Инструкция по подготовке рабочего места АРМ МВ

1. Описание

АРМ межведомственного взаимодействия (АРМ-МВ) предназначен для использования сотрудниками Исполнительных Органов государственной власти и ОМСУ, а также подведомственных им учреждений, в процессе оказания государственных и муниципальных услуг юридическим и физическим лицам. АРМ-МВ позволяет передавать запросы к федеральным и региональным ведомствам на предоставление сведений по каждому Заявителю услуги, а также, принимать ответы на эти запросы по интернет - каналам , через Систему Межведомственного Электронного Взаимодействия (СМЭВ) федерального и регионального уровней.

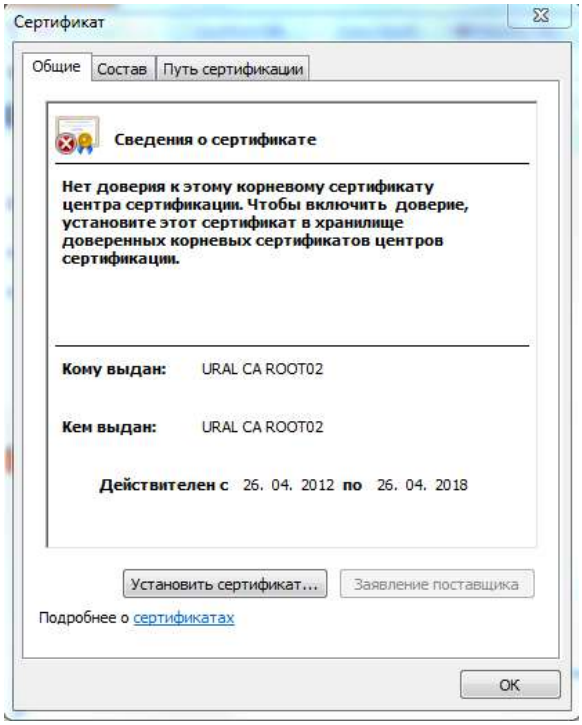
2. Общие положения

Для работы в АРМ ВМ на рабочей станции должна быть установлена ОС Windows XP или 7 32-bit и интернет-браузер Mozilla Firefox. Все необходимое программное обеспечение и инструкции для подготовки АРМ МВ находятся на сайте ГБУ СО «Оператор электронного правительства» по ссылке http://egov66.ru/home/information_systems/arm-mezhved . ЭЦП для подписания документов Вам необходимо получить на «Удостоверяющем центре Урал», во время подготовки рабочего места ЭЦП не должен быть подключен к рабочей станции.

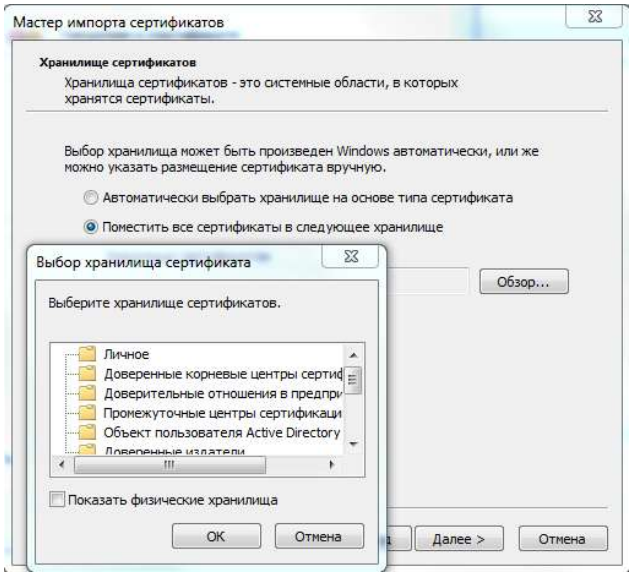
3. Подготовка рабочего места

Для подготовки рабочего места Вам необходимо:

1. Установить интернет-браузер Mozilla Firefox и следуя указаниям мастера выполнить установку
2. Установить плагин Java7 и следуя указаниям мастера выполнить установку
3. Установить крипто-провайдер Cryptopro CSP и следуя указаниям мастера выполнить установку
4. Установить плагин для Cryptopro и следуя указаниям мастера выполнить установку
5. Установить плагин для Etoken PKI client и следуя указаниям мастера выполнить установку
6. Установить корневой сертификат, далее кликнуть на Установить сертификат…,

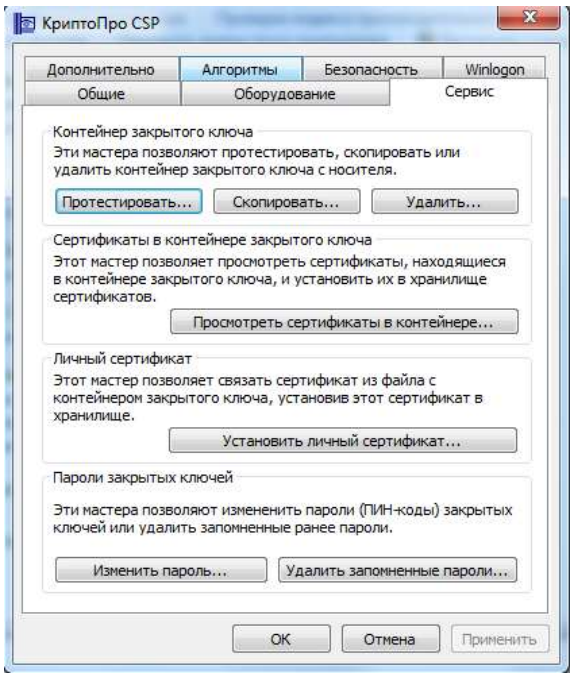


кликнуть Далее и поместить сертификат в Хранилище – Доверенные корневые центры сертификации,

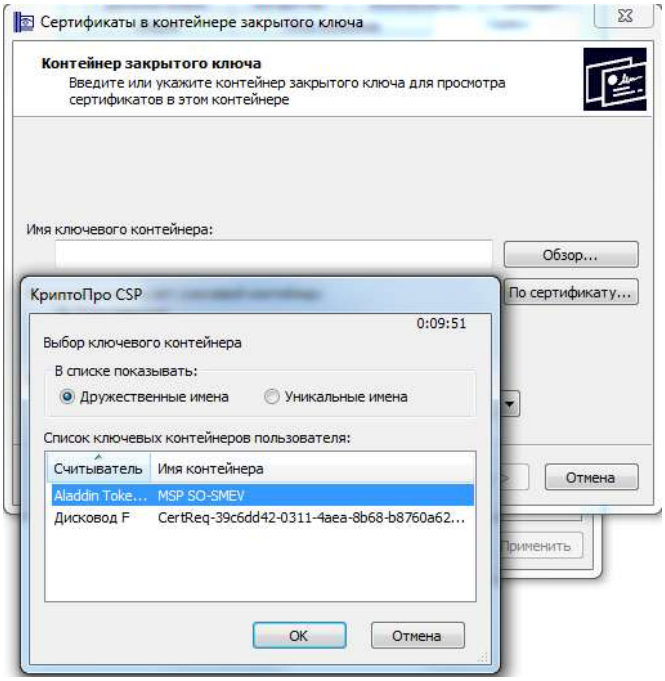


кликнуть Далее и Готово, дождаться пока импорт сертификата будет завершен и кликнуть Ок в меню сертификата

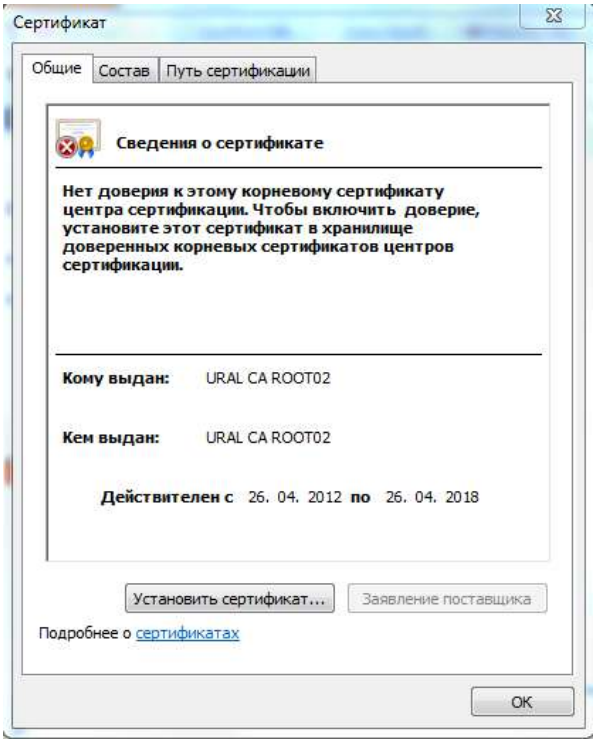
7. Установить подчиненный сертификат, установка подчиненного сертификата идентична установке корневого сертификата
8. Установить ЭЦП в Cryptopro, запустив Cryptopro в Панели управления. В Cryptopro кликнуть на вкладку Сервис и кликнуть Просмотреть сертификаты в контейнере…,



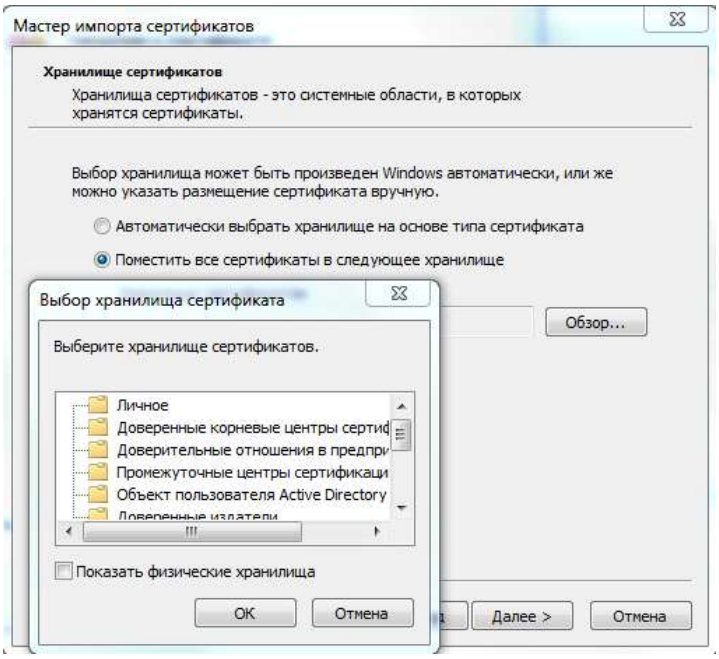
и кликнув Обзор, выберите ЭЦП для АРМа,



кликните Далее и войдите в Свойства, установите сертификат,



кликнуть Далее и поместить сертификат в Хранилище – Личные,

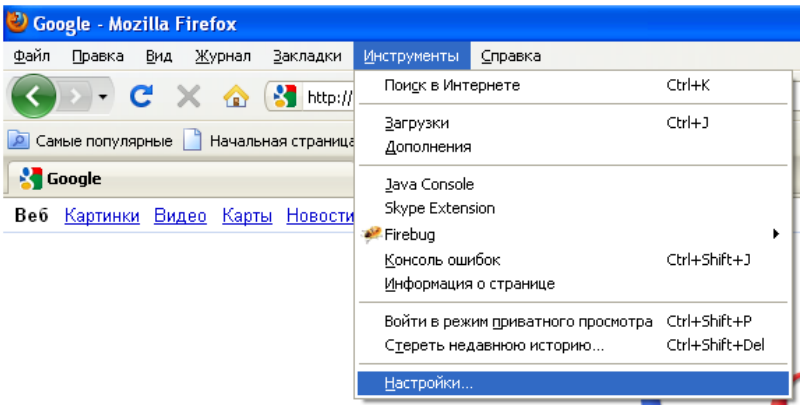


кликнуть Далее и Готово, дождаться пока импорт сертификата будет завершен и кликнуть Ок в меню сертификата и закрыть Cryptopro

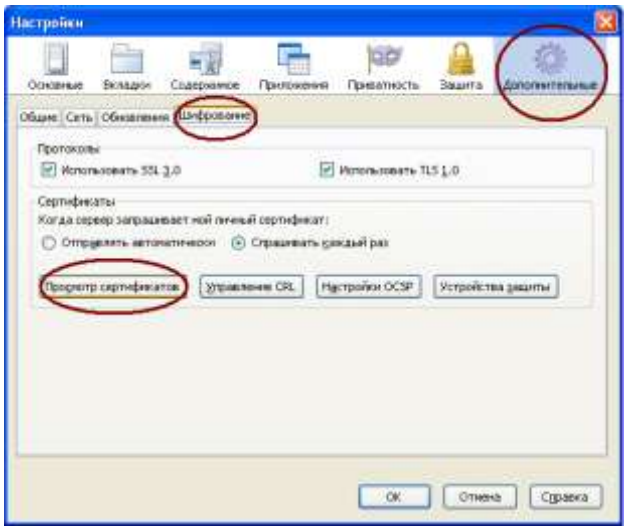
9. Установка персонального или универсального сертификата пользователя для доступа в АРМ-МВ.

1) Сохранить полученный от ОЭП файл сертификата доступа пользователя в АРМ –имя файла либо svo_userxx – для универсальных сертификатов, либо Фамилия пользователя

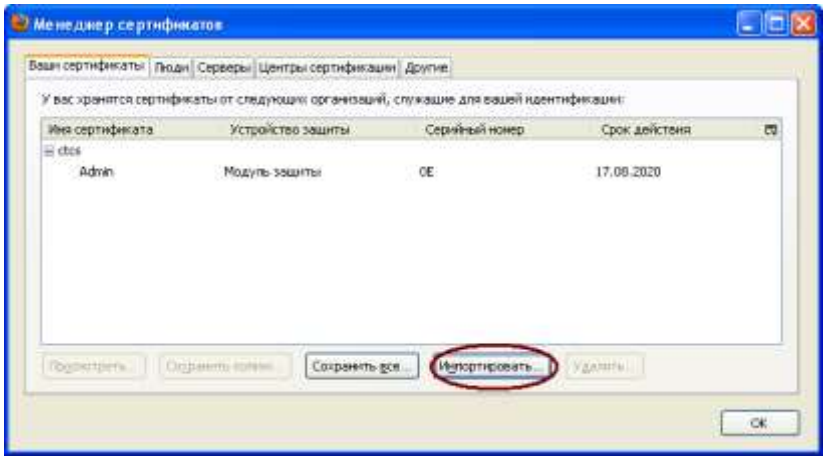
2) Зайти в пункт меню «Инструменты», выбрать «Настройки».



Зайти в пункт «Дополнительные», перейти на вкладку «Шифрование».

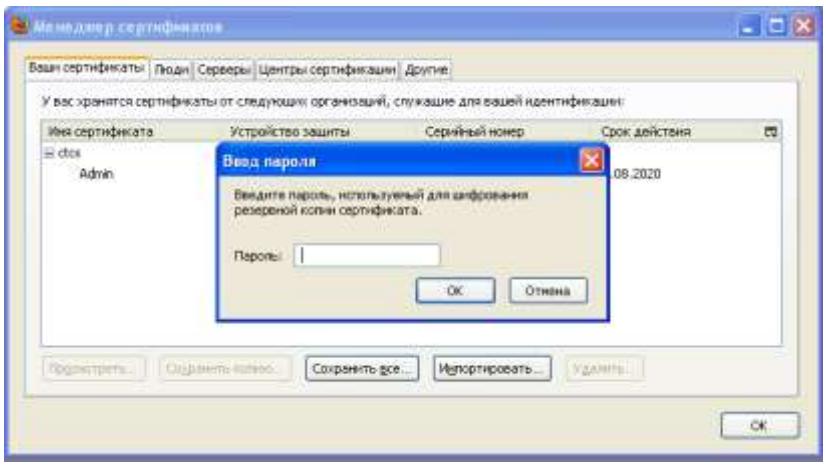


В окне Менеджера сертификатов выбрать вкладку «Ваши сертификаты». Нажать кнопку «Импортировать».

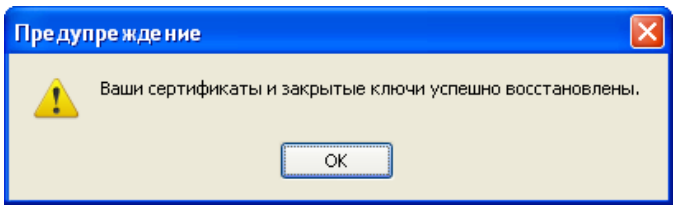


Выбрать нужный файл сертификата.

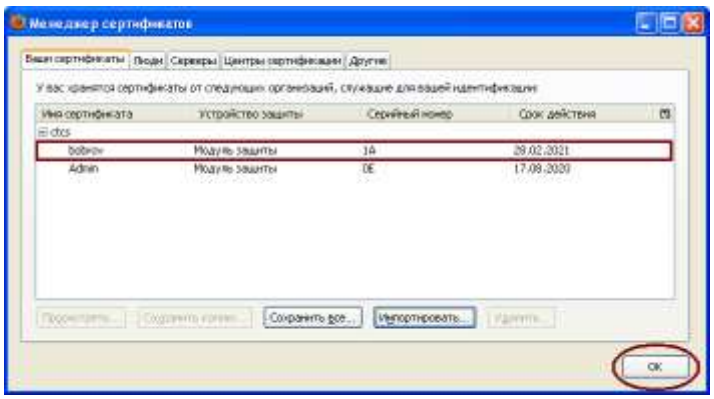
3) Ввести пароль, который соответствует имени сертификата



При успешном вводе на экране появится сообщение.



В списке сертификатов будет отображаться импортированный сертификат. Нажмите кнопку «ОК».



Нажмите кнопку «ОК».

Импорт завершен.

После того как Вы импортировали сертификат настройки можно закрыть, подготовка завершена, можно заходить на портал по адресу https://172.21.166.133/portal

4. Дополнительная настройка

4.1. С целью исключения появления окна для ввода пароля (вводить пароль нельзя!!!, т.к. блокируется eToken) при запуске АРМ

"Требуется пароль для доступа в etoken" ,

необходимо сделать следующее, чтобы исключить появление этого окна.

1. Открыть настройки Firefox (Firefox / настройки). Выбрать вкладку Дополнительные, перейти на вкладку Шифрование и нажать кнопку Устройства защиты.
2. В Окне Менеджера устройств нажать на кнопку <Выгрузить> для библиотеки поддержки PKCS#11.

4.2. Прописать в файле:

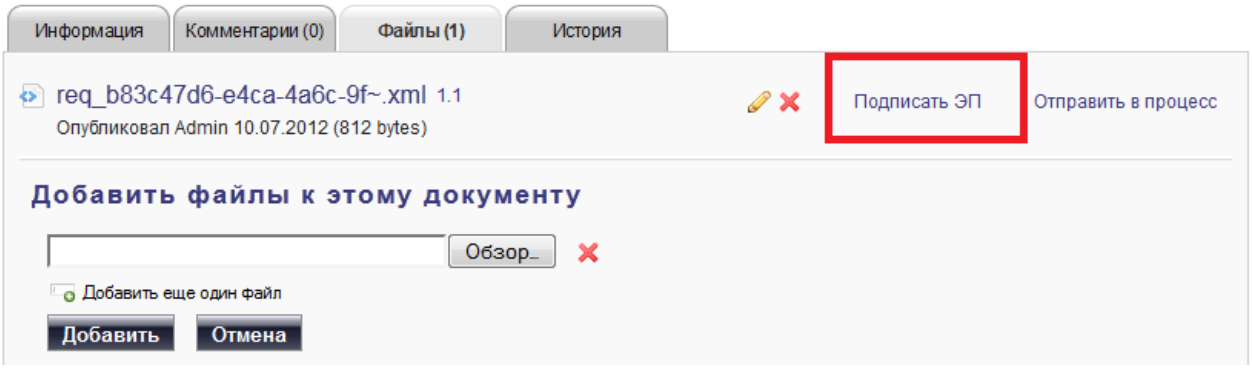
C:\windows\systems32\drivers\etc\host (открыть этот файл можно блокнотом) значение

172.21.166.133 66.sir.egov.local

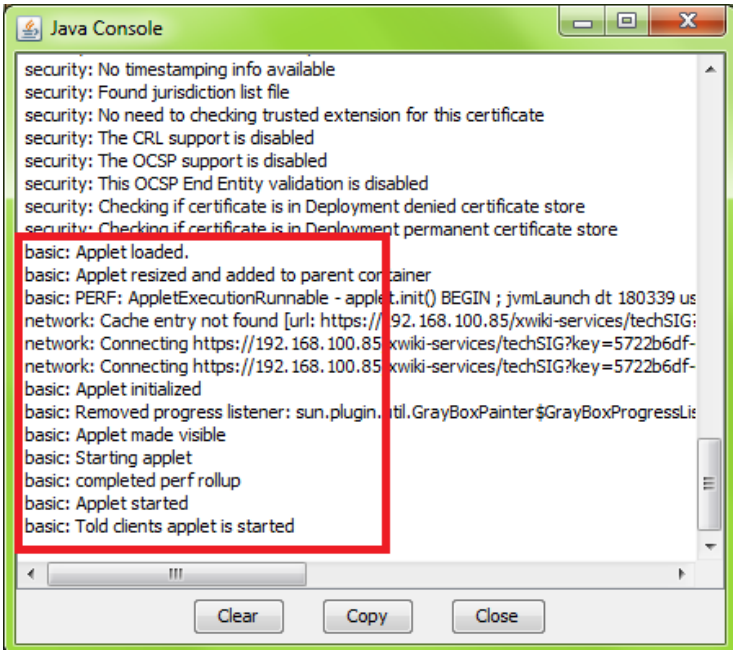
5. Проверка работоспособности

Открыть технологический документ, у которого есть прикрепленный файл.

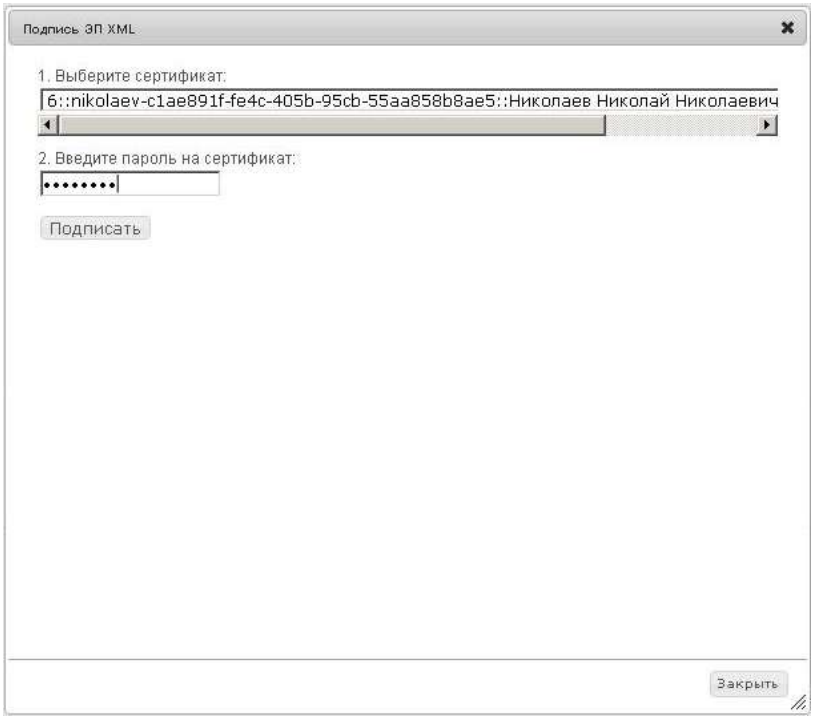
Напротив имени файла нажать "Подписать"



Об успешном запуске плагина подписи говорит открывшаяся Java Console



Выбрать сертификат из списка, ввести пароль, нажать кнопку "Подписать"



После обновления страницы в список файлов добавится подписанный файл.