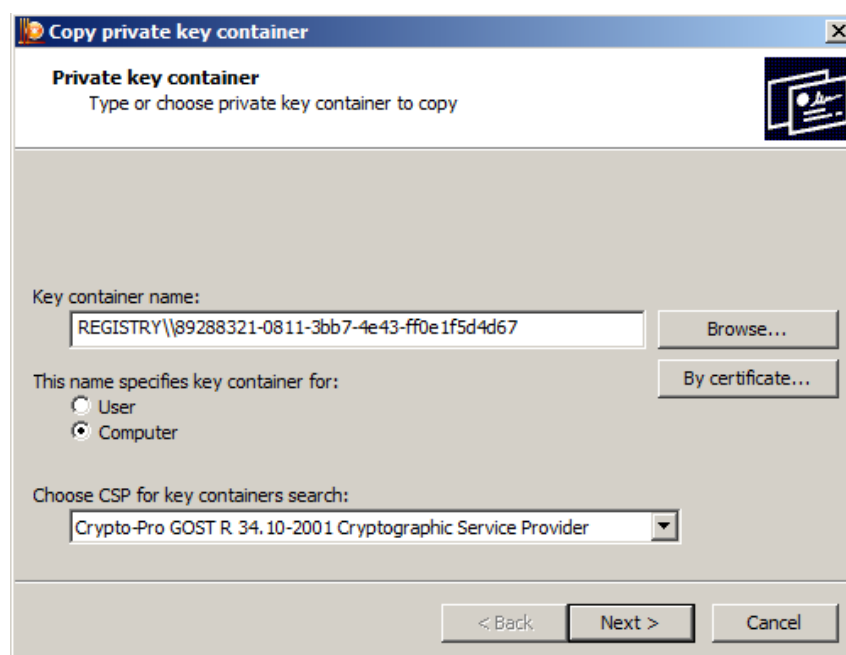


Рисунок 11

Шаг 11 Введите пароль на контейнер с секретным ключом, который задавался при создании СА-сертификата на Сервере управления (Рисунок 12).

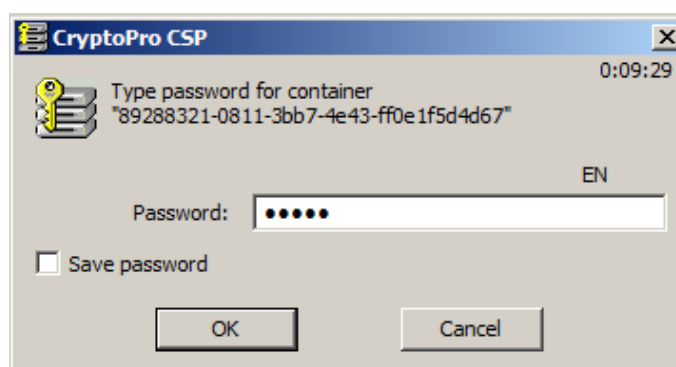


Рисунок 12

Шаг12: В появившемся окне введите имя нового контейнера, в который будет скопирован секретный ключ СА-сертификата, нажмите **Finish** (Рисунок 13).

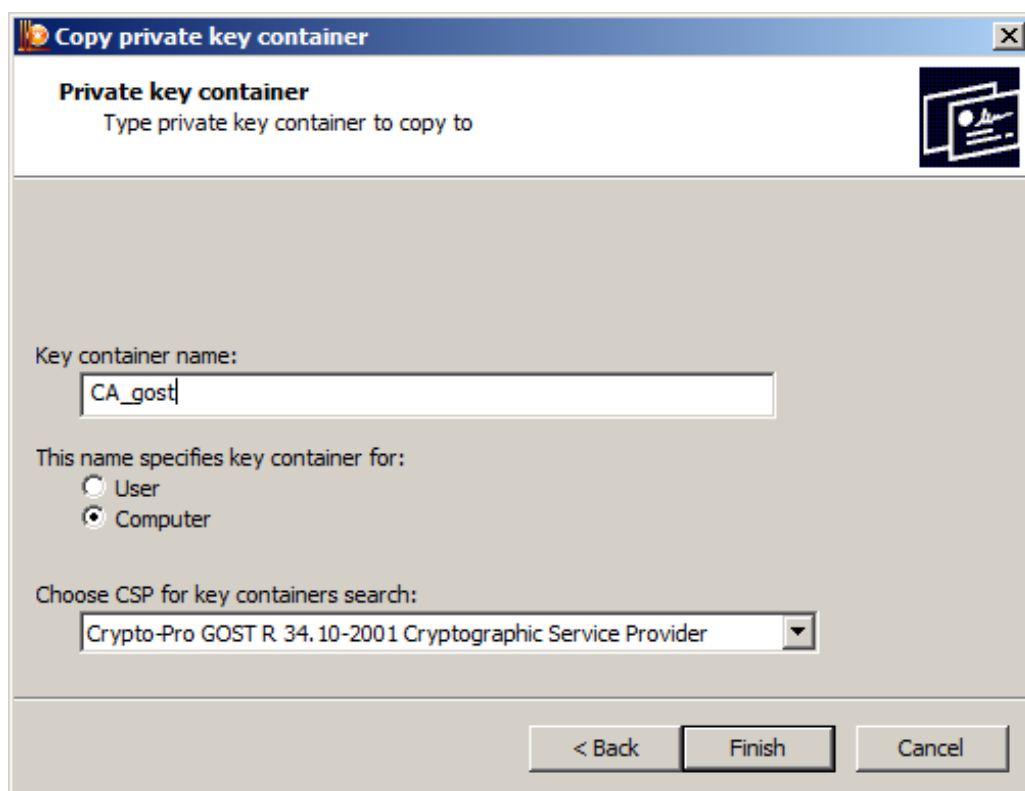


Рисунок 13

Шаг 13: Выберите ключевой носитель для нового контейнера – USB-флеш, нажмите **OK** (Рисунок 14).

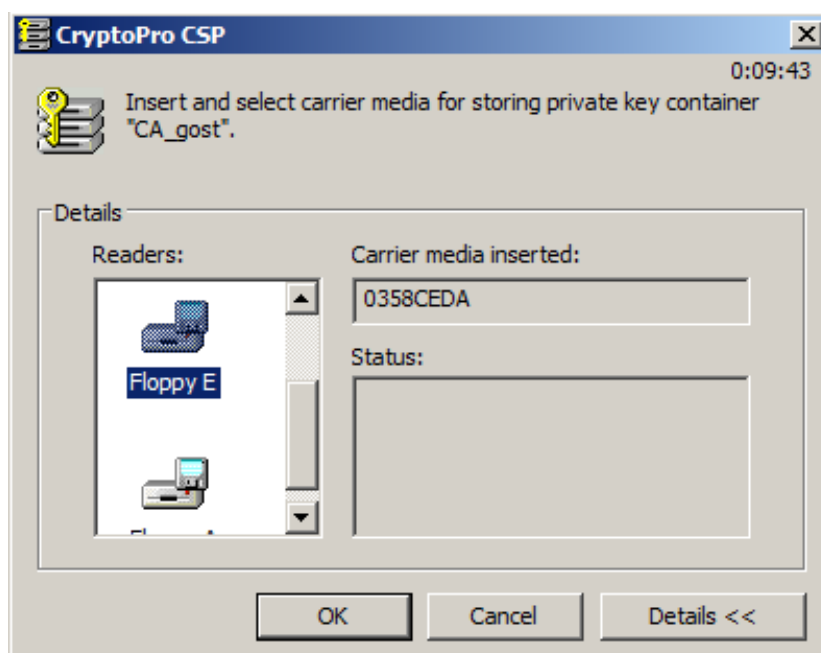


Рисунок 14

Шаг 14: Установите пароль на новый контейнер, нажмите **OK** (Рисунок 15).

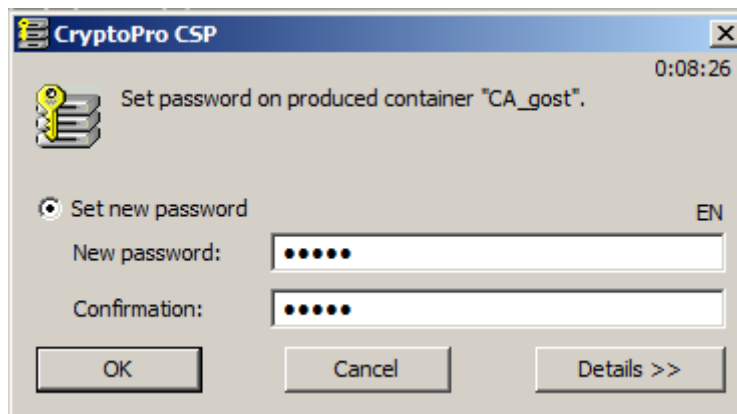


Рисунок 15

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



Экспортировать рабочий сертификат необязательно. Впоследствии, после восстановления СА-сертификата на новом ПК, можно заново создать рабочий сертификат, нажав кнопку **Renew** в группе Work certificate вкладки Settings Сервера управления.

Далее перейдите к разделу [«Восстановление Сервера управления»](#).

2. Восстановление Сервера управления

На новом (восстанавливаемом) 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» (подробнее про установку – раздел «Установка Сервера управления» [Руководства администратора](#)), для восстановления всех сохраненных настроек Сервера управления, сертификатов, учетных записей управляемых устройств выполните следующие процедуры.

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

Шаг 2: Из консоли запустите команду для восстановления настроек (Рисунок 16), 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.

```
C:\Program Files\S-Terra\S-Terra KP>upmgr restore -f C:\backup01.bin
Locking upserver data...
Clearing C:\ProgramData\UPServerNEW

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

Processing archive: C:\backup01.bin
Extracting backup_info.txt
Everything is Ok
Size: 16
Compressed: 23083338

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

Processing archive: C:\backup01.bin
Extracting csettings.txt
Extracting filezilla.cf
Extracting regvars.txt
Extracting ssettings.txt
Extracting upserver.lic
Everything is Ok
Files: 5
Size: 5473
Compressed: 23083338

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

Processing archive: C:\backup01.bin
Extracting copy_of_upserver.log
Everything is Ok
Size: 6490
Compressed: 23083338

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

Рисунок 16

Для импортирования контейнеров сертификатов Сервера управления с USB-флеш перейдите к разделу [«Импорт контейнеров к ГОСТ-сертификатам»](#).

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 17).

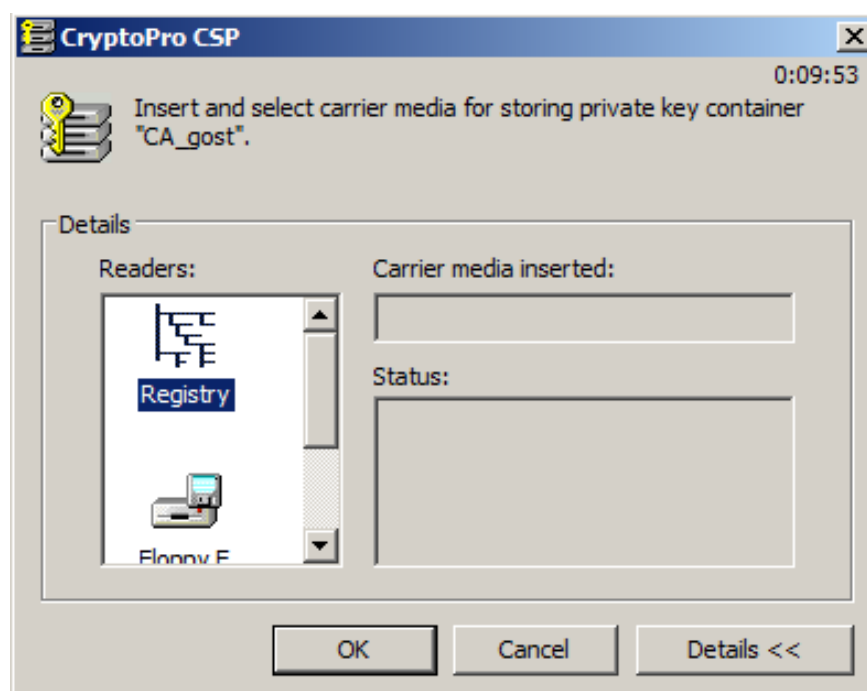


Рисунок 17

Шаг 2: Перейдите на вкладку **CryptoPro CSP – Service – Install my certificate...** (Рисунок 19).

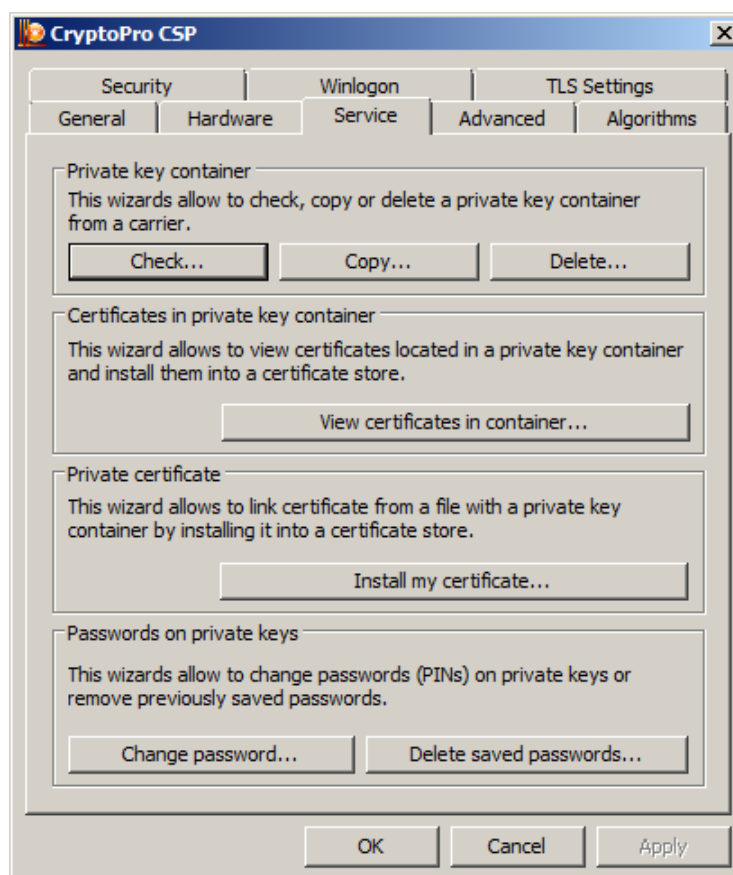


Рисунок 18

Шаг 3: В появившемся окне нажмите кнопку **Browse** для выбора перенесенных сертификатов (Рисунок 19).

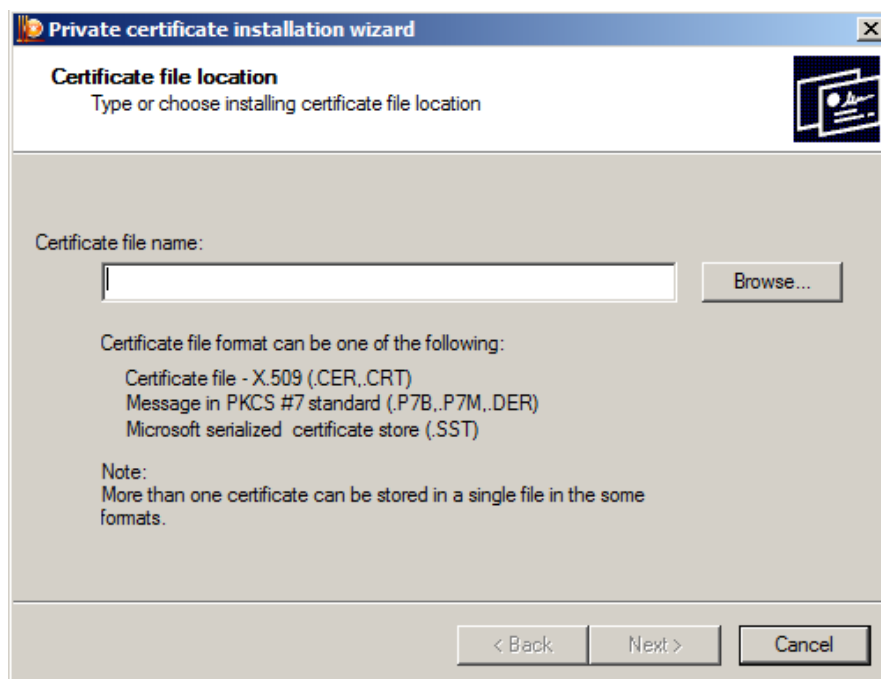


Рисунок 19

Шаг 4: В окне выбора сертификатов выберите путь до перенесенных сертификатов Сервера управления: `C:\ProgramData\UPServer\certs` (Рисунок 20). Выберите СА-сертификат и нажмите кнопку **Open**.



Рисунок 20

- Шаг 5:** Путь до СА-сертификата будет прописан в окне Мастера установки сертификата. Нажмите кнопку **Next >** (Рисунок 21).

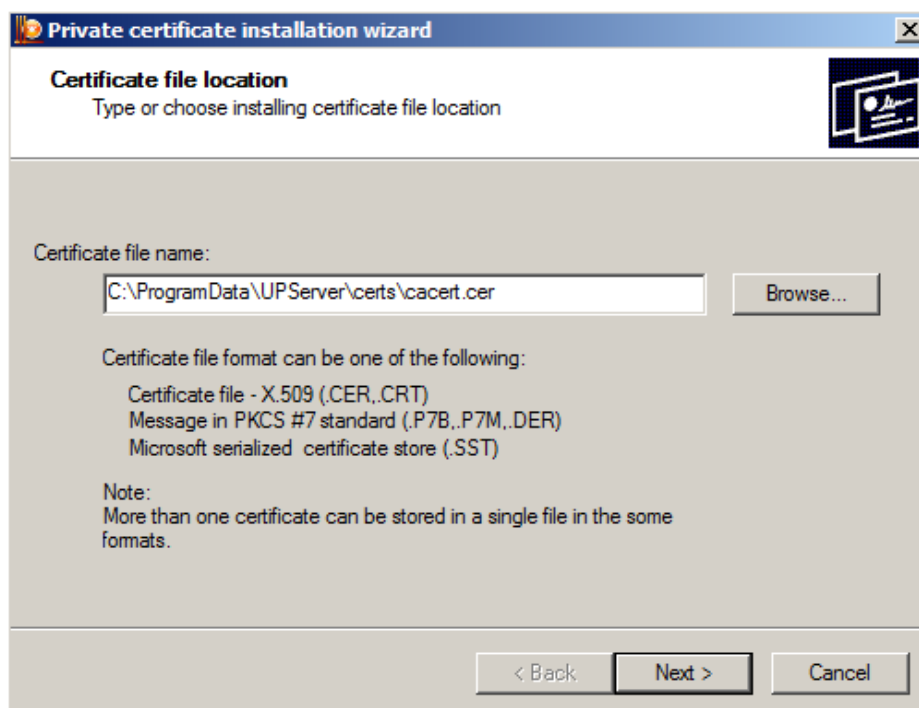


Рисунок 21

- Шаг 6:** Подтвердите данные о сертификате, нажав **Next >** (Рисунок 22).

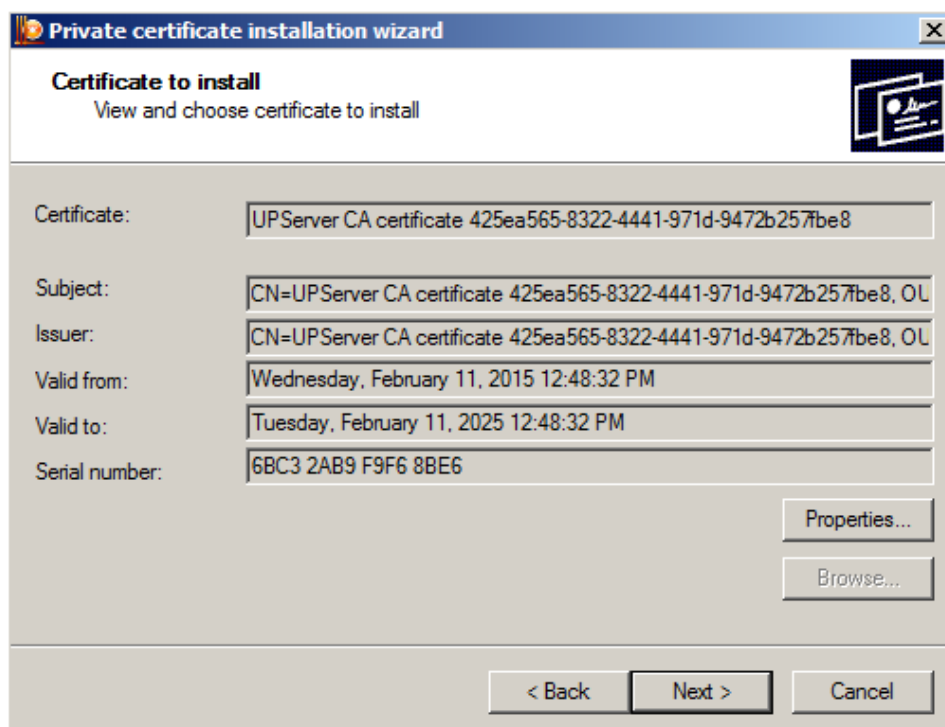


Рисунок 22

Шаг 7: В появившемся окне выбора ключевого контейнера поставьте переключатель в положение **Computer** и нажмите **Browse** (Рисунок 23).

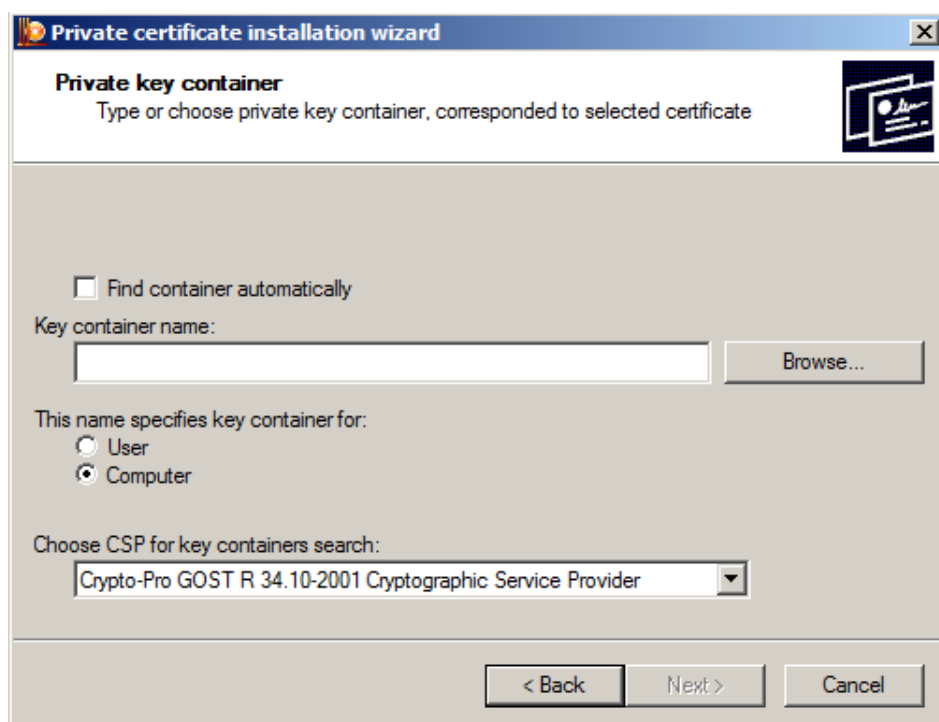


Рисунок 23

Шаг 8: Выберите скопированный ранее в Registry ключевой контейнер для данного сертификата и нажмите **OK** (Рисунок 24)..

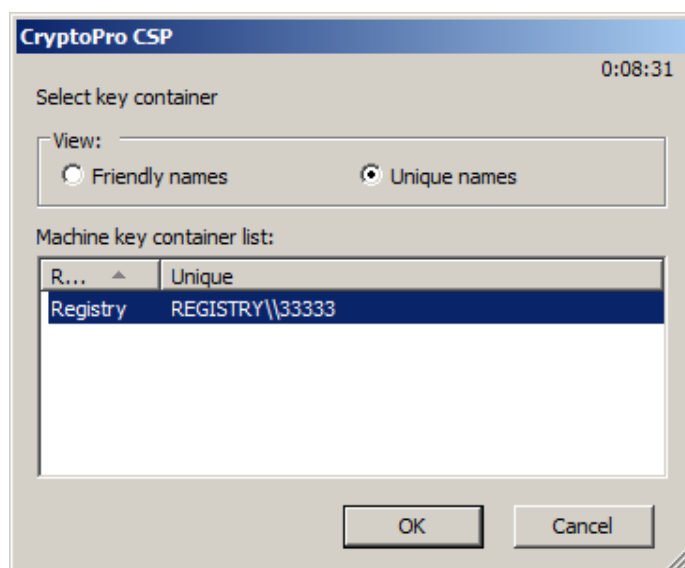


Рисунок 24

Шаг 9: После этого имя контейнера прописывается в окне Мастера установки сертификата, нажмите **Next** (Рисунок 25).

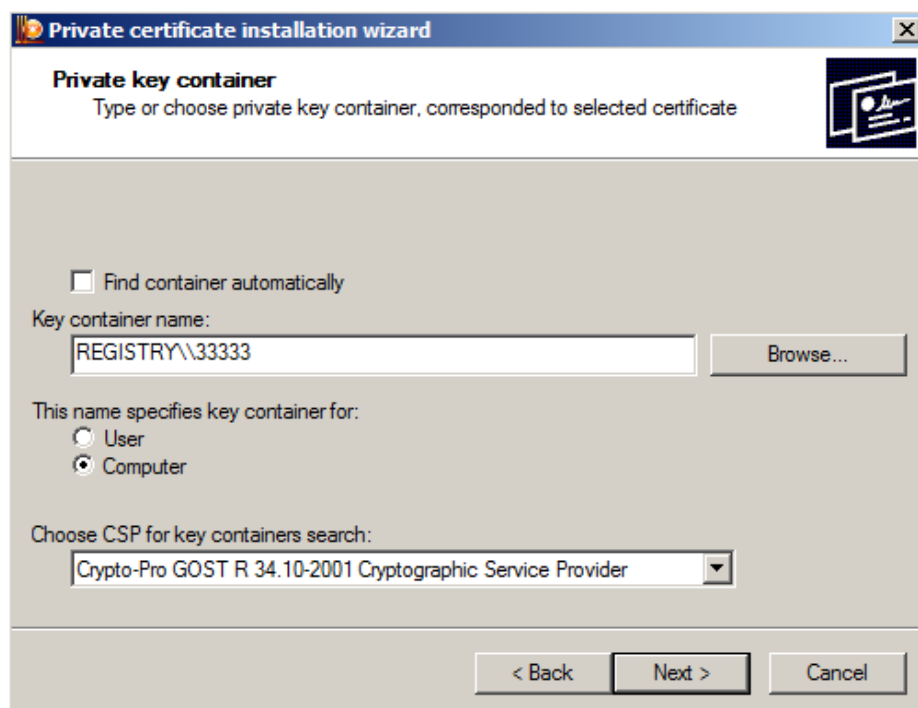


Рисунок 25

Шаг 10: Введите пароль к выбранному контейнеру, нажмите **OK**. (Рисунок 26)

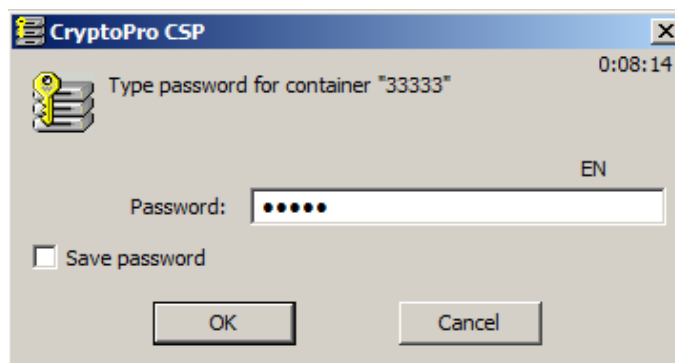


Рисунок 26

Шаг 11: В окне выбора хранилища сертификатов (Рисунок 27) при копировании СА сертификата важно указать папку корневых доверенных центров сертификации. Для этого нажмите **Browse...** и в появившемся окне выберите **Trusted root Certification Authorities** – **OK** (Рисунок 28). В следующем окне нажмите **Next >** (Рисунок 29).

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

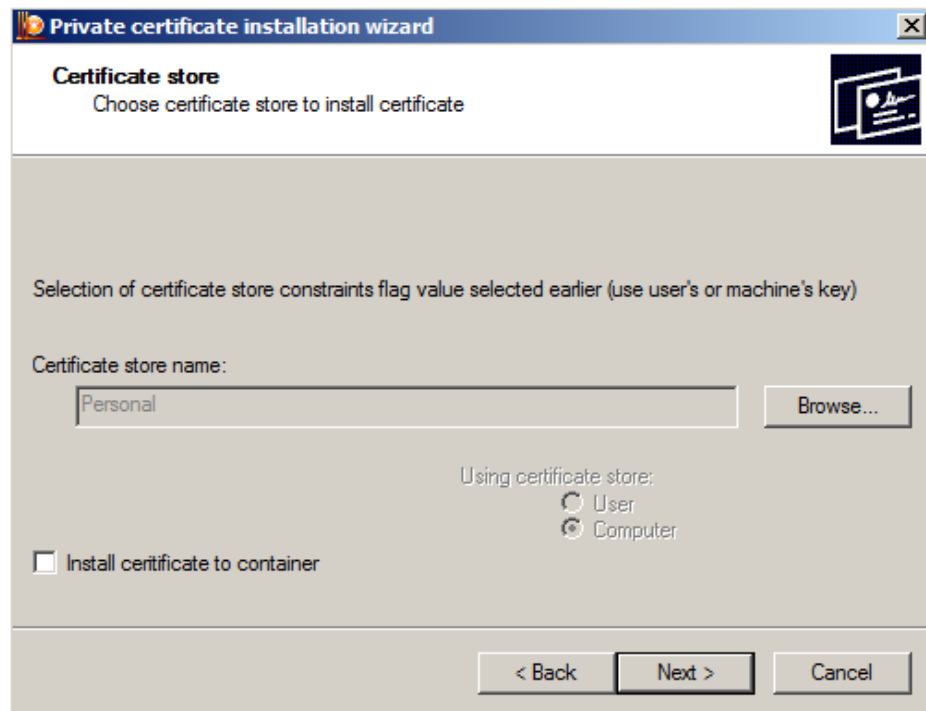


Рисунок 27

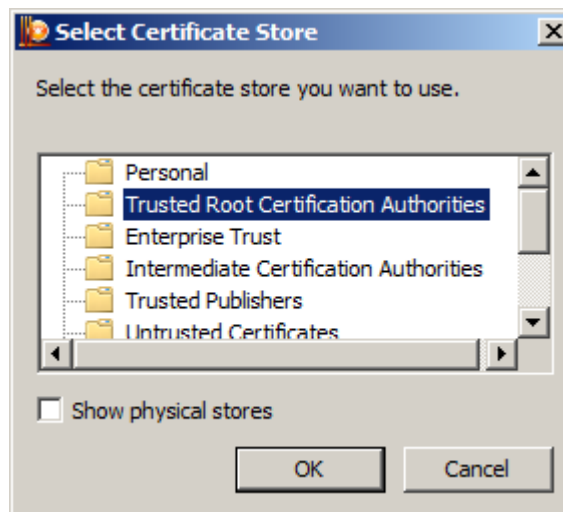


Рисунок 28

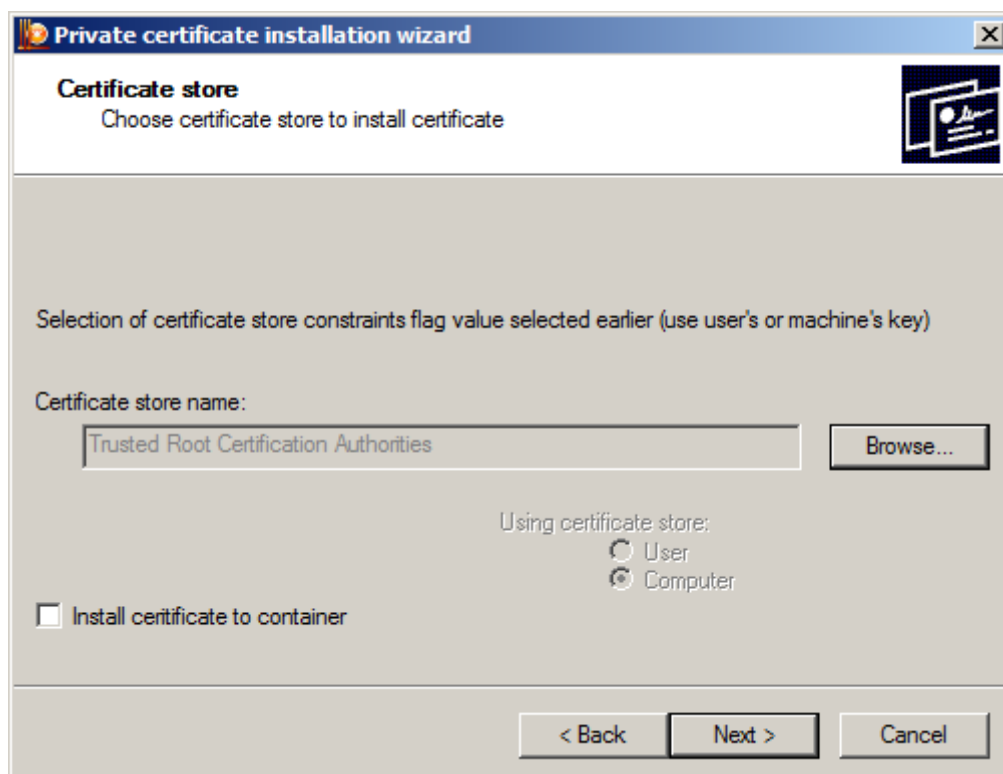


Рисунок 29

Шаг 12: Подтвердите завершение операции - **Finish** (Рисунок 30).

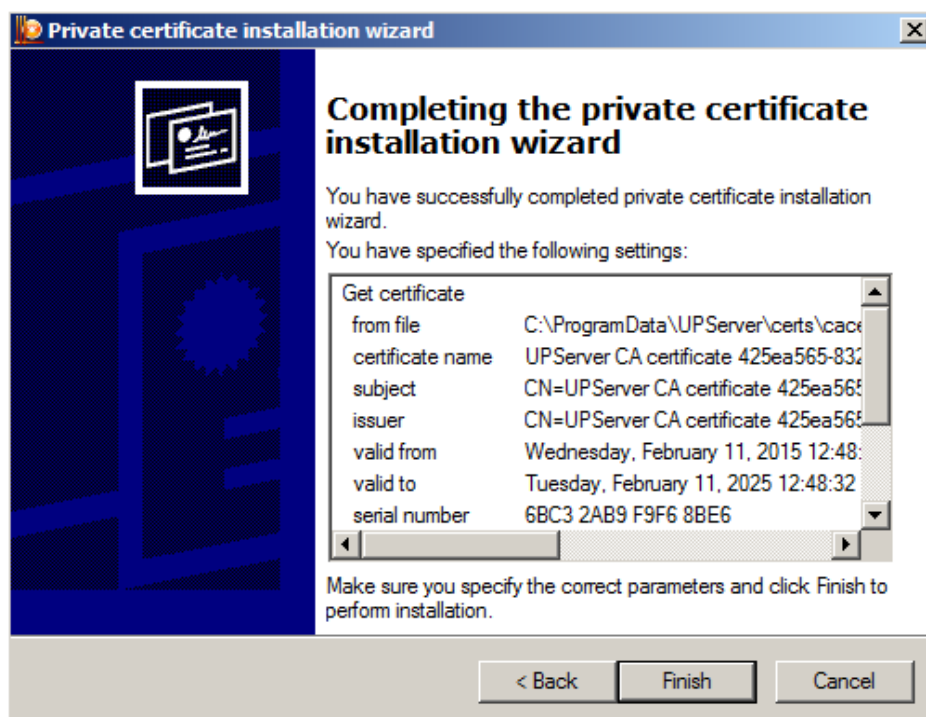


Рисунок 30

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 31).

Work certificate

Organization O= test organization

Organization Unit OU= test organization unit View...

Common Name CN= UPServer work certificate <GUID> Renew

Lifetime 12 months Import...

Рисунок 31

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 32).

Field	Value
Version	3
Serial number	40 9E E1 31 1D 08 42 54
Signature algorithm	GOST_R_341001_3411 (Crypto-Pro)
Issuer	CN=UPServer CA certificate 4f90ecd6-bbc0-40cc-977e-...
Valid from	Thu Mar 12 10:34:07 2015
Valid to	Sat Mar 12 10:34:07 2016
Subject	CN=UPServer work certificate 3842b333-bdf0-41ff-b1c3...
Public key	GOST R 341001(512)
Alt-subject	<None>
Hash MD5	47 C3 C2 0F C3 87 CC A9 73 39 EF C5 A3 F4 E8 E2
Hash SHA1	42 F3 55 CA 2E 4D 87 6B 71 80 EB A4 EA 1A D3 EB 8C 5...

Key container name \\.\REGISTRY\REGISTRY\\44444

Key container password *****

Save as... OK Cancel

Рисунок 32



Если рабочий сертификат не был экспортирован, его необходимо создать заново, нажав кнопку [Renew](#) в группе Work certificate вкладки Settings Сервера управления.

Процесс восстановления Сервера управления завершен.