# Лабораторная работа №3

# «Изучение принципа шифрования с открытым ключом, библиотеки ssl»

## Цель работы

Изучение принципа шифрования с открытым ключом, библиотеки ssl.

## Постановка задачи

Необходимо сгенерировать сертификат УЦ, сгенерировать сертификат, подписать сертификат созданным УЦ.

## Ход работы

1. Был создан закрытый RSA ключ, результат представлен на рисунках 1-2.

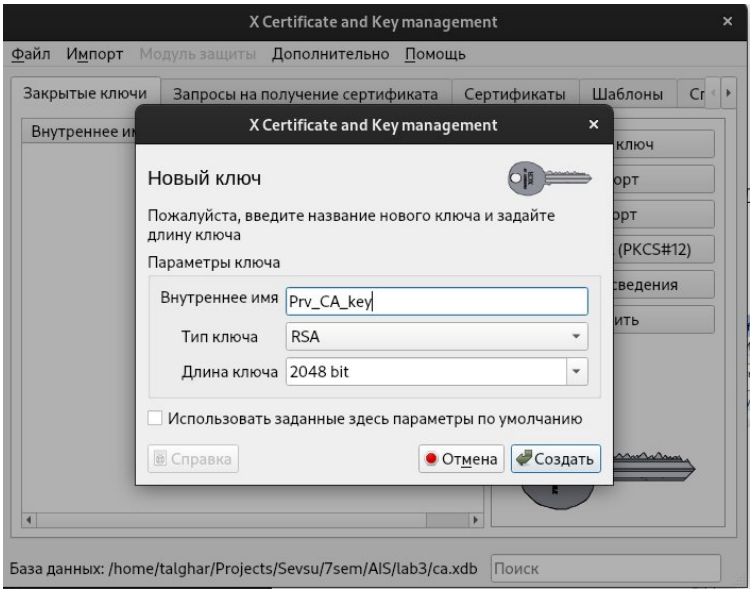


Рисунок 1 – Добавление закрытого ключа

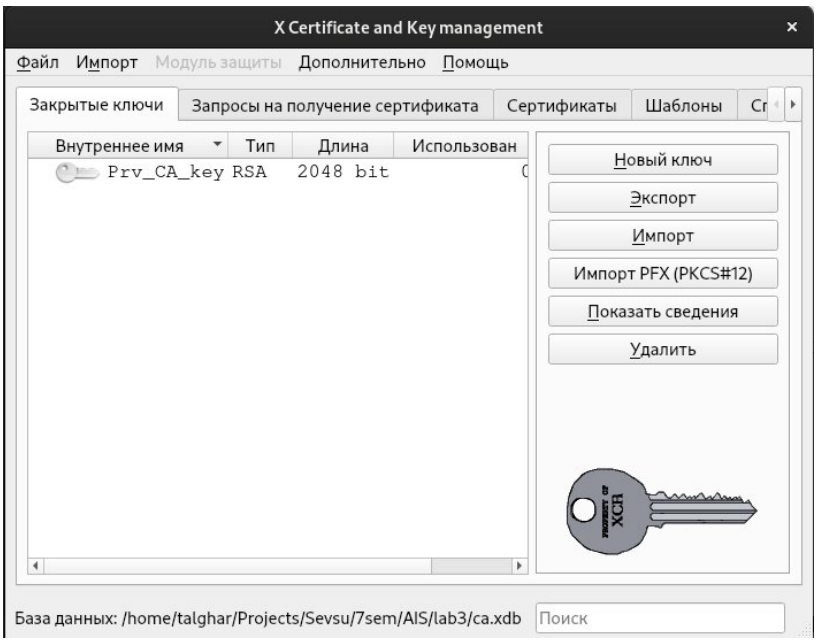


Рисунок 2 – Созданный закрытый ключ

2. Далее был создан сертификат УЦ компании. Результат продемонстрирован на рисунках 3-8.

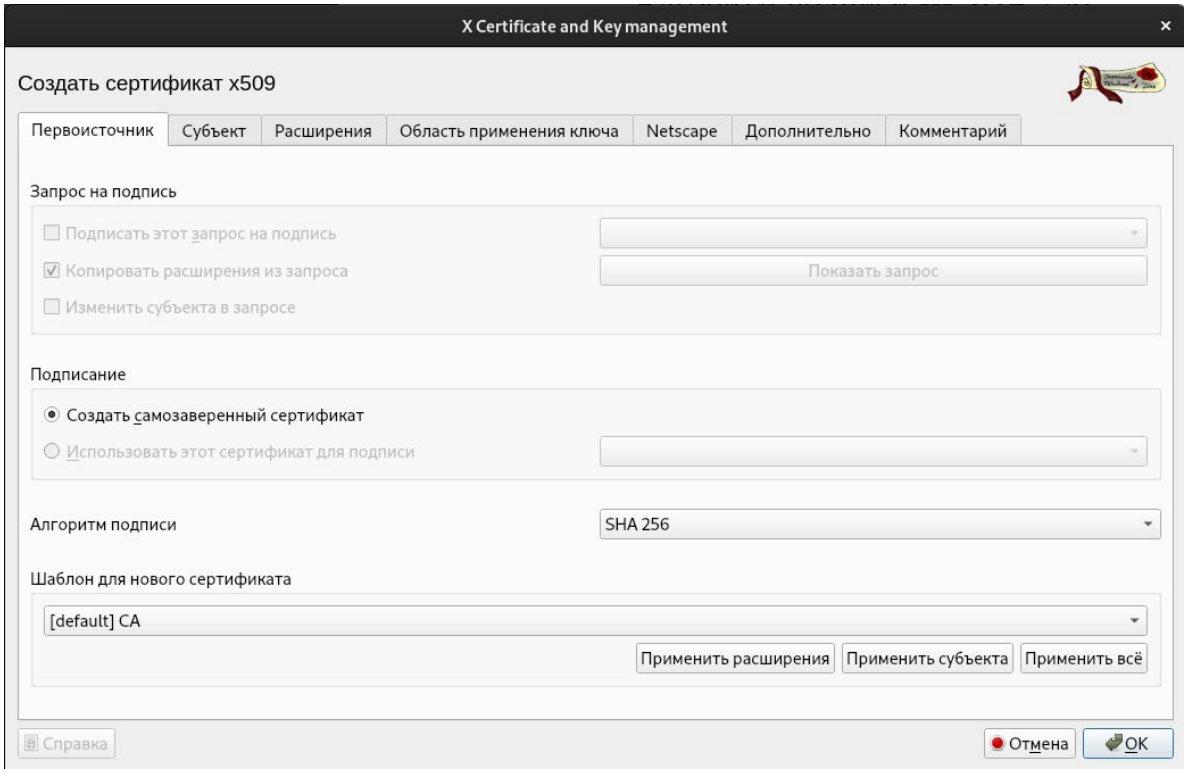


Рисунок 3 – Вкладка первоисточник

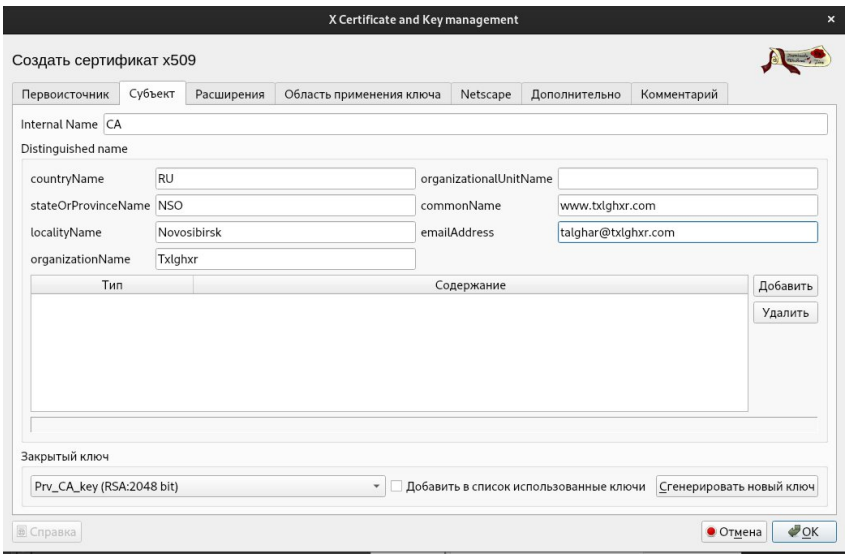


Рисунок 4 – Вкладка субъект

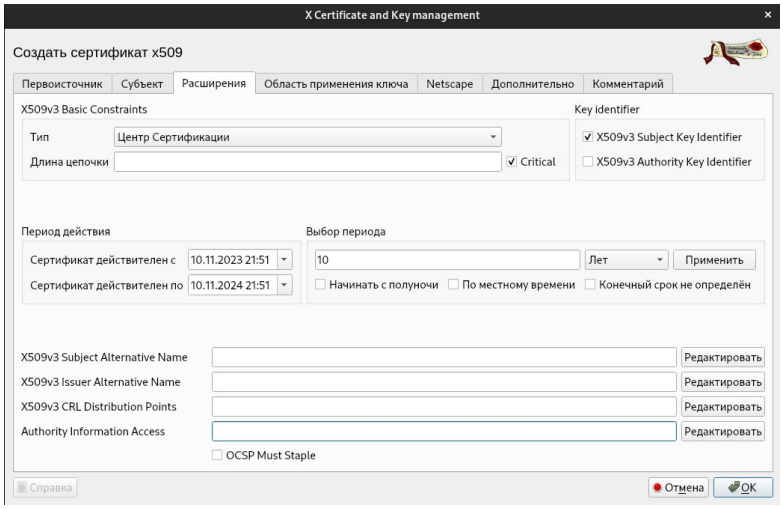


Рисунок 5 – Вкладка расширения

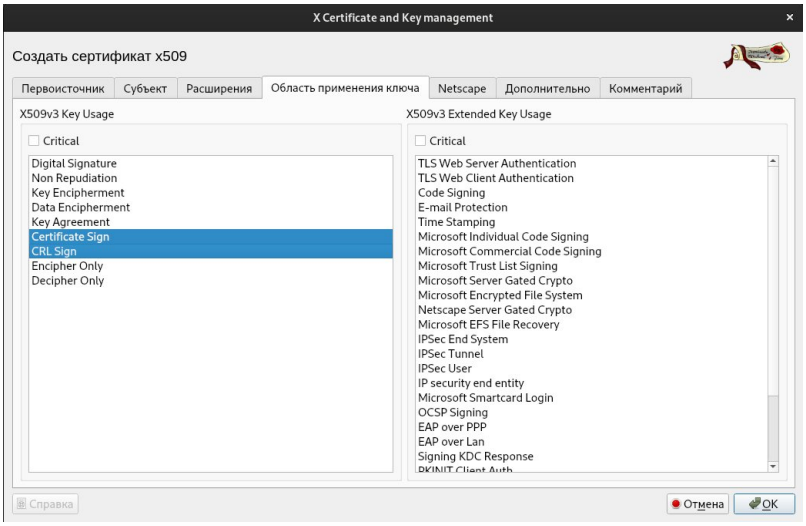


Рисунок 6 – Вкладка область применения ключа

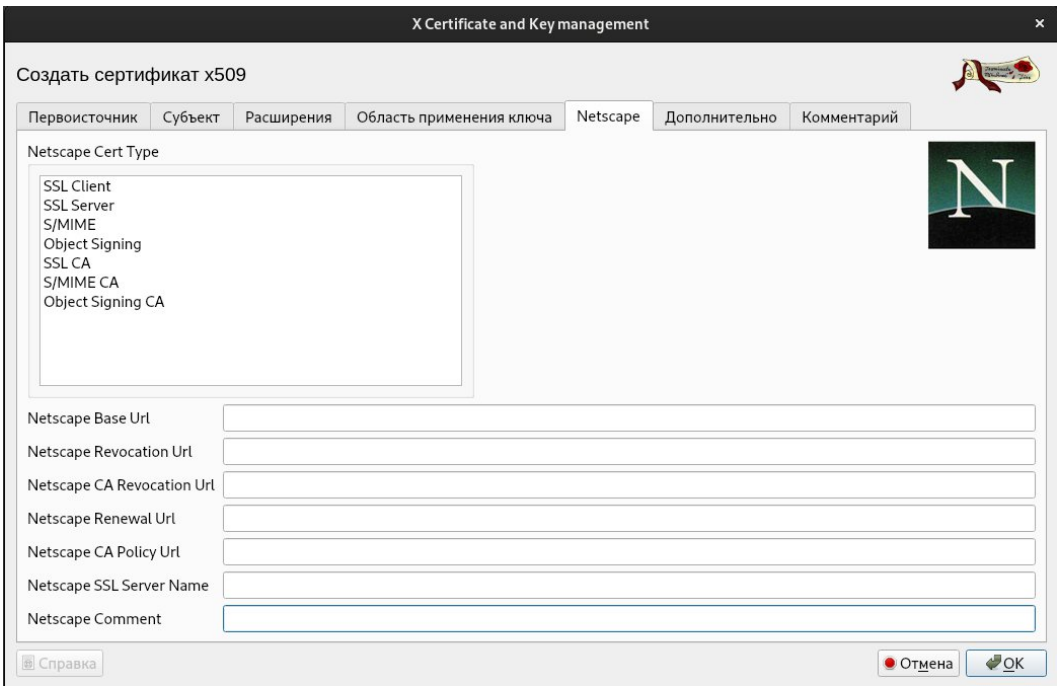


Рисунок 7 – Вкладка Netscape

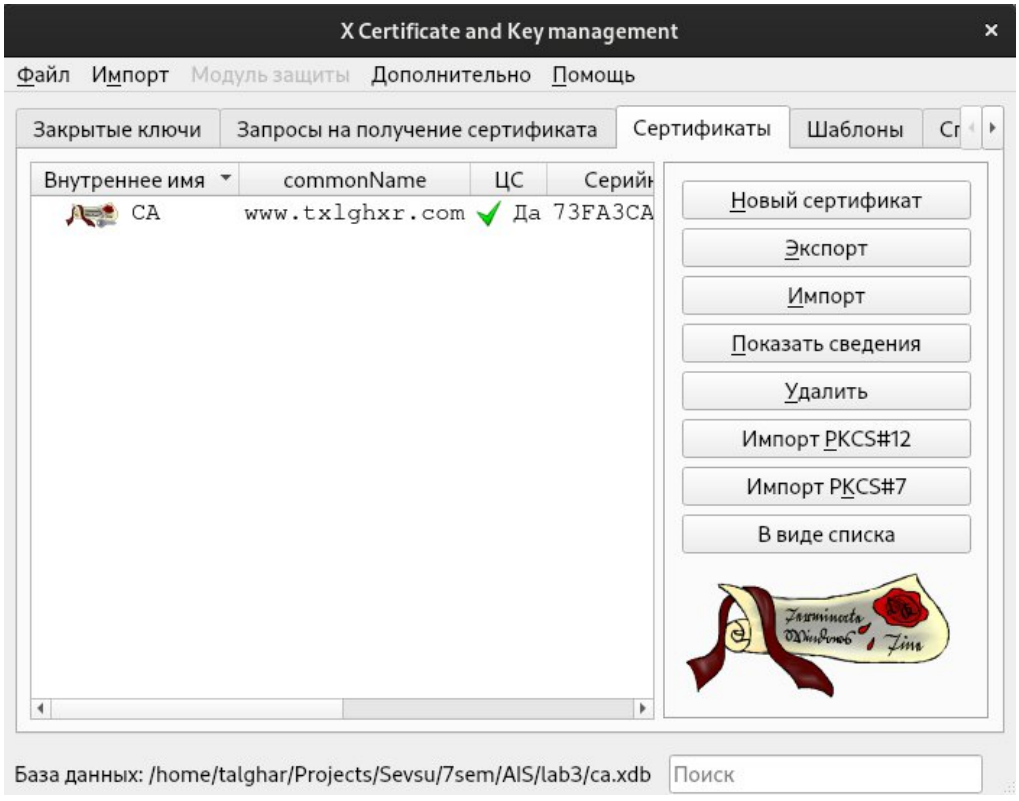


Рисунок 8 – Созданный сертификат

3. После чего созданный закрытый ключ и сертификат были экспортированы в файлы. Результат продемонстрирован на рисунках 9-10.

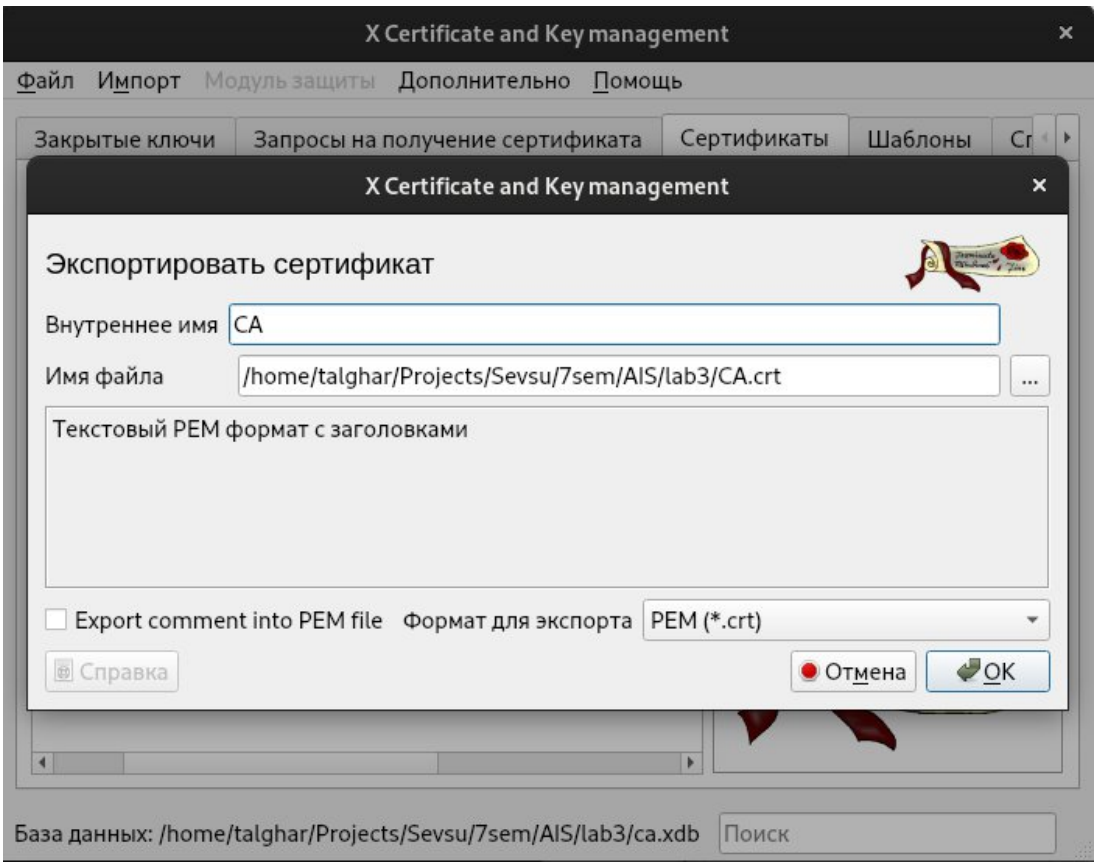


Рисунок 9 – Экспорт сертификата

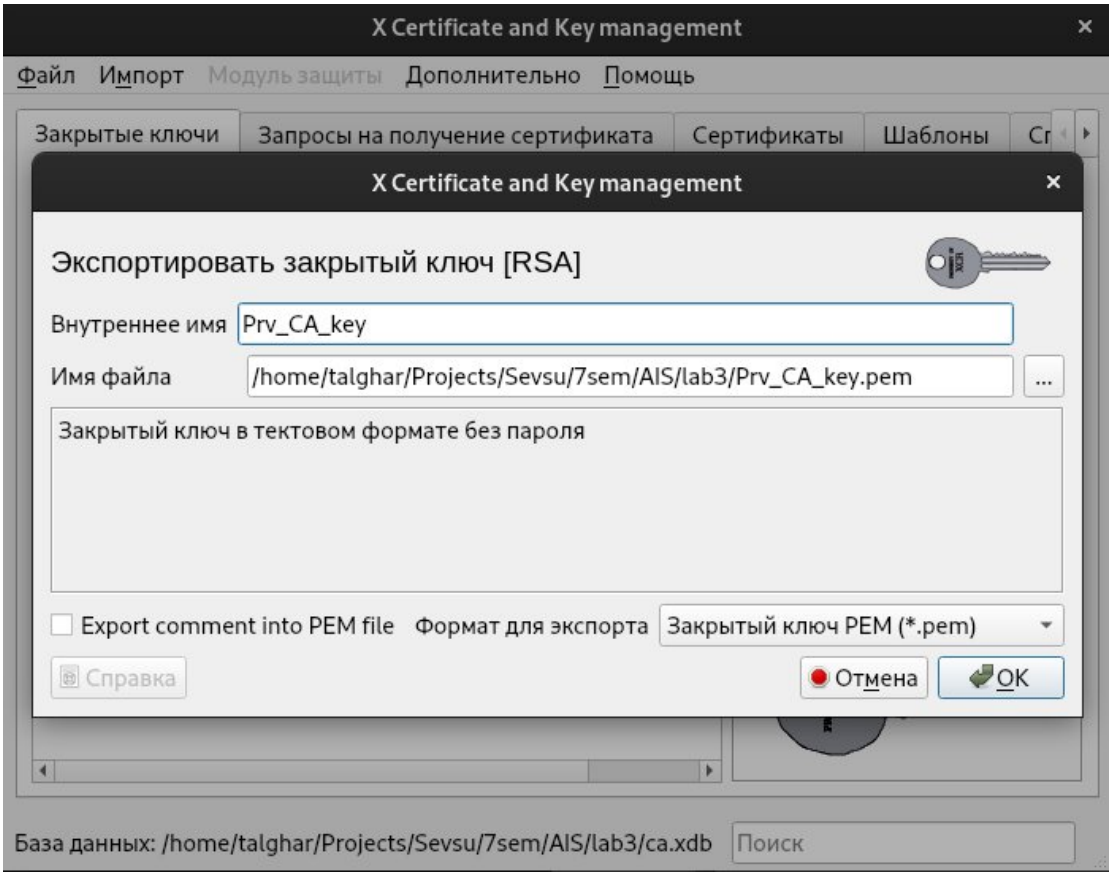


Рисунок 10 – Экспорт закрытого ключа

# Выводы

В ходе выполнения лабораторной работы были изучены принципы шифрования с открытым ключом, библиотека ssl.

Шифрование с открытым ключом – это метод шифрования, при котором используются два ключа: открытый и закрытый. Открытый ключ может быть распространен широко, в то время как закрытый ключ должен быть известен только владельцу. Любой может использовать открытый ключ для шифрования сообщения, но только владелец закрытого ключа может расшифровать его. Этот метод шифрования используется в различных системах, таких как SSL, SSH и PGP.

Библиотека SSL (Secure Sockets Layer) – это криптографический протокол, который обеспечивает безопасную связь между клиентом и сервером в Интернете. Он использует шифрование с открытым ключом для защиты данных, передаваемых между клиентом и сервером. Библиотека SSL широко используется для защиты онлайн-транзакций, таких как покупки в интернет-магазинах и банковские операции.