Лабораторная работа №4.

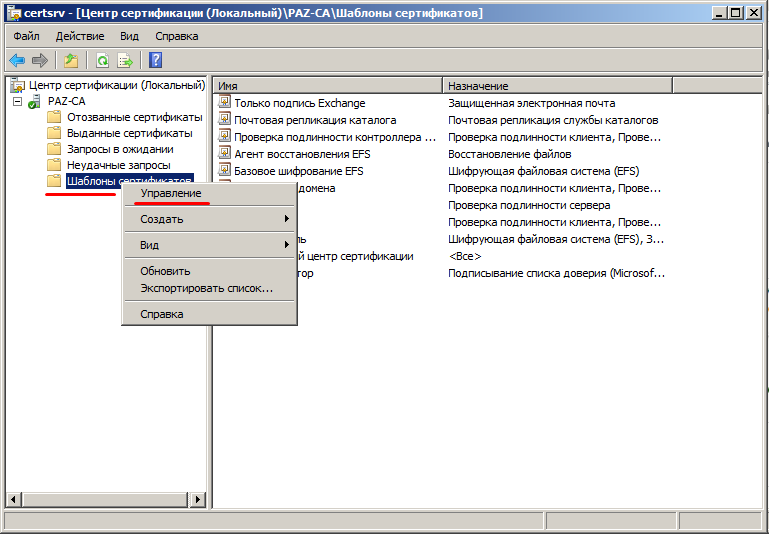
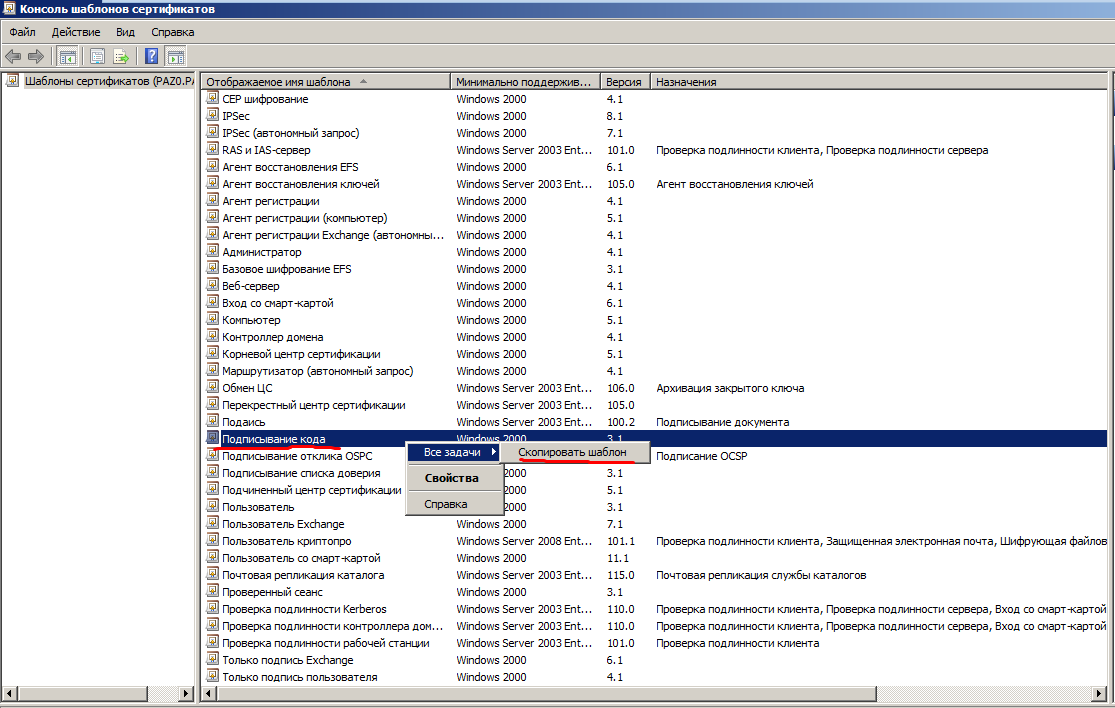
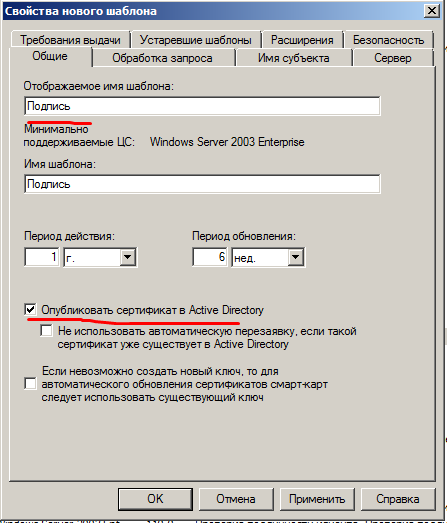
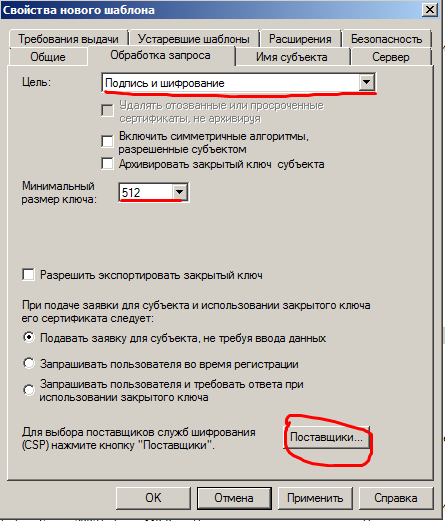
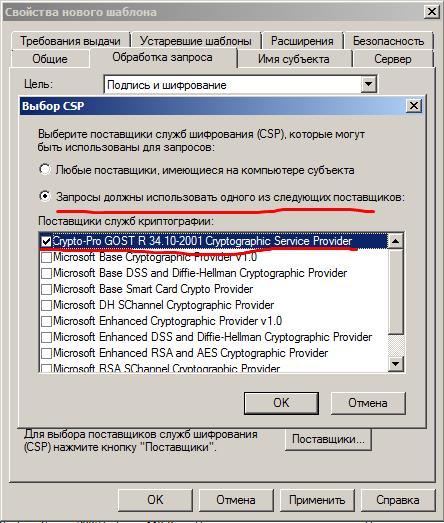
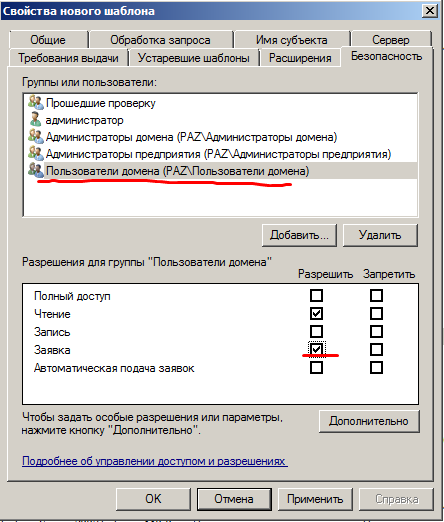
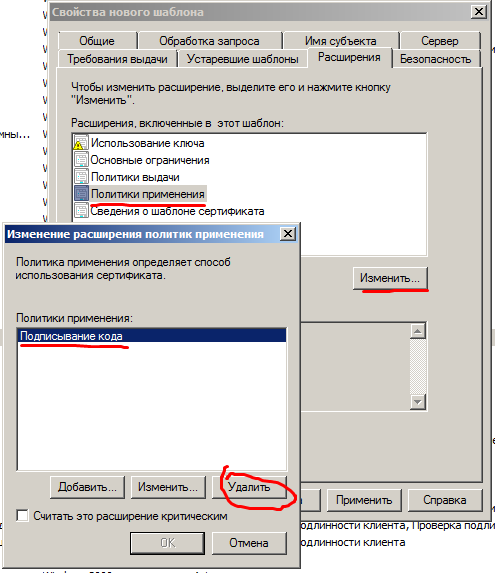
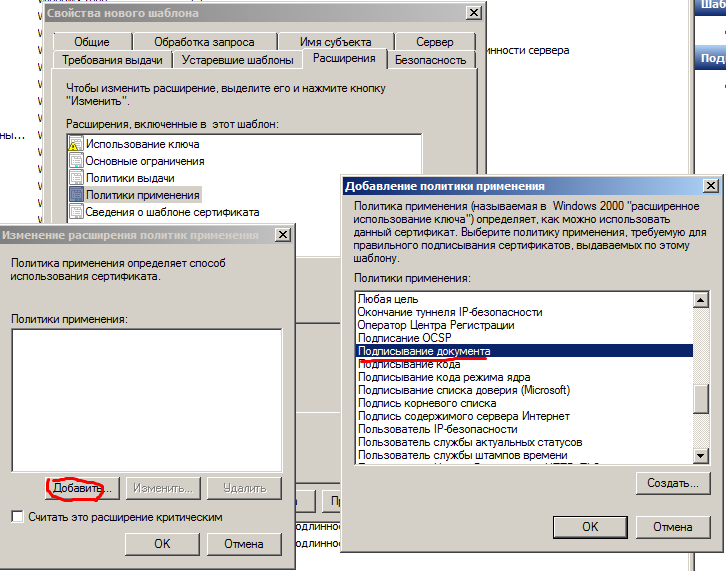
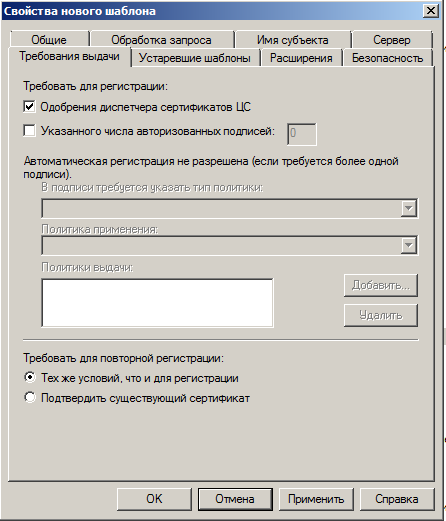
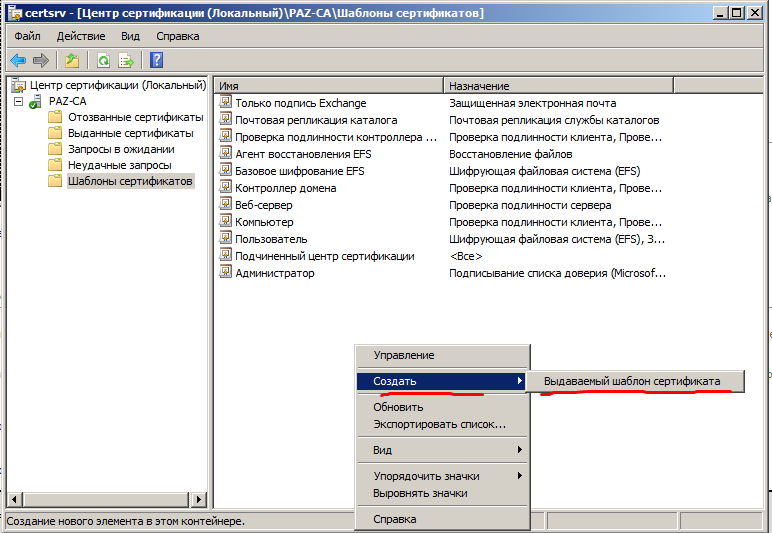
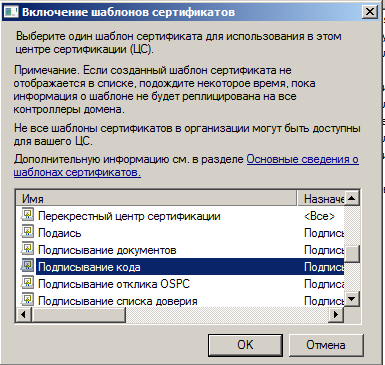
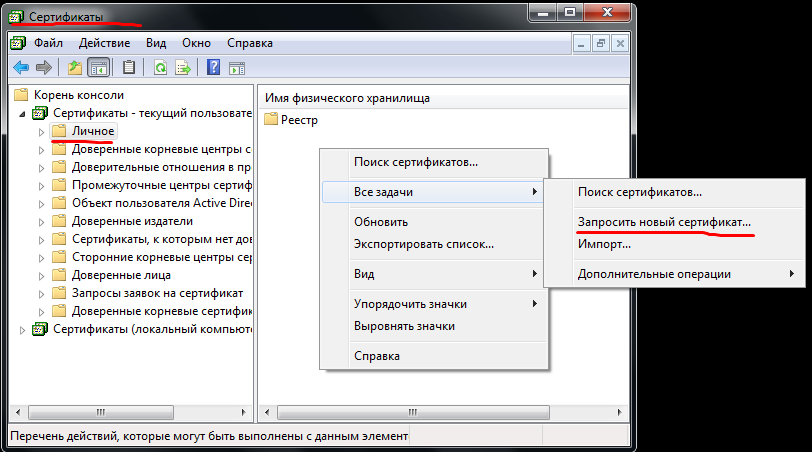
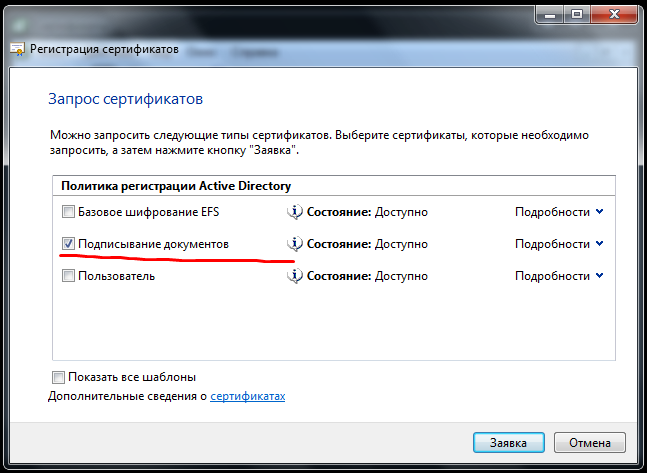
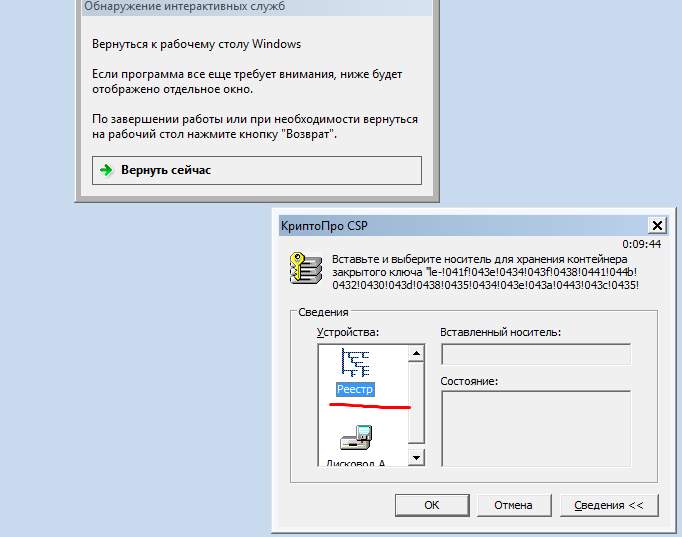
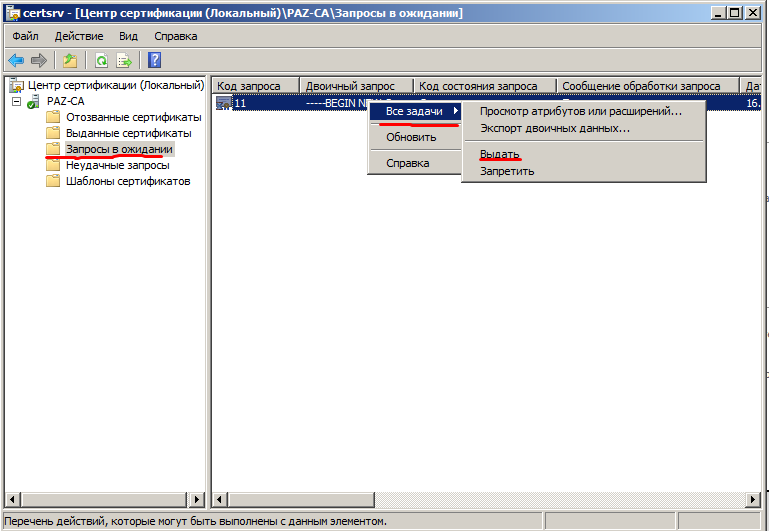
**Удостоверяющий центр.**

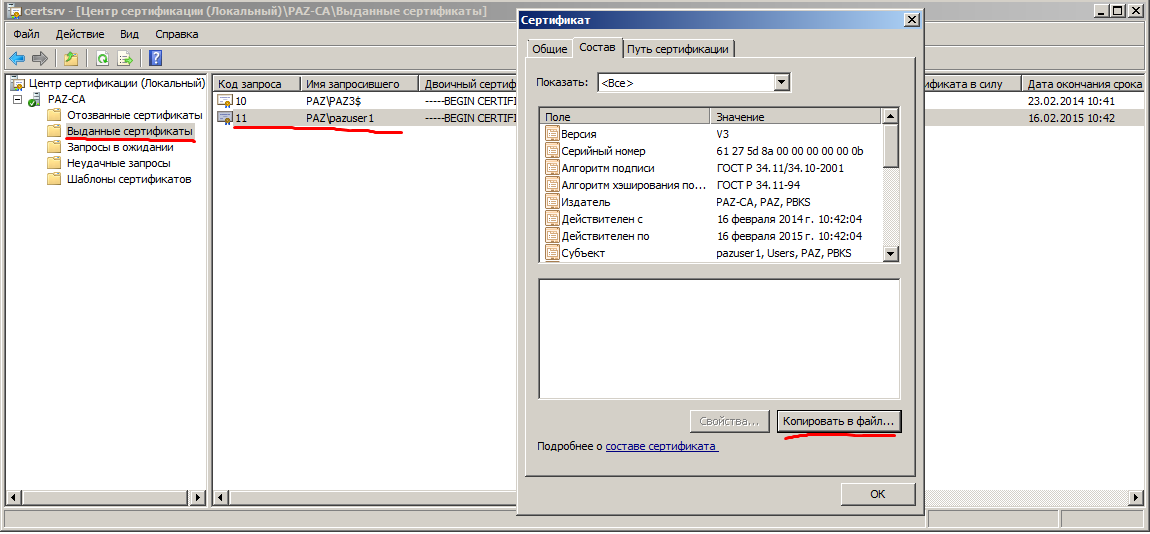
Выполнил: Мамбреян З.А.

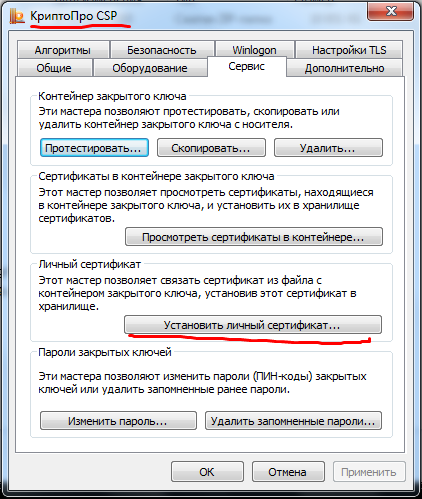
Группа: К3440

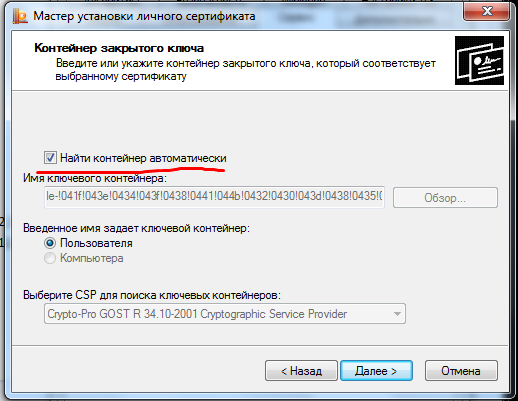
Санкт-Петербург

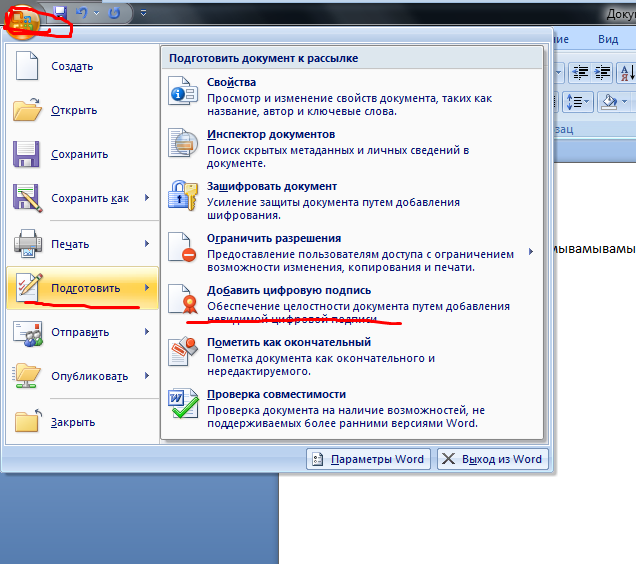
2016

1. Откатите ВМ PAZ0, PAZ3, PAZUSER1 до снапшота “Lab 2” и запустите их.
2. Войдите в PAZ3 под доменным логином **администратор:PAZ\_LOCAL1**
3. Запустите центр сертификации
4. Выберете в контекстном меню «Шаблоны сертификатов» пункт «Управление» 
5. После этого в «Консоли шаблонов сертификатов» найдите шаблон «Подписывание кода» и в контекстном меню кликните пункт «Скопировать шаблон» 
6. Далее выберете пункт Windows Server 2003 Enterprise
7. Переименовываем новый шаблон в «Подписывание документа» 
8. В цели выставляем подписывание и шифрование, хотя хватило бы и подписывания, минимальный размер ключа выставляем в 512 (кстати почему?) и настраиваем поставщика 
9. Добавляем в безопасность группу «Пользователи домена» и выставляем ей разрешение на запрос
10. В расширениях в «Политики применения» удаляем все что есть и добавляем «Подписывание доокументов» 
11. В требованиях выдачи ставим галочку напротив «Одобрение диспетчера…» 
12. Жмем «ОК» и собственно шаблом мы создали. Закрываем остнаску.
13. Теперь создадим выдаваемы шаблн сертификата на базе созданного шаблона 14. Выбираем «Подписывание документов» или как вы его там назвали
14. Теперь мы готовы получить сертификат. Переключаемся на ВМ PAZUSER1 и выполняем вход под учетной записью домена PAZ **pazuser1:plotter\_12.** Открываем оснастку «Сертификаты» (если нет, то гуглим как добавить) и переходим в личные сертификаты текущего пользователя, и выполняем запрос нового сертификата.
15. Выбираем «Подписывание документов» и жмем кнопку «Заявка»
16. Тут должно замигать окошко перехода на генерацию контейнера, переходим туда, выбираем в качестве ключевого носителя реестр, генерируем ключ (там рассказано чего делать) и задаем пароль для контейнера. Собственно на это действия на стороне клиента по запросу сертификата закончились.
17. Теперь нам необходимо подтвердить или отклонить запрос. Для этого возвращаемся в ВМ PAZ3 если осуществляли выход из системы то заходим обратно под тем же пользователем и открываем оснастку «Центр сертификации», переходим на вкладку «Запросы в ожидании» и видим там наш запрос. На всякий случай смотрим поля (а вдруг враги) и, если все хорошо выдаем сертификат.
18. После этого сертификат необходимо передать на машину с которой производился запрос сертификата. Для этого переходим во вкладку «Выданные сертификаты», открываем свойства сертификата, выбираем «копировать в файл», выполняем сохранение сертификата, а затем переносим его любым доступным способом на ВМ PAZUSER1 (по средствам флешки, и передав по сети)

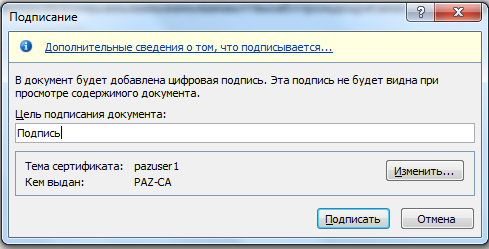


1. Возвращаемся на ВМ PAZUSER1 и запускаем «КриптоПро CSP» , на вкладке сервис жмем «Установить личный…»
2. Указываем мастеру на перенесенным нами файл сертификата и при выборе контейнера выставляем галочку «Найти автоматически…», далее ничего не меняя доходим до конца импорта (Можно поместить ключ в контейнер, но нам это не критично)

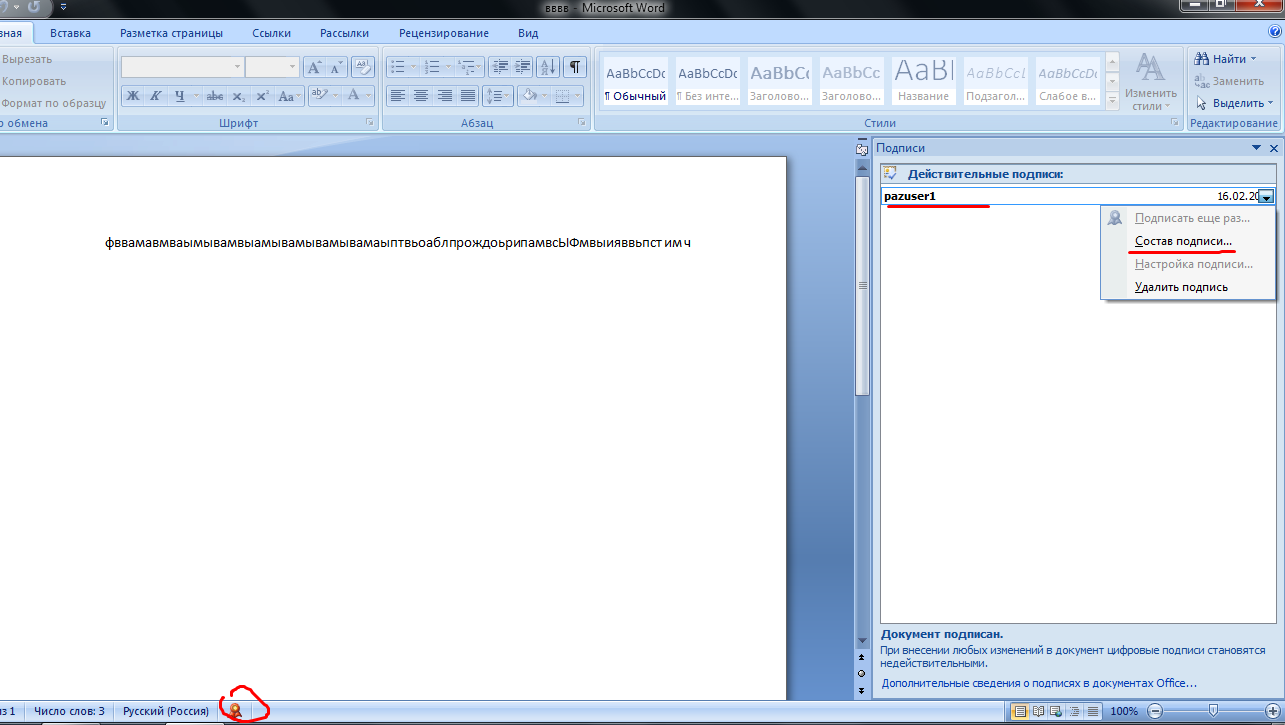


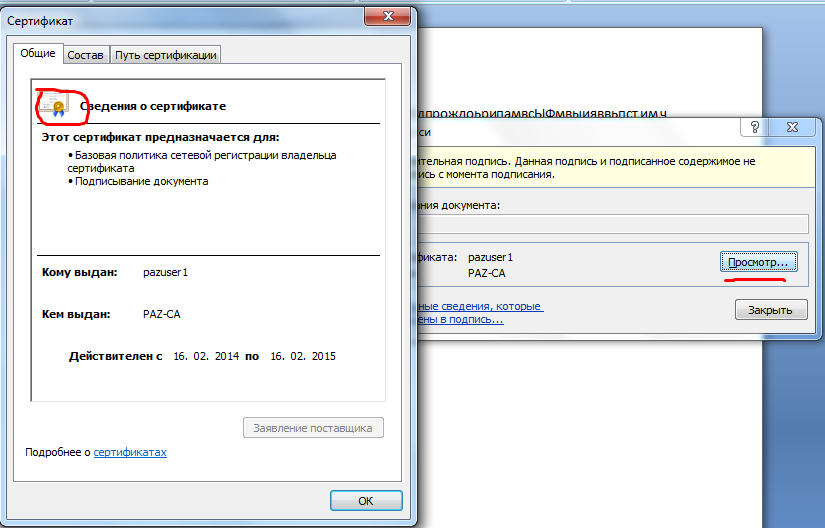
1. Далее открываем Word, набираем произвольный текст и жмем кнопку главного меню 🡪Подготовить 🡪 Добавить цифровую подпись.

Соглашаемся с предложением сохранить документ и сохраняем в папку «C:\Для общих документов» для избежание проблем с ограничениями доступа, и подписываем полученный документ.

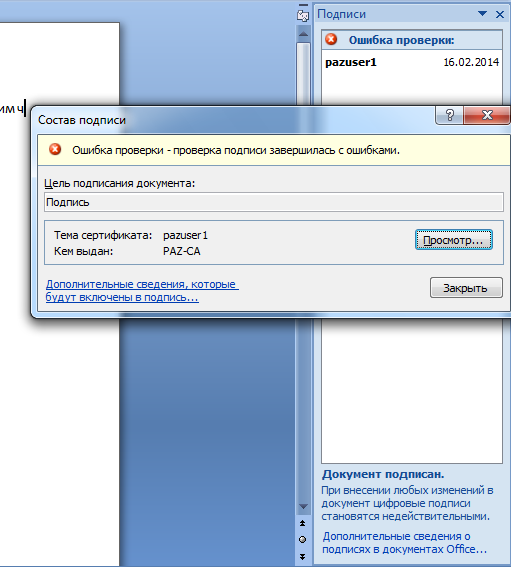


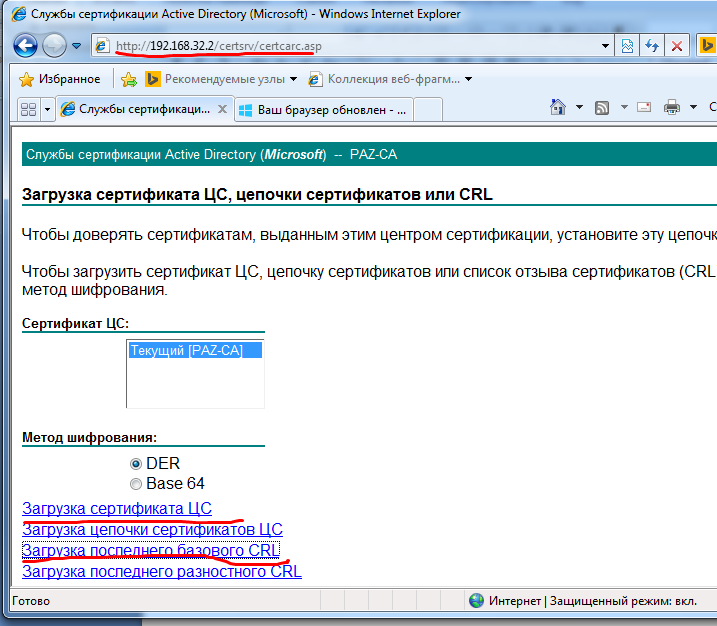
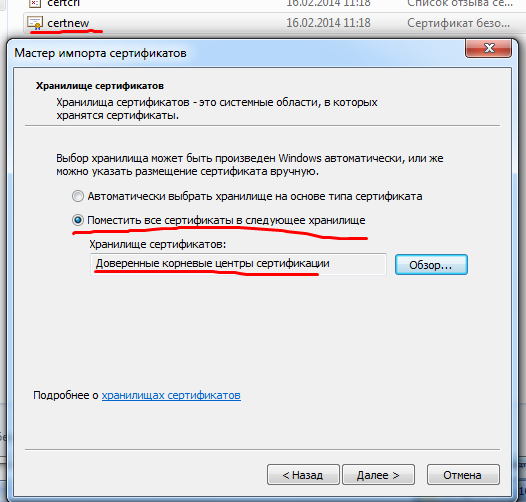
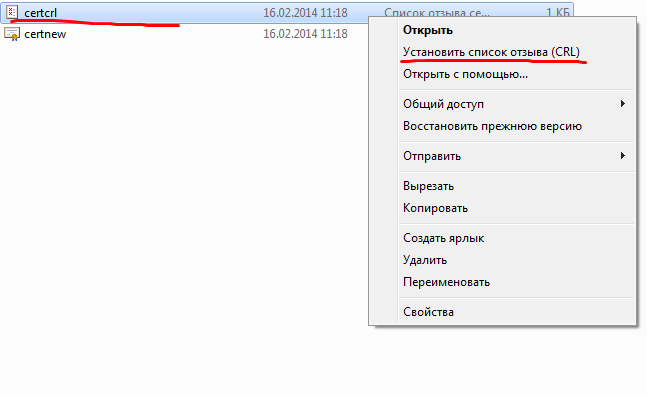
1. Далее выполняем вход на эту же ВМ под пользователем **pazuser2:plotter\_13**, открываем сохраненный нами документ, смотрим наличие подписи и проверяем ее валидность. Все отлично.





1. Теперь выполняем вход на эту же ВМ, но уже под локальной учетной записью PAZUSER1\ADMIN**:PAZ\_LOCAL1**, выводим ее из домена в какую-нибудь рабочую группу (аналогично вводу в домен только в обратную сторону) и перезагружаемся. После этого выполняем вход под той же локальной учетной записью, открываем подписанный документ и смотрим на валидность подписи. Подпись не проверена (Почему?)



1. Нас такой антивариант ни в коей мере не устраивает и поэтому мы открываем единственный доступный браузер и идем по адресу [**http://192.168.32.2/certsrv/**](http://192.168.32.2/certsrv/), входим под учетной запись домена PAZ **pazuser1:plotter\_12.** Переходим к «загруска сертификата ЦС…» и загружаем сертификат ЦС и последний базовый CRL (в чем разница между ним и более другим CLR?)
2. Переходим в туда куда сохранились сертификат и CLR и выполняем установку сертификата, при этом помещаем его в «Доверенные корневые центр...»
3. Теперь устанавливаем CRL (а что будет если не установим?), здесь все оставляем как есть- само подтяниться. 
4. Заново открываем подписанный документ и… и подпись валидная.

