

КриптоПро УЦ 2.0

Пошаговый практикум по развёртыванию
КриптоПро УЦ версии 2 с настройками для
выпуска квалифицированных сертификатов

АННОТАЦИЯ

Настоящий документ содержит описание процесса развёртывания программного комплекса «Удостоверяющий Центр «КриптоПро УЦ» версии 2 и его настройки для выпуска квалифицированных сертификатов.

Предполагаемое время прохождения практикума: 90 минут

После прохождения практикума вы будете уметь:

- добавлять и настраивать роли КриптоПро УЦ 2.0;
- производить настройки для выпуска квалифицированных сертификатов;
- регистрировать пользователей в КриптоПро УЦ 2.0;
- выпускать для пользователей квалифицированные сертификаты;
- отзываться сертификаты;
- осуществлять внеочередной выпуск CRL.

Виртуальное окружение:

Выполнение практикума возможно в различных виртуальных окружениях:

Oracle VM Virtual Box, VMware Workstation, VMware vSphere, Hyper-V.

В качестве гостевой ОС используется ознакомительная версия Windows Server 2012 R2 Standard.

Информация о разработчике ПАК «КриптоПро УЦ»:

ООО "КРИПТО-ПРО"

127018, Москва, улица Суцеский вал, 18

Телефон/факс: +7 (495) 995-48-

20 Сайт: <http://www.CryptoPro.ru>

E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Упражнение: Настройка Сервера ЦС	4
1.1. Создание запроса на клиентский сертификат ЦР	4
1.2. Настройка роли Сервер ЦС	4
2. Упражнение: Проверка квалифицированного сертификата ЦС	6
3. Упражнение: Настройка ЦС для выпуска квалифицированных сертификатов	7
3.1. Настройка политики имен	7
3.2. Настройка шаблонов сертификатов	7
4. Упражнение: Настройка Сервера ЦР	9
4.1. Создание запроса на сертификат Администратора ЦР	9
4.2. Настройка роли Сервер ЦР	9
5. Упражнение: Настройка Консоли управления ЦР	11
6. Упражнение: Создание квалифицированного сертификата по 63-ФЗ	12
6.1. Регистрация нового пользователя	12
6.2. Выпуск сертификата.	12
7. Упражнение: Отзыв сертификата.	13
8. Упражнение: Выпуск списка отозванных сертификатов	14

1. Упражнение: Настройка Сервера ЦС

1.1. Создание запроса на клиентский сертификат ЦР

1. Откройте оснастку **Диспетчера УЦ**.
2. Выделите в окне **Диспетчера УЦ** узел **Роли УЦ** и кликните справа в панели **Действия** пункт **Добавить роль Сервер ЦР**.
3. На странице мастера **Выбор действия** выберите **Создание запроса на клиентский сертификат**.
4. На странице **Создание запроса на сертификат** оставьте значения по умолчанию и нажмите **Далее**.
5. При создании запроса не устанавливайте пин-код на контейнер.
6. На странице сохранения файла запроса выберите **Сохранить запрос на клиентский сертификат Центра Регистрации**. Файл запроса сохраните со значениями по умолчанию.
7. На странице **Операция завершена** нажмите **Завершить**.

1.2. Настройка роли Сервер ЦС

1. Выделите в окне **Диспетчера УЦ** узел **Роли УЦ**, и щелкните справа в панели **Действия** на пункт **Добавить роль Сервер ЦС**.
2. На страницах **Создание базы данных**, **Настройка веб-служб** оставьте значения по умолчанию.
3. На странице **Выбор типа Центра Сертификации** укажите **Корневой Центр Сертификации**.
4. На странице **Основные параметры Центра Сертификации** в поле **Название** введите название центра сертификации **Пробный Корневой УЦ**. Значение срока действия ключа проверки ЭП ЦС оставьте по умолчанию и нажмите **Далее**.
5. На странице **Дополнительные атрибуты имени ЦС** введите значения, указанные на рис. ниже

Дополнительные атрибуты:	
Атрибут	Значение
Общее имя	Пробный Корневой УЦ
Организация	ООО "Пробный Корневой УЦ"
Почтовый адрес	ул. Суцёвский вал д. 18
Город	Москва
Область	г. Москва
Страна/регион	RU
ИНН	007717107991
ОГРН	1037700085444

6. На странице **Расширения сертификатов администраторов Центра Сертификации**:

- Нажмите кнопку **Добавить**, выберите расширение **Политики сертификата**, нажмите кнопку **Изменить**, отметьте два идентификатора (**Класс средства ЭП КС1** и **Класс средства ЭП КС2**) и идентификатор **Все политики выдачи**.
- Добавьте расширение **Средство Электронной подписи и УЦ издателя** и введите для него значения, указанные на рис. ниже

Средство ЭП:	"КриптоПро CSP" (версия 3.9)
Заключение на средство ЭП:	Сертификат соответствия № СФ/111 от 01.01.01
Средство УЦ:	"КриптоПро УЦ" версии 2.0
Заключение на средство УЦ:	Сертификат соответствия № СФ/222 от 01.01.01

- Добавьте расширение **Средство ЭП владельца** и введите для него значение **"КриптоПро CSP" (версия 3.9)**.
- Нажмите **Далее**.

7. На странице **ФИО администратора «Центра Сертификации»** введите следующие значения:

- **Имя** – Иванов Иван Иванович

8. На странице **Дополнительные атрибуты имени администратора ЦС** оставьте значения по умолчанию и нажмите **Далее**.

9. На странице **Параметры учётной записи администратора ЦС** отметьте чекбокс **Использовать существующую учётную запись** и укажите:

- **Имя пользователя** – Администратор
- **Пароль и Подтверждение пароля** – пароль, заданный вами на момент запуска ОС.

10. На странице **Сертификат администратора ЦС** оставьте значения по умолчанию и нажмите **Далее**.

11. На страницах **Сертификат веб-узла сервера ЦС** оставьте значения по умолчанию и нажмите **Далее**.

12. На странице **Основные параметры Центра Регистрации** введите в поля:

- **Имя** – Пробный ЦР
- **Доменное имя** – srqualcalab

13. На странице **Службы ЦР** оставьте значения по умолчанию и нажмите **Далее**.

14. На странице **Параметры учётной записи ЦР** введите в поля:

- **Имя пользователя** – Пробный ЦР
- **Пароль и Подтверждение пароля** – Pa\$\$w0rd

15. На странице **Сертификат аутентификации ЦР** выберите для пункта **Отправить или проверить состояние запроса** файл запроса, полученный на шаге **1.1**.

16. На странице **Подтверждение** нажмите **Далее**.

17. На странице **Выполнение действий** дождитесь выполнения всех действий и нажмите **Далее**.

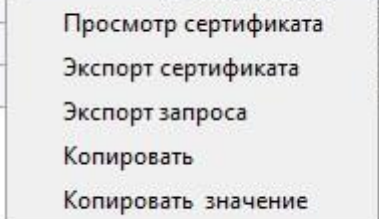
18. На странице **Сохранить в файл** выберите **Сохранить сертификат «Службы Регистрации»**. Файл сертификата сохраните со значениями по умолчанию.

19. Завершите работу мастера нажатием на кнопку **Завершить**.

Упражнение: Проверка квалифицированного сертификата ЦС

1. В **Диспетчере УЦ** раскройте узел **Сервер ЦС** и выберите Центры Сертификации **Пробный Корневой УЦ**. Выберите дочерний узел **Журнал**.
2. Экспортируйте сертификат ЦС в файл

ID запроса	Серийный номер	Дата начала	Дата окончания
		29.04.2016 ...	29.04.2021 14:09
		29.04.2016 ...	29.07.2017 14:20
		29.04.2016 ...	29.07.2017 14:20



3. Откройте в проводнике **«C:\Проверка квалифицированных сертификатов»** и запустите утилиту **TestQualifiedCertificate2.exe**. Проверьте, соответствует ли сертификат ЦС требованиям к квалифицированному сертификату.
4. Официальные ссылки:
 - Утилита для проверки квалифицированных сертификатов –
<http://e-trust.gosuslugi.ru/download/TestQualifiedCertificate2.zip>
 - Инструкция-
http://etrust.gosuslugi.ru/download/man_TestQualifiedCertificate2.pdf

2. Упражнение: Настройка ЦС для выпуска квалифицированных сертификатов

2.1. Настройка политики имен

1. В **Диспетчере УЦ** откройте раздел **Политики**.
2. Отметьте в поле **Допустим в профиле** и в поле **Допустим в имени субъекта** компоненты имени: ОГРН, ИНН, СНИЛС, Фамилия, Имя и Отчество, Адрес, Должность или Звание.
3. После установки значений нажмите кнопку **Применить**.
4. Нажмите правой кнопкой мыши на узел **Роли УЦ** и выберите **Обновить**.

2.2. Настройка шаблонов сертификатов

1. В подразделе **Шаблоны** выберите шаблон **Пользователь**.
2. В параметрах **«Правила формирования имени субъекта сертификата»** добавьте значения, указанные на рис. ниже
SN=<Фамилия>
G=<Имя и отчество>
T=<Должность или звание>
STREET=<Адрес>
CN=<ФИО или псевдоним>
OU=<Подразделение>
O=<Организация>
L=<Город>
S=<Область>
C=<Страна/регион>
E=<Адрес E-Mail>
INN=<ИНН>
OGRN=<ОГРН>
SNILS=<СНИЛС>
3. После установки значений нажмите кнопку **Применить**.
4. В параметрах **Настройка расширений сертификата**:
 - Нажмите кнопку **Добавить**, выберите расширение **Политики сертификата**, нажмите кнопку **Изменить**, отметьте два идентификатора (**Класс средства ЭП КС1** и **Класс средства ЭП КС2**).
 - Добавьте расширение **Средство Электронной подписи и УЦ издателя** и введите для него значения, указанные на рис. ниже

Средство ЭП:	"КриптоПро CSP" (версия 3.9)
Заключение на средство ЭП:	Сертификат соответствия № СФ/111 от 01.01.01
Средство УЦ:	"КриптоПро УЦ" версии 2.0
Заключение на средство УЦ:	Сертификат соответствия № СФ/222 от 01.01.01

- Добавьте расширение **Средство ЭП владельца** и введите для него значение **"КриптоПро CSP" (версия 3.9)**.

5. После установки значений нажмите кнопку **Применить**.
6. Нажмите правой кнопкой мыши на узел **Роли УЦ** и выберите **Обновить**.

3. Упражнение: Настройка Сервера ЦР

3.1. Создание запроса на сертификат Администратора ЦР

1. Запустите **Консоль управления ЦР**.
2. В главном меню **Консоли управления ЦР** выберите пункт **Добавить подключение**.
3. В меню открывшемся окне **Подключение к центру регистрации** выберите пункт **Создать запрос**.
4. В следующем окне нажмите **Сохранить и закрыть**.
5. В диалоговом окне сохранения файла запроса нажмите **Сохранить** со значениями по умолчанию.

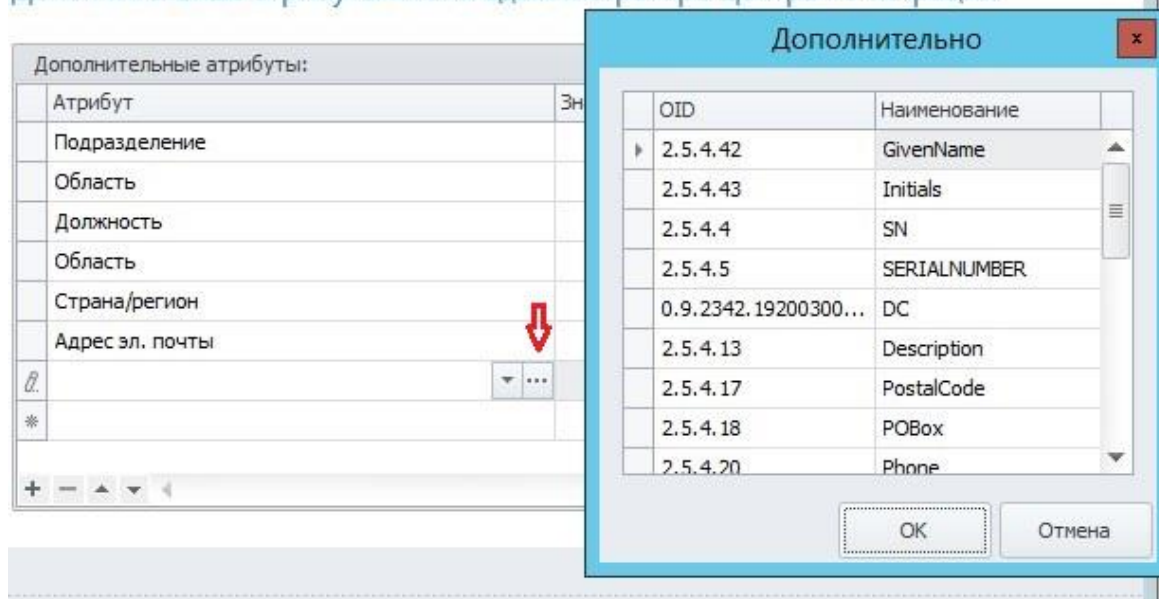
3.2. Настройка роли Сервер ЦР

1. Выделите в окне **Диспетчера УЦ** узел **Роли УЦ**, и щелкните справа в панели **Действия** на пункт **Добавить роль Сервер ЦР**.
2. На странице мастера **Выбор действия** выберите **Добавление роли Сервер ЦР**.
3. На страницах **Создание базы данных, Настройка веб-служб, Выбор устанавливаемых служб «Службы Регистрации»** оставьте значения по умолчанию.
4. На странице **Подключение к Центру Сертификации** в поле **Адрес** введите **https://срqualcalab/са** нажмите **Далее**.
5. На странице **Выбор клиентского сертификата ЦР** выберите для пункта **Установить ответ на запрос из файла** путь к файлу сертификата, полученного на шаге **18** пункта **1.2** и нажмите **Далее**.
6. На странице **Выбор подключения к Центру Сертификации** оставьте значение по умолчанию и нажмите **Далее**.
7. На странице **Сертификат веб-узла сервера ЦР** снимите галочку **Изготовить сертификат веб-сервера** и нажмите **Далее**.
8. На странице **ФИО и почтовый адрес Администратора ЦР** введите в поля:
 - **Имя** – Петров
9. На странице **Дополнительные атрибуты имени администратора ЦР** введите значения, указанные на рис. ниже

Дополнительные атрибуты:	
Атрибут	Значение
Фамилия	Петров
Имя	Петр Петрович
Должность	Администратор ЦР
Почтовый адрес	ул. Суцёвский вал д. 18
Организация	ООО "Тробный Корневой УЦ"
Город	Москва
Область	77 г. Москва
Страна/регион	RU
ИНН	007717107991
ОГРН	1037700085444
СНИЛС	52222222222

Если необходимый атрибут отсутствует добавляем как показано на рис. ниже

Дополнительные атрибуты имени администратора Центра Регистрации



10. На странице **Сертификат администратора ЦР** выберите для пункта **Отправить или проверить состояние запроса** файл запроса, полученный на шаге **4.1**.
11. На странице **Подтверждение** нажмите **Далее**.
12. На странице **Выполнение действий** дождитесь выполнения всех действий и нажмите **Далее**.
13. На странице **Сохранить в файл** выберите **Сохранить сертификат аутентификации администратора «Службы регистрации»**. Файл сертификата сохраните со значениями по умолчанию.
14. Завершите работу мастера нажатием на кнопку **Завершить**.

4. Упражнение: Настройка Консоли управления ЦР

1. Запустите **Консоль управления ЦР**.
2. В главном меню **Консоли управления ЦР** выберите пункт **Добавить подключение**.
3. В меню открывшемся окне **Подключение к центру регистрации**:
 - Введите в поле **Адрес службы регистрации**: **https://срqualcalab/ra**
 - Нажмите на кнопку **Установить сертификат** и укажите путь к файлу сертификата, полученного на шаге **13** пункта **4.2**.
 - Нажмите на кнопку **Проверить соединение**, а после получения сообщения об удачном соединении с ЦР нажмите на кнопку меню **Сохранить и закрыть**.
4. Нажмите **Подключиться** для установления соединения с ЦР.

5. Упражнение: Создание квалифицированного сертификата по 63-ФЗ

5.1. Регистрация нового пользователя

1. В Консоли управления ЦР выбрать в навигационной панели **Пользователи** и нажать в ленте кнопку **Новый пользователь**.
2. В окне **Запрос на регистрацию пользователя** отметьте галочкой **Одобрить** и **Открыть пользователя** и заполните компоненты имени как указано на рис. ниже, после чего нажмите **Сохранить и закрыть**.

Компонент	Значение
ФИО или псевдоним	Сидоров Сидор Сидорович
Фамилия	Сидоров
Имя и отчество	Сидор Сидорович
Страна/регион	RU
Область	77 г. Москва
Город	Москва
Адрес	Ул. Тверская, д. 5 кор. 1, строение 1
Организация	QA
Подразделение	Отдел Тестирования
Должность или звание	Инженер отдела тестирования
ОГРН	1037700085444
СНИЛС	12345678912
ИНН	007717107991
Адрес E-Mail	qa@mail.ru

5.2. Выпуск сертификата.

1. В окне просмотра пользователя Сидоров Сидор Сидорович нажмите в ленте **Запросить сертификат**.
2. В окне создания запроса на сертификат отметьте галочкой **Одобрить** и **Открыть сертификат**, остальные значения оставьте по умолчанию, после чего нажмите **Создать и закрыть**.

6. Упражнение: Отзыв сертификата.

1. В **Консоли управления ЦР** выберите в навигационной панели **Сертификаты**, выберите сертификат Сидоров Сидор Сидорович.
2. В ленте **Консоли управления ЦР** нажмите **Аннулировать**.
3. В выпадающем меню выберите пункт **Сертификат заменен** и нажмите кнопку **Отозвать**.
4. В ленте **Консоли управления ЦР** нажмите **Обновить** и убедитесь, что сертификат пользователя перешел в состояние **Отозван**.

7. Упражнение: Выпуск списка отозванных сертификатов

1. В **Диспетчере УЦ** раскройте узел **Сервер ЦС** и выберите Центр Сертификации **Пробный Корневой УЦ**.
2. В разделе **Публикация информации об отзыве сертификатов** нажмите **Выпустить внеочередной CRL**.

Публикация информации об отзыве сертификатов: [Добавить адрес публикации](#)

Точность часов: [↻](#) минуты

Интервал перекрытия: [↻](#) часы

Используемый интервал перекрытия: 12 ч.

Следующий выпуск: 29.04.2016 18:00

Выпускать разностные CRL

Интервал перекрытия разностных CRL: [↻](#) минуты

Используемый интервал перекрытия разностных CRL: 7 ч, 12 мин.

Следующий выпуск разностных CRL: 29.04.2016 18:00

Адреса публикации:

<http://byeuu/cdp/<SigningKeyId><DeltaCRLAllowed>.crl>

Актуальные CRL:

Индекс ключа	Номер CRL	Действителен с	Следую обновление
0	1	29.04.2016 14:09	29.04.2016

< >

[Настроить расписание выпуска CRL](#)
[Настроить расписание выпуска разностных CRL](#)
[Выпустить внеочередной CRL](#)

3. Убедитесь, что в опубликованном CRL указан серийный номер сертификата, выданный на имя Сидоров Сидор Сидорович.