Установка и конфигурирование СКЗИ «КриптоПро CSP»

НПО «Криста» 2011

Содержание

1. Общий алгоритм установки и настройка СКЗИ «КриптоПро CSP»

Перед установкой модулей подсистемы криптографии АС «Бюджет» и АС «УРМ» необходимо на всех рабочих станциях ФО, ГРБС, РБС, ПБС, ТПФО где предполагается подписание и проверка ЭЦП, установить СКЗИ «КриптоПро CSP» согласно перечню:

- На сервер обмена данными:
  - Установка программного обеспечения СКЗИ «КриптоПро CSP» (без ключевого носителя, т.е. без драйверов eToken[1]);
  - Установка корневого сертификата;
  - Установка списка отозванных сертификатов (CRL);
- На клиентах АС «УРМ»:
  - Установка программного обеспечения СКЗИ «КриптоПро CSP» с драйверами eToken;
  - Установка корневого сертификата;
  - Установка сертификата открытого ключа с ключевого носителя eToken;
  - Установка списка отозванных сертификатов (CRL);
- В ФО на станциях клиентов АС «Бюджет» для наложения ЭЦП на отправляемые документы, прикрепленные файлы, пакеты:
  - Установка программного обеспечения СКЗИ «КриптоПро CSP» с драйверами eToken;
  - Установка корневого сертификата;
  - Установка сертификата открытого ключа с ключевого носителя eToken;
  - Установка списка отозванных сертификатов (CRL).
- В ФО на станциях клиентов АС «Бюджет» для проверки ЭЦП на получаемых документах, пакетах, прикрепленных файлах:
  - Установка программного обеспечения СКЗИ «КриптоПро CSP» без драйверов eToken;
  - Установка корневого сертификата;
  - Установка списка отозванных сертификатов (CRL).

[1] В данном руководстве в качестве примера приводится описание использования ключевого носителя eToken.

Таким образом:

- На станциях клиентов АС «Бюджет» и АС «УРМ», на которых происходит наложение ЭЦП и отправка документов, пакетов, прикрепленных файлов, устанавливается:
  - СКЗИ «КриптоПро CSP» с драйверами eToken,
  - Носитель eToken;
  - корневой сертификат;
  - личный сертификат с носителя eToken;
  - список отозванных сертификатов (CRL).
- На станциях клиентов АС «Бюджет» и АС «УРМ», на которых происходит получение и проверка корректности ЭЦП документов, пакетов, прикрепленных файлов, устанавливается:
  - СКЗИ «КриптоПро CSP» без драйверов eToken;
  - корневой сертификат;
  - список отозванных сертификатов (CRL).

Установка СКЗИ «КриптоПро CSP» производится пользователем, имеющим права администратора. При этом ключевой носитель eToken не должен быть подключен к станции. После завершения установки требуется перезагрузить компьютер.

Настройка СКЗИ «КриптоПро CSP» осуществляется в окне настроек «Свойства: КриптоПро CSP», которое вызывается запуском значка **КриптоПро CSP**, появившемся после установки программы на панели управления компьютером (**Пуск\Настройка\Панель управления**).

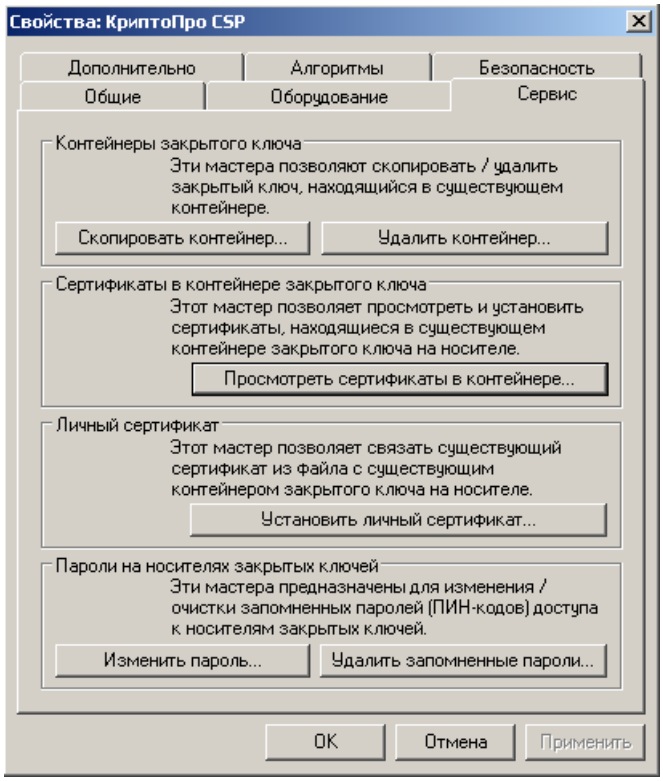
2. Возможности настройки СКЗИ «КриптоПро CSP»

❖ **Закладка «Сервис»**

На закладке Сервис окна настроек «Свойства: КриптоПро CSP» (рисунок 1) существует возможность следующих настроек:

- скопировать/удалить закрытый ключ, находящийся в существующем контейнере (в группе настроек Контейнеры закрытого ключа кнопки **Скопировать контейнер…** и **Удалить контейнер…**, функциональность которых соответствует названию);
- просмотреть и установить сертификаты, находящиеся в существующем контейнере закрытого ключа на носителе (в группе настроек Сертификаты в контейнере закрытого ключа кнопка **Просмотреть сертификаты в контейнере…**);
- связать существующий сертификат из файла с существующем контейнером закрытого ключа на носителе (в группе настроек Личный сертификат кнопка **Установить личный сертификат…**). Подробнее о порядке установки сертификата читайте в пункте 6 «Установка сертификата открытого ключа с ключевого носителя»;
- изменить/очистить пароль (Пин-код) доступа к носителям закрытых ключей (в группе настроек Пароли на носителях закрытых ключей кнопки **Изменить пароль** и **Удалить запомненные пароли**, функциональность которых соответствует названию).

Рисунок 1 – Закладка «Сервис» окна настроек «Свойства: КриптоПро CSP»



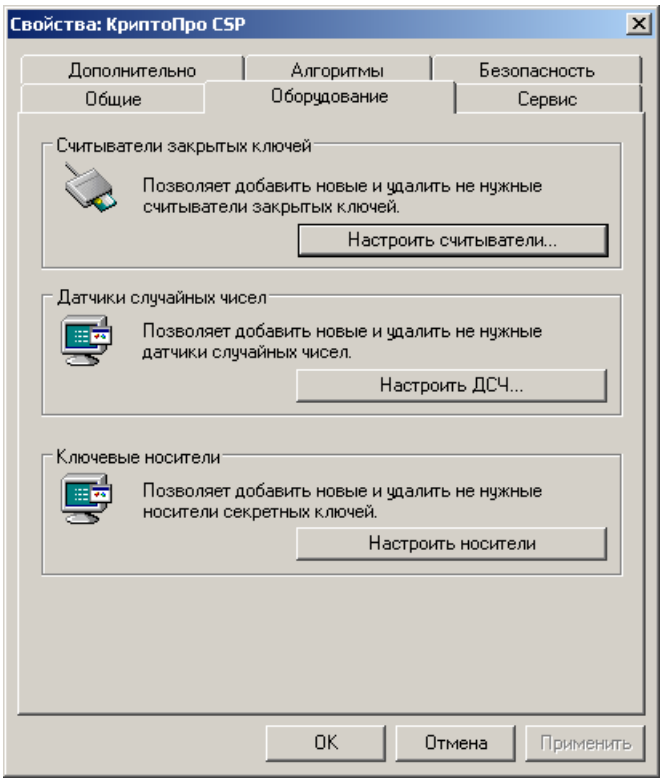
При установке пин-кода запрещается использовать галочку **Запомнить пароль**, так как в этом случае он будет вводиться автоматически (без запроса к пользователю), что увеличивает риск несанкционированного использования ЭЦП.

❖ **Закладка «Оборудование»**

На закладке Оборудование окна настроек «Свойства: КриптоПро CSP» (рисунок 2) существует возможность следующих настроек:

- добавить новые и удалить ненужные считыватели закрытых ключей (в группе Считыватели закрытых ключей кнопка **Настроить считыватели…**);
- добавить новые и удалить ненужные датчики случайных чисел (в группе Датчики случайных чисел кнопка **Настроить ДСЧ…**);
- добавить новые и удалить ненужные носители секретных ключей (в группе Ключевые носители кнопка **Настроить носители…**).

Рисунок 2 – Закладка «Оборудование» окна настроек «Свойства: КриптоПро CSP»



3. Установка считывателей

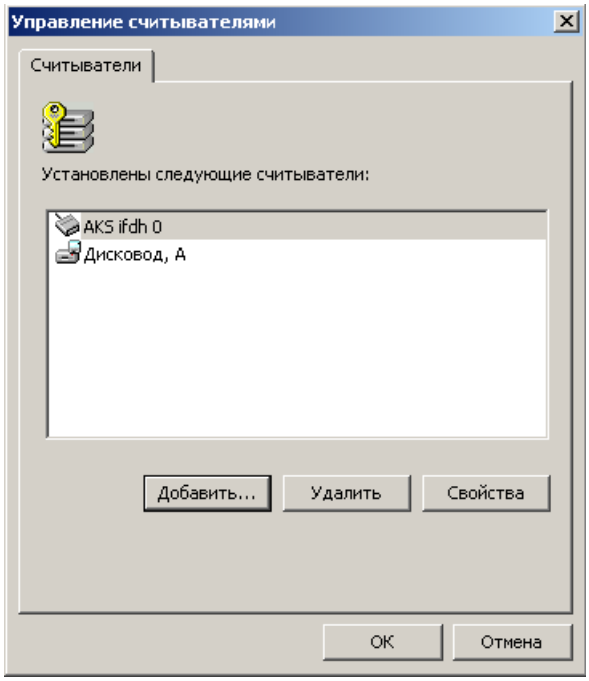
Для хранения ключевой контейнер размещают на внешнем физическом носителе, который может быть одного из следующих видов:

- Дискета 3.5”;
- Электронный идентификатор eToken;
- Электронный идентификатор ruToken;
- Таблетки Touch-Memory DS1993 – DS1996 с использованием устройств Аккорд-АМДЗ, электронный замок «Соболь» или устройство чтения таблеток Touch-Memory DALLAS;
- Процессорные карты MPCOS-EMV и российские интеллектуальные карты (РИК) с использованием считывателя smart card GemPlus GCR-410.

В данном руководстве в качестве примера приводится описание процесса установки ключевого носителя eToken для СКЗИ «КриптоПро CSP» 3.0.

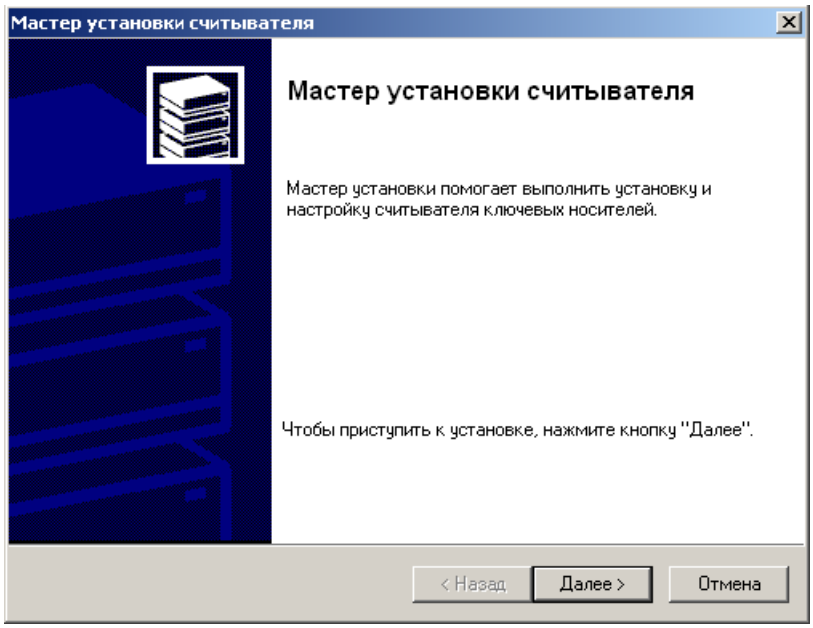
Для установки считывателей необходимо на закладке Оборудование окна настроек «Свойства: КриптоПро CSP» (см. рисунок 2) в группе Считыватели закрытых ключей нажать кнопку **Настроить считыватели...**. При нажатии на кнопку появляется окно «Управление считывателями» (рисунок 3) с информацией об установленных в системе считывателях.

Рисунок 3 – Окно «Управление считывателями»



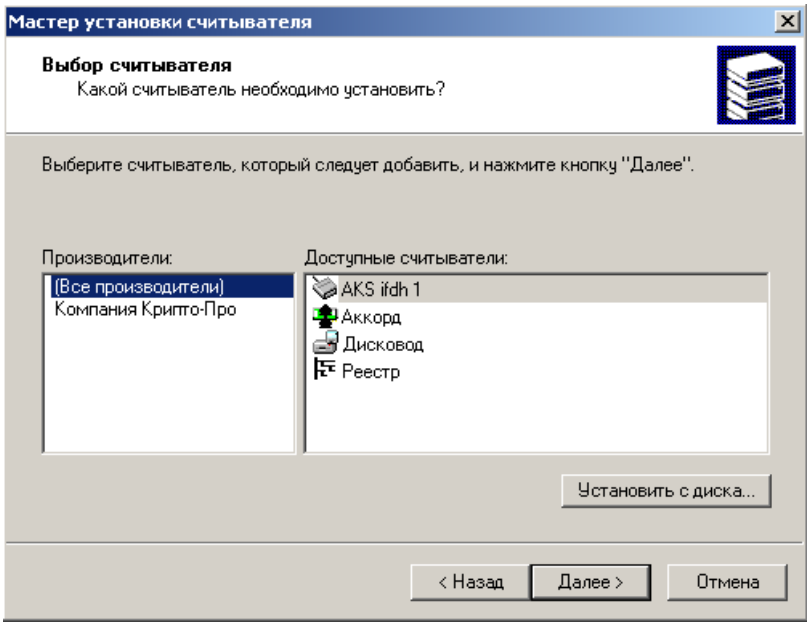
Для добавление нового считывателя нажмите кнопку **Добавить**, посредством которой запустится мастер установки считывателя (рисунок 4).

Рисунок 4 – Окно «Мастер установки считывателя»



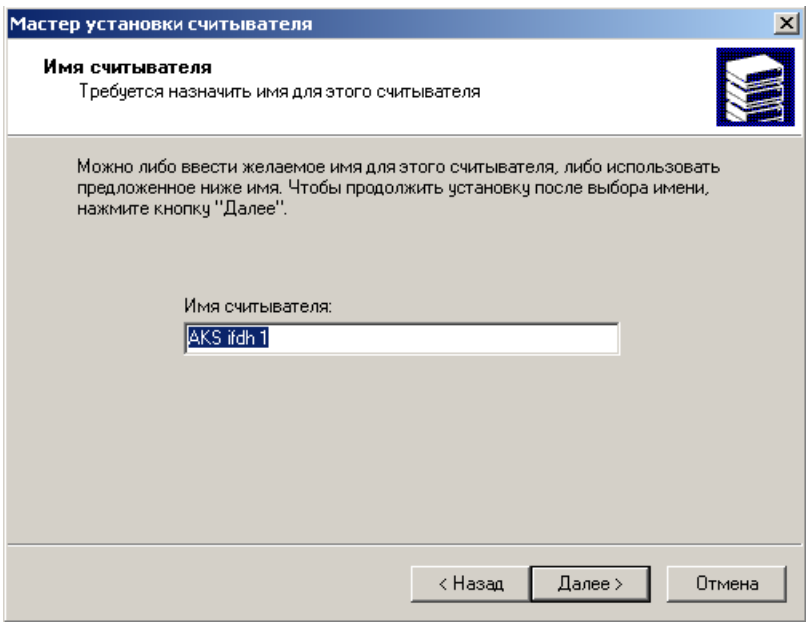
После нажатия кнопки **Далее**, в открывшемся окне «Выбор считывателя» (рисунок 5) выберите из списка тип считывателя, который следует добавить. Нажмите кнопку **Далее** для продолжения операции установки.

Рисунок 5 – Окно «Выбор считывателя»



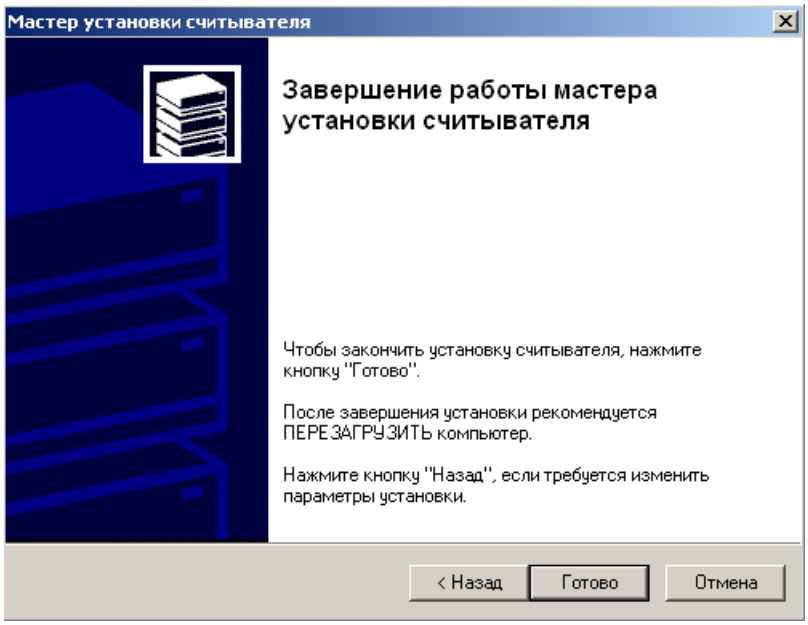
В окне «Имя считывателя» (рисунок 6) введите имя выбранного считывателя, которое будет в дальнейшем использоваться в системе. Нажмите кнопку **Далее**.

Рисунок 6 – Окно «Имя считывателя»



Завершите процесс установки считывателя нажатием кнопки **Готово** и перезагрузите компьютер.

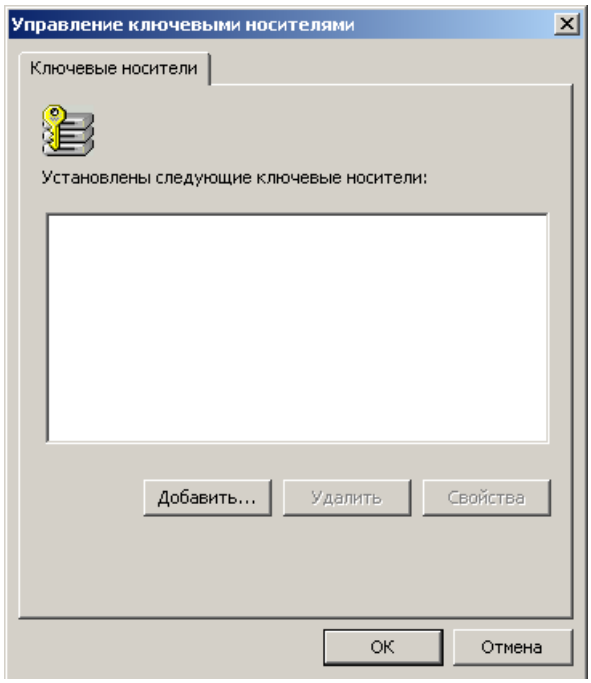
Рисунок 7 – Окно «Завершение мастера установки считывателя»



4. Установка ключевых носителей

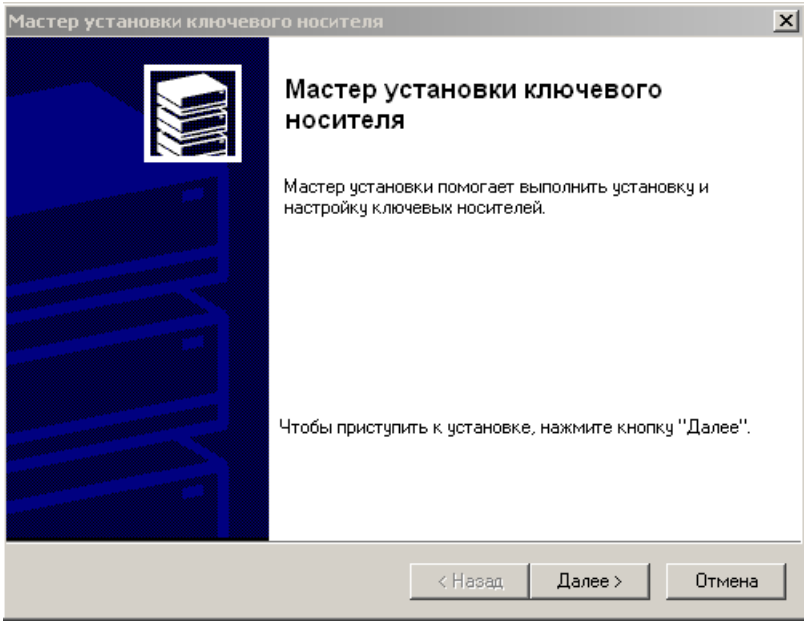
Для установки ключевого носителя необходимо на закладке Оборудование окна настроек «Свойства: КриптоПро CSP» (см. рисунок 2) в группе Ключевые носители нажать кнопку **Настроить носители**. При нажатии на кнопку появляется окно «Управление ключевыми носителями» (рисунок 8) с информацией об установленных в системе носителях.

Рисунок 8 – Окно «Управление ключевыми носителями»



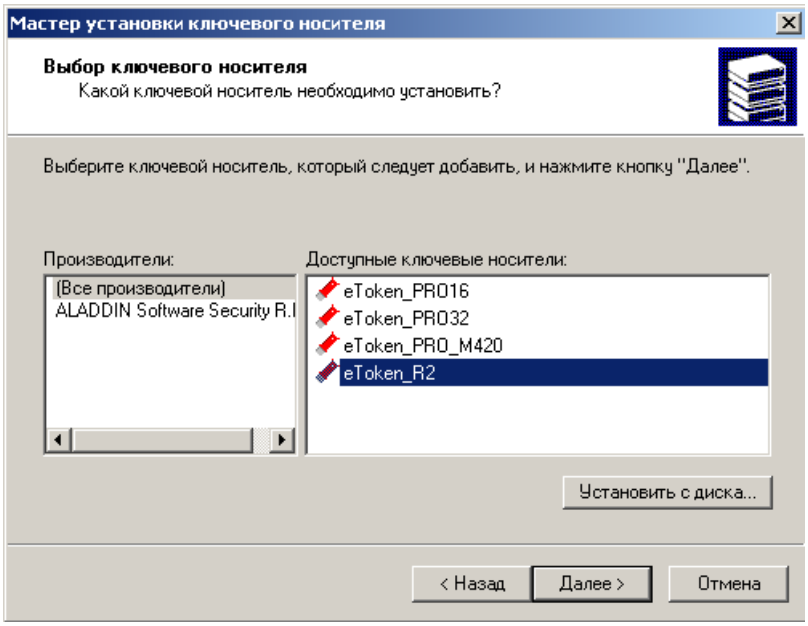
Для добавление нового носителя нажмите кнопку **Добавить**, посредством которой запустится мастер установки ключевого носителя (рисунок 9).

Рисунок 9 – Окно «Мастер установки ключевого носителя»



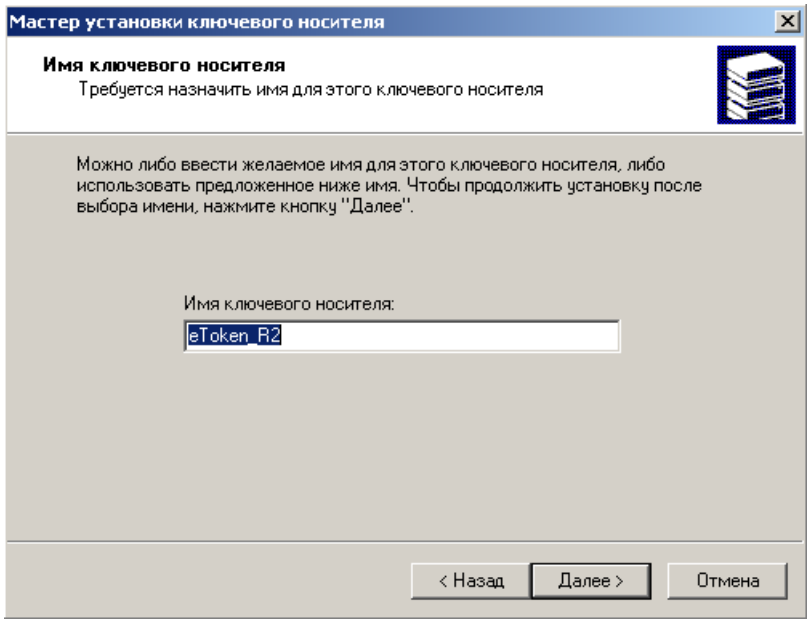
После нажатия кнопки **Далее**, в открывшемся окне «Выбор ключевого носителя» (рисунок 10) выберите из списка тип ключевого носителя, который следует добавить. Нажмите кнопку **Далее** для продолжения операции установки.

Рисунок 10 – Окно «Выбор ключевого носителя»



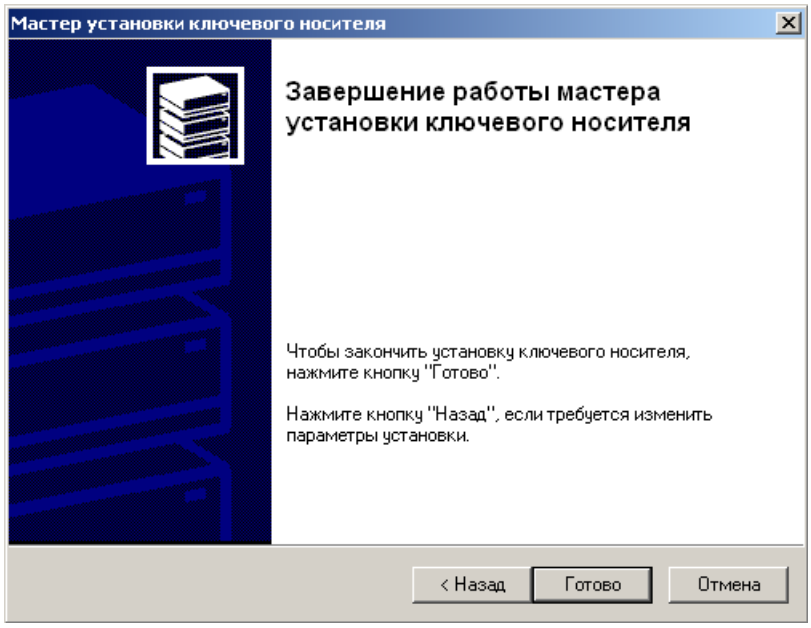
В окне «Имя ключевого носителя» (рисунок 11) введите имя выбранного ключевого носителя, которое будет в дальнейшем использоваться в системе. Нажмите кнопку **Далее**.

Рисунок 11 – Окно «Имя ключевого носителя»



Завершите процесс установки считывателя нажатием кнопки **Готово** и перезагрузите компьютер.

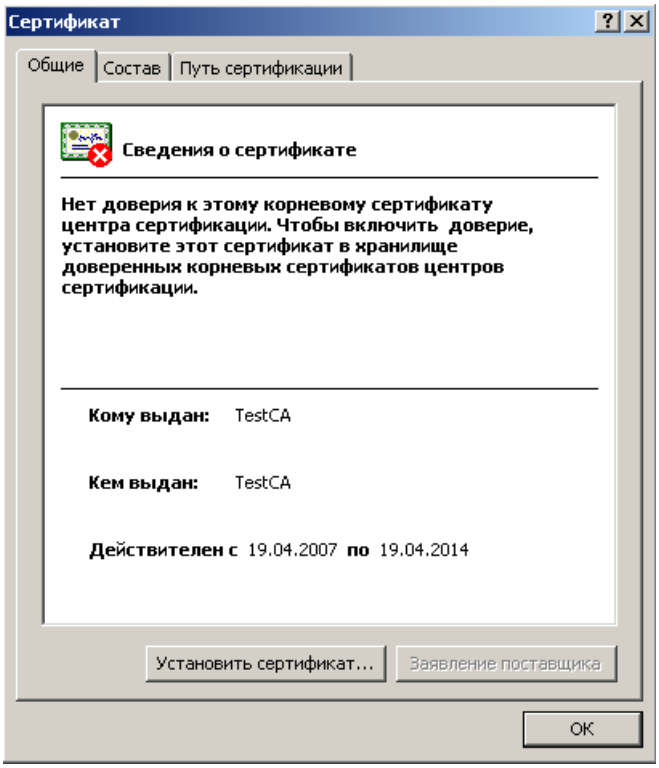
Рисунок 12 – Окно «Завершение мастера установки ключевого носителя»



5. Установка корневого сертификата

Для установки корневого сертификата необходимо открыть файл сертификата с расширением *.cer двойным щелчком левой кнопки мыши, после чего появится окно «Сертификат» (рисунок 13).

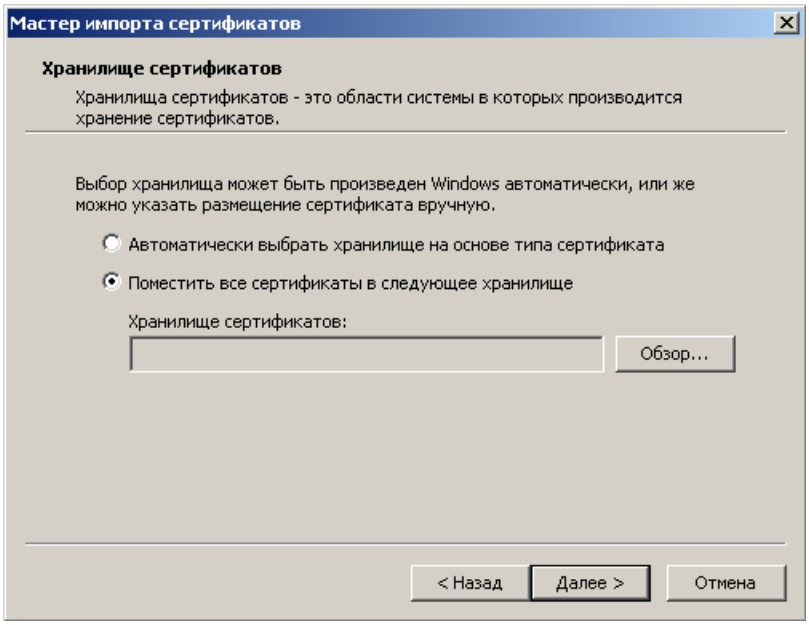
Рисунок 13 – Отображение информации о сертификате



Далее выполните следующие действия:

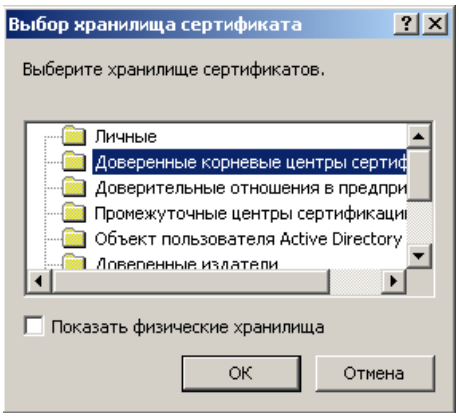
1. На закладке Общие окна «Сертификат» нажмите кнопку **Установить сертификат…**, посредством которой запустится мастер импорта сертификатов. Далее необходимо следовать инструкциям мастера.
2. При выборе хранилища сертификатов в окне мастера импорта сертификатов (рисунок 14) отметьте пункт Поместить все сертификаты в следующее хранилище флагом-точкой, нажмите на кнопку **Обзор**.

Рисунок 14 – Окно «Мастер импорта сертификатов»



3. В появившемся окне «Выбор хранилища сертификатов» (рисунок 15) укажите в качестве хранилища сертификатов «Доверенные корневые центры сертификации». Подтвердите выбор кнопкой **ОК**.

Рисунок 15 – Вид окна выбора хранилища сертификатов



4. Нажмите кнопку **Далее**, после чего мастер установки сертификатов завершит работу.
5. При успешной установке сертификата процедура будет завершена сообщением «Импорт успешно выполнен».

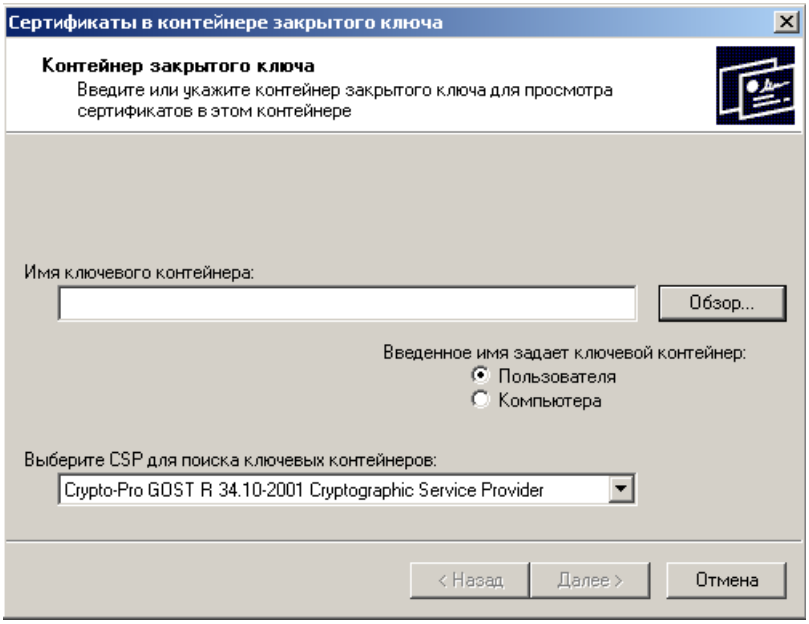
6. Установка сертификата открытого ключа с ключевого носителя

Данная настройка требуется лишь на тех станциях АС «Бюджет» и АС «УРМ», на которых будет происходить наложение ЭЦП. На сервере обмена данными и станциях ФО, на которых выполняется только проверка корректности ЭЦП, данную установку проводить не требуется.

Перед установкой сертификата необходимо подключить ключевой носитель к станции. Установка сертификата открытого ключа осуществляется в окне настроек «Свойства: КриптоПро CSP». Для этого выполните следующие действия:

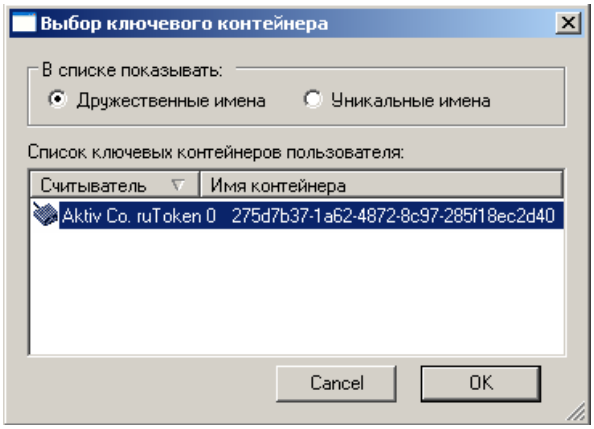
1. В окне настроек перейдите на закладку Сервис (см. рисунок 1) и нажмите кнопку **Просмотреть сертификаты в контейнере**.
2. В появившемся окне «Сертификаты в контейнере закрытого ключа» (рисунок 16) в поле Выберите CSP для поисков ключевых контейнеров укажите CSP. На данный момент все ключи должны выдаваться с использованием Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider. Если не выбрать значение, или выбрать его неправильно, то при работе будет появляться сообщение об ошибке: «Сертификат не связан с контейнером».

Рисунок 16 – Окно поиска сертификатов в контейнере закрытого ключа



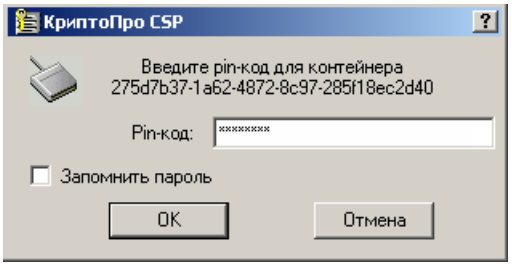
3. Затем для выбора ключевого контейнера в окне поиска сертификатов (см. рисунок 16) нажмите кнопку **Обзор**, в появившемся окне «Выбор ключевого контейнера» (рисунок 17) выберите ключевой контейнер и подтвердите свой выбор нажатием кнопки **ОК**.

Рисунок 17 – Вид окна выбора ключевого контейнера



При появлении окна ввода пин-кода для контейнера (рисунок 18) введите стандартный пароль носителя eToken, сообщаемый Вам при получении, и нажмите OK.

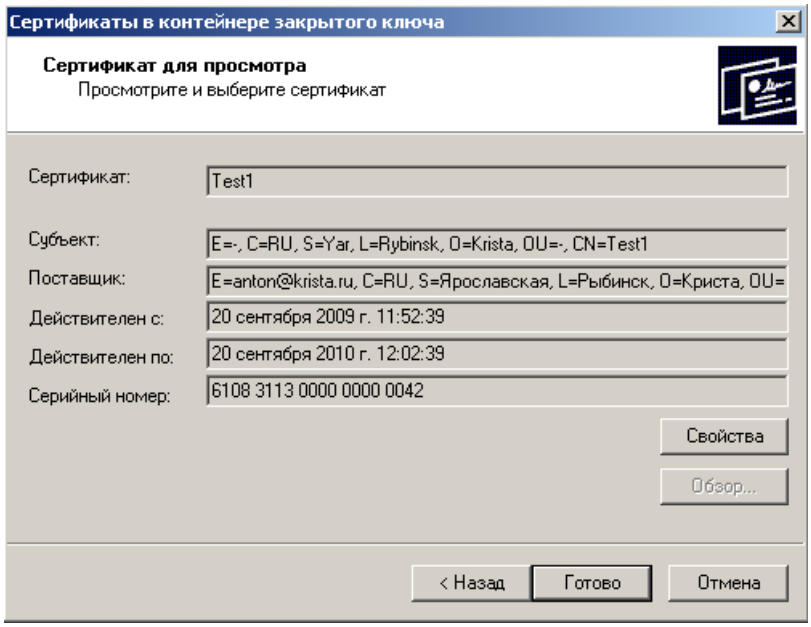
Рисунок 18 – Окно ввода пин-кода



При установке пин-кода запрещается использовать галочку **Запомнить пароль**, так как в этом случае он будет вводиться автоматически (без запроса к пользователю), что увеличивает риск несанкционированного использования ЭЦП.

4. Нажмите кнопку **Далее** в окне «Сертификаты в контейнере закрытого ключа». В результате с ключевого носителя будут считаны данные сертификата, и появится окно, отображающее эти данные (рисунок 19). Рекомендуется скопировать серийный номер, т.к. он понадобится при последующей настройке АС «Бюджет» и/или АС «УРМ».

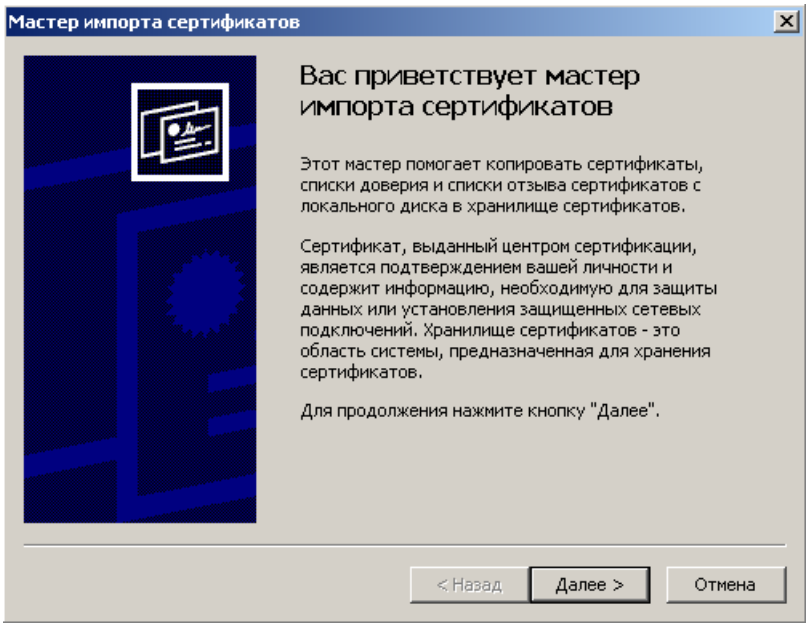
Рисунок 19 – Окно отображения сертификатов контейнера закрытого ключа



В появившемся окне (см. рисунок 19) нажмите кнопку **Свойства**, после чего появится окно «Сертификат» с основными свойствами сертификата (см. рисунок 13).

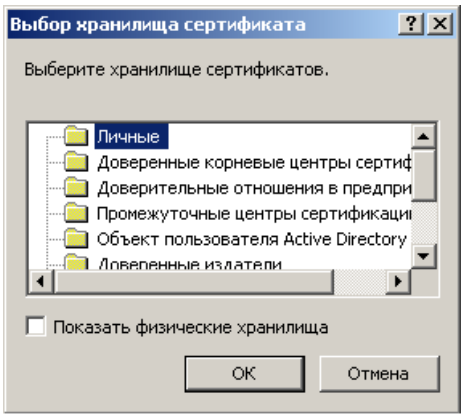
5. На закладке Общие нажмите кнопку **Установить сертификат…**, после чего запустится мастер импорта сертификата, инструкциям которого надо следовать в дальнейшем.
6. В первом окне «Мастера импорта сертификата» (рисунок 20) ознакомьтесь с информацией об устанавливаемом сертификате и нажмите кнопку **Далее** для продолжения операции установки сертификата.

Рисунок 20 – Окно «Мастер импорта сертификатов»



7. Во втором окне «Мастера импорта сертификата» (см. рисунок 14) при выборе хранилища сертификатов отметьте пункт Поместить все сертификаты в следующее хранилище флагом-точкой, нажмите на кнопку **Обзор**.
8. В окне «Выбор хранилища сертификатов» в качестве хранилища выберите «Личные» (рисунок 21), подтвердите выбор нажатием кнопки **ОК**.

Рисунок 21 – Вид окна выбора хранилища сертификатов



9. В третьем окне «Мастера импорта сертификата» завершите установку сертификата нажатием кнопки **Готово**.

В процессе установки личного сертификата, в случае несоответствия открытого ключа сертификата и ключевого контейнера, появляется сообщение: «Закрытый ключ на указанном контейнере не соответствует открытому ключу в сертификате, выберите другой ключевой контейнер».

10. При успешной установке сертификата процедура будет завершена сообщением «Импорт успешно выполнен».

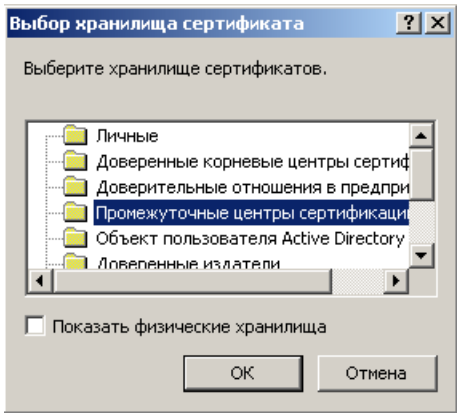
7. Установка списков отзыва сертификатов

При проверке валидности сертификата нужен список отзыва сертификатов (CRL). Список отозванных сертификатов (CRL – Certificate Revocation List) – это электронный документ, который содержит перечень сертификатов, являющихся отозванными из обращения в УЦ. Удостоверяющий центр поддерживает отзыв сертификатов и публикацию списков отозванных сертификатов. Абоненты могут получить эту информацию и записать ее в свое локальное хранилище, чтобы использовать для последующей проверки сертификатов.

Список отзыва нужно устанавливать на все станции, на которые устанавливаются сертификаты, и периодически (в соответствии со сроком его действия) обновлять.

1. Для установки списков отзыва выполните следующие действия:
2. Щелкнув на файле списка отзыва с расширением *.crl правой кнопкой мыши, выберите в появившемся контекстном меню пункт «Установить список отзыва (CRL)», посредством которого запустится мастер импорта сертификатов. Далее необходимо следовать инструкциям мастера.
3. При выборе хранилища сертификатов в окне мастера импорта сертификатов (см. рисунок 14) отметьте пункт Поместить все сертификаты в следующее хранилище флагом-точкой, нажмите на кнопку **Обзор**.
4. В появившемся окне «Выбор хранилища сертификатов» (рисунок 22) укажите в качестве хранилища сертификатов «Промежуточные центры сертификации». Подтвердите выбор кнопкой **ОК**.

Рисунок 22 – Вид окна выбора хранилища сертификатов



5. Нажмите кнопку **Далее**, после чего мастер установки сертификатов завершит работу.
6. При успешной установке сертификата процедура будет завершена сообщением «Импорт успешно выполнен».