Инструкция по настройке автоматизированного рабочего места для работы с электронной подписью

ООО «Стандарт безопасности»
2014 г.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Документ предназначен для пользователей, осуществляющих самостоятельную установку средства криптографической защиты информации (СКЗИ) КриптоПро CSP и настройку автоматизированного рабочего места для работы с электронной подписью (ЭП).

Для правильной работы СКЗИ КриптоПро CSP необходимо выполнить все пункты данного руководства в указанной последовательности.

Для корректной работы с электронной подписью (ЭП) на различных интернет-порталах (электронные торговые площадки, порталы контролирующих органов, различные федеральные информационные ресурсы и т.д.) в качестве интернет-обозревателя рекомендуется использовать Microsoft Internet Explorer версии 8.0 и выше.

Внимание! Устанавливать СКЗИ "КриптоПро CSP" на компьютер, где уже установлено СКЗИ ViPNet CSP крайне не рекомендуется. ООО "Стандарт безопасности" не несет ответственности за корректную работу СКЗИ ViPNet CSP и СКЗИ "КриптоПро CSP" при несоблюдении пользователем данного условия.

СОВМЕСТИМОСТЬ КриптоПро CSP С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ ViPNet CSP

Программа КриптоПро CSP может быть установлена на одном компьютере с программным обеспечением ViPNet CSP. Однако при этом необходимо соблюдать следующие условия:

Если для выполнения криптографических операций в поддерживаемых приложениях требуется использовать криптопровайдер ViPNet CSP, в программе ViPNet CSP в разделе Общие должен быть установлен флажок Включить поддержку работы ViPNet CSP через MS Crypto API. При этом убедитесь, что на компьютере не установлен компонент «Совместимость с продуктами Microsoft», входящий в ПО КриптоПро CSP версии 3.6.

Если для выполнения криптографических операций в поддерживаемых приложениях требуется использовать криптопровайдер КриптоПро CSP, на компьютере должен быть установлен компонент КриптоПро CSP «Совместимость с продуктами Microsoft». При этом в программе ViPNet CSP в разделе Общие должен быть снят флажок Включить поддержку работы ViPNet CSP через MS Crypto API. Кроме того, для подписи документов Microsoft Office необходимо дополнительно установить программу КриптоПро Office Signature.

Внимание! Не следует одновременно устанавливать компонент КриптоПро CSP «Совместимость с продуктами Microsoft» и в программе ViPNet CSP устанавливать флажок Включить поддержку работы ViPNet CSP через MS Crypto API.

ПОЛУЧЕНИЕ КриптоПро CSP

Для получения КриптоПро CSP необходимо перейти на официальный сайт разработчика по адресу http://www.cryptopro.ru/cryptopro/products/csp/default.htm и затем к странице для загрузки файла с сайта: Дистрибутив -> Перейти к загрузке.

Получение демо-версии КриптоПро CSP возможно только после предварительной регистрации. Это формальная, но обязательная процедура, абсолютно бесплатная. Пройдите регистрацию, заполнив все поля.

Скачайте дистрибутив КриптоПро CSP (При выборе версии КриптоПро CSP учитывайте версию операционной системы. Для Windows 7 необходимо использовать только версию 3.6.1 и выше). Сохраните загружаемый файл на своем компьютере, а затем запустите установку программы.

Для штатной эксплуатации средств криптографической защиты информации (СКЗИ), к которым относятся КриптоПро, эти средства должны быть установлены с дистрибутива, полученного у производителя или у официального дилера на материальном носителе.

- ✓ Перед началом установки КриптоПро CSP закройте все запущенные приложения.
- ✓ Убедитесь, что вы обладаете достаточными правами для установки ПО и записи информации в реестр (рекомендуется выполнять установку и настройку с правами локального администратора, пароль локального администратора должен быть непустой).
- ✓ Выполняйте установку и настройку КриптоПро CSP локально на компьютере, а не через клиента удаленного доступа.

В появившемся окне нажмите кнопку «Далее».

В окне «Лицензионное соглашение» выберите пункт «Я принимаю условия лицензионного соглашения» и нажмите кнопку «Далее».

В окне «Сведения о пользователе» заполните поля «Пользователь», «Организация», введите «Серийный номер» (выдается на бумажном носителе – Лицензия на КриптоПро CSP) и нажмите кнопку «Далее» (При вводе серийного номера КриптоПро CSP все символы вводятся заглавными латинскими буквами. В серийном номере букв «О» нет – это цифра «0»).

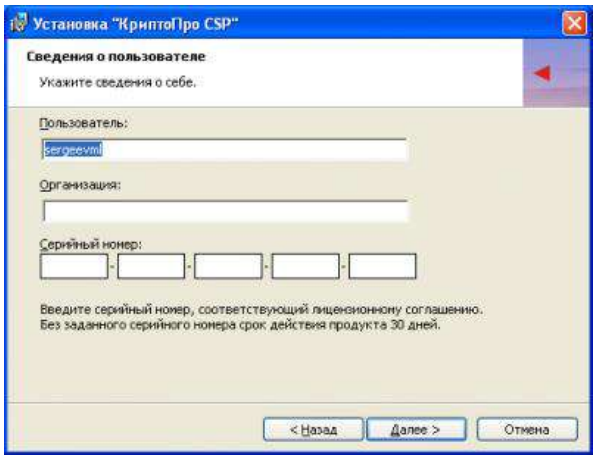


Рисунок 1

ОГРАНИЧЕНИЯ НЕЗАРЕГИСТРИРОВАННОЙ ВЕРСИИ

С незарегистрированной версией программы КриптоПро CSP можно работать по демо-лицензии.

Особенности демо-лицензии:

- **Срок действия:** 3 месяца.
- **Функциональных ограничений нет.**

По истечении срока действия демо-лицензии запуск незарегистрированной программы невозможен. Чтобы продолжить работу с КриптоПро CSP, необходимо приобрести лицензию.

УСТАНОВКА ДРАЙВЕРОВ ДЛЯ КЛЮЧЕВОГО НОСИТЕЛЯ eToken

1. Для корректной работы ключевого носителя eToken под управлением операционной системы Microsoft Windows необходимо установить программное обеспечение компании Аладдин РД "eToken PKI Client" актуальной версии.
2. Для получения "eToken PKI Client" необходимо перейти на официальный сайт разработчика по адресу http://www.aladdin-rd.ru/support/downloads/etoken/ и выбрать дистрибутив драйверов "eToken PKI Client", соответствующий версии Microsoft Windows, установленной у вас на компьютере. Например, для операционных систем Windows XP SP2/Vista SP2/2003 SP2/2008/2008 R2/7/2008 R2 необходимо выбрать дистрибутив "eToken PKI Client 5.1 SP1 для Microsoft Windows".
3. Загрузите архив с дистрибутивом в любое место компьютера и извлеките файлы в папку.
4. Запустите установку "eToken PKI Client" файлом PKIClient_x32_xx_xxx.msi (или PKIClient_x64_xx_xxx.msi) из папки архива. Выполните установку "eToken PKI Client", следуя инструкциям мастера установки (Рисунки 2- 8)

Рисунок 2

Рисунок 3

Рисунок 4

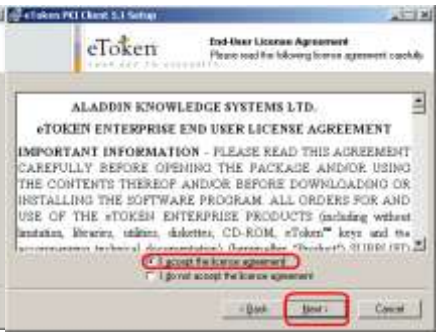


Рисунок 5

Рисунок 6

Рисунок 7

Рисунок 8

На шаге Рисунка 6 нажмите «Next», если вы согласны установить eToken PKI Client 5.1 в предложенное место (рекомендуется), либо выберите путь для установки с помощью кнопки «Browse».

5. Перезагрузите компьютер.

УСТАНОВКА ЛИЧНОГО СЕРТИФИКАТА С КЛЮЧЕВОГО НОСИТЕЛЯ eToken

1. **Вставьте eToken в USB-порт компьютера.**

2. **Перейдите на вкладку «Сервис» нажмите кнопку «Просмотреть сертификаты в контейнере» (Рисунок 10)**

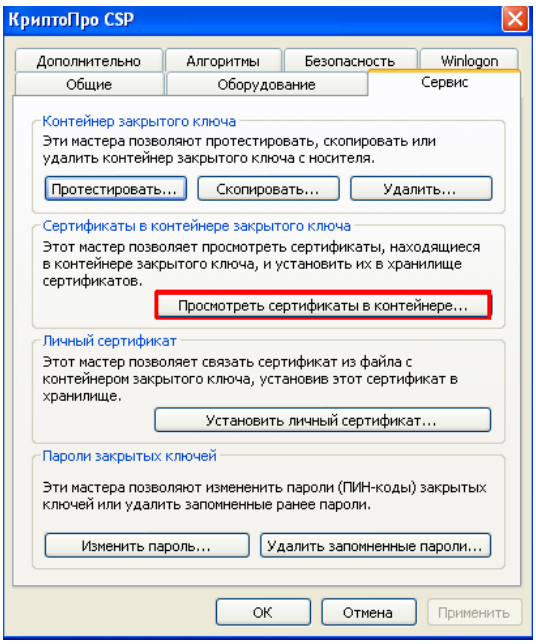


Рисунок 10

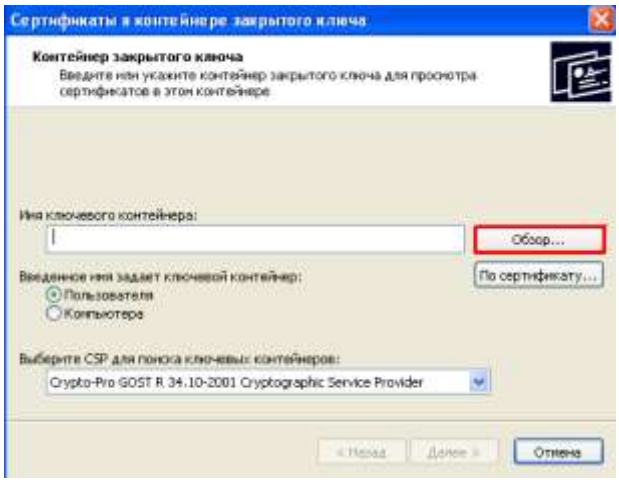


Рисунок 11

3. **В открывшемся окне нажать кнопку «Обзор», чтобы выбрать контейнер для просмотра. После выбора контейнера нажать на кнопку «Ок» (Рисунок 11)**

4. **В следующем окне кликнуть по кнопке «Далее».**
   (Если после нажатия на кнопку «Далее» появляется сообщение: «В контейнере закрытого ключа отсутствует открытый ключ шифрования», обратитесь к специалисту удостоверяющего центра, выдававшему вам ключ.

5. **В окне Сертификат для просмотра необходимо нажать кнопку Свойства. (Рисунок 12).**

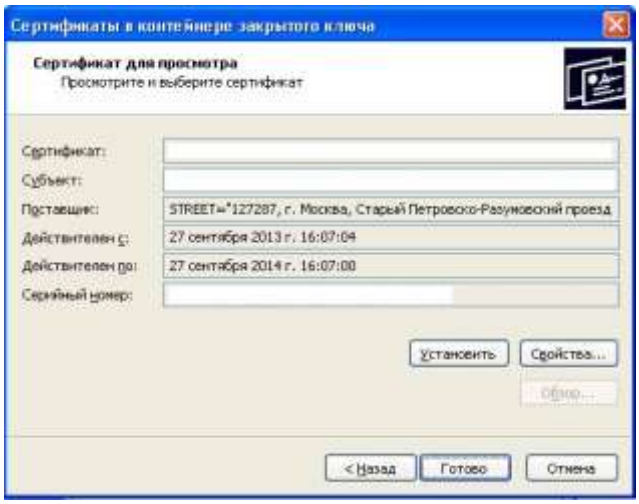


Рисунок 12

6. **В открывшемся окне выбрать «Установить сертификат».**
7. **В окне «Мастер импорта сертификатов» следует выбрать кнопку «Далее».**
8. **В окне «Выбор хранилища» нажать кнопку «Обзор» и выбрать папку с названием «Личные».**

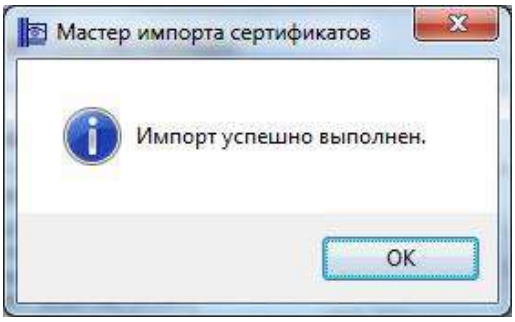


Рисунок 13

9. **В следующем окне следует выбрать «Далее», затем нажать на кнопку «Готово» и дождаться сообщения об успешной установке (*Рисунок 13*).**

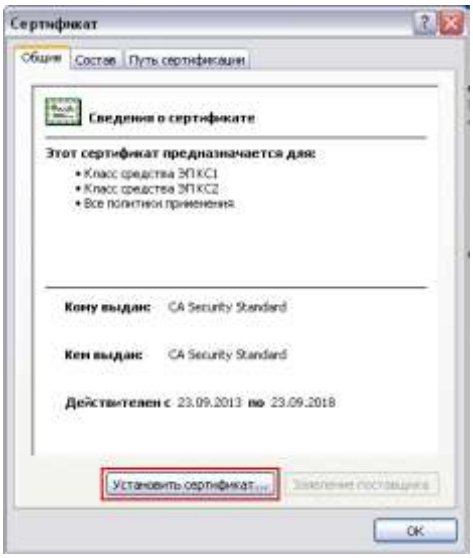
10. **Если откроется окно «Введите PIN -код для контейнера», необходимо ввести PIN -код для носителя.**

Внимание! PIN -код на носитель следует узнавать в Удостоверяющем центре.
PIN-код по умолчанию: 1234567890

11. **Если появится окно «Импорт сертификата eToken», нажмите «Cancel».**

УСТАНОВКА КОРНЕВОГО СЕРТИФИКАТА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

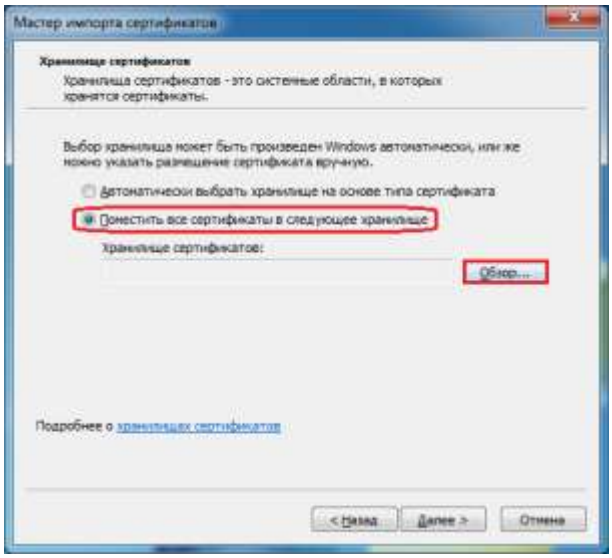
1. **Для скачивания корневого сертификата Удостоверяющего центра ООО "Стандарт безопасности" перейдите на сайт Удостоверяющего центра, и слева выберете соответствующий раздел или же перейдите по ссылке** http://www.yarsec.ru/UDC
2. **Выберите нужный сертификат (Корневой сертификат УЦ), нажмите "Сохранить". Для Квалифицированных сертификатов корневым является** CA Security Standart (2013).
3. **Извлеките (распакуйте) файл из сохранённого архива.**
4. **Нажмите по файлу сертификата двойным щелчком левой кнопки мыши.**



5. **В открывшемся окне нажмите "Установить сертификат…"(Рисунок 14)**

Выполните установку корневого сертификата удостоверяющего центра, следуя инструкциям мастера установки.
На шаге выбора "Хранилища сертификатов" укажите: "Поместить все сертификаты в следующее хранилище" нажмите "Обзор…" укажите "Доверенные корневые центры сертификации" нажмите "ОК"
(Рисунки 15, 16).

Рисунок 14



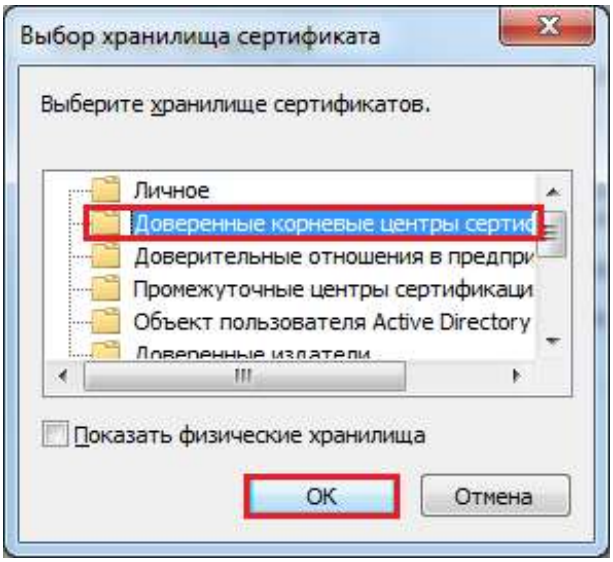


Рисунок 15

Рисунок 16

УСТАНОВКА СОС (СПИСКА ОТОЗВАННЫХ СЕРТИФИКАТОВ)

1. **Для скачивания СОС перейдите на сайт Удостоверяющего центра, и слева выберете соответствующий раздел или же перейдите по ссылке** http://www.yarsec.ru/UDC
2. **Выберите нужный пункт с сертификатом (Список отзыва сертификатов), нажмите "Сохранить".**
3. **Извлеките сертификат из архива и нажмите по нему правой кнопки мыши. Выберете пункт Установить список отзыва (Рисунок 17). Откроется мастер импорта сертификатов.**

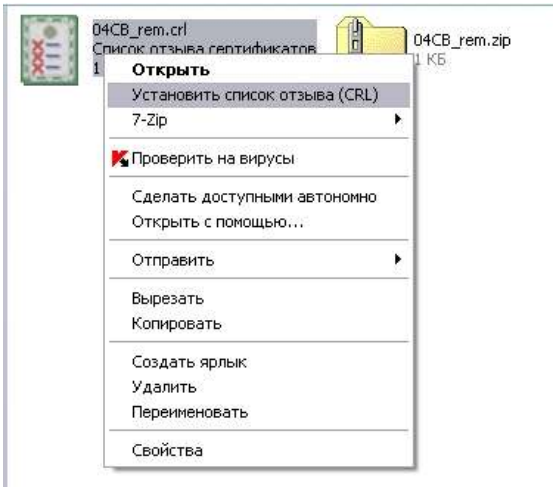


Рисунок 17

4. **Следуйте инструкциям мастера, на шаге выбора "Хранилища сертификатов" не меняйте положение точки и оставьте пункт Автоматически выбрать хранилище на основе типа сертификата.**
5. **По завершении установки появится окошко с надписью Импорт успешно выполнен (Рисунок 18)**

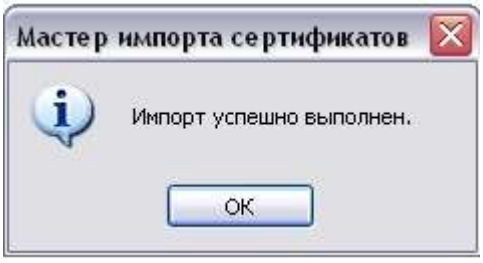


Рисунок 18

На этом процедура настройки автоматизированного рабочего места для работы с ЭП завершена.