

**РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ**  
по настройке рабочего места для корректной работы с  
ключами электронной цифровой подписи и  
сертификатами ключей подписи выпущенными  
удостоверяющим центром ОГИЦ

## 1 Общие сведения для пользователей

1.1 В Росинформтехнологии Вы получили конверт, который содержит:

- ключевой носитель с ключами электронной цифровой подписи (ЭЦП) и сертификатом ключа подписи;

- ПИН-код доступа к ключевому носителю (8 цифр);

- ключевую фразу для обращения в удостоверяющий центр и управления сертификатом ключа подписи в случае компрометации закрытого ключа ЭЦП (отзыв, приостановлении/возобновление действия).

1.2 Ключевой носитель содержит контейнер закрытого ключа. Необходимо обязательно:

- хранить в тайне закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, модифицирования или несанкционированного использования;

- не использовать закрытый ключ ЭЦП, если Вам стало известно, что эти ключи используются или использовались ранее другими лицами;

- немедленно обратиться в службу технической поддержки УЦ ОГИЦ для отзыва сертификата ключа подписи в случае, если Вам стало известно, что эти ключи используются или использовались ранее другими лицами.

1.3 ПИН-код доступа к ключевому носителю должен быть известен только Вам. При каждом обращении к контейнеру закрытого ключа средство криптографической защиты информации (СКЗИ) КриптоПро CSP будет требовать ввода данного ПИН-кода.

После установки СКЗИ КриптоПро CSP Вы можете поменять ПИН-код. Для этого запустите КриптоПро CSP (Пуск ---> Настройки ---> Панель управления ---> КриптоПро CSP), перейдите на вкладку «Сервис», нажмите кнопку «Изменить пароль» и следуйте указаниям КриптоПро CSP.

1.4 Ключевая фраза применяется в случае компрометации закрытого ключа ЭЦП и необходимости срочного отзыва (приостановления действия) сертификата ключа подписи.

При компрометации закрытого ключа ЭЦП необходимо немедленно обратиться в службу технической поддержки, назвать свои идентификационные данные и ключевую фразу сотруднику службы технической поддержки.

## 2 Настройка рабочего места

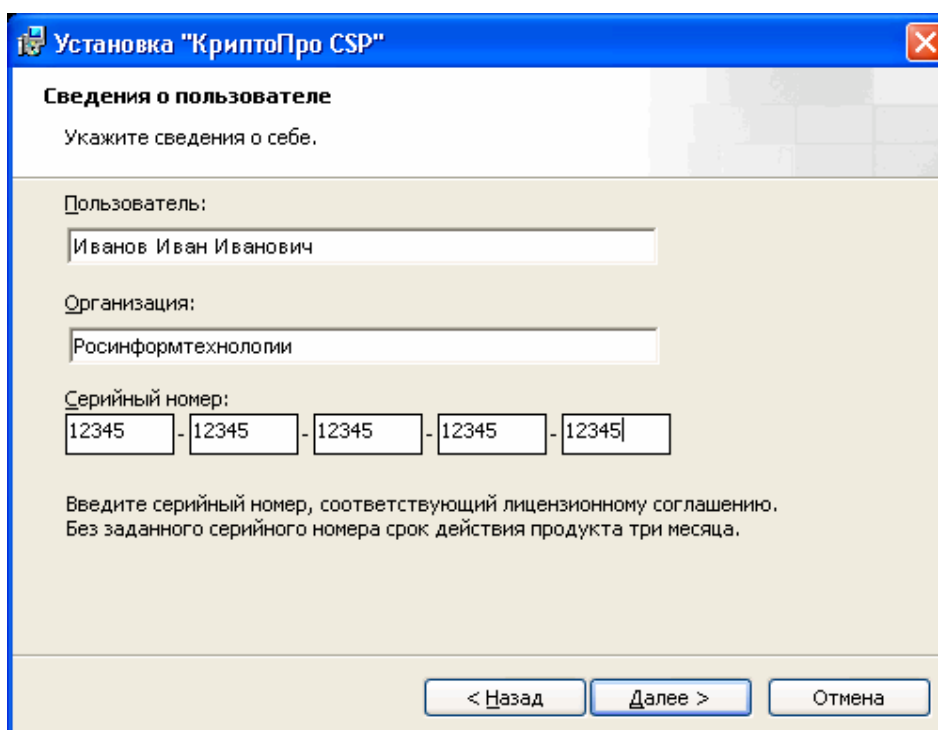
Для работы с полученными ключами ЭЦП и сертификатом ключа подписи необходимо:

2.1 Установить КриптоПро CSP версии 3.6. Для чего:

- Скачать КриптоПро CSP по ссылке <http://uc.ogic.ru/soft/csp-win32-kc1-rus.msi>;
- Запустить скаченный файл «csp-win32-kc1-rus.msi»;
- Установить КриптоПро CSP полностью соглашаясь с «Мастером установки».

В окне Сведения о пользователе введите данные с лицензионного соглашения, полученного в Росинформтехнологии (пример – рисунок 1).

*Рисунок 1. Пример заполнения сведений о пользователе.*



The screenshot shows a Windows-style dialog box titled "Установка 'КриптоПро CSP'" (Installation of 'CryptoPro CSP'). The main heading is "Сведения о пользователе" (User Information). Below the heading, it says "Укажите сведения о себе." (Specify information about yourself.).

The form contains three main sections:

- Пользователь:** (User) with a text input field containing "Иванов Иван Иванович".
- Организация:** (Organization) with a text input field containing "Росинформтехнологии".
- Серийный номер:** (Serial number) with five separate input fields, each containing "12345", separated by hyphens.

Below the input fields, there is a note: "Введите серийный номер, соответствующий лицензионному соглашению. Без заданного серийного номера срок действия продукта три месяца." (Enter the serial number corresponding to the license agreement. Without a specified serial number, the product's validity period is three months.).

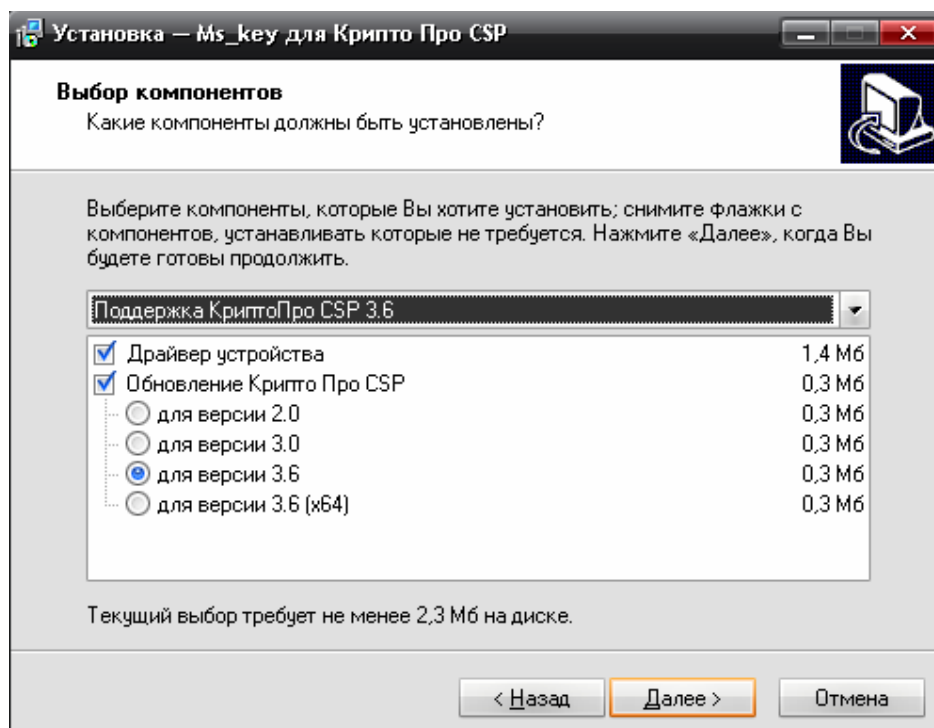
At the bottom of the dialog, there are three buttons: "< Назад" (Back), "Далее >" (Next), and "Отмена" (Cancel).

2.2 Установить драйвер для полученного ключевого носителя «MS\_Key». Для чего:

- Скачать драйвер по ссылке [http://uc.ogic.ru/soft/MS\\_Key\\_setup.exe](http://uc.ogic.ru/soft/MS_Key_setup.exe);
- Запустить скаченный файл «MS\_Key\_setup.exe»;
- Установить драйвер полностью соглашаясь с «Мастером установки».

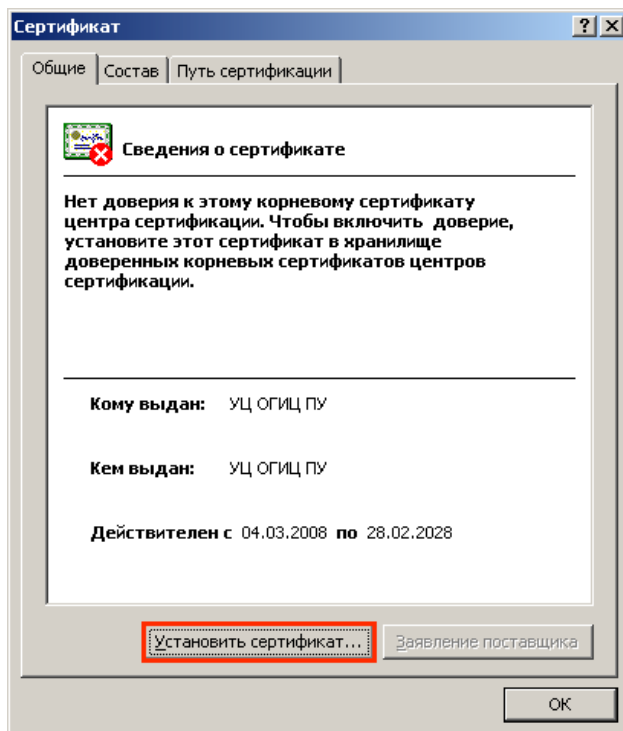
В окне **Выбор компонентов** выберите компоненты в соответствии с рисунком 2.

Рисунок 2. Выбор компонентов для установки.

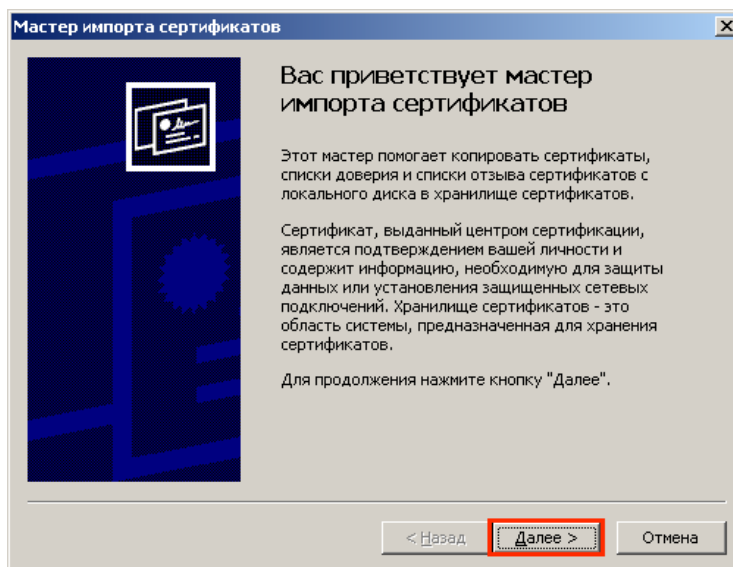


2.3 Установить сертификат уполномоченного лица удостоверяющего центра ОГИЦ первого уровня (УЦ ОГИЦ ПУ) в хранилище сертификатов «Доверенные корневые центры сертификации». Для чего:

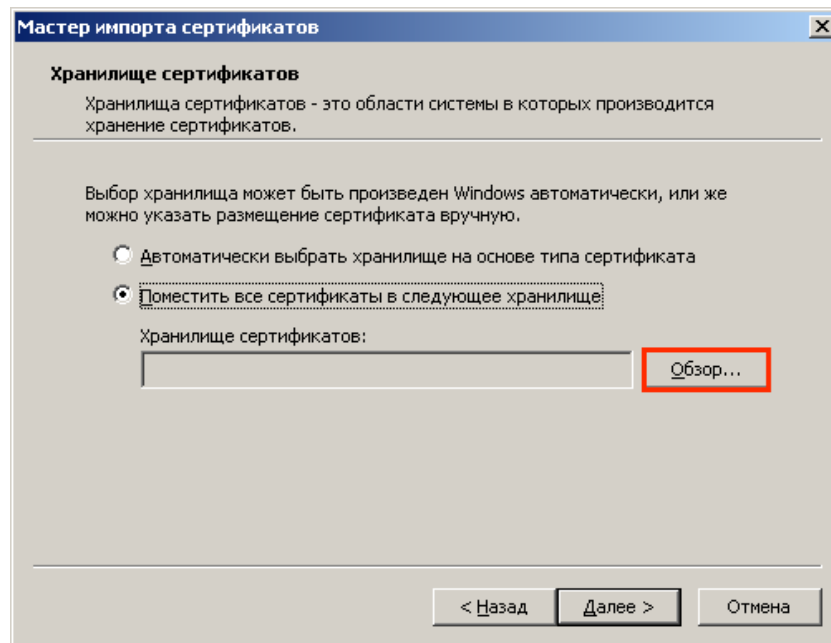
- Скачать архив с сертификатами УЦ ОГИЦ по ссылке <http://uc.ogic.ru/CERTS/OGIC.zip>. Распаковать архив на компьютер;
- Открыть сертификат уполномоченного лица УЦ ОГИЦ ПУ (дважды щелкнуть левой кнопкой мыши по файлу «UC\_OGIC\_PU.cer»);
- В появившемся окне нажать кнопку «Установить сертификат...»;



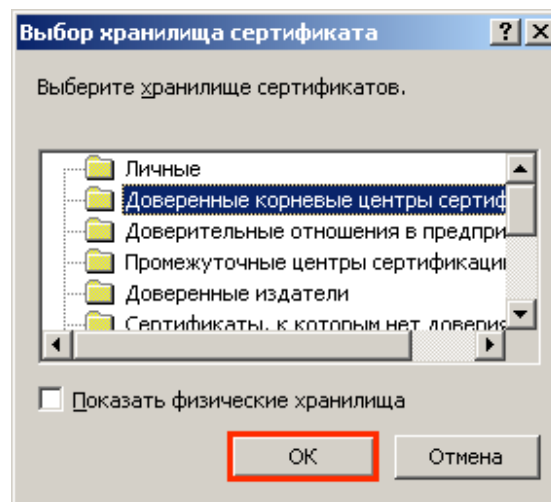
- В окне «Мастер импорта сертификатов» нажать кнопку «Далее >>»;



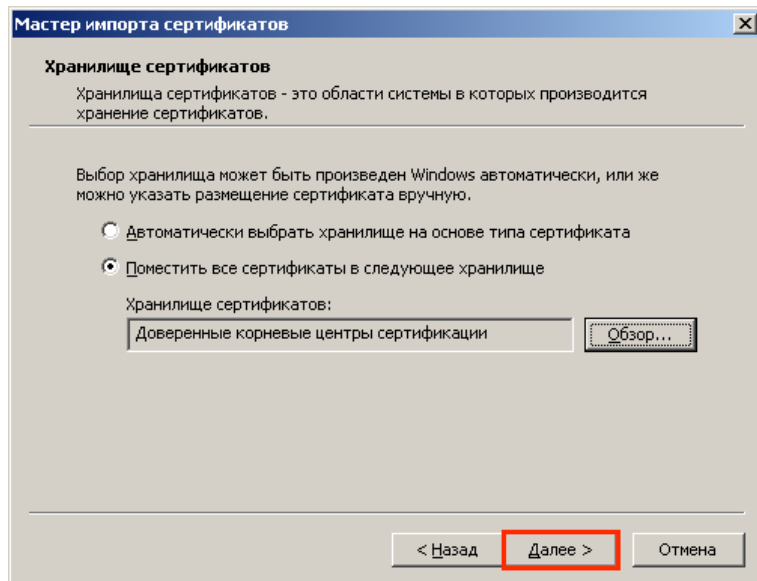
- Отметить строку «Поместить все сертификаты в следующее хранилище» и нажать кнопку «Обзор...»;



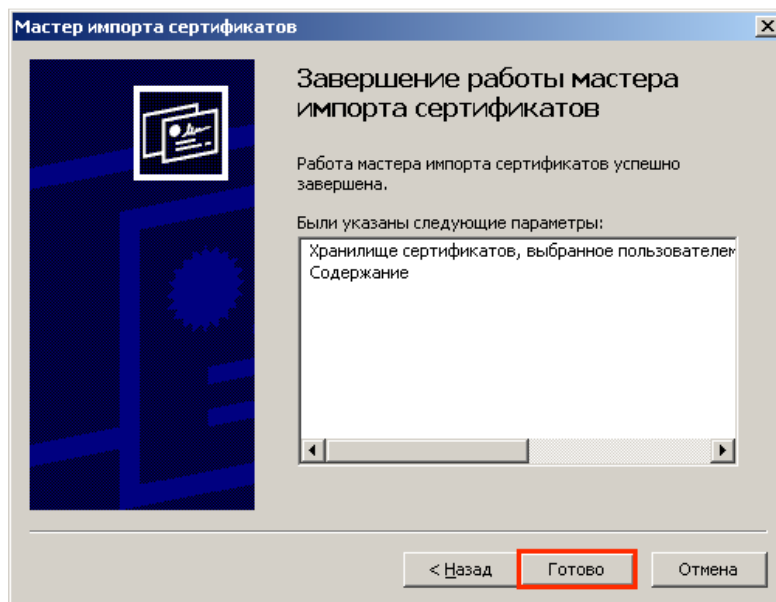
- Выбрать хранилище сертификатов «Доверенные корневые центры сертификации» и нажать кнопку «ОК»;



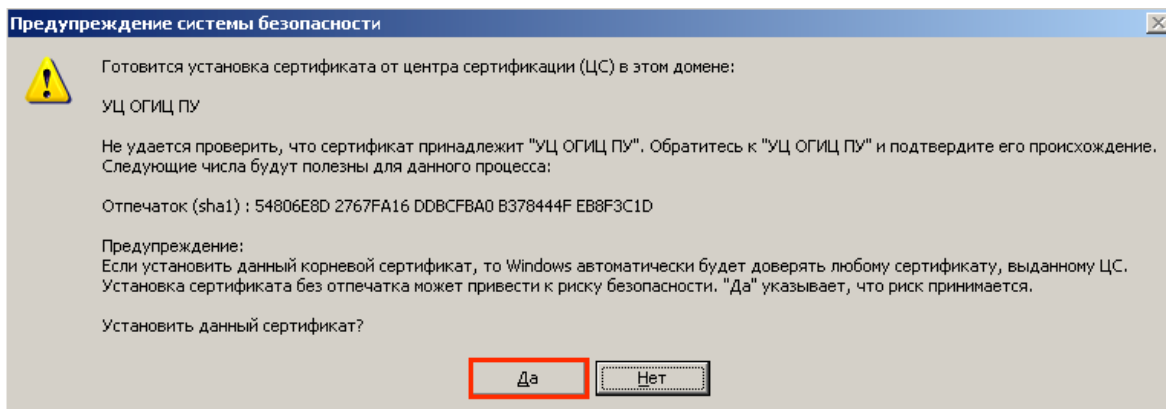
- Нажать кнопку «Далее >>»;



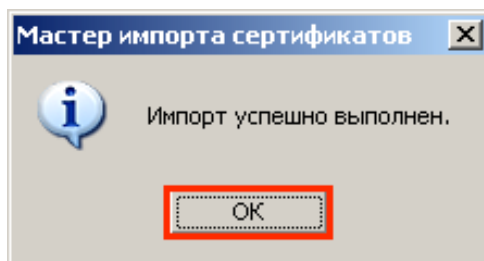
- Нажать кнопку «Готово»;



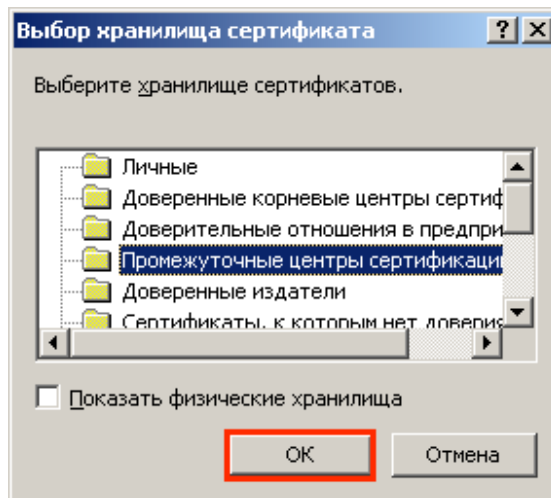
- В окне «Предупреждение системы безопасности» нажать кнопку «Да»;



- Нажать кнопку «ОК».



2.4 Установить сертификат уполномоченного лица удостоверяющего центра ОГИЦ второго уровня 1 (УЦ ОГИЦ ВУ 1) в хранилище сертификатов «Промежуточные центры сертификации», для чего необходимо выполнить действия с файлом «UC\_OGIC\_VU\_1.cer» аналогичные предыдущим, где на шаге выбора хранилища сертификатов необходимо указать «Промежуточные центры сертификации».

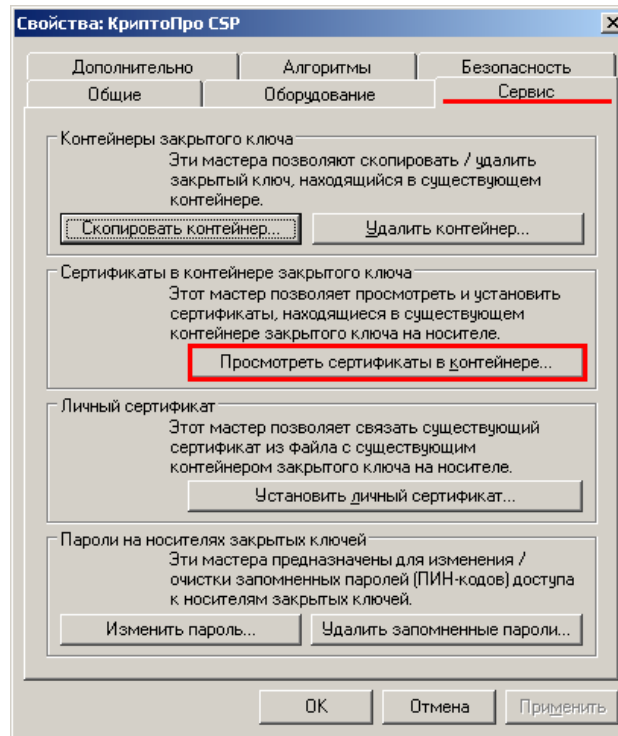


2.5 Установить сертификат пользователя (Ваш сертификат) в хранилище сертификатов «Личные». Для чего:

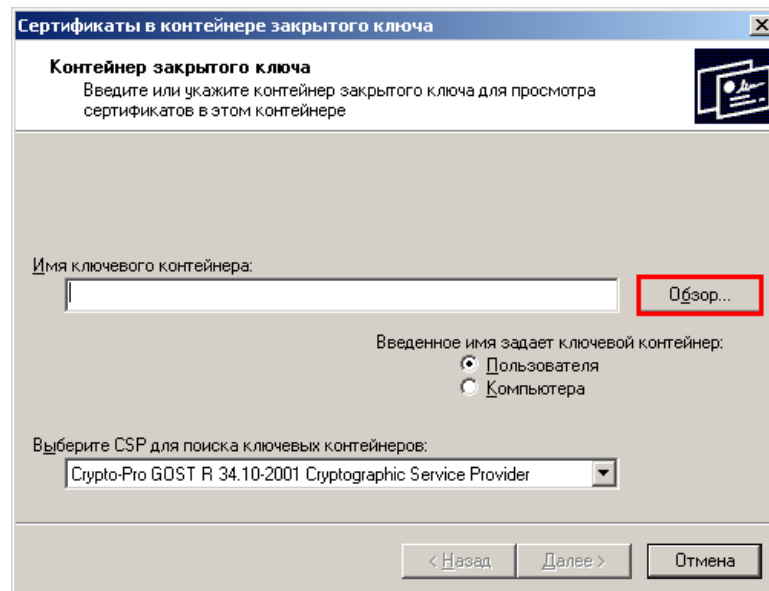
- Вставить полученный ключевой носитель в USB-порт компьютера;
- Открыть «КриптоПро CSP» (Пуск ---> Настройки ---> Панель управления --->

КриптоПро CSP);

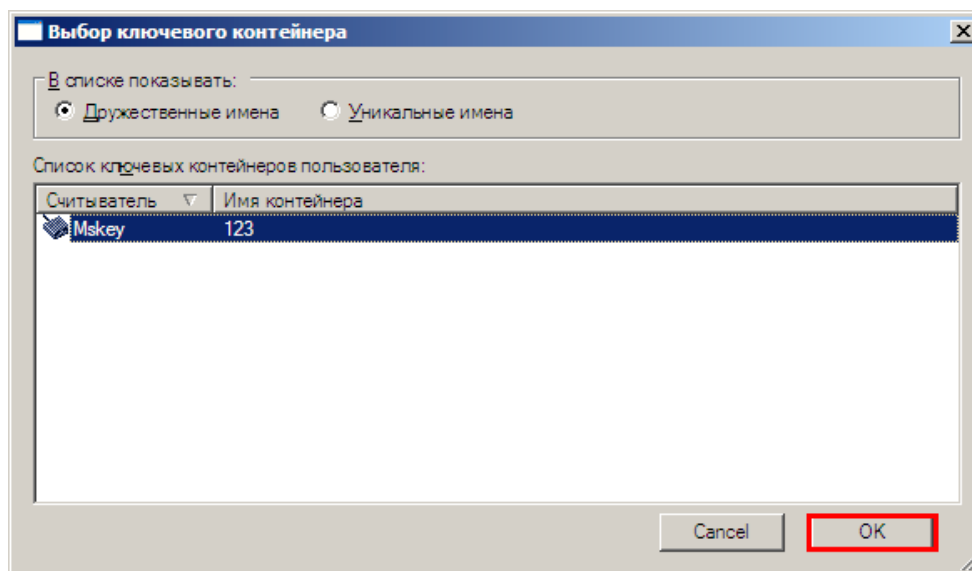
- Выбрать вкладку «Сервис»;
- Нажать кнопку «Просмотреть сертификаты в контейнере...»;



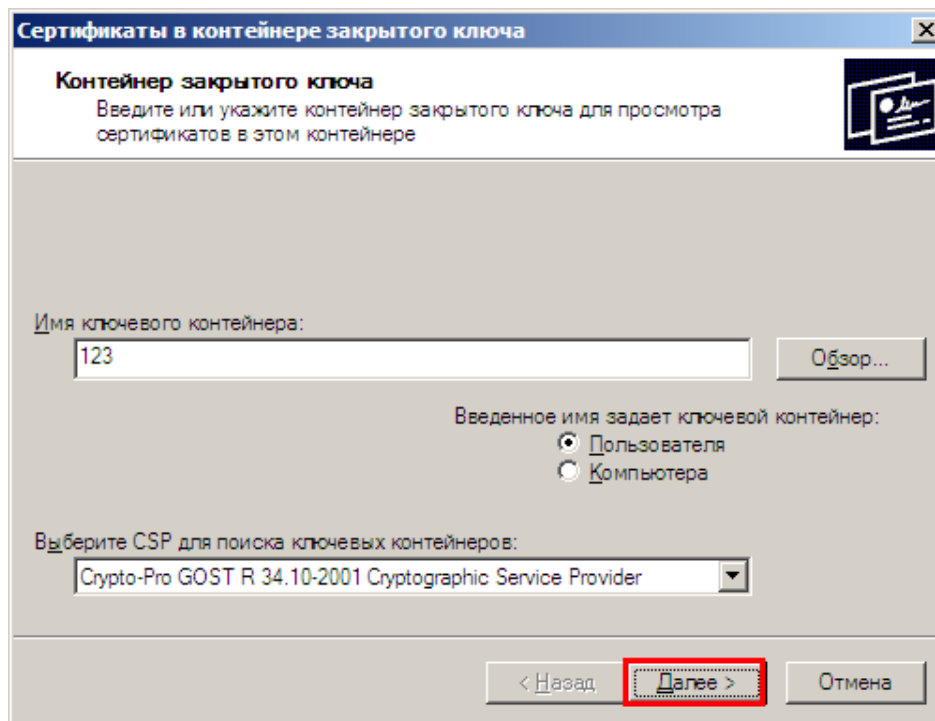
- Нажать кнопку «Обзор»;



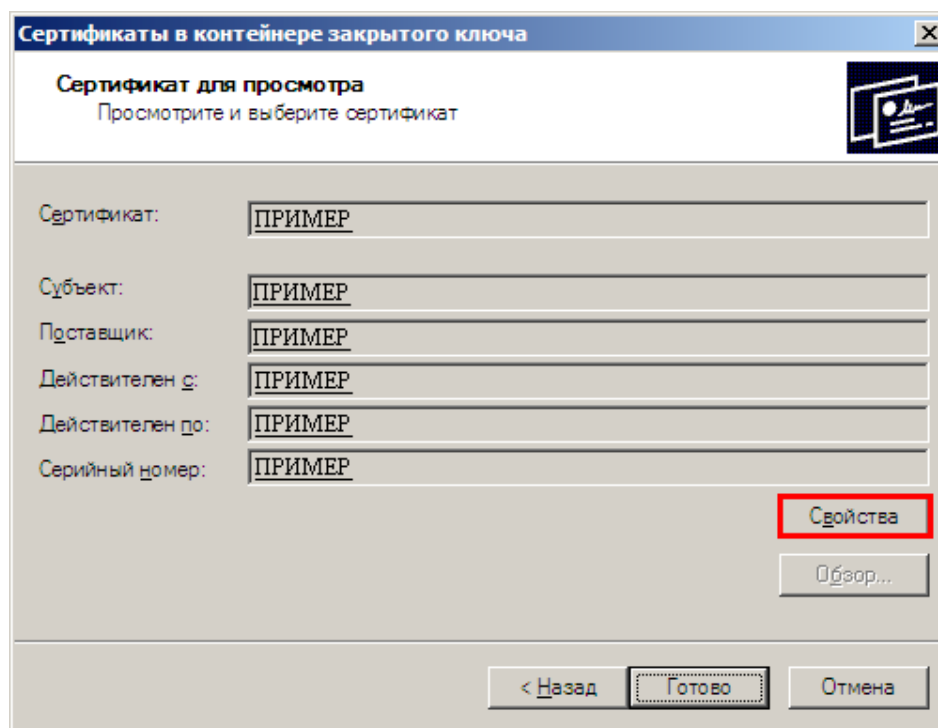
- Выбрать ключевой носитель, содержащий Ваш сертификат ключа подписи (MS\_Key) и нажать кнопку «ОК»;



- Нажать кнопку «Далее»;



- Нажать кнопку «Свойства»;



- Установить сертификат в хранилище сертификатов «Личные», для чего необходимо выполнить действия аналогичные пункту 2.3 и 2.4, где на шаге выбора хранилища сертификатов необходимо указать «Личные».

