**Инструкция по установке личного квалифицированного сертификата ключа проверки электронной подписи**

В данной инструкции описано как установить квалифицированный сертификат ключа проверки электронной подписи (далее - КСКП). Перед установкой сертификата необходимо знать, где находятся файл сертификата (Был получен в Удостоверяющем центре Федерального казначейства и имеет расширение .cer) и закрытый ключ (Был сгенерирован в программе АРМ Генерации ключей вместе с файлом запроса и заявлением на получение КСКП).

Запускаем программу Крипто-про. Для этого открываем меню «Пуск» - «Все программы» – «Крипто–про» – «Крипто-про CSP». В открывшемся окне программы открываем вкладку «Сервис» и нажимаем кнопку «Установить личный сертификат»



Рис. Запуск Крипто про в меню "Пуск" и открытие Вкладки «Сервис» и запуск установщика сертификата

 Нажимаем кнопку «Обзор», выбираем файл сертификата, нажимаем кнопку «Открыть»



Рис. Выбор файла сертификата

В строке «имя файла сертификата» появится путь к файлу сертификата, нажимаем кнопку «Далее»



Рис. Путь к файлу сертификата

В появившемся окне смотрим на данные сертификата, и если они совпадают с сертификатом, который хотим установить, нажимаем кнопку «Далее». (Если данные не совпадают, значит, на предыдущем шаге выбрали не тот)



Рис. Данных выбранного сертификата

 Теперь нужно указать закрытый ключ, соответствующий выбранному сертификату. Сделать это можно двумя способами – автоматически и вручную. Ставим галочку «Найти контейнер автоматически», и если контейнер определился, нажимаем кнопку «Далее». Если закрытый ключ был записан на защищенном носителе (например Рутокен или Etoken) то программа запросит Pin-код (этот Pin-код вы вводили при генерации ключа в АРМ Генерации ключей). Если при генерации на закрытый ключ был установлен пароль, то программа запросит этот пароль. Если вы забыли pin-код или пароль от закрытого ключа, придется делать новый КСКП. (стандартный pin-код для Рутокена 12345678, для Etoken 0123456789).

**Что делать, если контейнер не определился.** Если контейнер не определился, то необходимо вставить тот ключевой носитель, который был вставлен в компьютер на момент создания заявления на получение КСКП в программе АРМ генерации ключей. Если вы не обнаружили свой закрытый ключ ни на одном из съемных носителей, он мог остаться в реестре того компьютера, на котором происходила генерация. Если при генерации заявления на КСКП поле «Экспортируемый закрытый ключ» было оставлено по умолчанию в значении «ДА», то с помощью Программы «Крипто-про» - вкладка Сервис - кнопка «Скопировать» можно скопировать ключ из реестра на съемный диск, и продолжать полноценную работу (не забудьте после копирования удалить ключ из реестра). Так же важно понимать, что создать заявление и запрос на получение КСКП, при этом не создав закрытого ключа – **невозможно**. Если никто не удалил закрытый ключ, значит он где то есть. Если поиски ключа ни к чему не привели – необходимо готовить заявление на аннулирование и пакет документов на новый КСКП.



Рис. Выбор контейнера закрытого ключа

Перед вами появится окно выбора хранилища сертификатов. Нажимаем кнопку «Обзор», в появившемся окне выбираем «Личное», нажимаем «ОК». Галочку «Установить сертифкат в контейнер» ставить необязательно, но желательно. Если в поле «имя хранилища сертификатов» появилась запись «Личное» нажимаем кнопку «Далее».



Рис. Выбор хранилища сертификатов

Еще раз сравниваем данные и нажимаем «Готово»



Всё, личный сертификат установлен.

**Инструкция по установке корневого сертификата (квалифицированного)**

В данной инструкции описано как установить корневой (квалифицированный) сертификат Удостоверяющего центра Федерального казначейства (Далее - корневой сертификат). Перед установкой сертификата необходимо скачать его с сайта Управления Федерального казначейства по г. Москве из раздела ГИС / Удостоверяющий центр / Формы документов и программное обеспечение / Программное обеспечение /

Для установки корневого сертификата необходимо щелкнуть по скачанному сертификату левой кнопкой мыши два раза. Откроется окно сертификата. Выбираем кнопку «Установить сертификат».

 

Рис. Открытие сертификата

Откроется Мастер импорта сертификатов, Нажимаем кнопку «Далее» 

Рис. Окно мастера импорта сертификатов

В появившемся окне выбираем «Поместить все сертификаты в следующее хранилище», затем нажимаем кнопку «Обзор» и в появившемся списке выбираем «Доверенные корневые центры сертификации», нажимаем «ОК». В поле «Хранилище сертификатов» появится запись «Доверенные корневые центры сертификации», нажимаем кнопку «Далее»

 

Рисунок Выбор хранилища сертификатов

В завершающем окне мастера импорта сертификатов выбираем «Хранилище сертификатов, выбранное пользователем», нажимаем кнопку «Готово».



При появлении предупреждения безопасности выбираем «ДА»



Рис. Предупреждение безопасности

Всё, корневой сертификат установлен.