

Министерство науки и высшего образования Российской Федерации  
Севастопольский государственный университет

## **АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ**

**Методические указания**  
к лабораторным работам  
по дисциплине  
«Администрирование информационных систем»  
для студентов дневной и заочной форм обучения  
направления 09.03.02 «Информационные системы и технологии»

Севастополь  
2020

**Содержание**

1. Цель работы .....	3
2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ .....	3
2.1. Создание сертификата удостоверяющего центра (УЦ) компании.	4
3 СОДЕРЖАНИЕ ОТЧЕТА .....	9
4 ЗАДАНИЕ НА РАБОТУ .....	9
5 КОНТРОЛЬНЫЕ ВОПРОСЫ .....	10

## 1. ЦЕЛЬ РАБОТЫ

Изучение принципа шифрования с открытым ключом, библиотеки ssl.

## 2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Удостоверяющий Центр (УЦ, Certification authority — CA) — это достаточно сложный организм, который включает в свой состав не только программно-аппаратный комплекс, состоящий из множества компонент, но и требующий наличия целого штата высококвалифицированных специалистов для обеспечения его работоспособности и т.д.

Главная функция УЦ центра — изготовление и сопровождение сертификатов ключей проверки электронной подписи (СКПЭП), включая создание ключевой пары по обращению владельца сертификата.

Тот, кто получил сертификат и ключевую пару (закрытый и публичный ключ или как его еще называют ключ проверки электронной подписи), в любой момент может отказаться от своей электронной подписи (ЭП) под документом и заявить, что у него ключ могли украдь в УЦ в момент его генерации. Поэтому ключевую пару правильно генерировать самому и надежно хранить, а если и генерировать его в УЦ, то только на токене/смарткарте PKCS#11 с неизвлекаемым ключом.

УЦ выпускают сертификаты в соответствии со стандартом X.509 v.3 (RFC 5280).

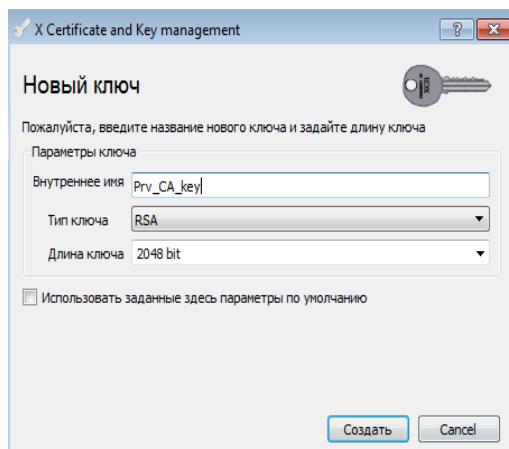
Для выпуска для издания сертификатов x509v.3 можно воспользоваться широко используемой командной утилитой OpenSSL, в частности, она позволяет выполнять следующие функции:

- генерация ключей (например, opensslgenrsa...);
  - формирование запроса в формате PKCS#10 на получение сертификата x509 v.3;
  - издание сертификата x509 v.3;
  - формирование списка аннулированных сертификатов (CAC/CRL);
- Для удобства использования будет рассматриваться проект с открытым кодом (Copyright) XCA, в котором для криптографических преобразований

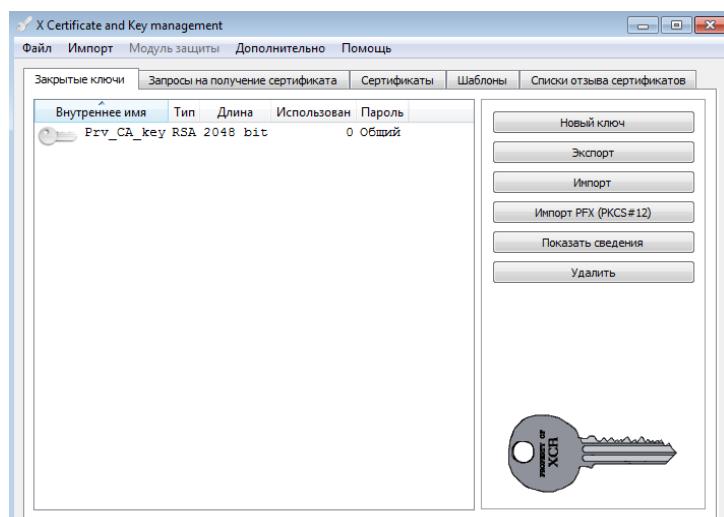
используется библиотека OpenSSL, для графического интерфейса используется библиотека Qt, а в качестве языка программирования язык C++. Для проектирования графического интерфейса использован QtDesigner (утилита designer), что делает весьма простым доработку графического интерфейса с учетом специфических требований российского законодательства и нормативных актов регуляторов, например, форму графического интерфейса для нового сертификата (файл ~/src/ui/NewX509.ui).

## 2.1. Создание сертификата удостоверяющего центра (УЦ) компании.

Вкладка Закрытые ключи → Новый ключ.



Далее необходимо заполнение параметров ключа и нажать кнопку создать.

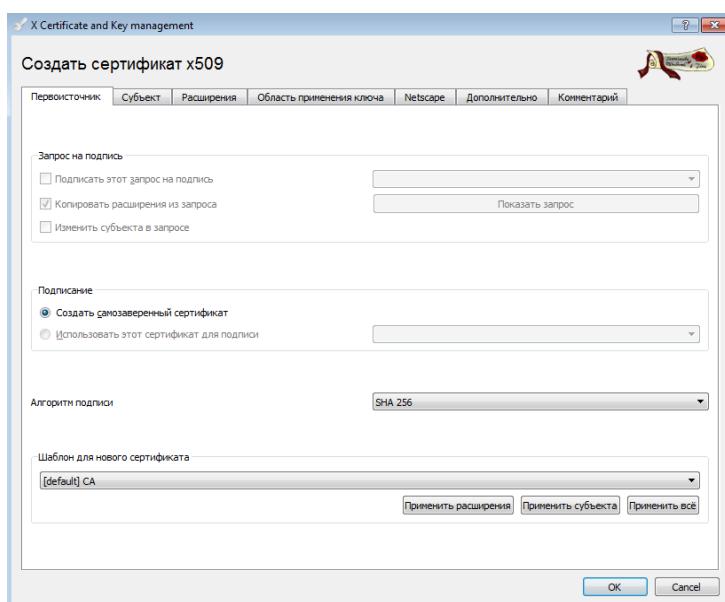


Далее необходимо перейти во вкладку Сертификаты и создать сертификат УЦ компании.

Далее необходимо нажать кнопку новый сертификат - вкладка Первоисточник.

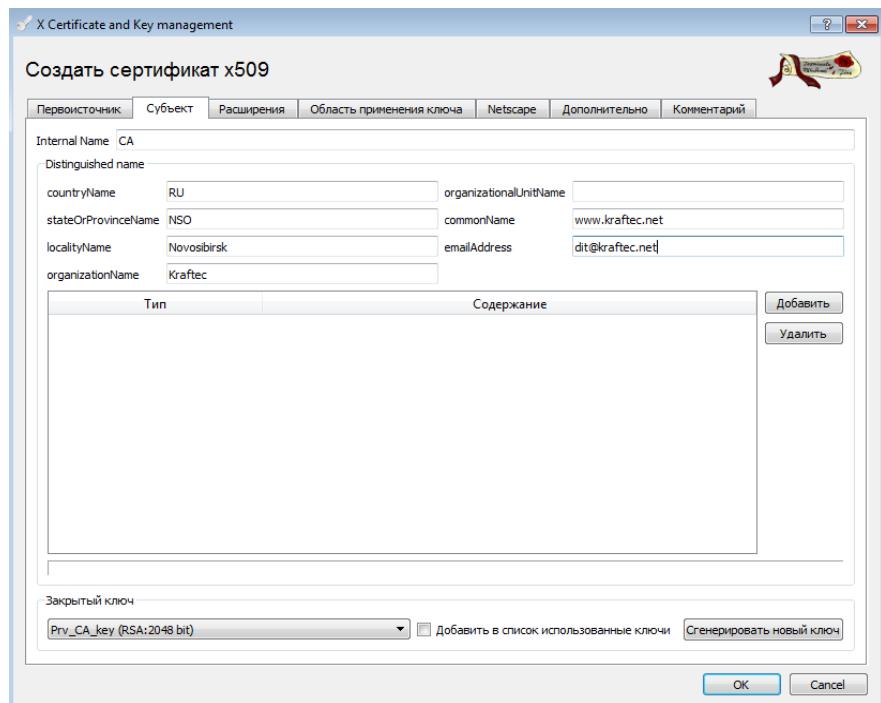
Алгоритм подписи --- SHA 256

Шаблон для нового сертификата - по умолчанию для УЦ (CA - Certificateauthority)



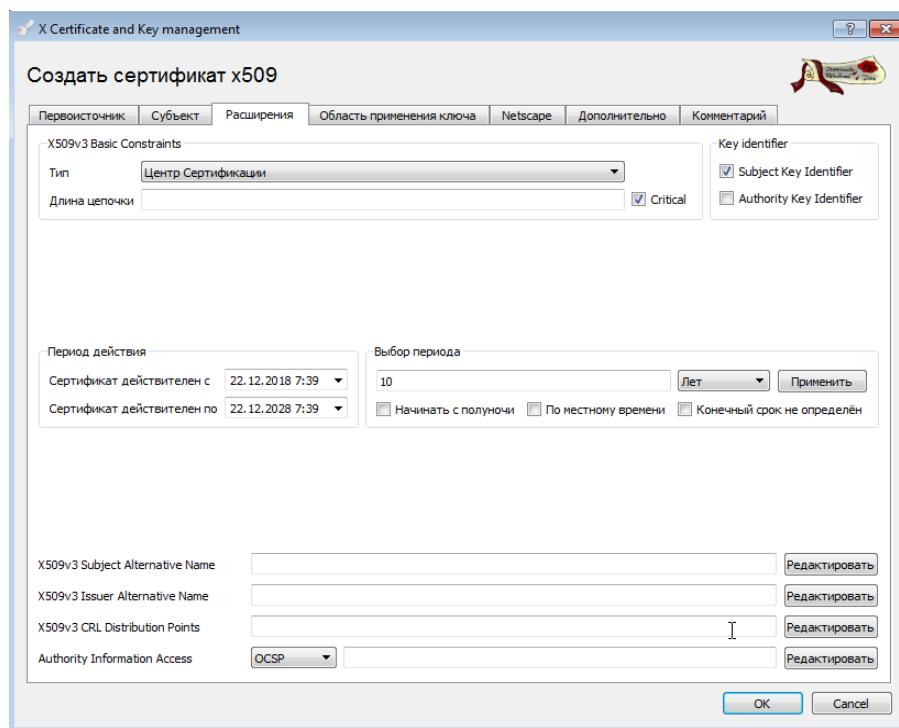
Вкладка Субъект.

Далее заполнить данные на сертификат, выбирать закрытый ключ.

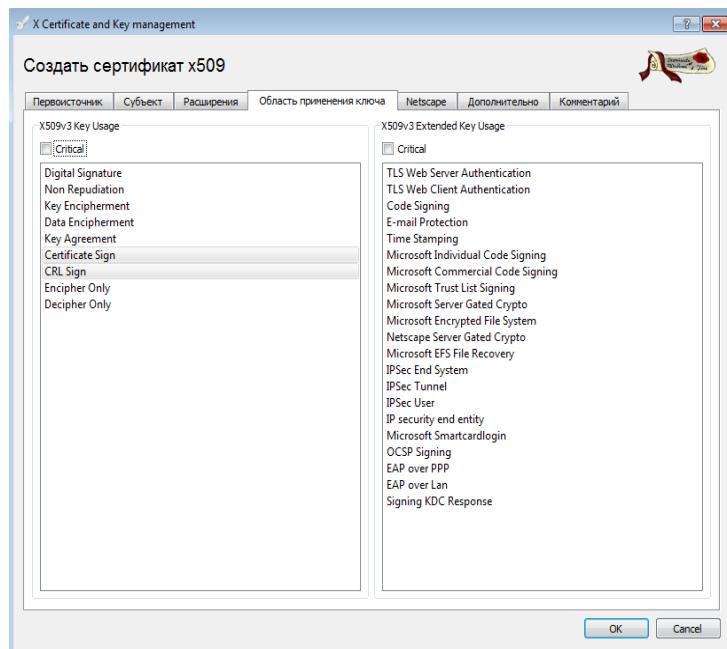


**Вкладка Расширение.**

**Тип базового контейнера - Центр Сертификации.**

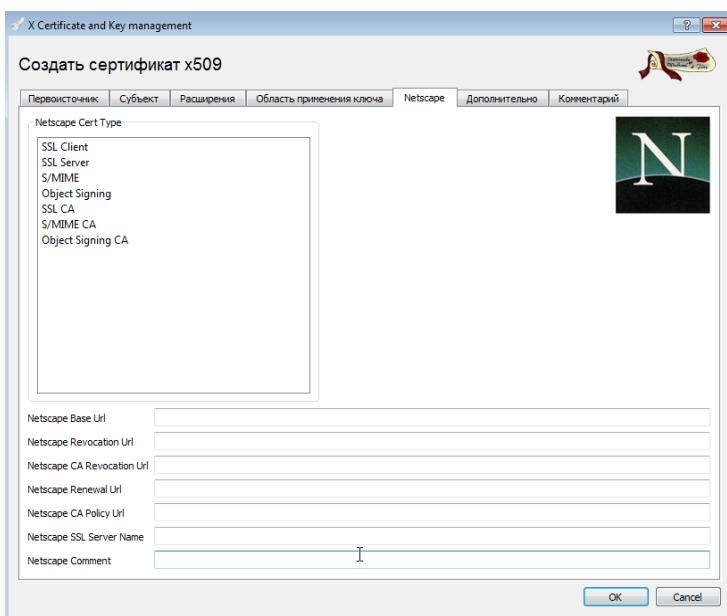


**Вкладка Область применения ключа.**



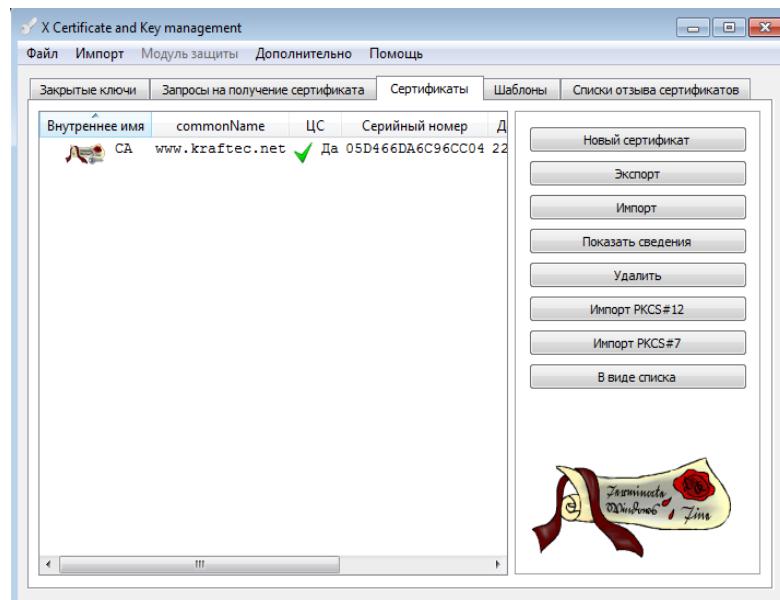
**Вкладка Netscape.**

**Можно убрать выбранные типы шаблона CA**

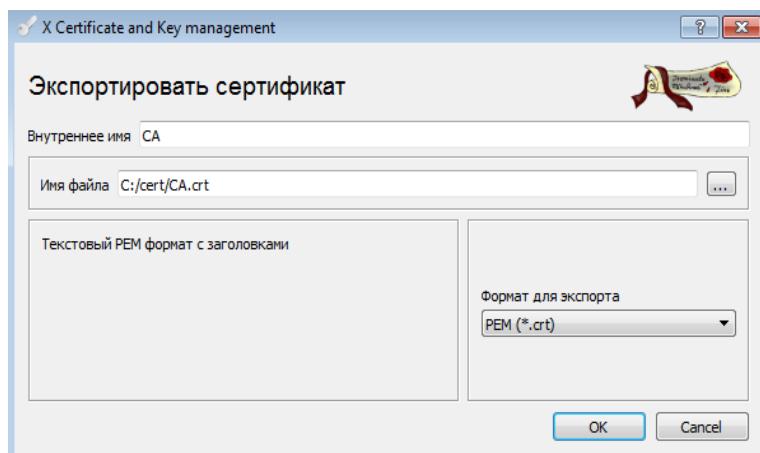


**Нажимаем кнопку Ok для создания сертификата.**

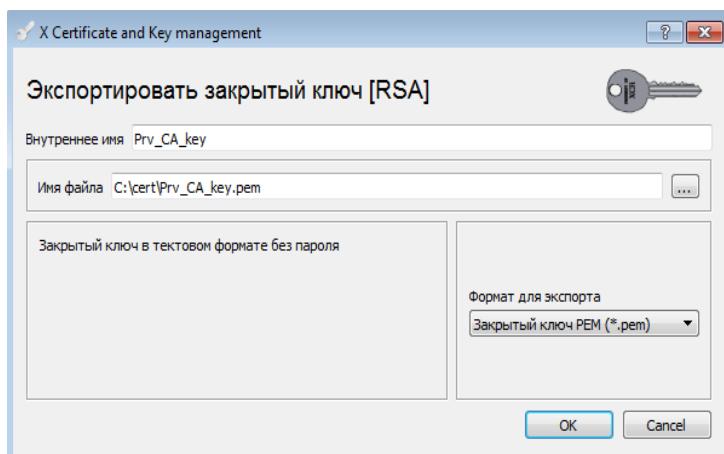
**Во вкладке Сертификаты появился сертификат УЦ.**



Выполнение экспорт данного сертификата для импорта в нужную информационную систему.



Экспортируем закрытый ключ.



### **3 СОДЕРЖАНИЕ ОТЧЕТА**

Титульный лист, цель работы, описание выполненной работы с иллюстрациями (скриншоты выполненных действий) и выводы по проделанной работе.

### **4 ЗАДАНИЕ НА РАБОТУ**

Необходимо сгенерировать сертификат УЦ, сгенерировать новый сертификат, подписать сертификат созданным УЦ. Импортировать созданный сертификат в вэб сервер системы установленной в лабораторной работе №2.

## 5 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое УЦ?
2. В чем отличие открытого ключа и сертификата?
3. Какой функционал несет закрытый ключ?
4. В чем особенности Формата сертификата \*.pfx?
5. Какие УЦ являются доверенными?
6. Что такое список отзываемых сертификатов?
7. можно ли с помощью одного закрытого ключа создать несколько сертификатов?
8. Какова основная уязвимость в шифровании с открытым ключом?
9. Какие основные форматы файлов открытого ключа и сертификата?
10. Что такое цепочка сертификатов УЦ?
11. Каким образом сертификаты попадают в список отзываемых?
12. Как производится браузером проверка сертификата?