

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.

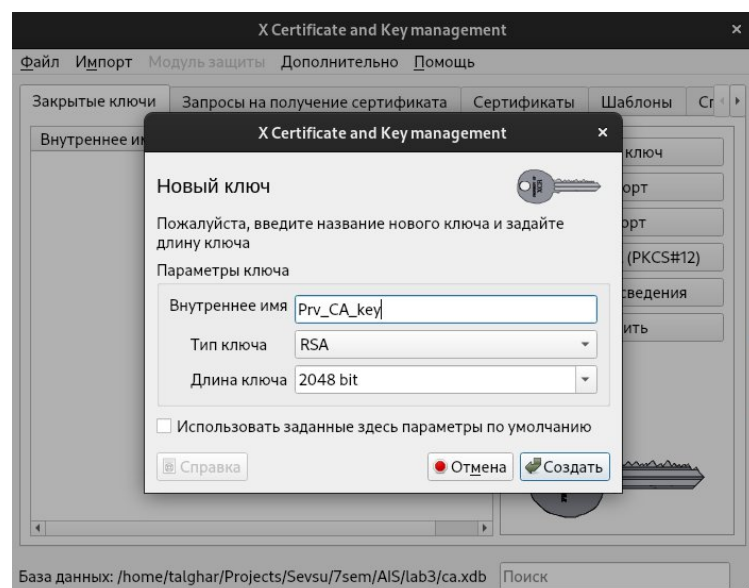


Рисунок 1 – Добавление закрытого ключа

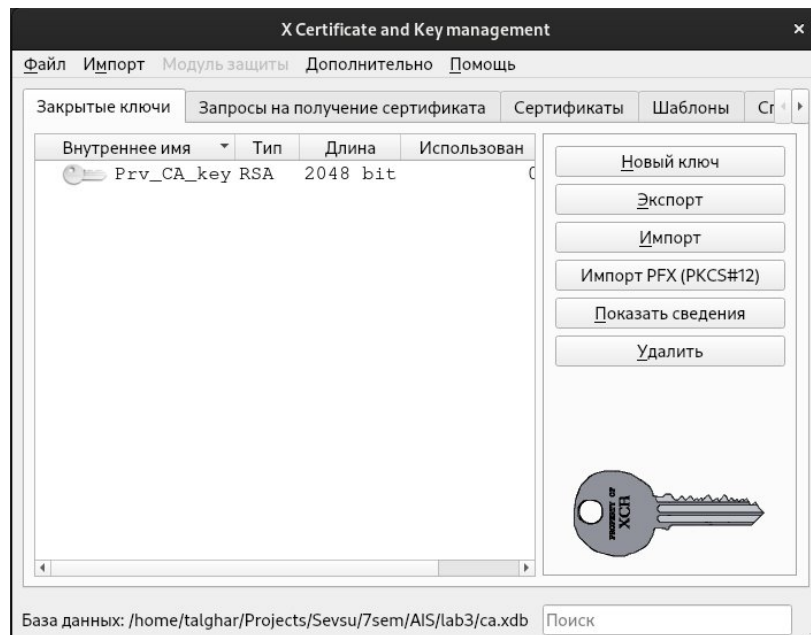


Рисунок 2 – Созданный закрытый ключ

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

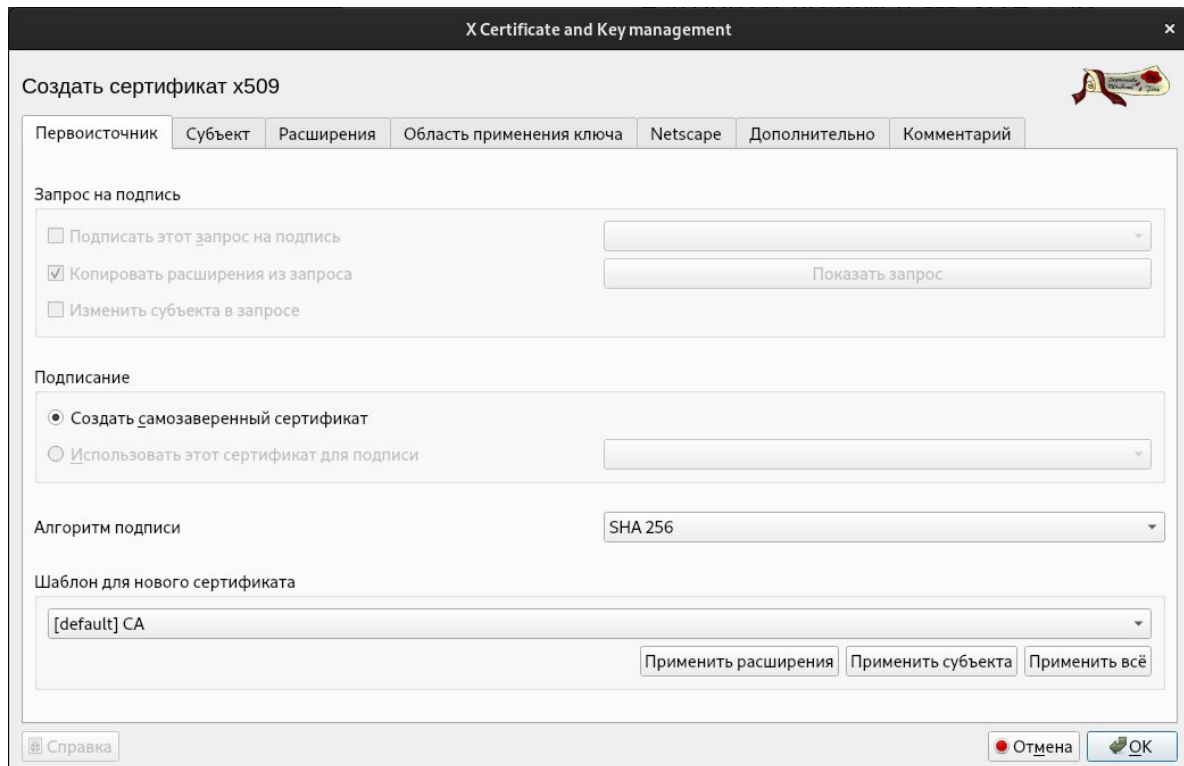


Рисунок 3 – Вкладка первоисточник

X Certificate and Key management

Создать сертификат x509

Первоисточник Субъект Расширения Область применения ключа Netscape Дополнительно Комментарий

Internal Name CA

Distinguished name

countryName	RU	organizationalUnitName	
stateOrProvinceName	NSO	commonName	www.txlghxr.com
localityName	Novosibirsk	emailAddress	talghar@txlghxr.com
organizationName	Txlghxr		

Тип	Содержание	Добавить	Удалить

Закрытый ключ

Prv_CA_key (RSA:2048 bit) ☐ Добавить в список использованные ключи

Справка Отмена OK

Рисунок 4 – Вкладка субъект

X Certificate and Key management

Создать сертификат x509

Первоисточник Субъект Расширения Область применения ключа Netscape Дополнительно Комментарий

X509v3 Basic Constraints

Тип Центр Сертификации

Длина цепочки ☒ Critical

Key Identifier

☒ X509v3 Subject Key Identifier ☐ X509v3 Authority Key Identifier

Период действия

Сертификат действителен с 10.11.2023 21:51

Сертификат действителен по 10.11.2024 21:51

Выбор периода

10 Лет Применить

☐ Начинать с полуночи ☐ По местному времени ☐ Конечный срок не определен

X509v3 Subject Alternative Name Редактировать

X509v3 Issuer Alternative Name Редактировать

X509v3 CRL Distribution Points Редактировать

Authority Information Access Редактировать

☐ OCSP Must Staple

Справка Отмена OK

Рисунок 5 – Вкладка расширения

X Certificate and Key management

Создать сертификат x509

Первоисточник Субъект Расширения Область применения ключа Netscape Дополнительно Комментарий

X509v3 Key Usage

☐ Critical

- Digital Signature
- Non Repudiation
- Key Encipherment
- Data Encipherment
- Key Agreement
- Certificate Sign
- CRL Sign
- Encipher Only
- Decipher Only

X509v3 Extended Key Usage

☐ Critical

- TLS Web Server Authentication
- TLS Web Client Authentication
- Code Signing
- E-mail Protection
- Time Stamping
- Microsoft Individual Code Signing
- Microsoft Commercial Code Signing
- Microsoft Trust List Signing
- Microsoft Server Gated Crypto
- Microsoft Encrypted File System
- Netscape Server Gated Crypto
- Microsoft EFS File Recovery
- IPSec End System
- IPSec Tunnel
- IPSec User
- IP-security end entity
- Microsoft Smartcard Login
- OCSP Signing
- EAP over PPP
- EAP over Lan
- Signing KDC Response
- DKIM/TLS Client Auth

Справка Отмена OK

Рисунок 6 – Вкладка область применения ключа

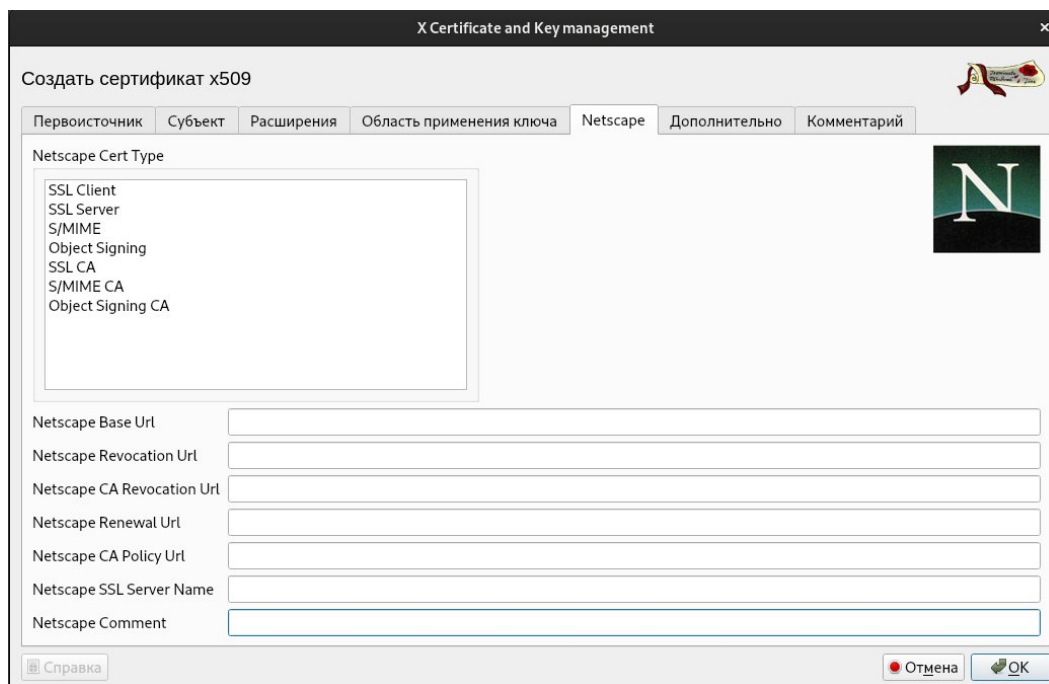


Рисунок 7 – Вкладка Netscape

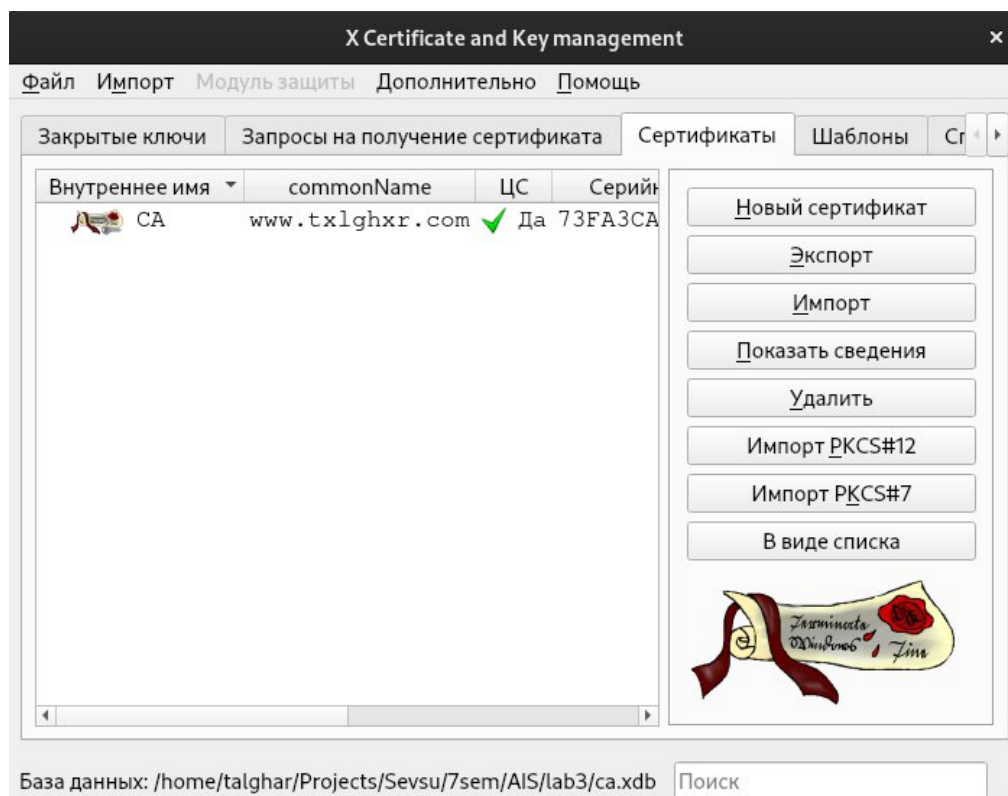


Рисунок 8 – Созданный сертификат

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

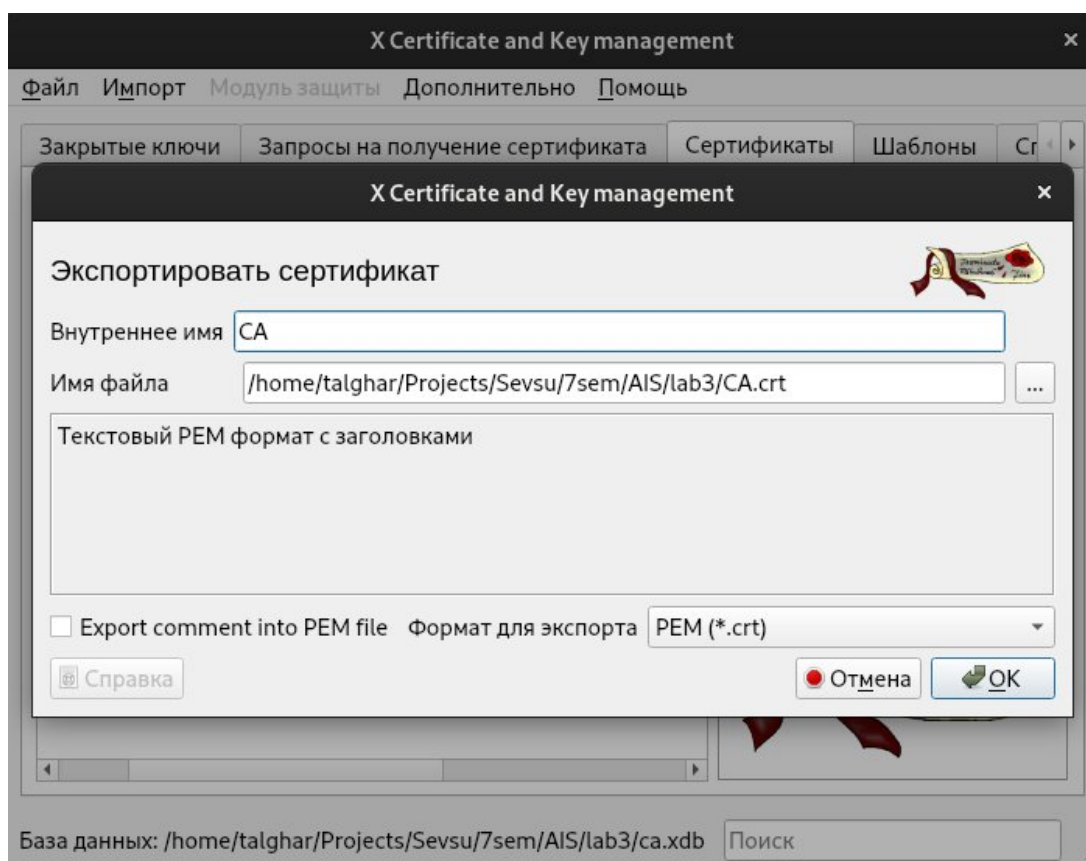


Рисунок 9 – Экспорт сертификата

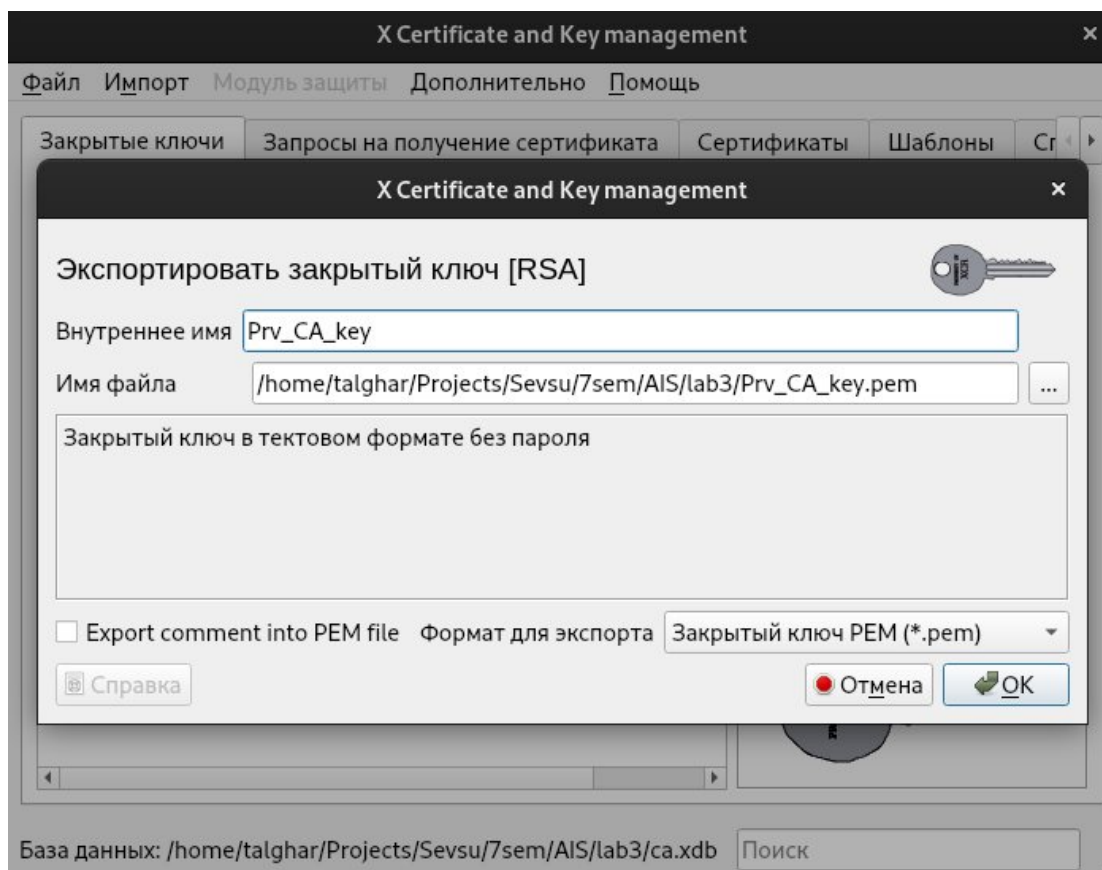


Рисунок 10 – Экспорт закрытого ключа

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.