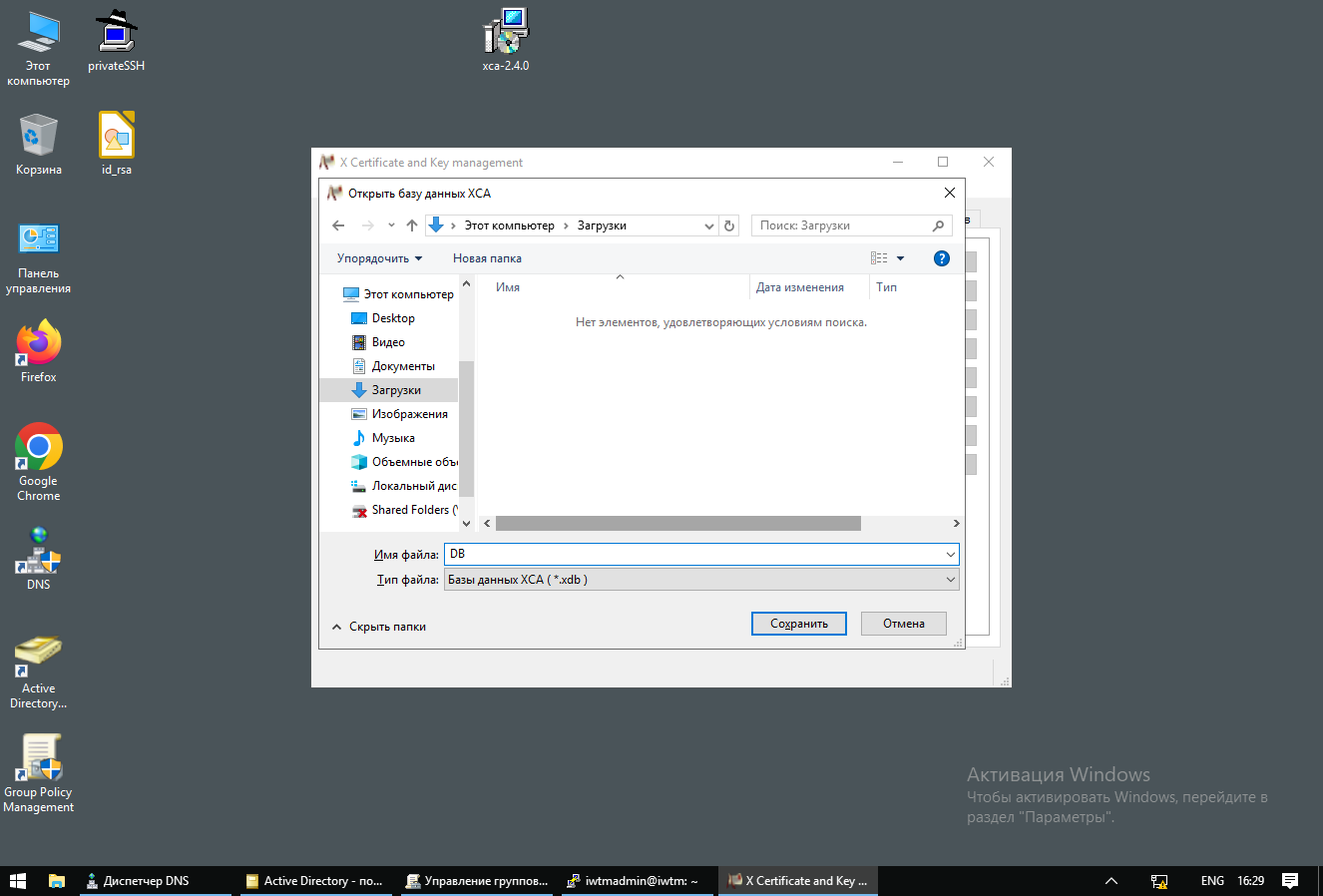
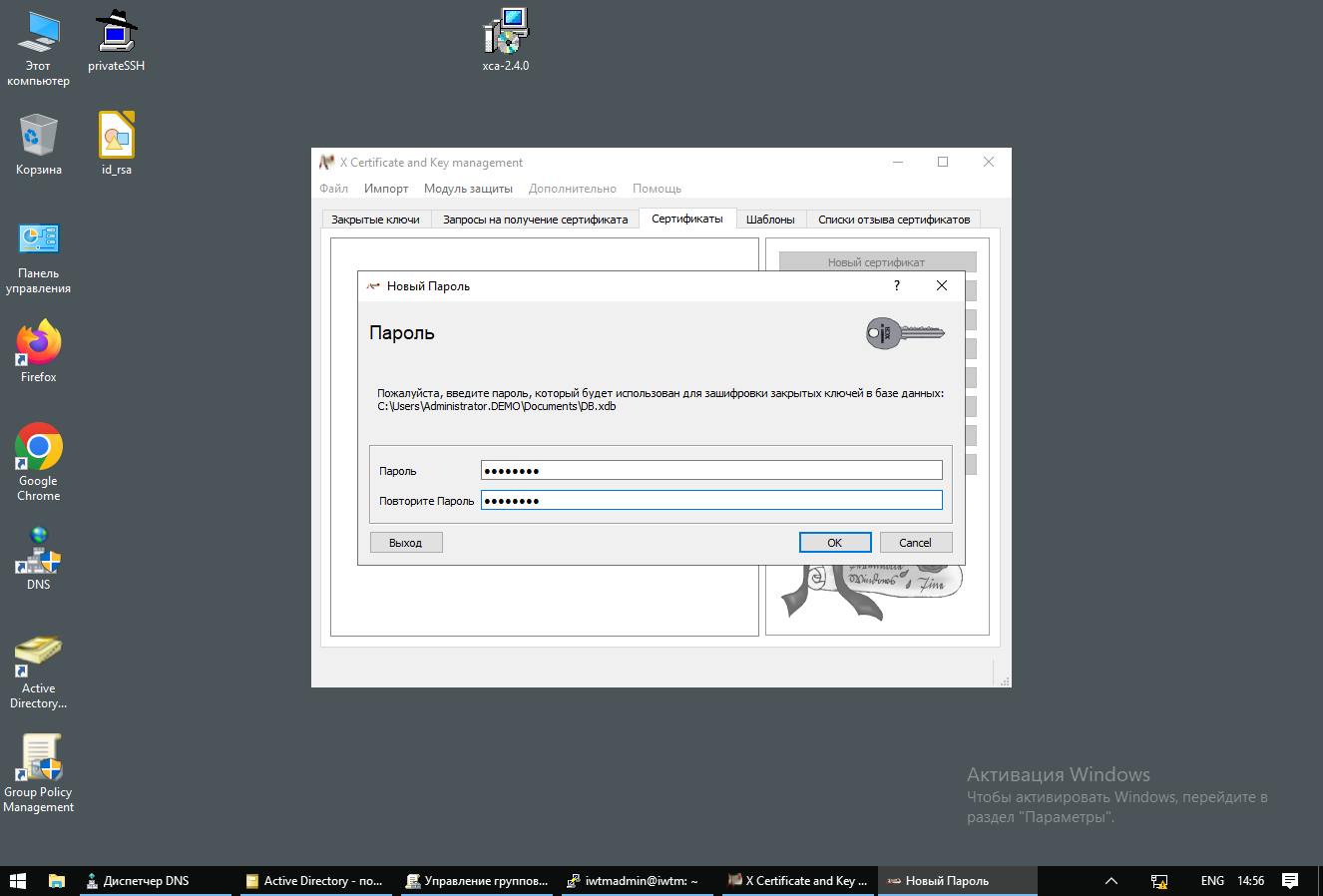
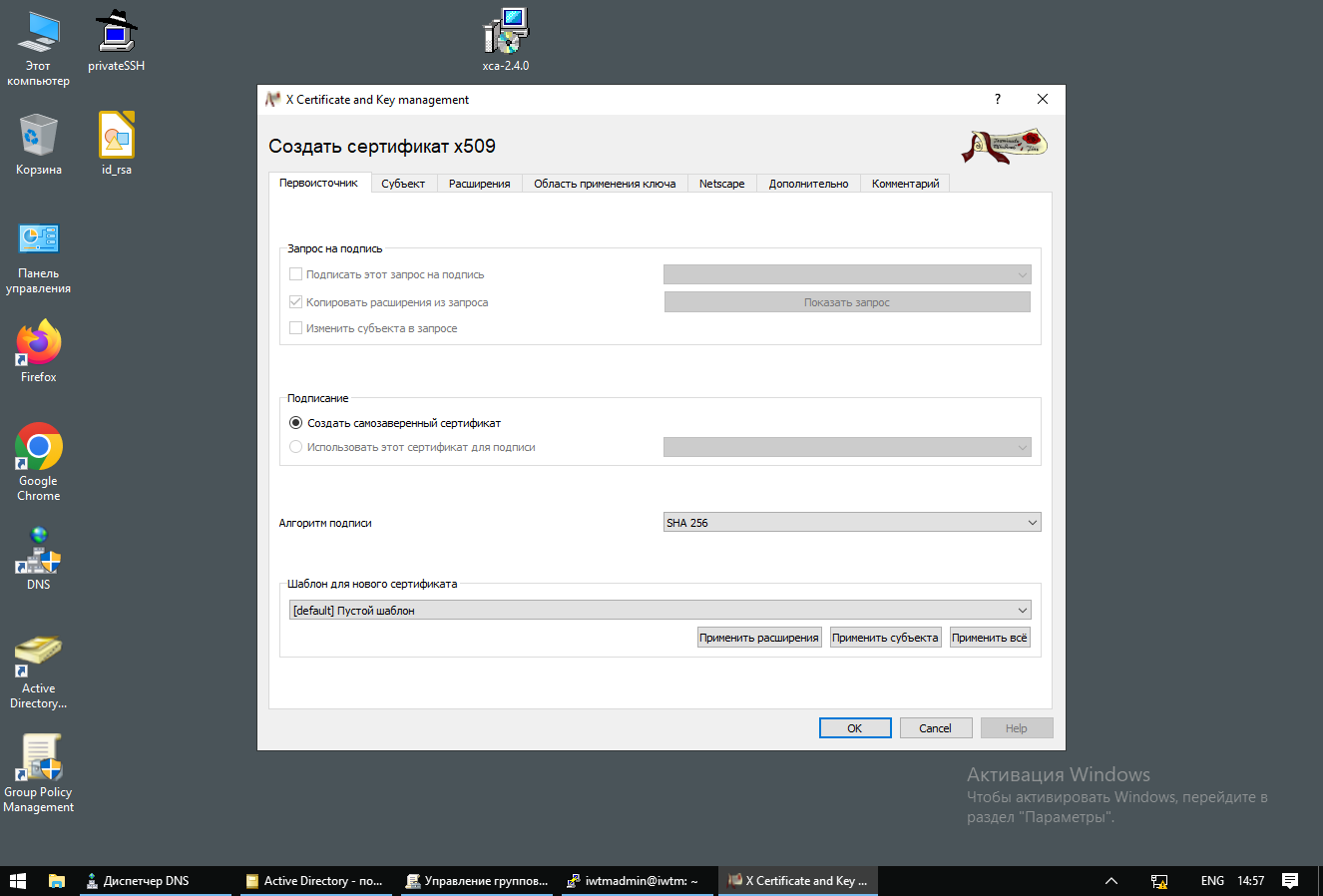
1. Устанавливаем XCA.
2. Создам новую базу данных. Сохраняем в любое место. Задаем пароль.



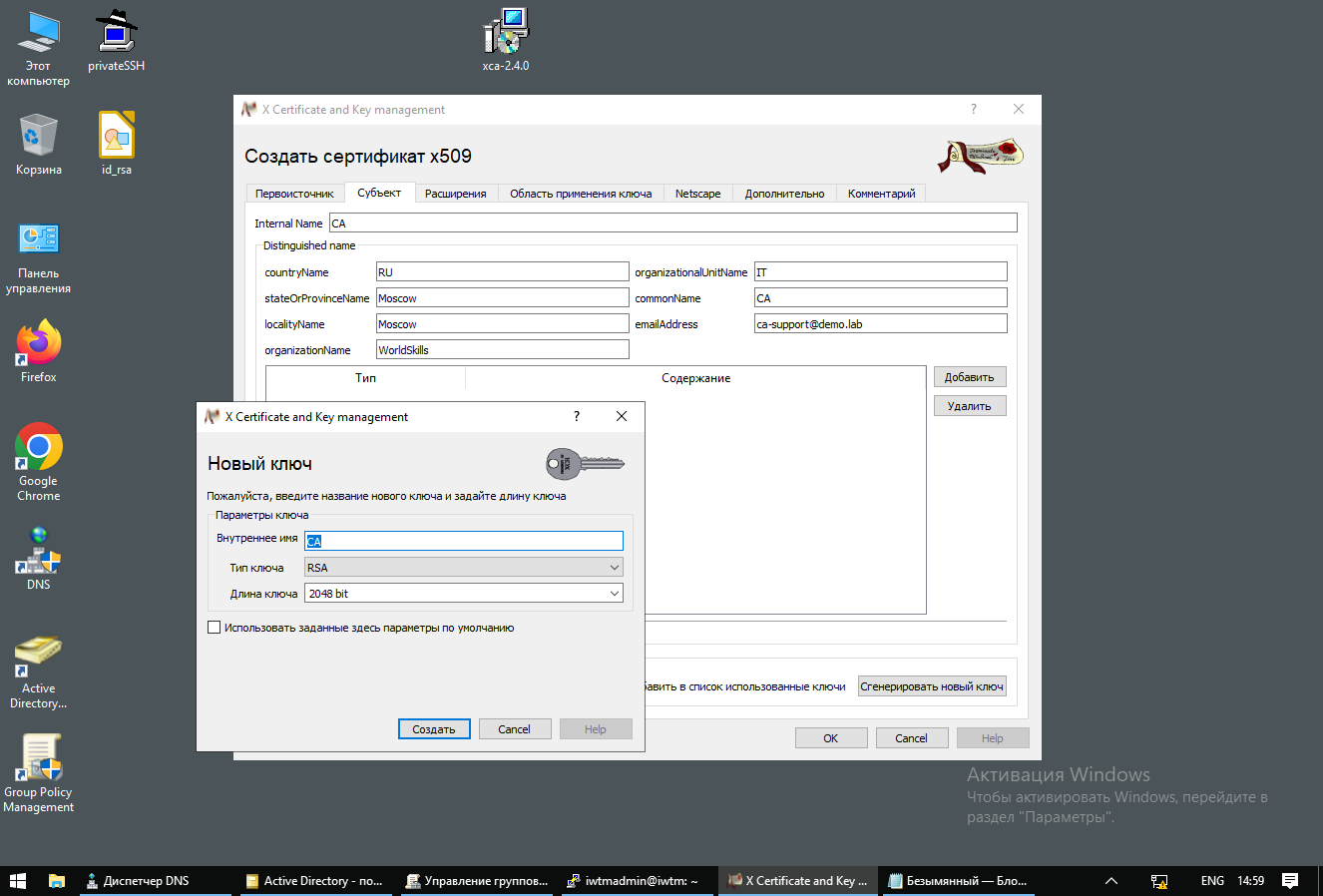


1. Создаем корневой сертификат CA

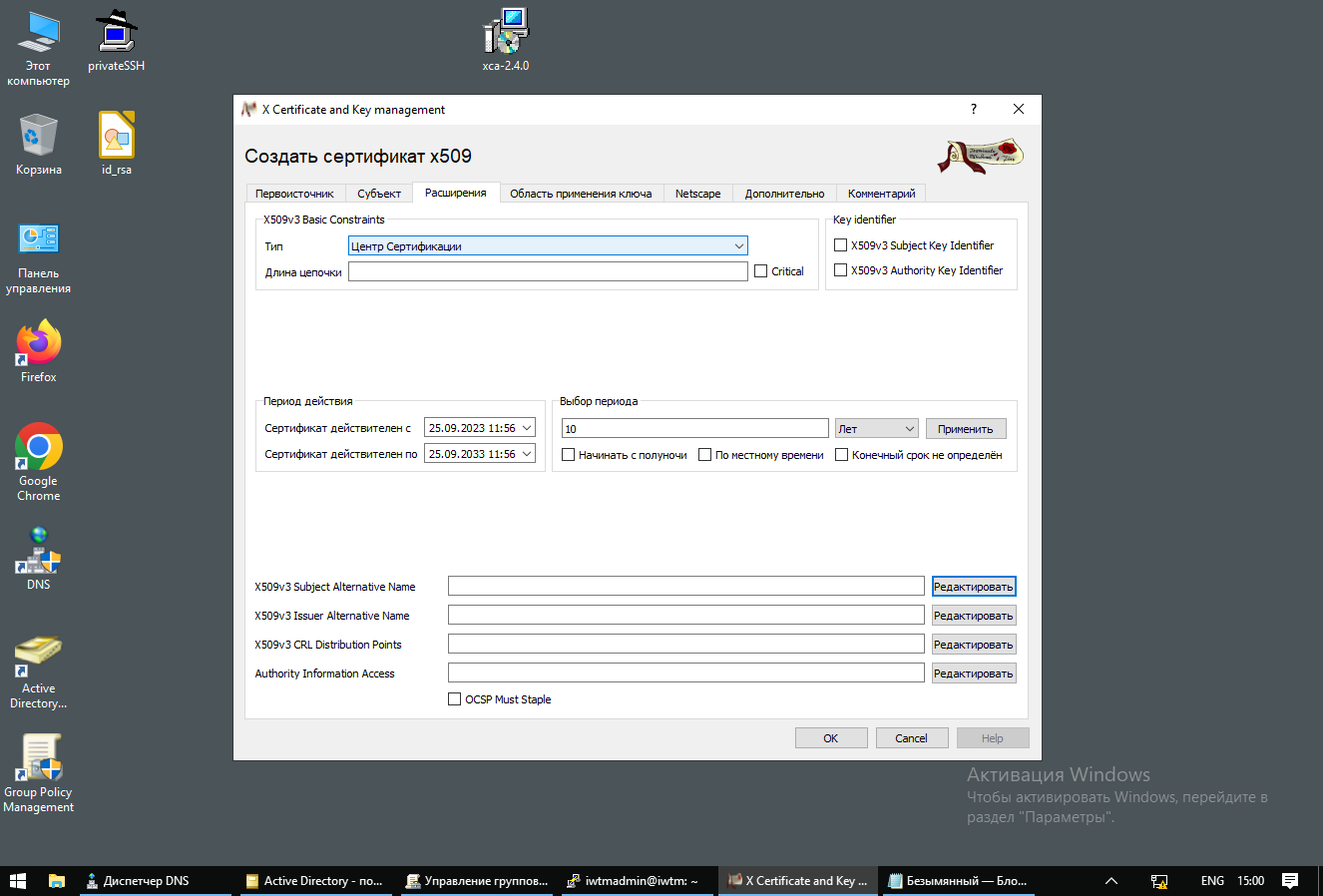
Во вкладке Первоисточник оставляем все по умолчанию.



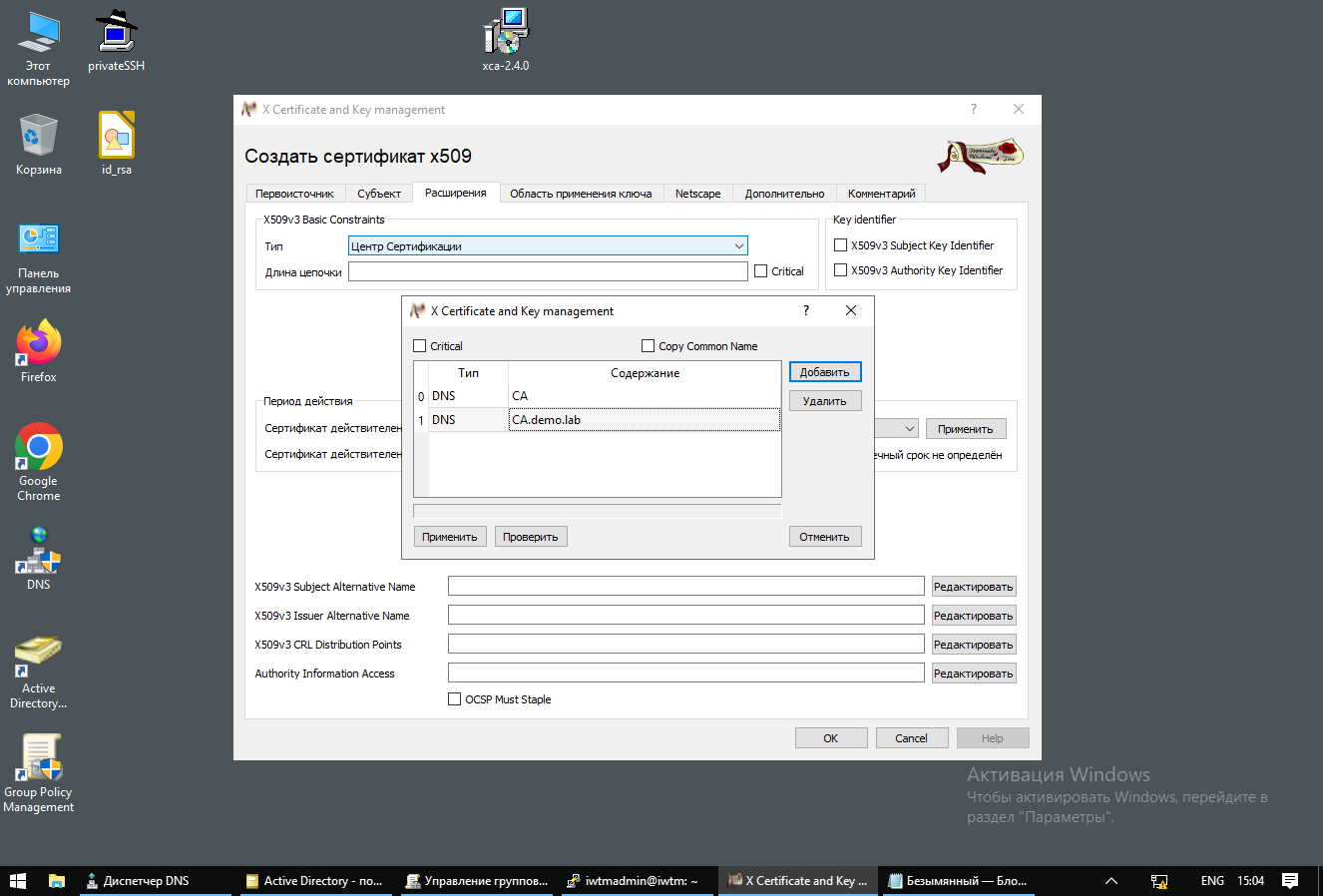
Во вкладке Субъект заполняем все поля и в этом же окне генерируем новый ключ.

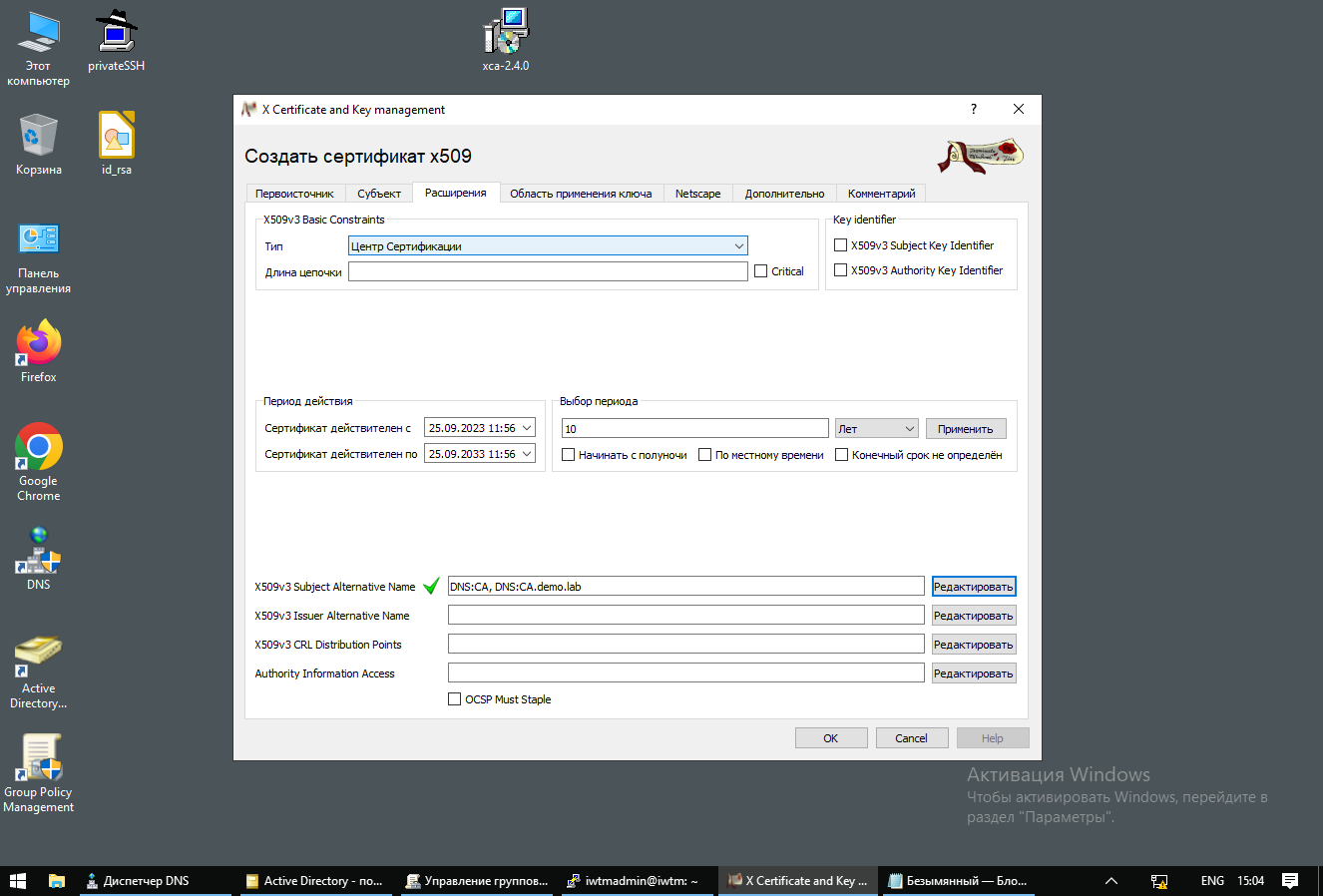


На вкладке Расширения выбираем Тип Центр Сертификации, а также задаем срок действия сертификата.



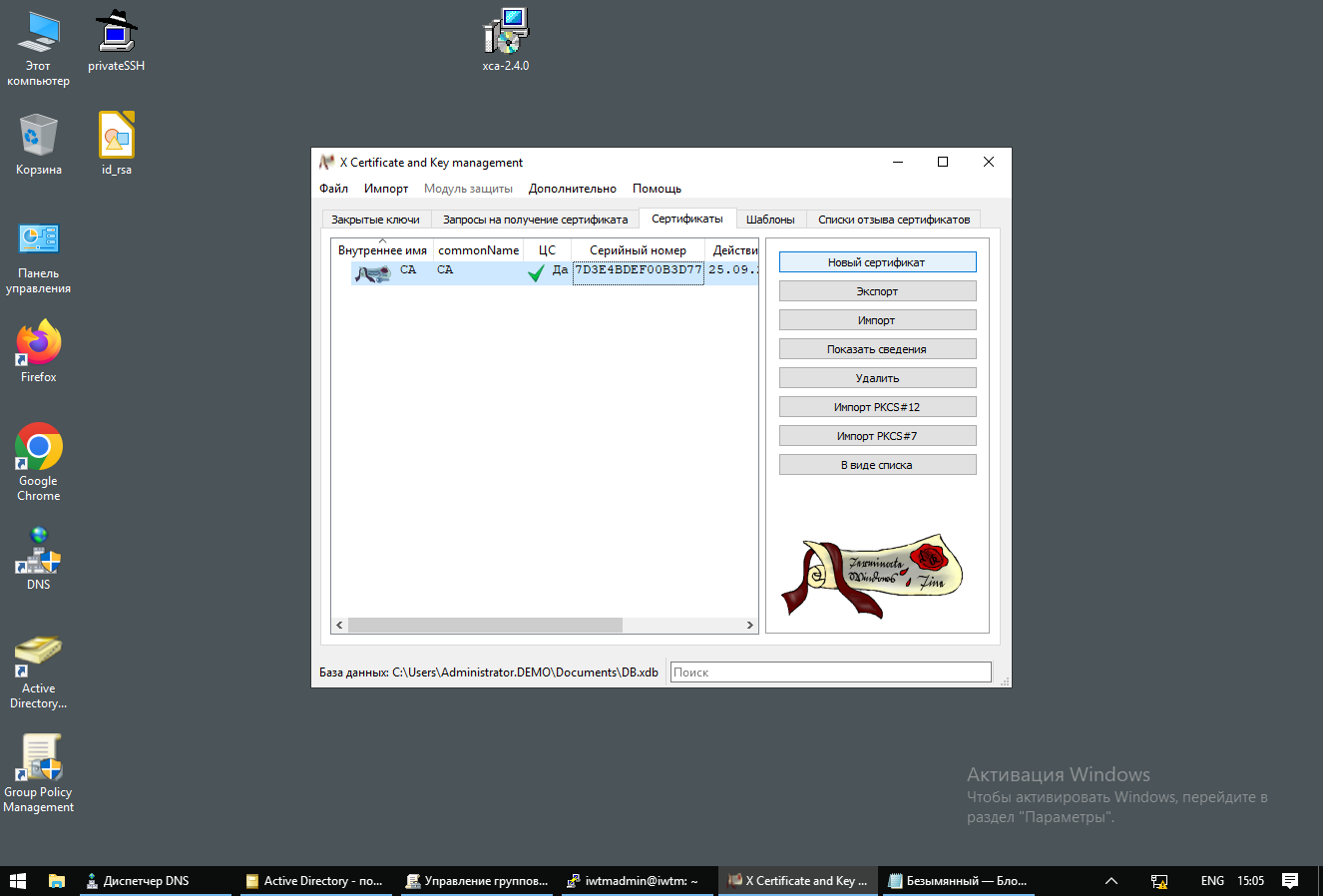
Задаем Альтернативные имена субъекта по DNS в X509v3 Subject Alternative Name.



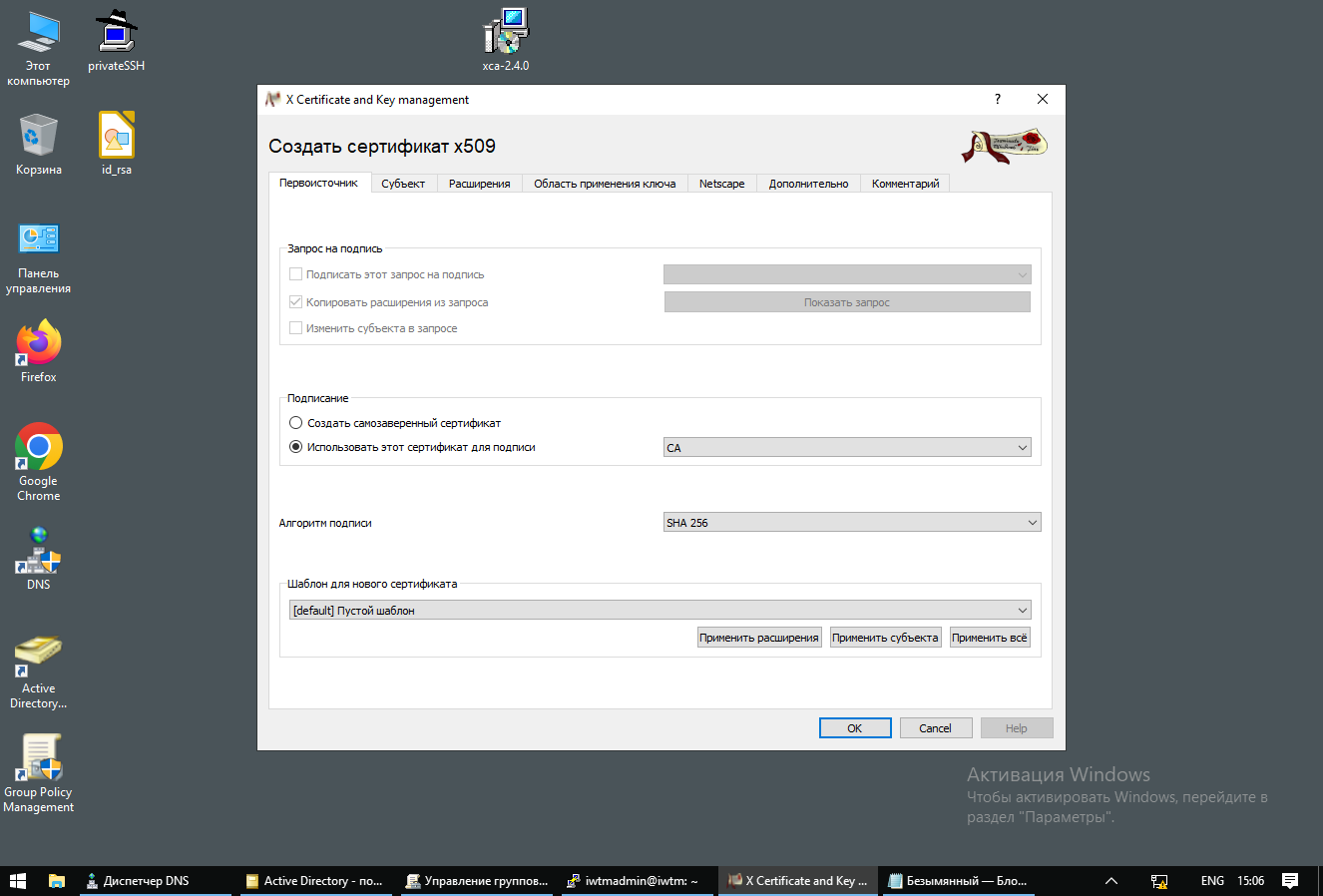


Нажимаем Ок.

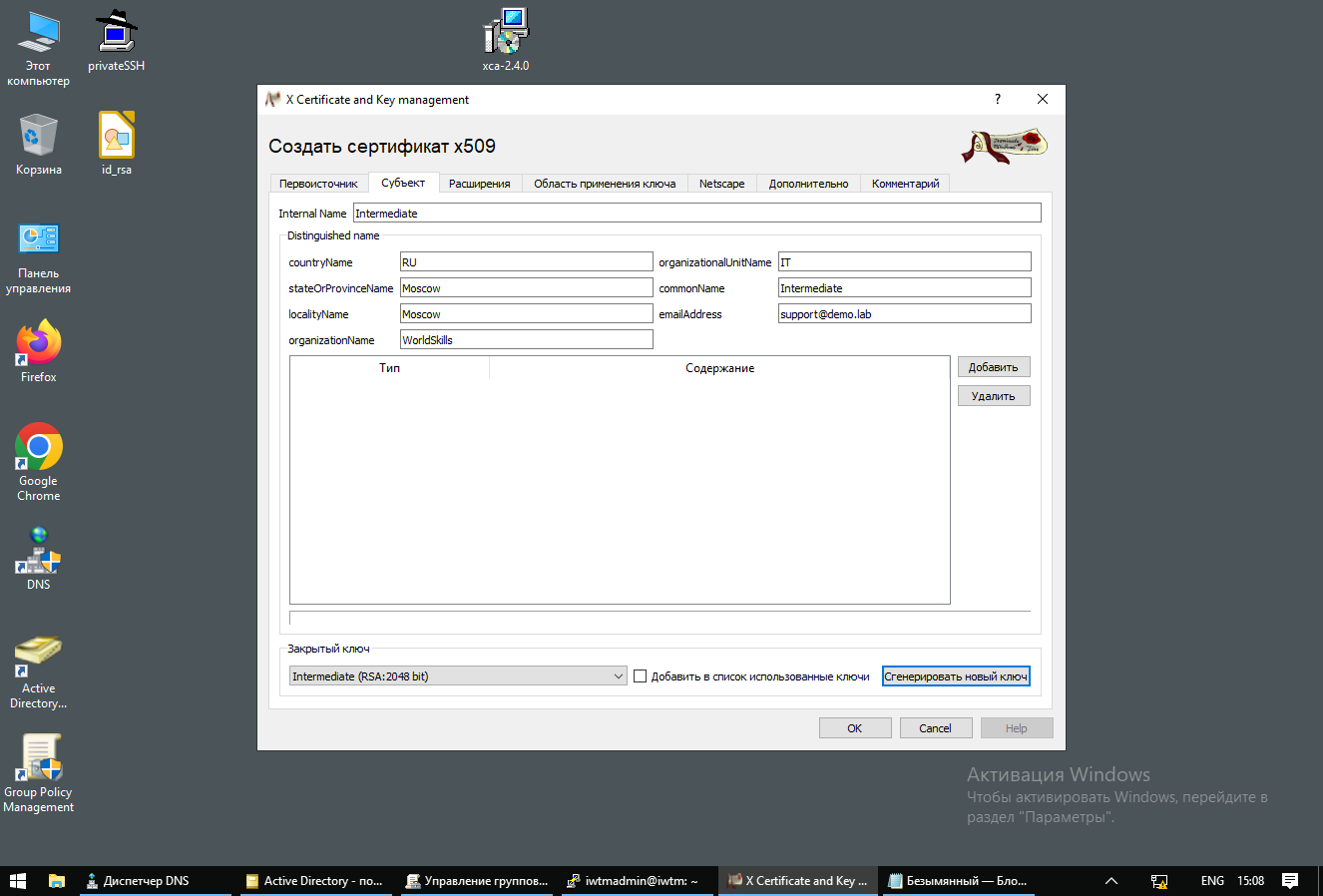
1. Т.к. нам необходимо создать древо сертификатов – нажимаем на только что созданный сертификат CA и нажимаем Новый сертификат

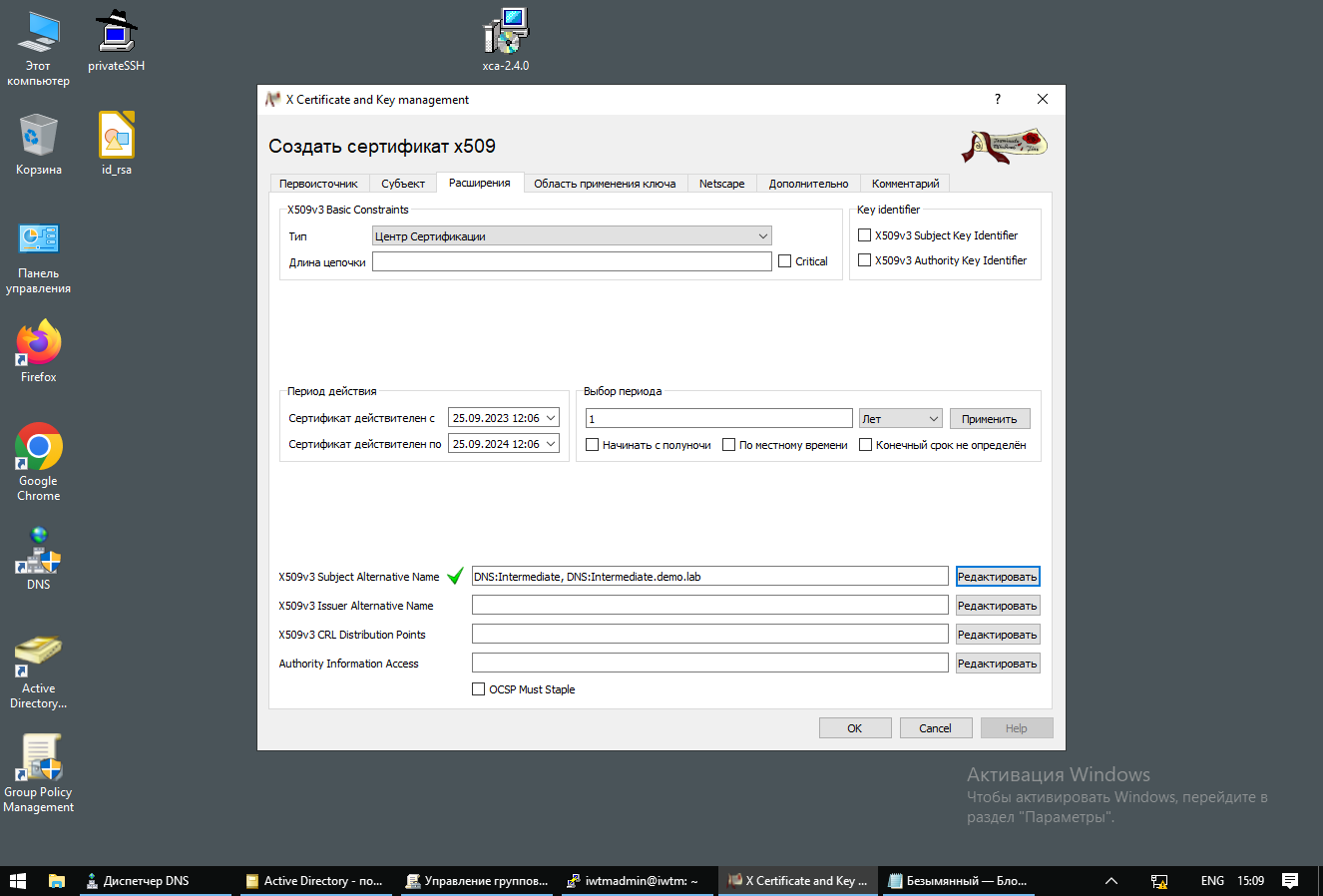


На вкладке Первоисточник оставляем все по умолчанию.



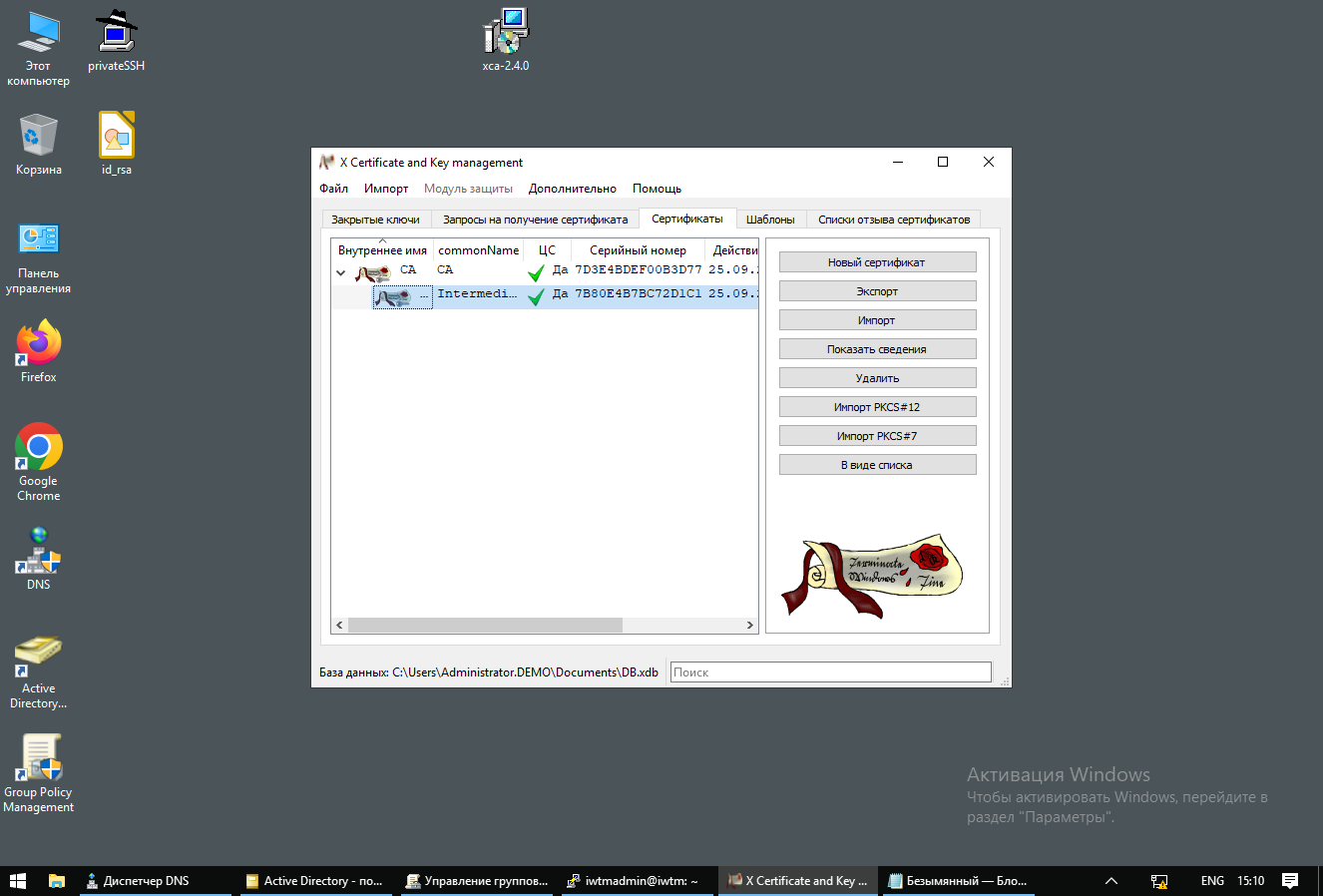
Во вкладке субъект и расширения делаем все по аналогии с сертификатом CA. Также генерируем закрытый ключ.



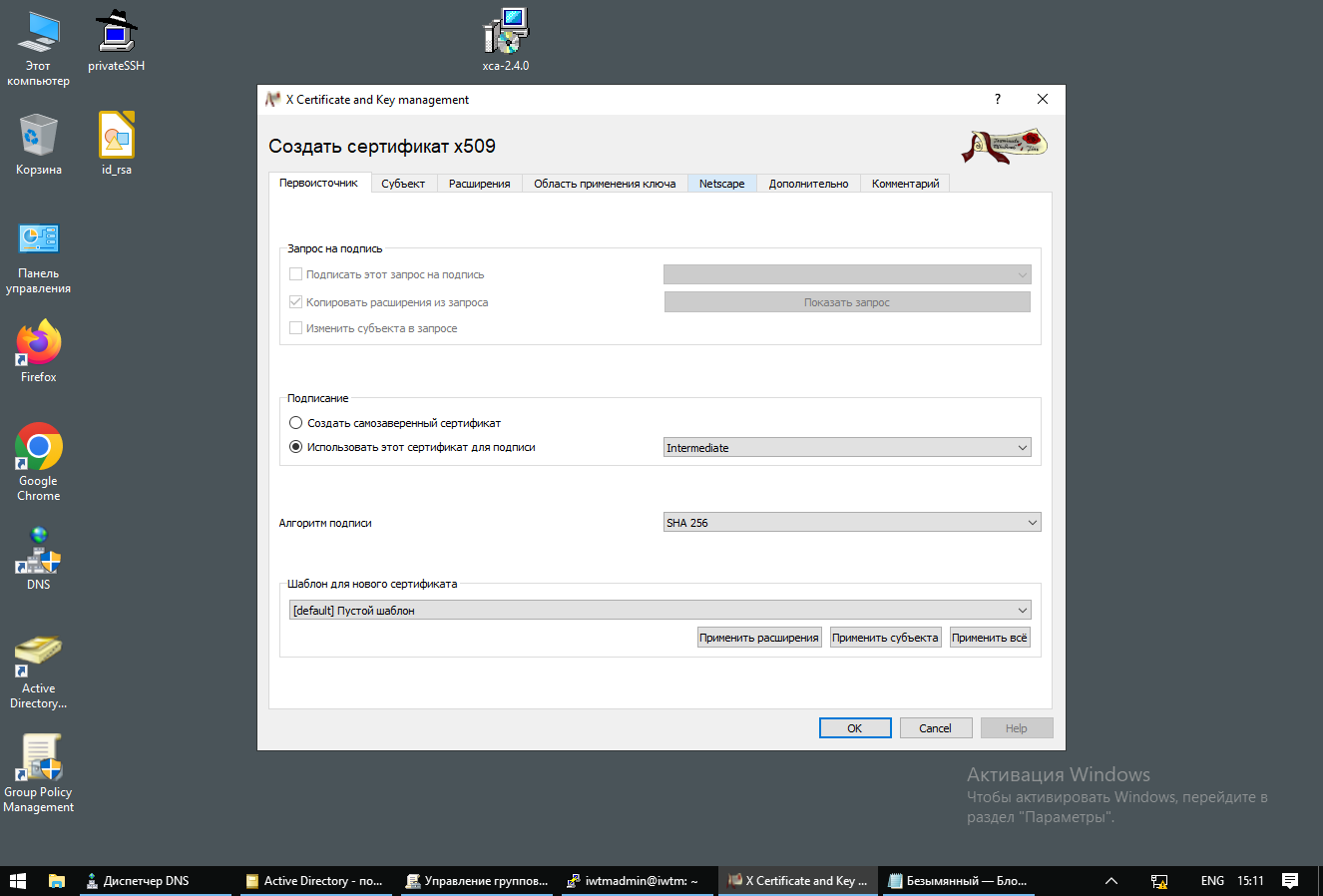


Нажимаем Ок

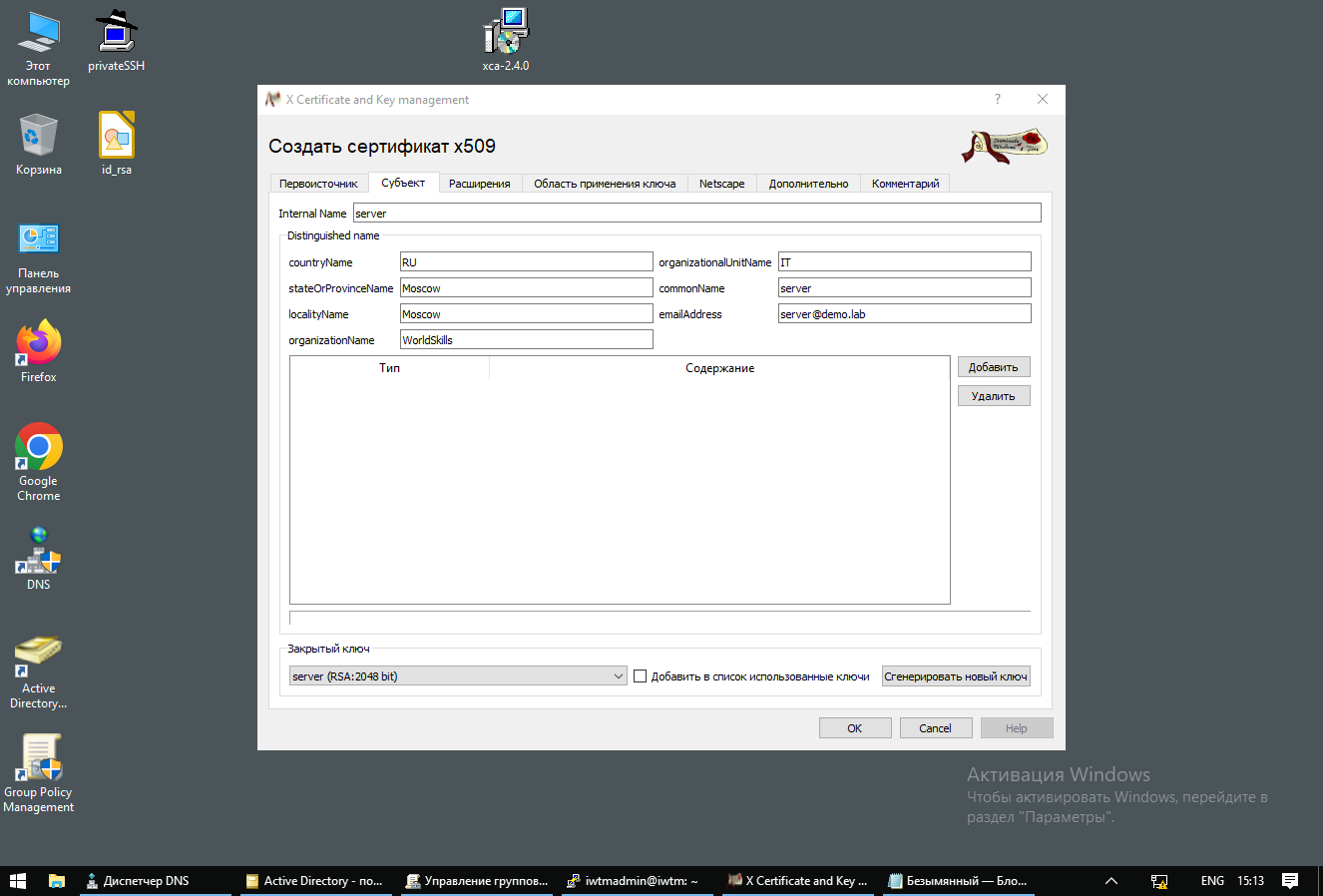
1. Разворачиваем древо сертификатов. Нажимаем на только что созданный сертификат Intermediate и нажимаем Новый сертификат



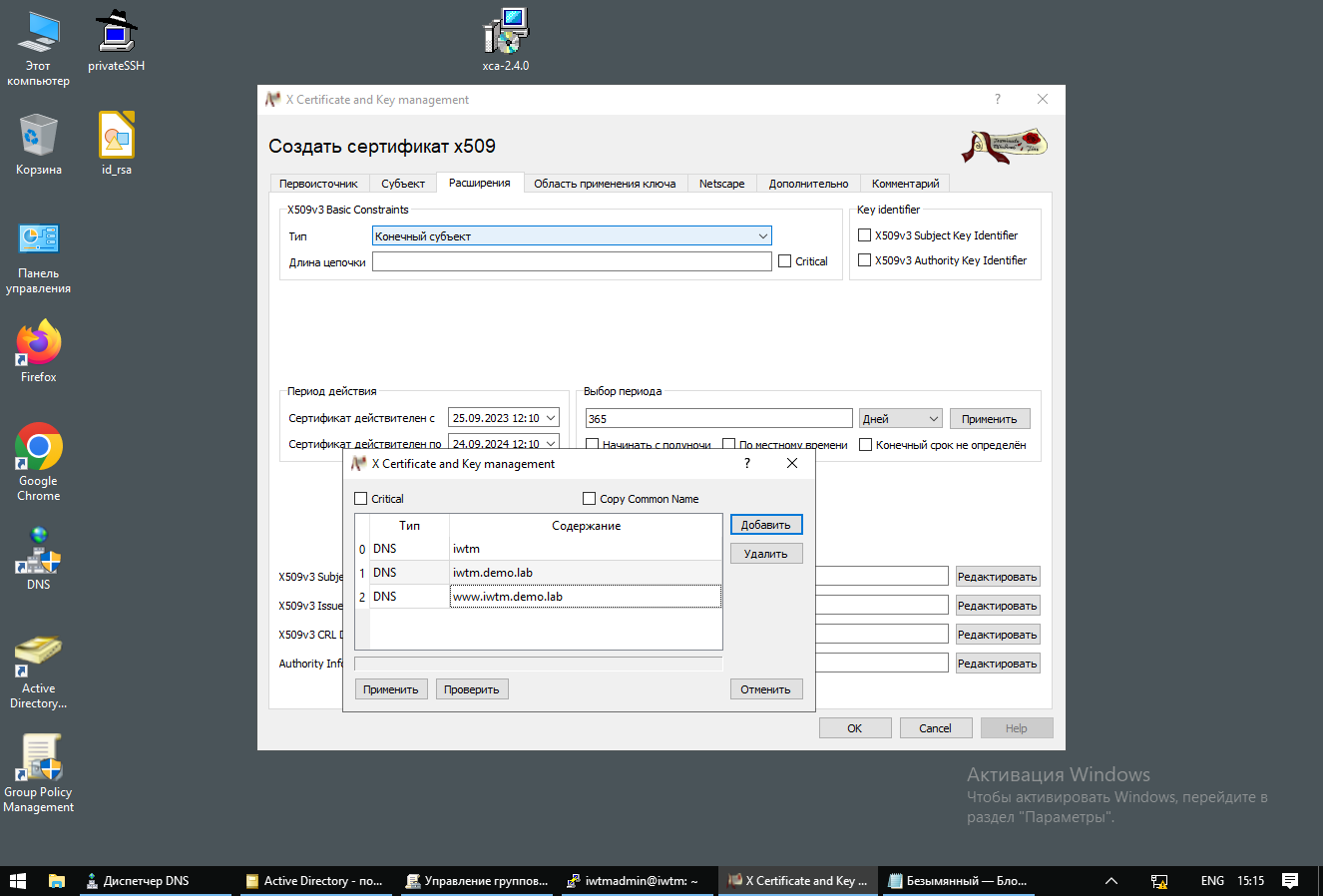
На вкладке Первоисточник оставляем все по умолчанию.



Во вкладке Субъект заполняем все по аналогии с предыдущими сертификатами и также генерируем закрытый ключ.

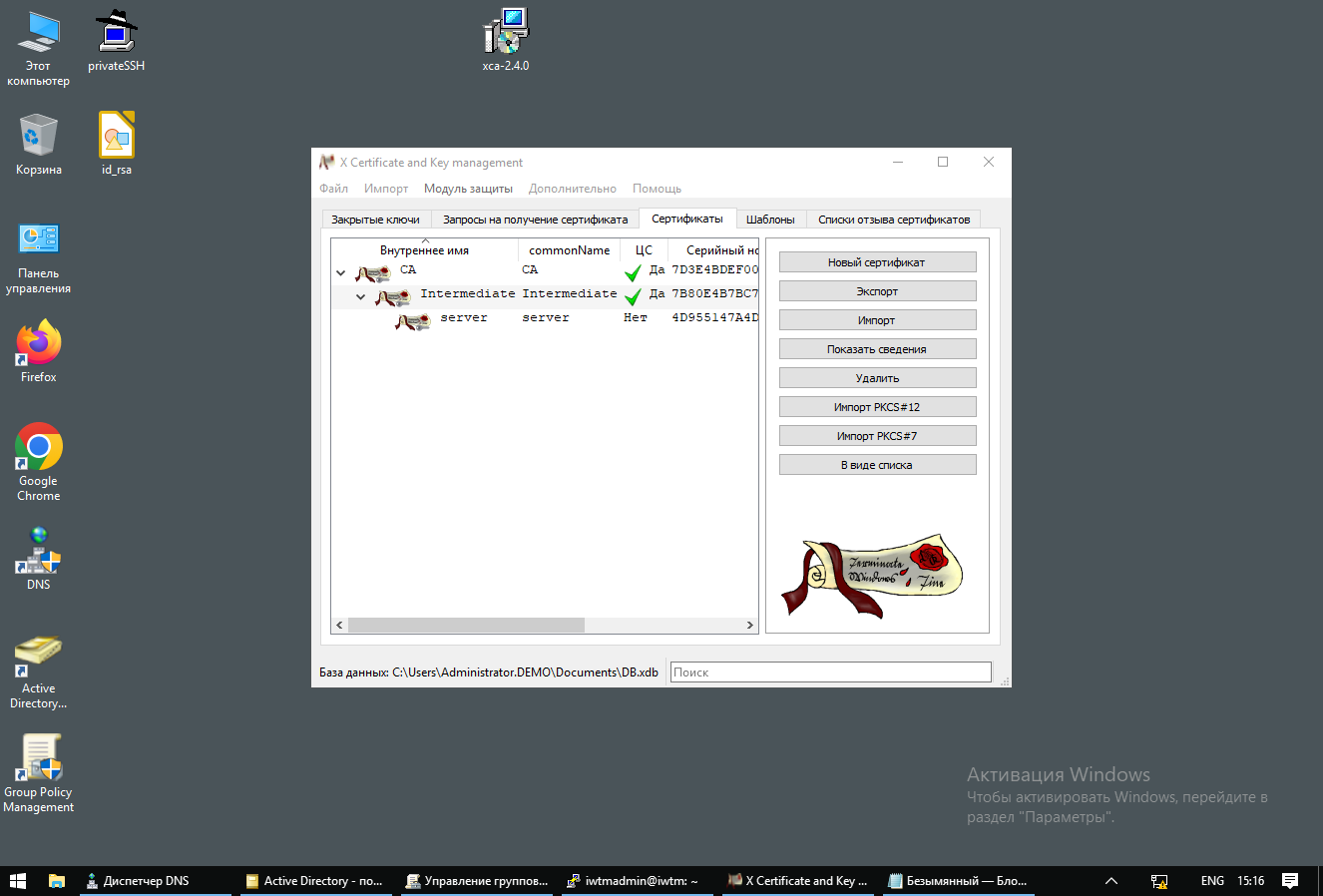


Во вкладке Расширения выбираем Тип – Конечный субъект. В DNS прописываем адрес iwtm.



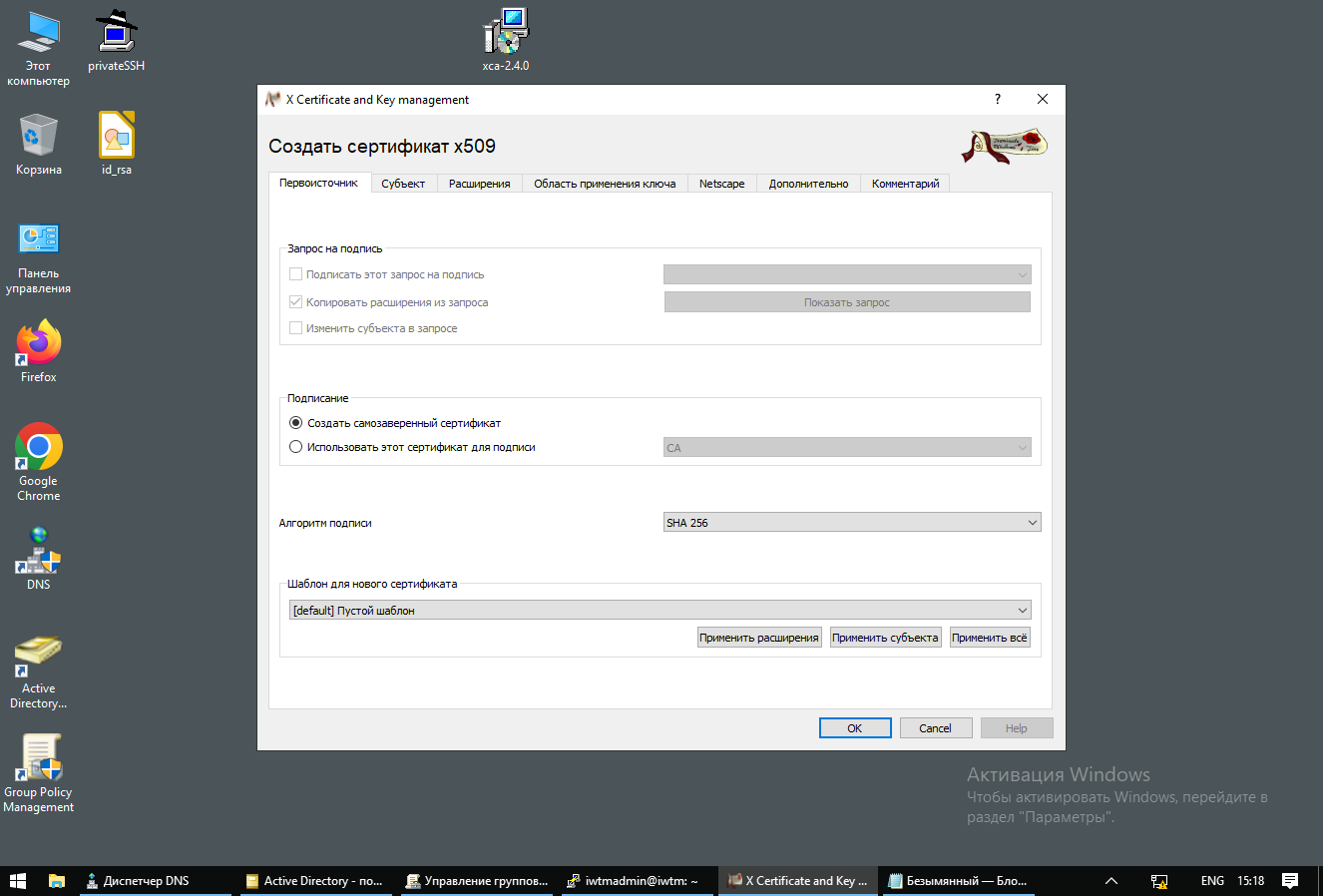
Нажимаем Ок.

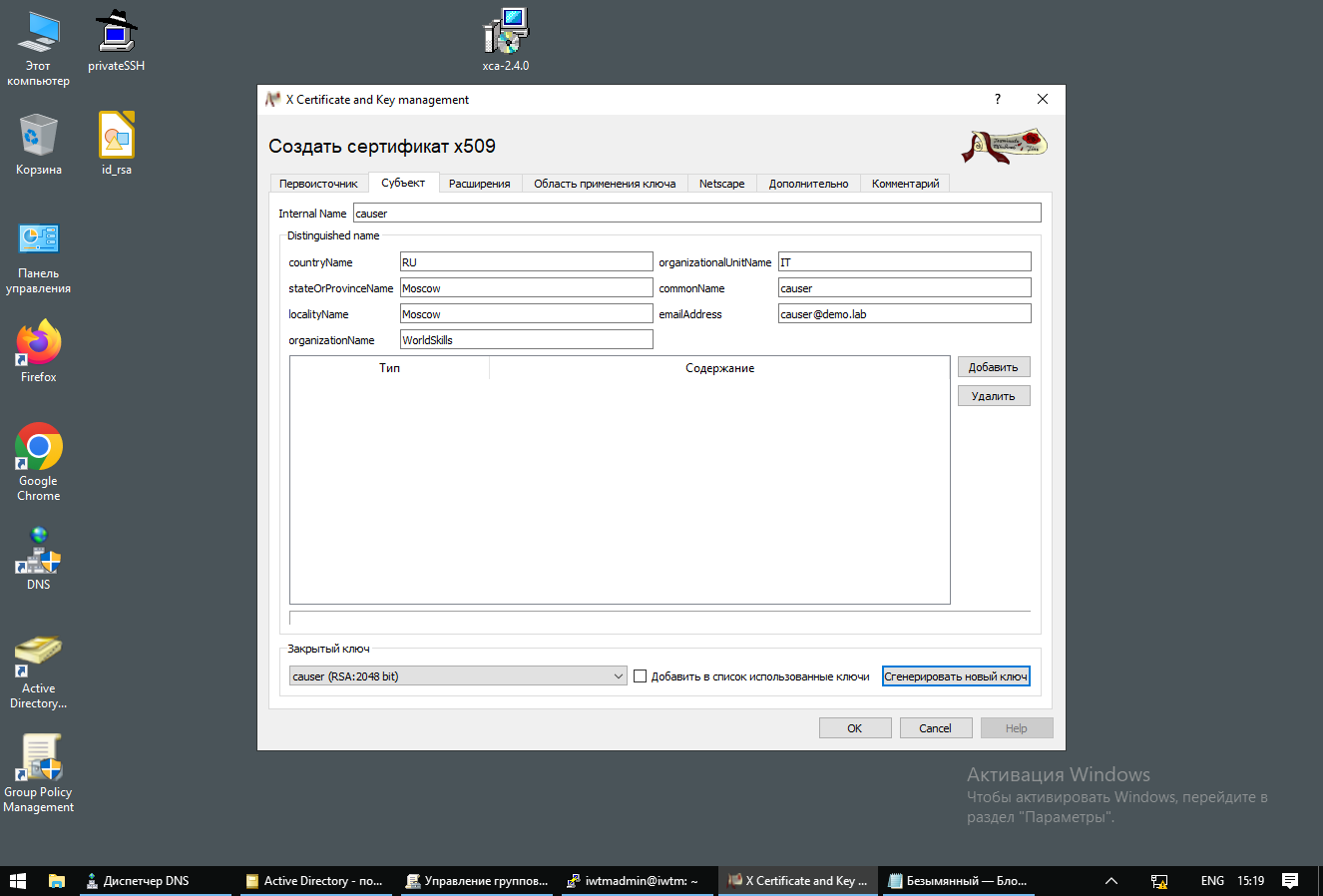
1. У нас есть древо сертификатов

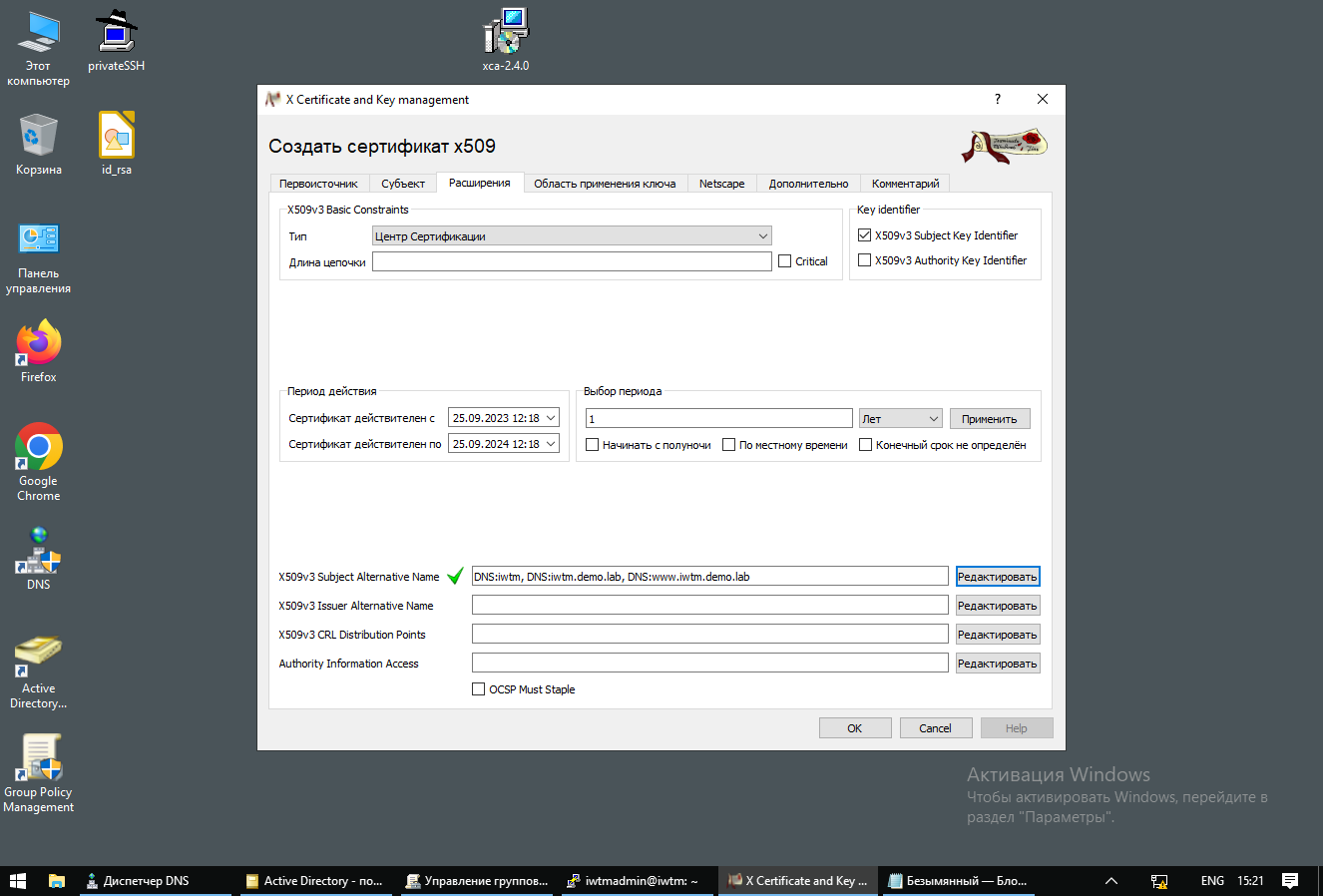


1. Теперь создаем пользовательский сертификат

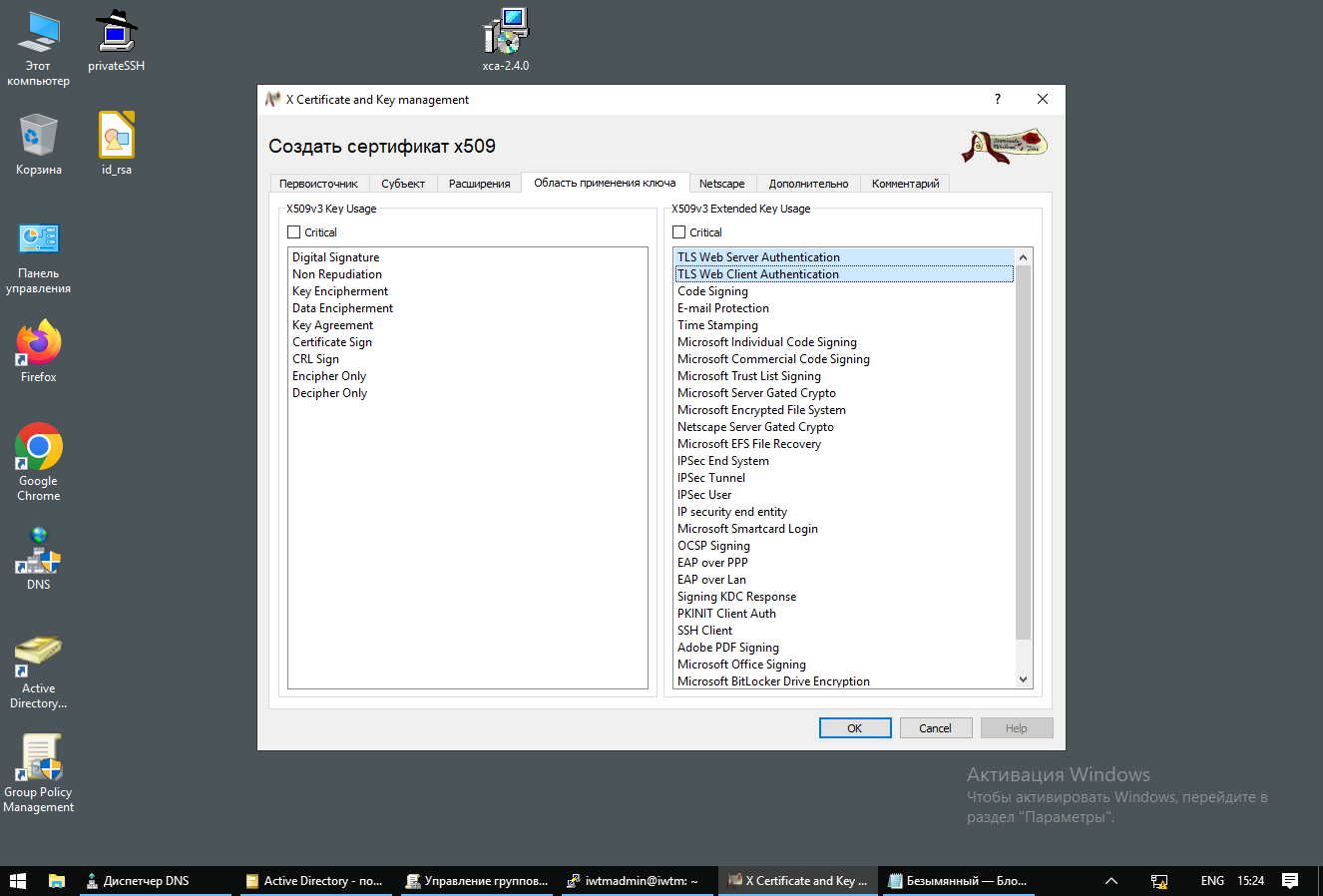
Создаем корневой пользовательский сертификат. Все, до вкладки Область применения делаем как на шаге 3. Во вкладке Расширения ставим галочку X509v3 Subject Key Identidier





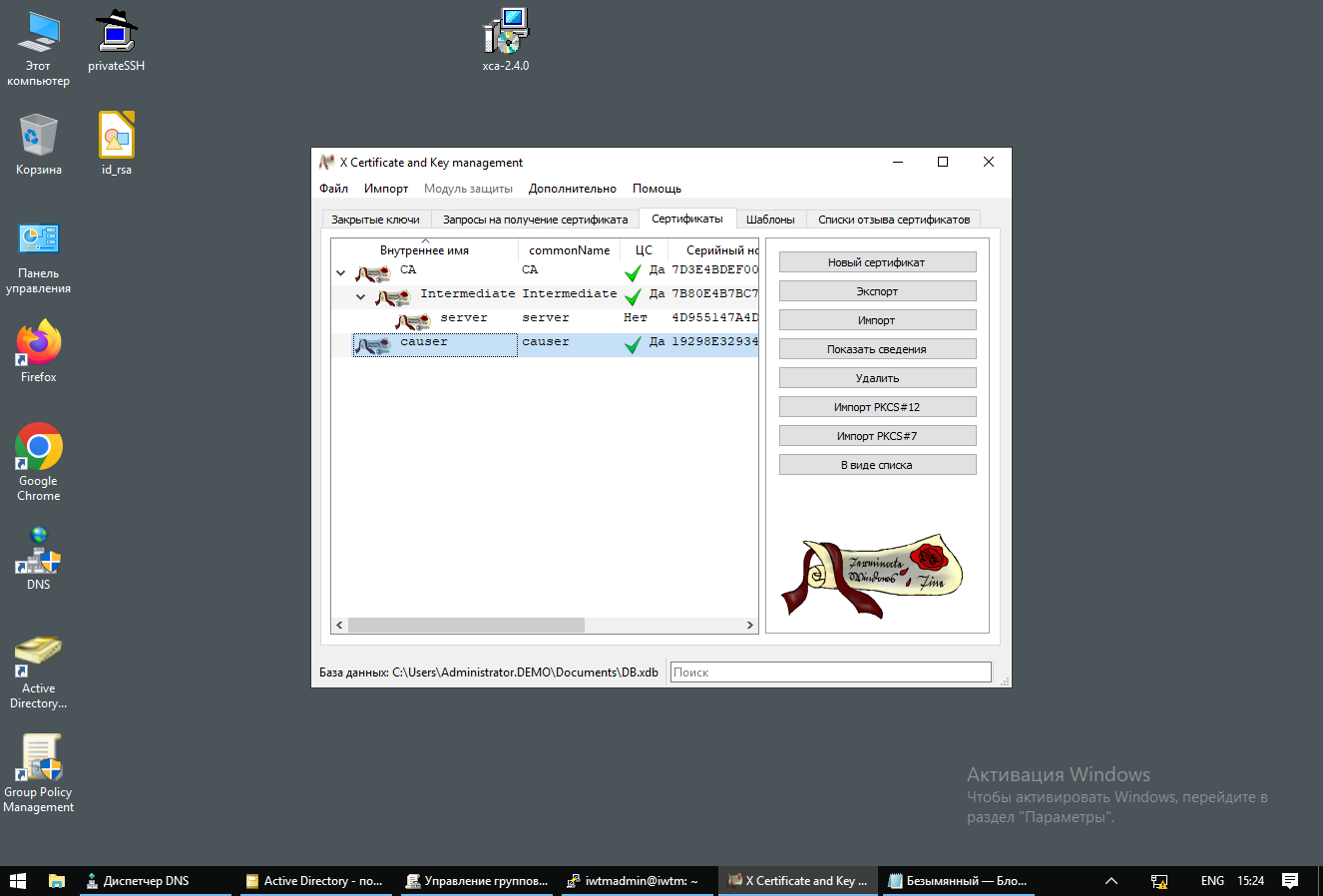


В области применения ключа выбираем TLS Web Server Authentication и TLS Web Client Authentication.

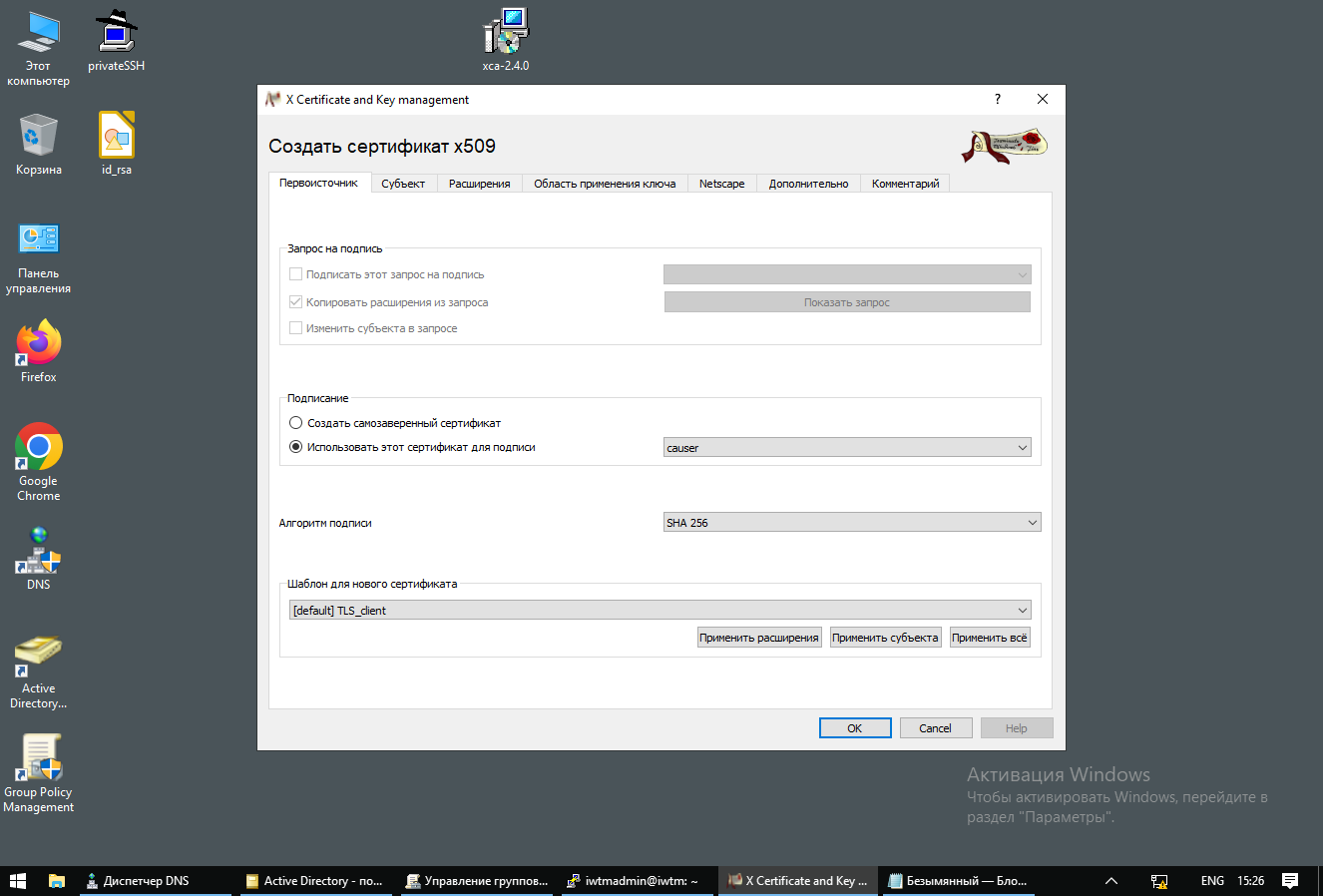


Нажимаем Ок.

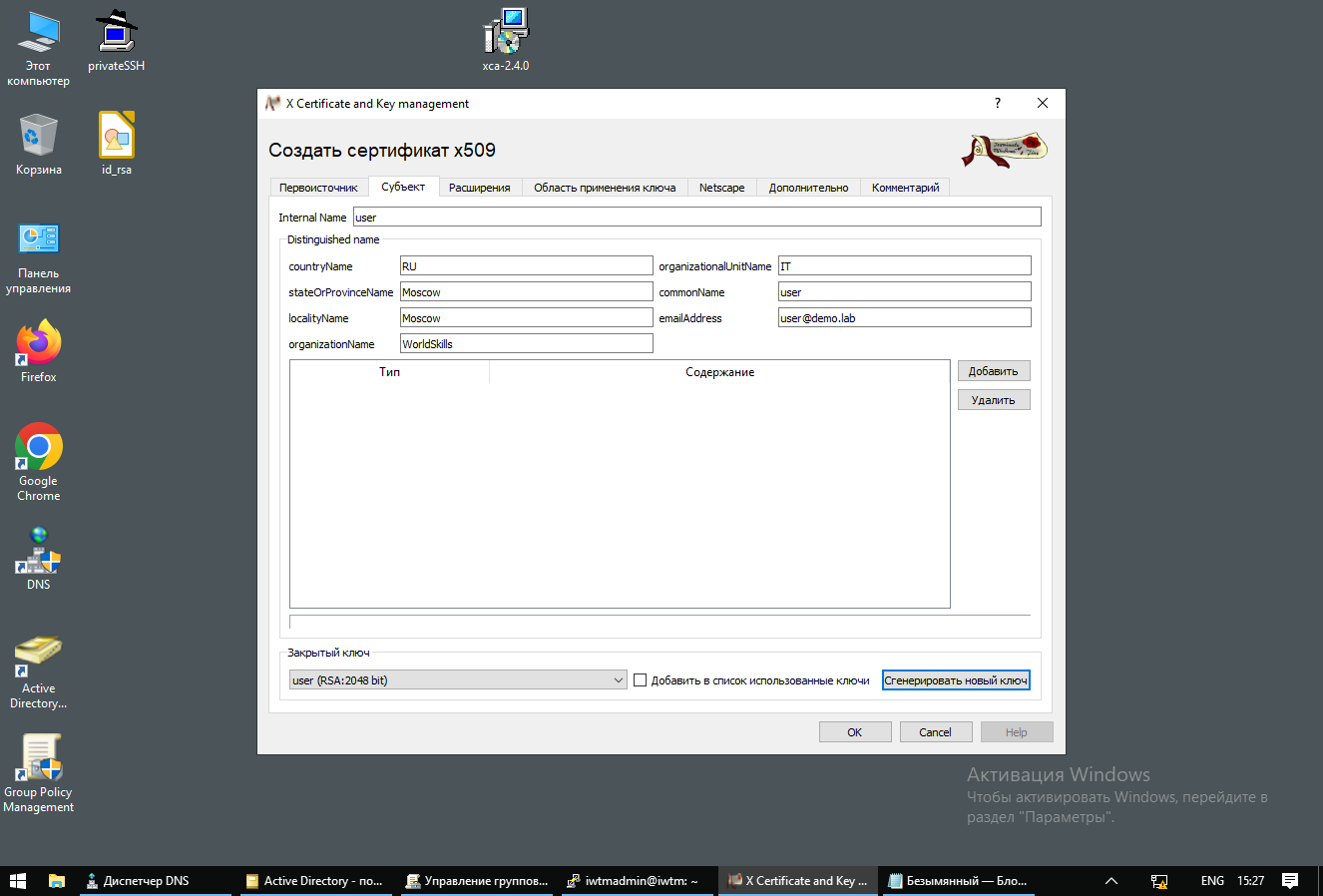
1. Нажимаем на созданный сертификат и нажимаем Новый сертификат.



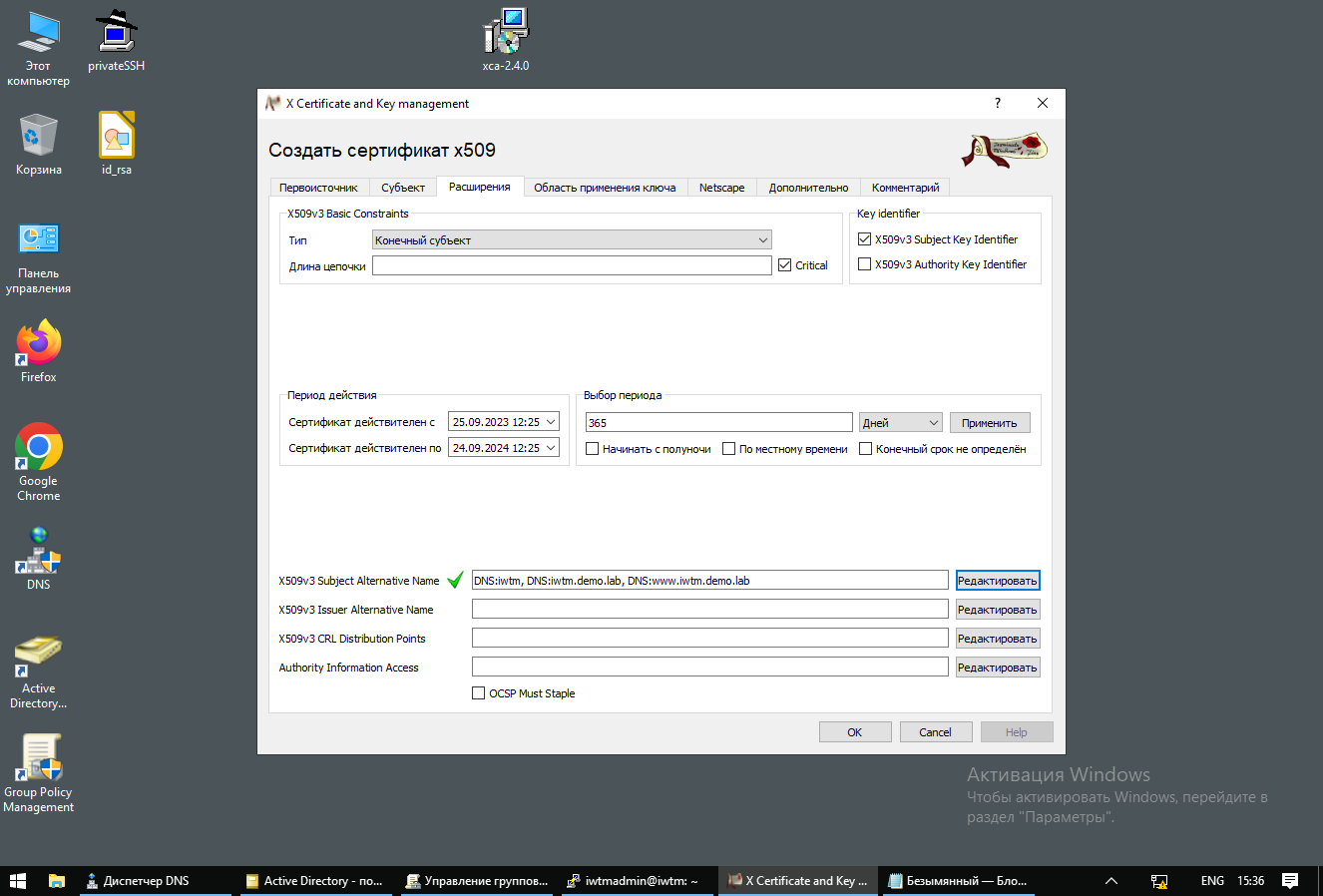
В шаблонах, для простоты выбираем TLS\_client и Нажимаем применить расширения.



В Субъекте, все по заданию.

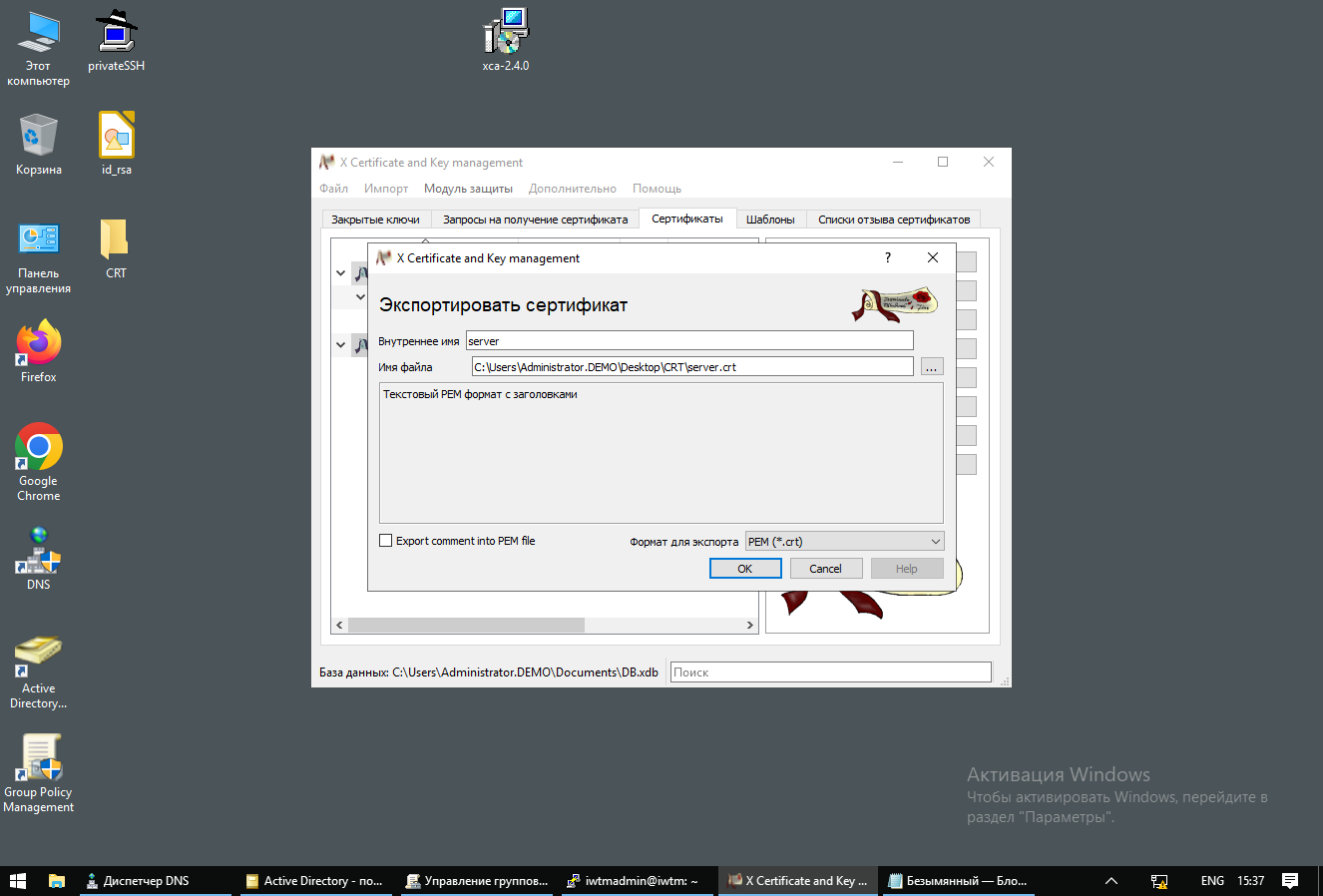


В Расширениях добавляем DNS.

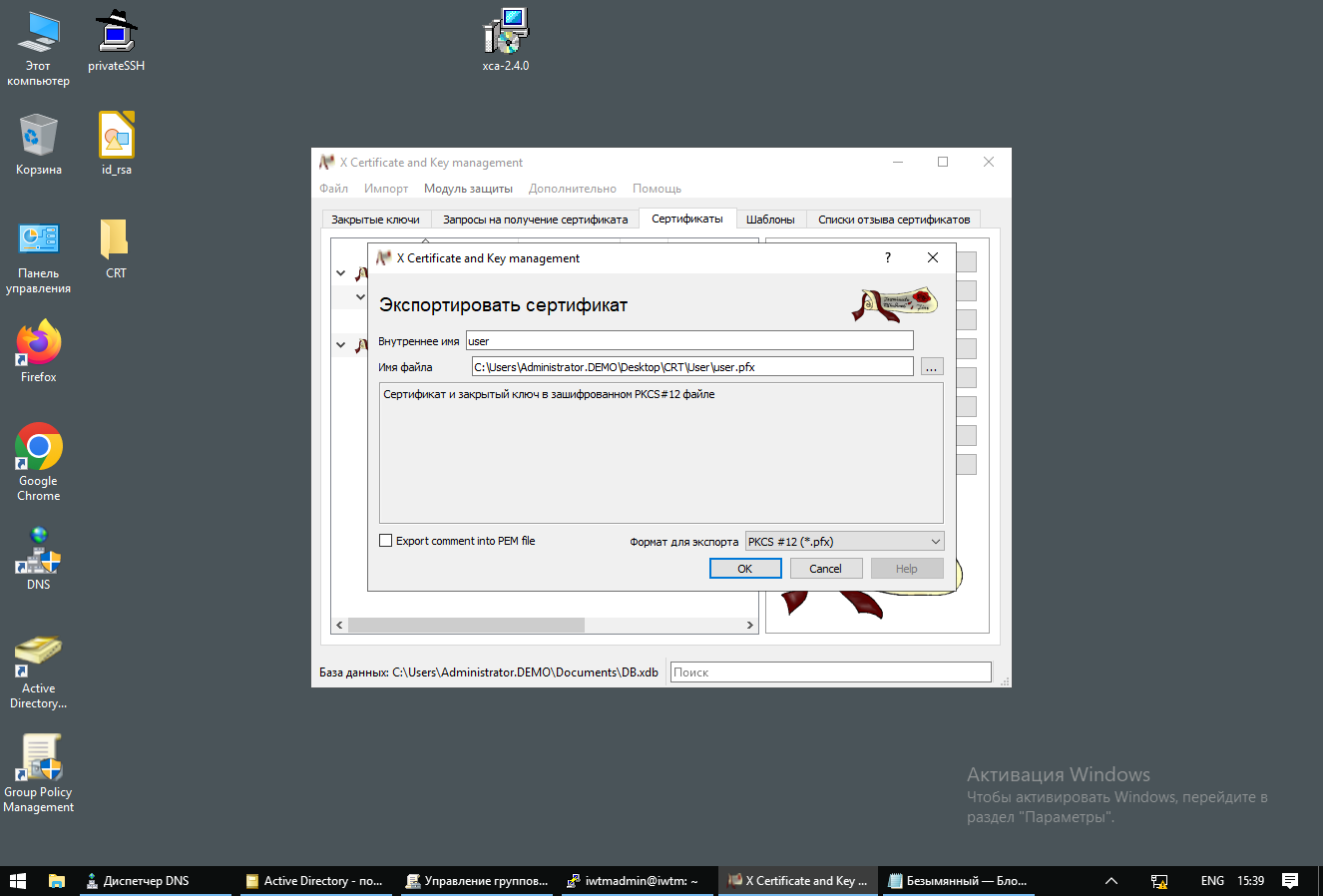


Нажимаем Ок.

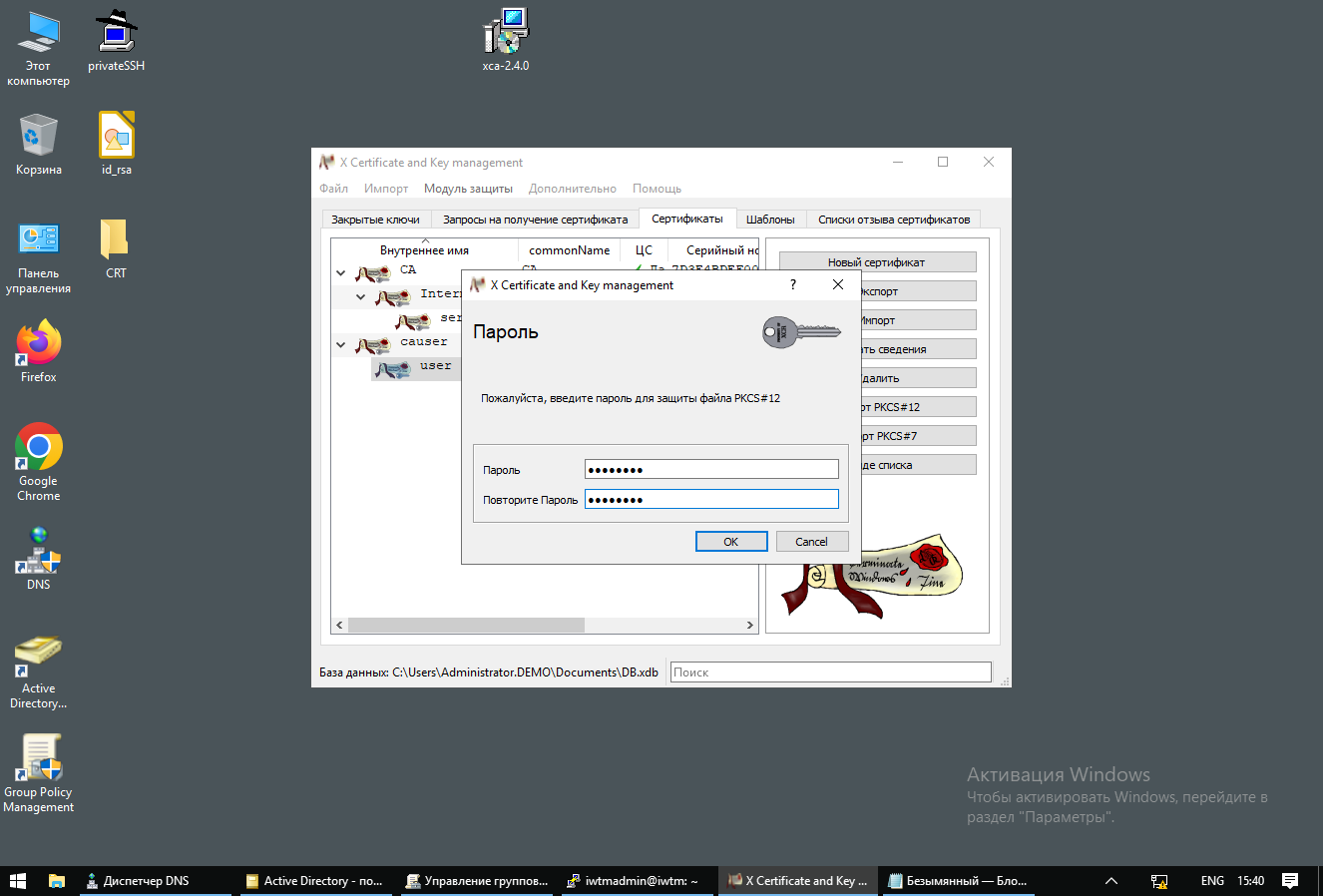
1. Далее Экспортируем наши сертификаты. Все, кроме сертификата user в формате PEM(\*.crt)



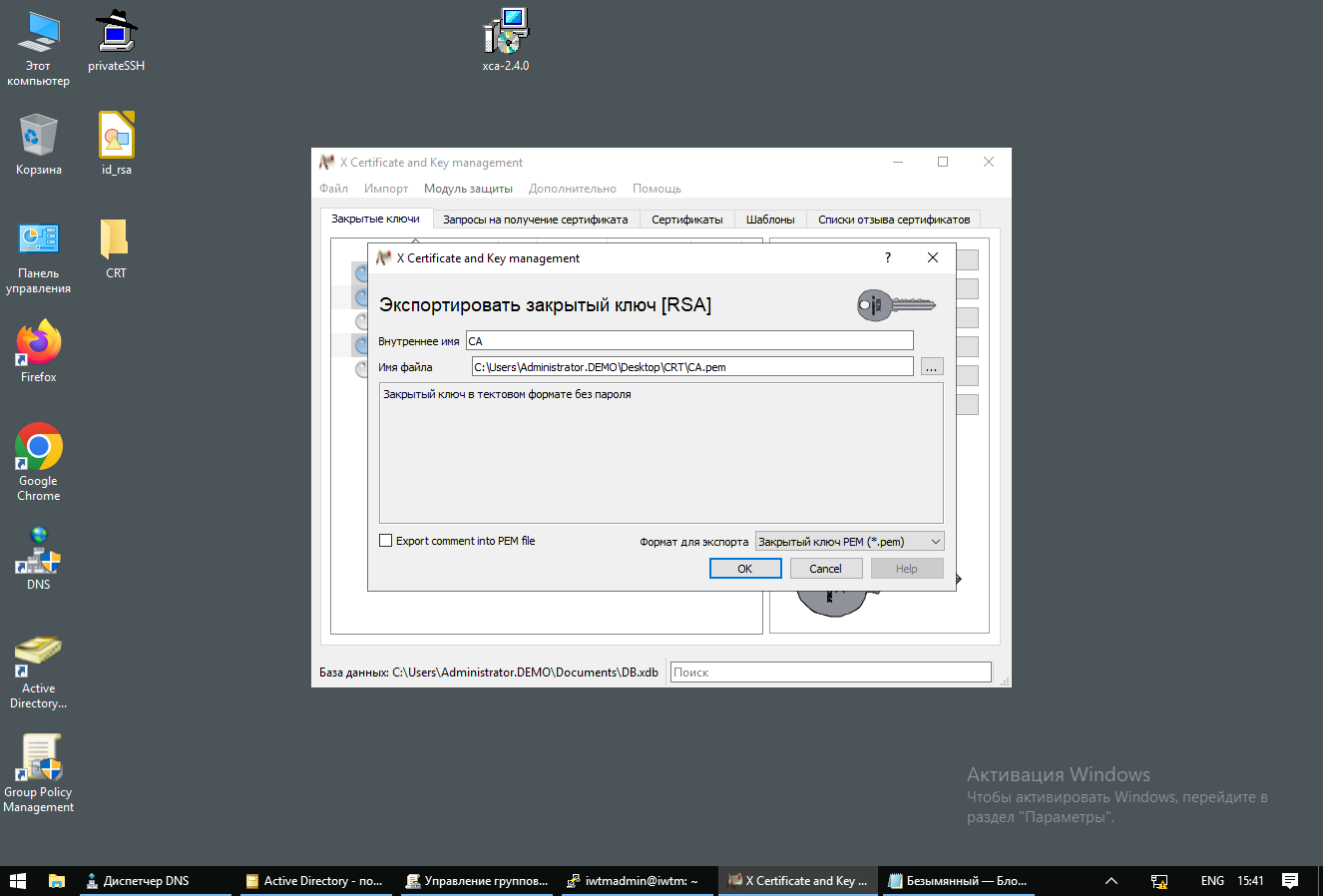
Пользовательский сертификат user экспортируем в формате PKCS #12(\*.pfx)



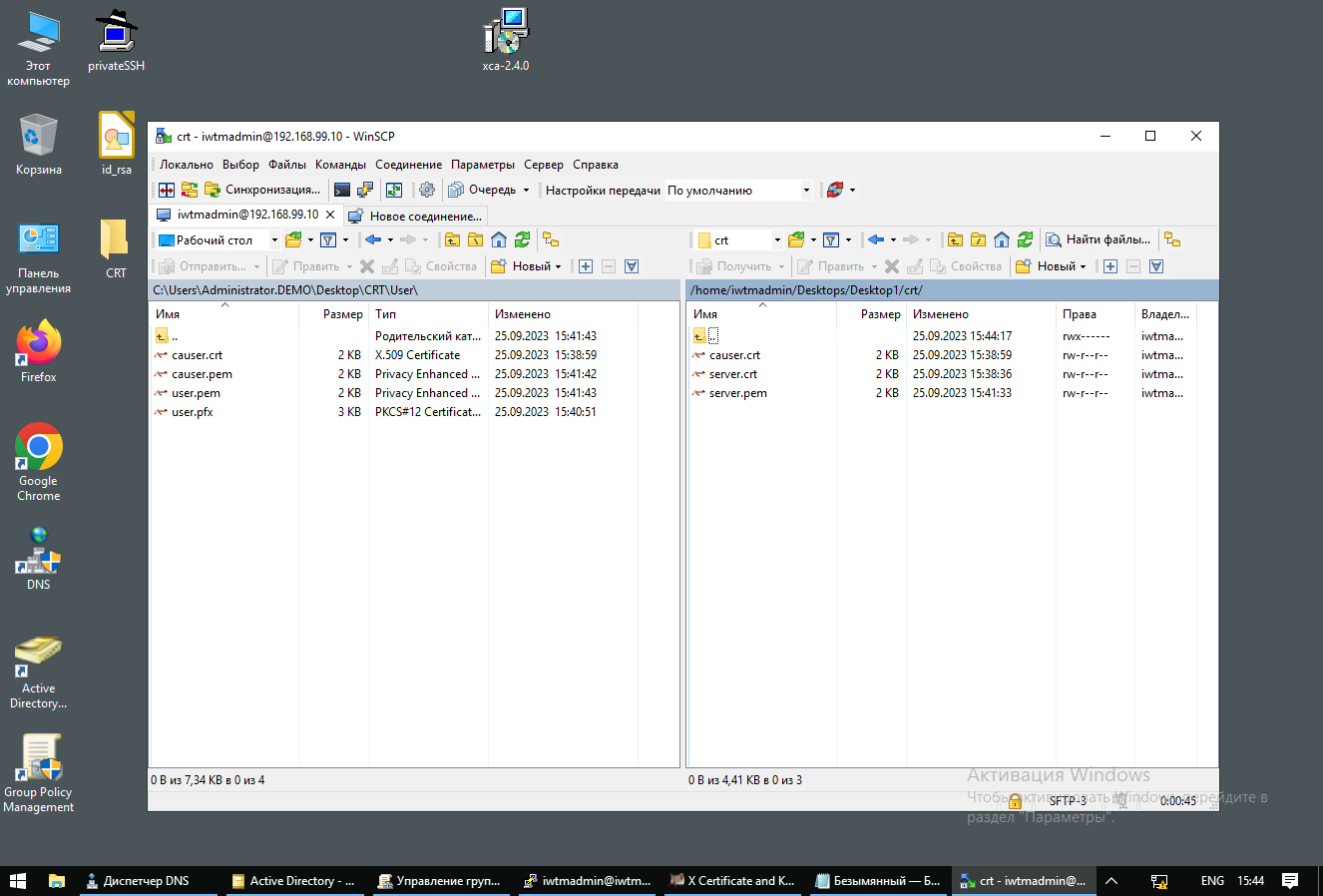
Задаем пароль пользовательскому сертификату



1. Также экспортируем Закрытые ключи

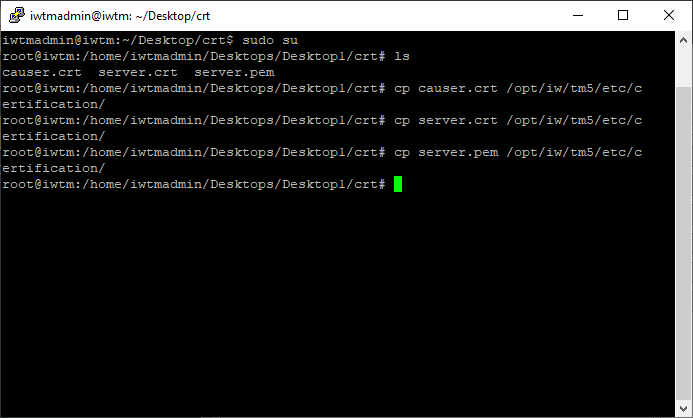


1. Далее закидываем сертификаты server.crt, causer.crt и ключ server.pem на IWTM



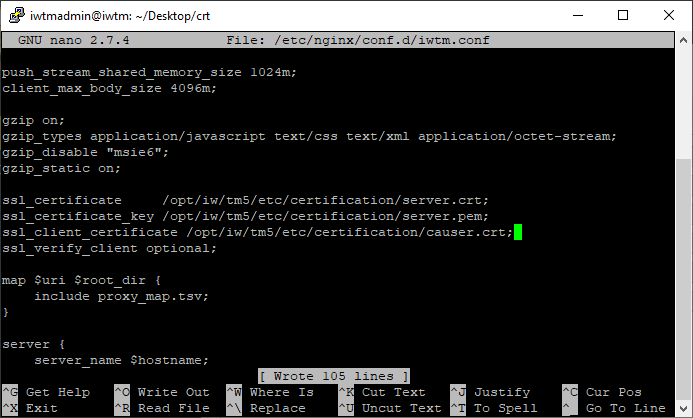
Подключаемся по ssh к iwtm или прям на ней.

Копируем три наших файлика в /opt/iw/tm5/etc/certification/



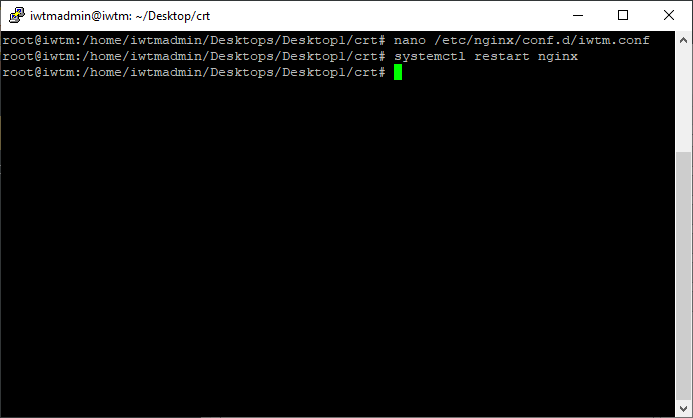
Далее редактируем файл /etc/nginx/conf.d/iwtm.conf

В файле меняем имя и расширение сертификата и ключа, а также добавляем две строки для работы пользовательского сертификата



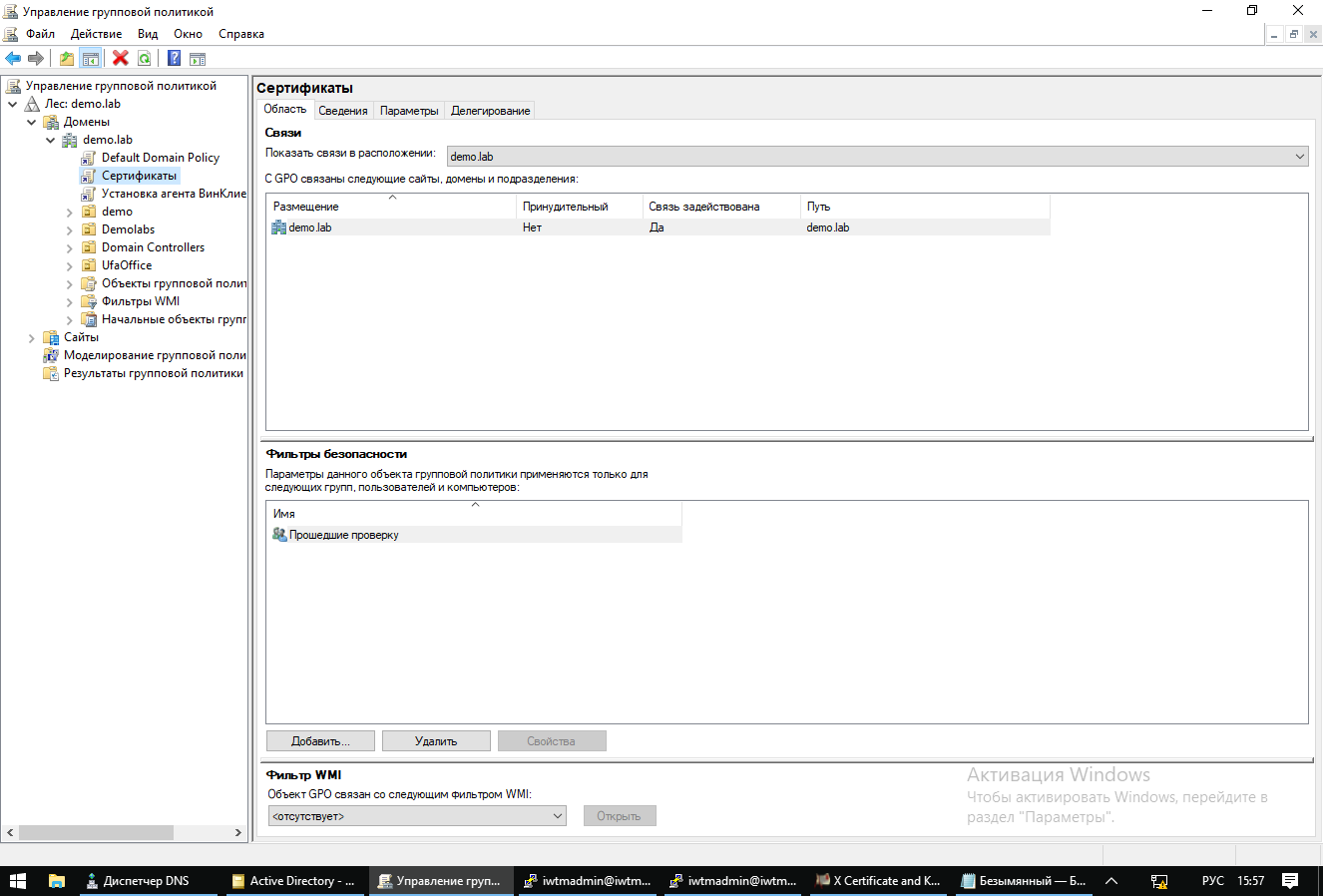


Далее перезапускаем службу nginx. Если служба не перезапустилась значит в файле есть ошибки.

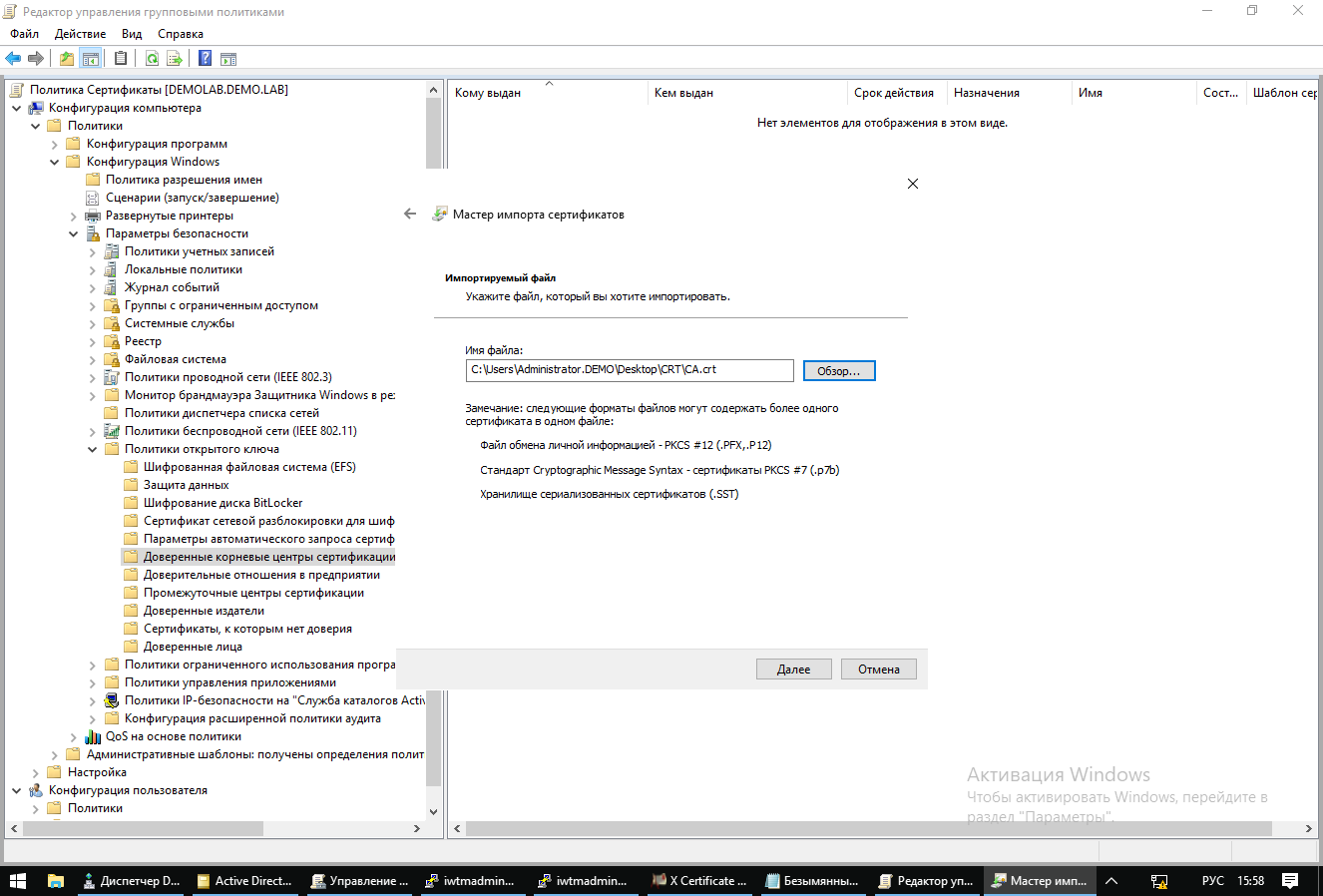


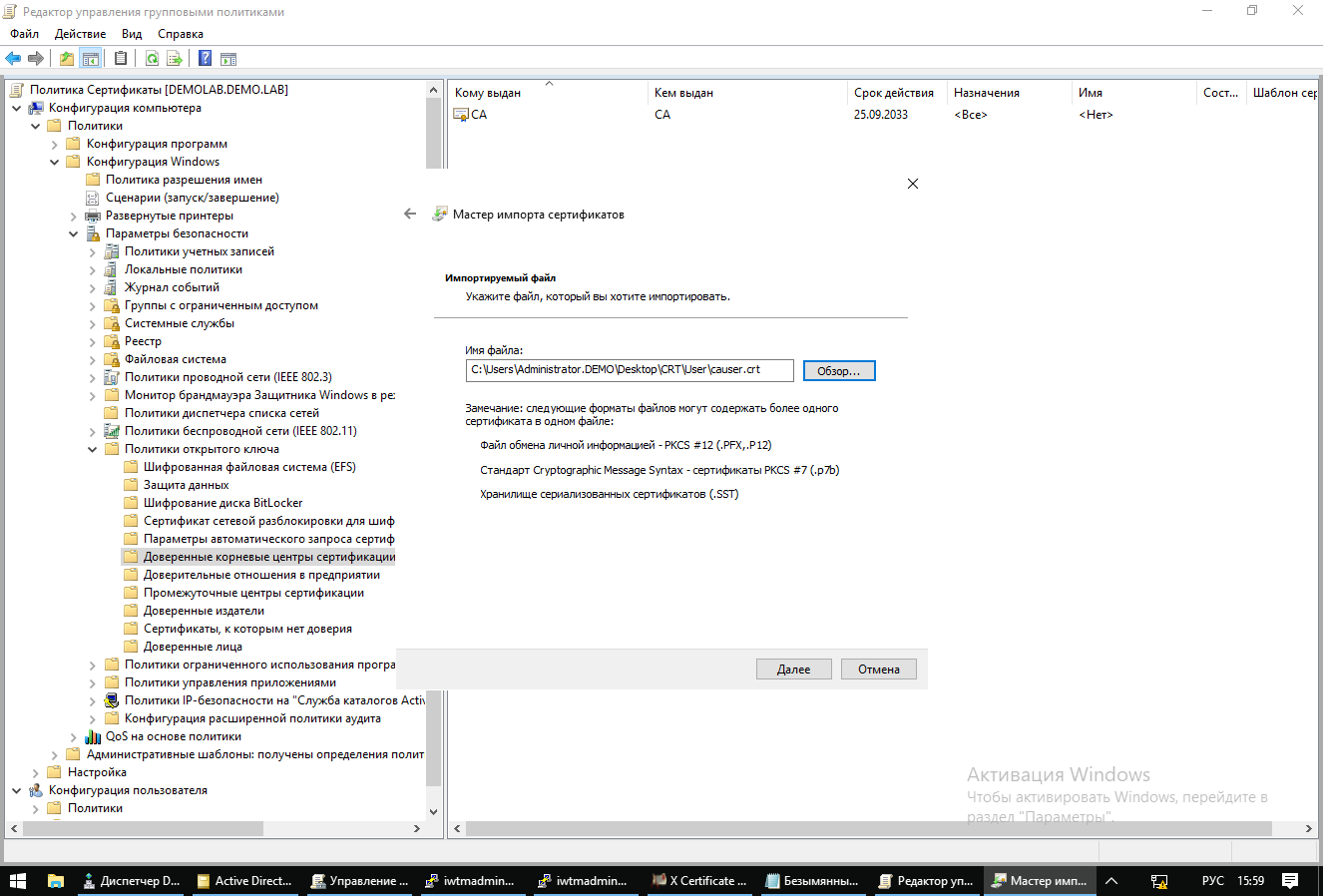
1. Далее добавляем наши сертификаты через групповые политики

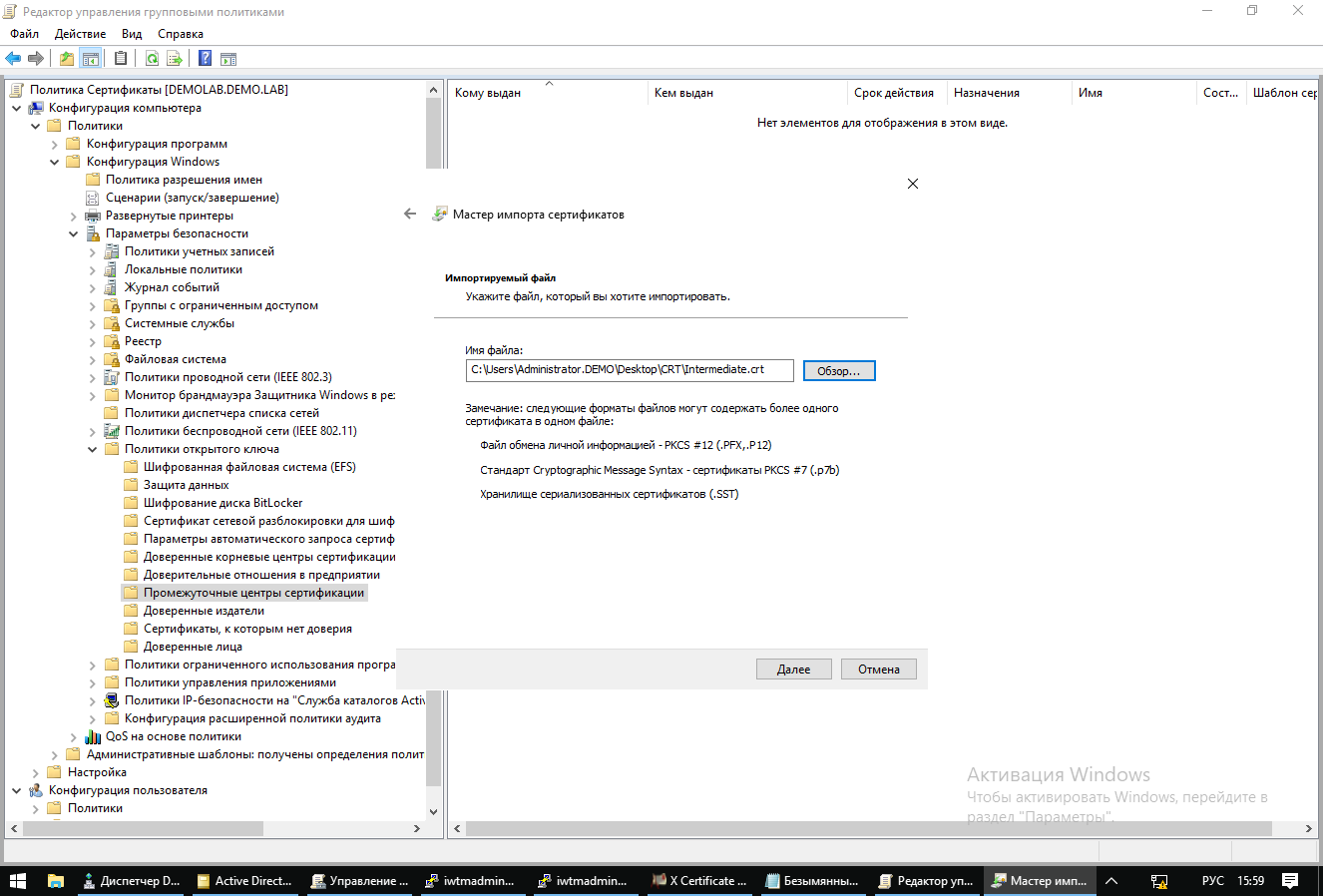
Создаем объект групповой политики



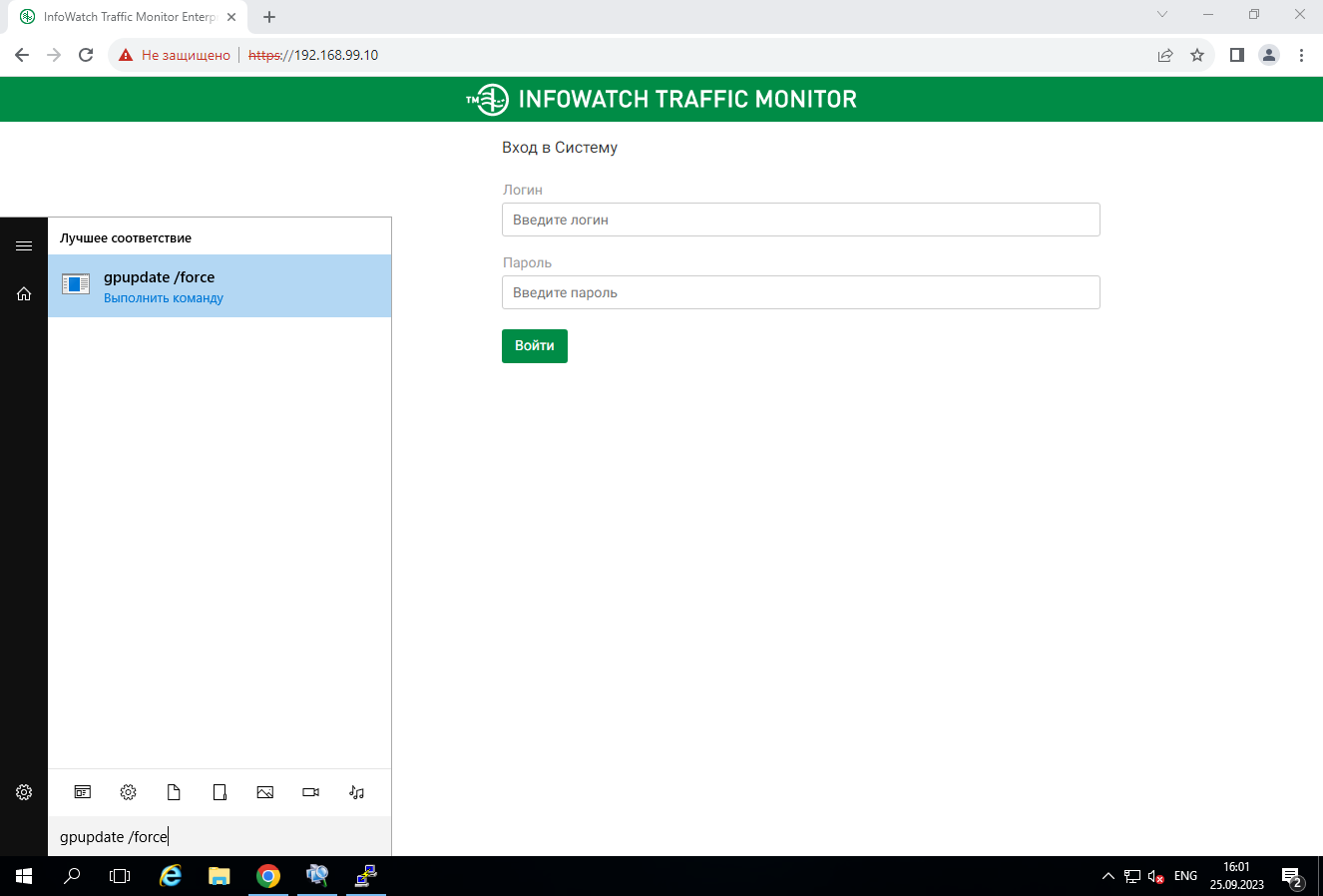
Добавляем в политику корневые сертификаты CA.crt, causer.crt и промежуточный Intermidiate.crt



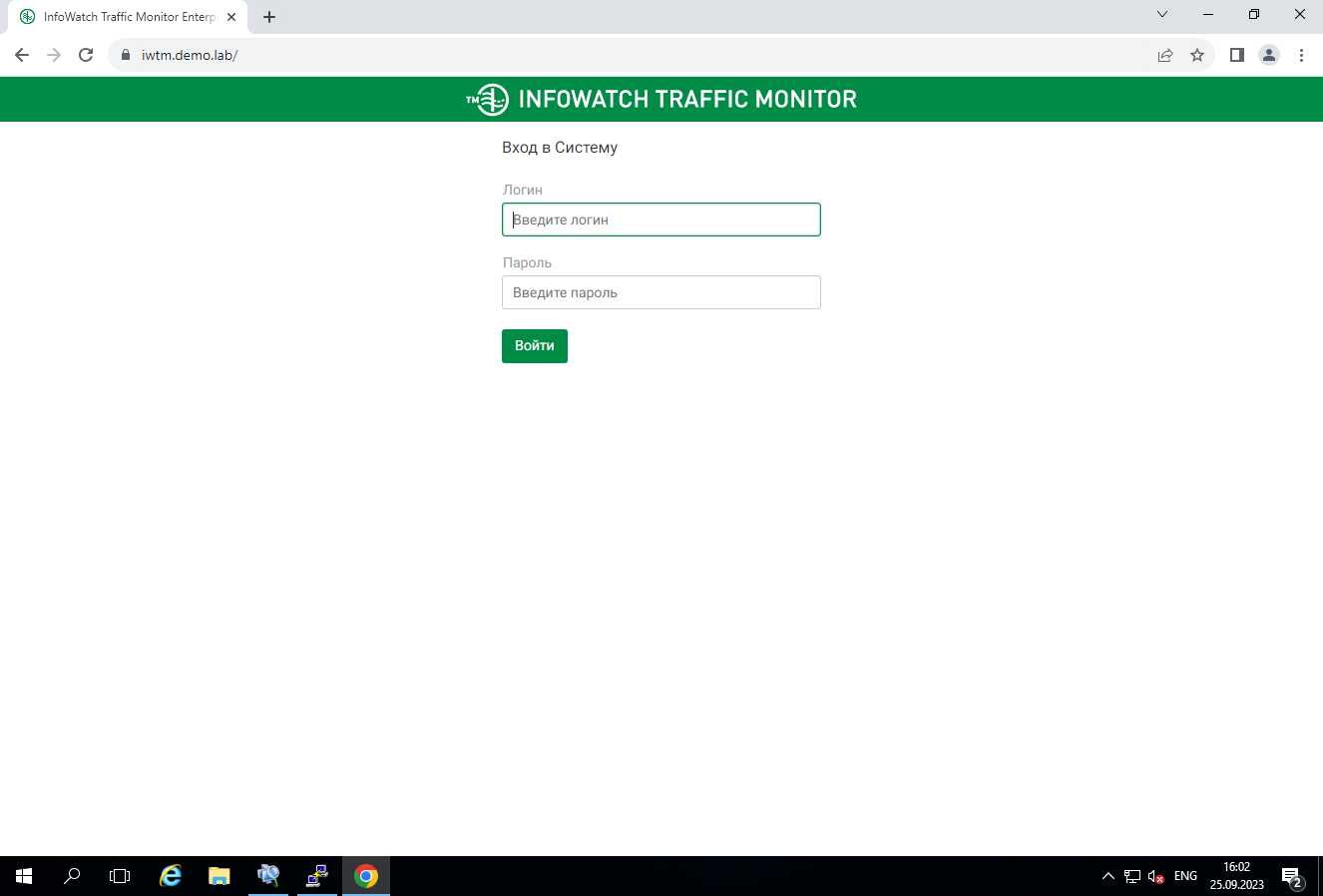


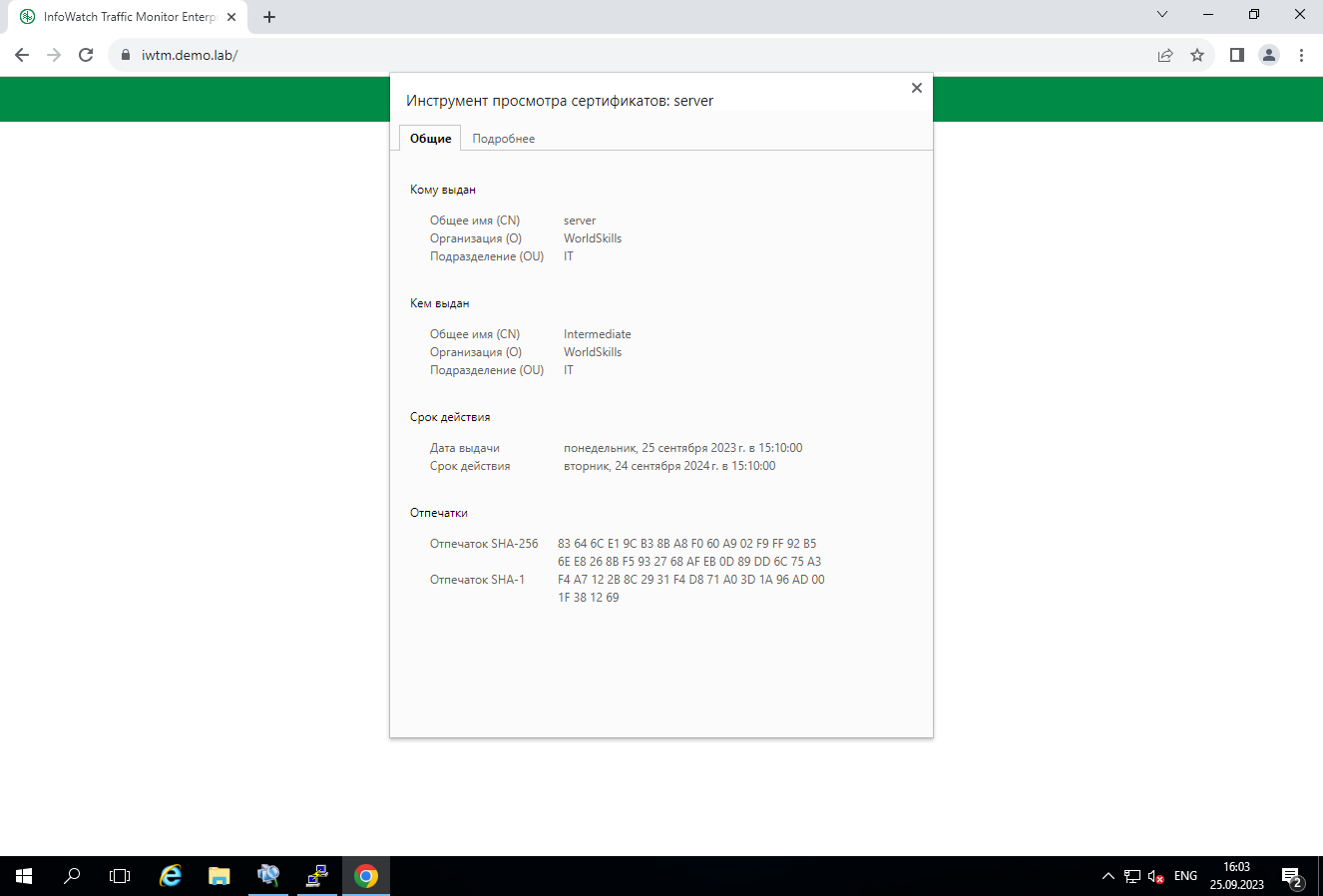


1. Проверяем работу сертификата обновив политику gpupdate/force



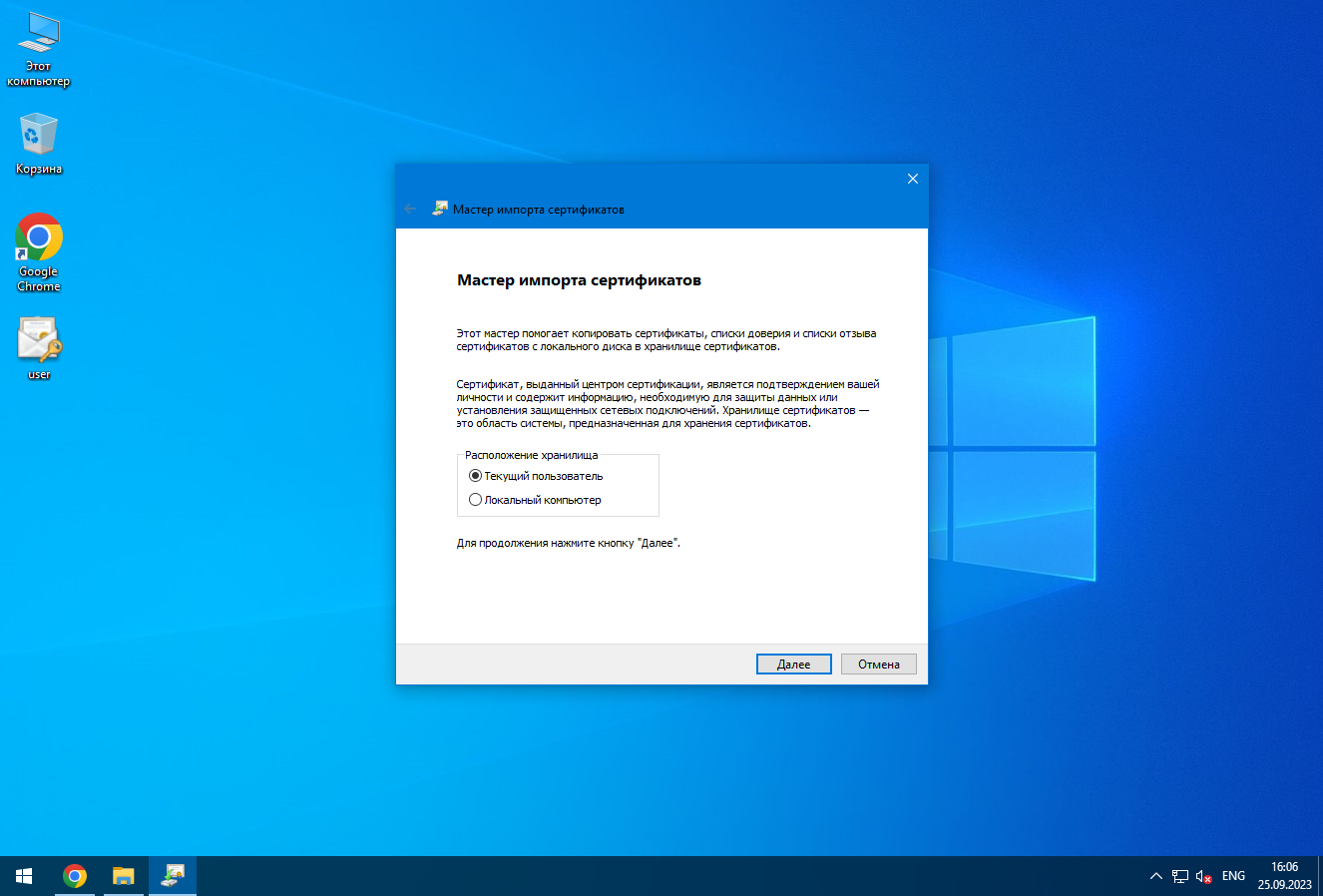
Сертификат подхватился

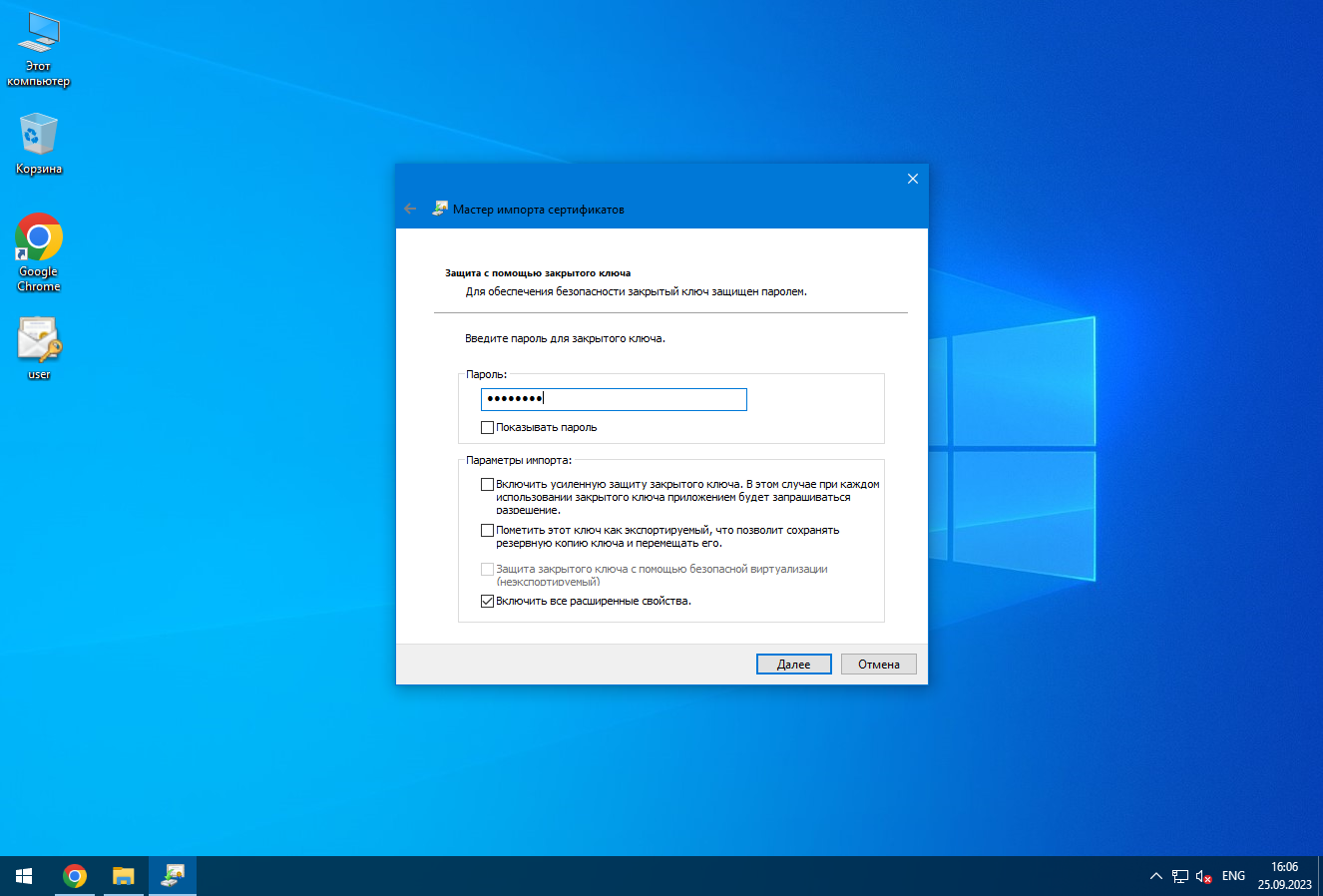


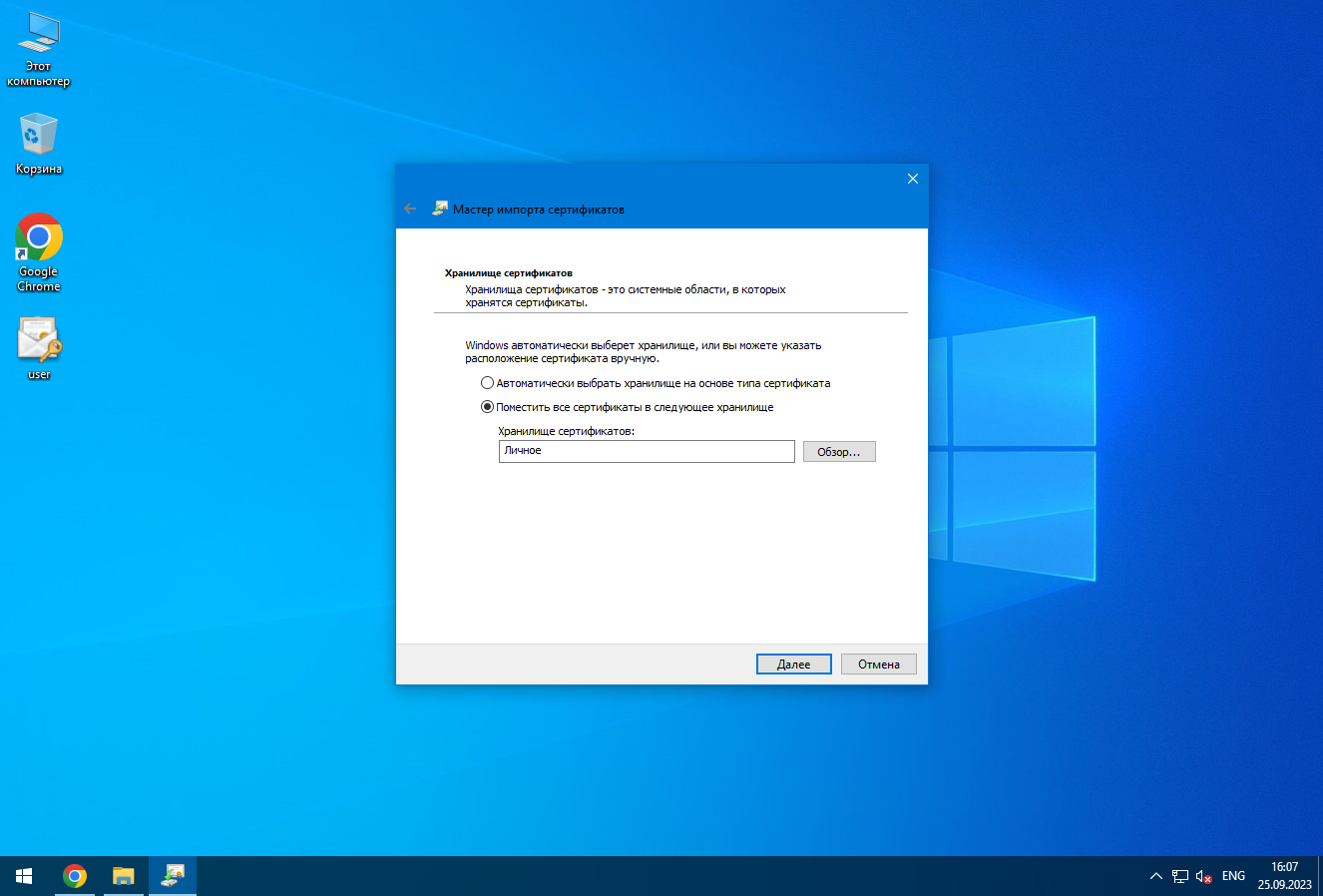


1. Далее проверяем работу пользовательского сертификата.

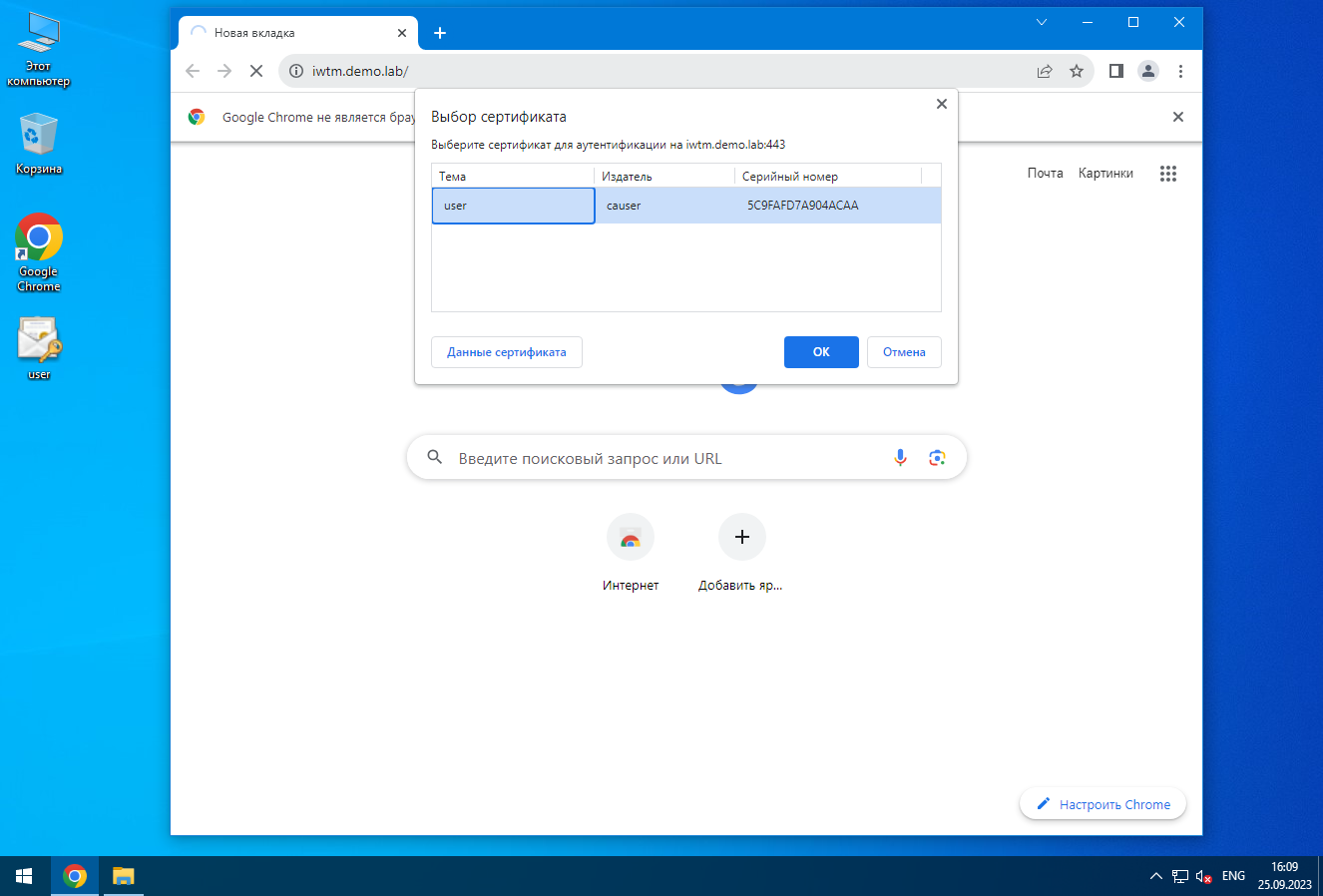
Закидываем сертификат user.pfx на пользовательскую машину и экспортируем его в Текущие пользователи, личная папка. Обновляем политику gpupdate/force







При попытке зайти на iwtm.demo.lab/ запрашивается пользовательский сертификат



И нас пускает в веб-консоль

