НИИ СОКБ
ЦЕНТР РАЗРАБОТКИ

КОМПЛЕКСНАЯ ЦИФРОВАЯ МУЛЬТИПЛАТФОРМА УПРАВЛЕНИЯ МОБИЛЬНЫМИ СРЕДСТВАМИ КОММУНИКАЦИЙ

РУКОВОДСТВО ПО УСТАНОВКЕ SCEP

SAFEMOBILE

Москва

2022

Установка серверного компонента.

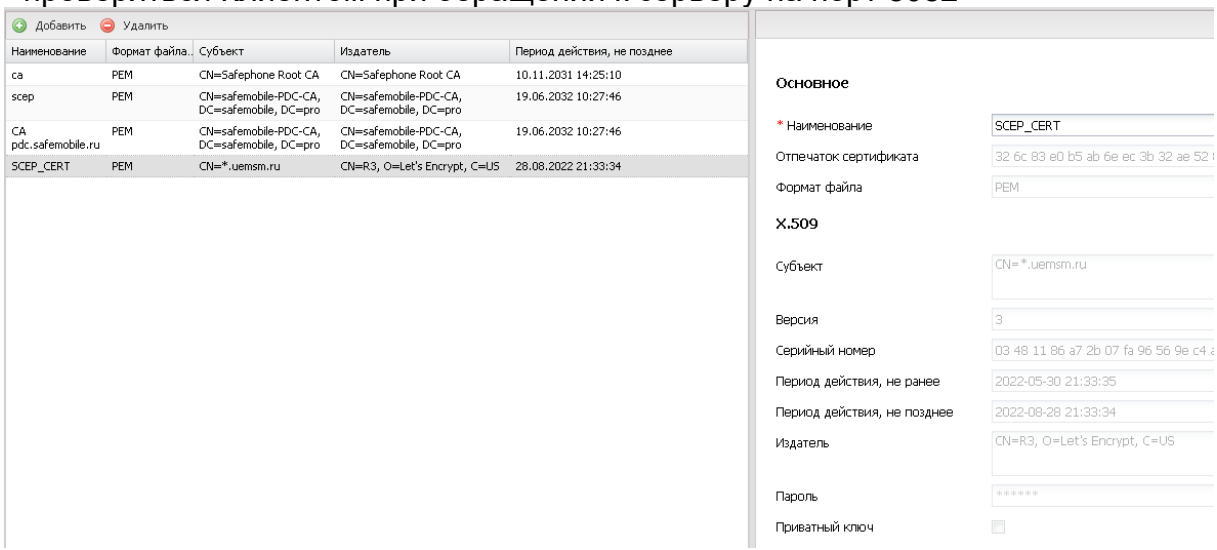
На ВМ, предназначенной для SCEP-сервера, при прохождении мастера первоначальной настройки setup.sh, выбрать:

```
SCEP server? [y/n/q/?] y
SCEP server: Create TLS certificate? [y/n/q/?] y
Generating RSA private key, 4096 bit long modulus (2 primes)
......++++
.....................................................................
e is 65537 (0x010001)
SCEP server: Common Name (IP or domain name): t70.uemsm.ru
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................++++
.....................................................................
e is 65537 (0x010001)
Signature ok
subject=CN = t70.uemsm.ru
Getting CA Private Key
Generating a RSA private key
.........+++++
...................+++++
writing new private key to '.scep.key.pem'
-----
```

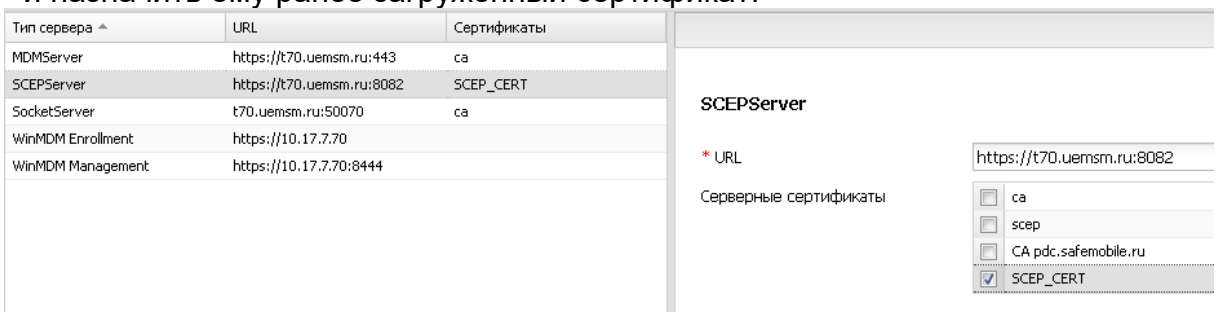
заполнив Common Name своим значением.

Настройка в АРМ администратора

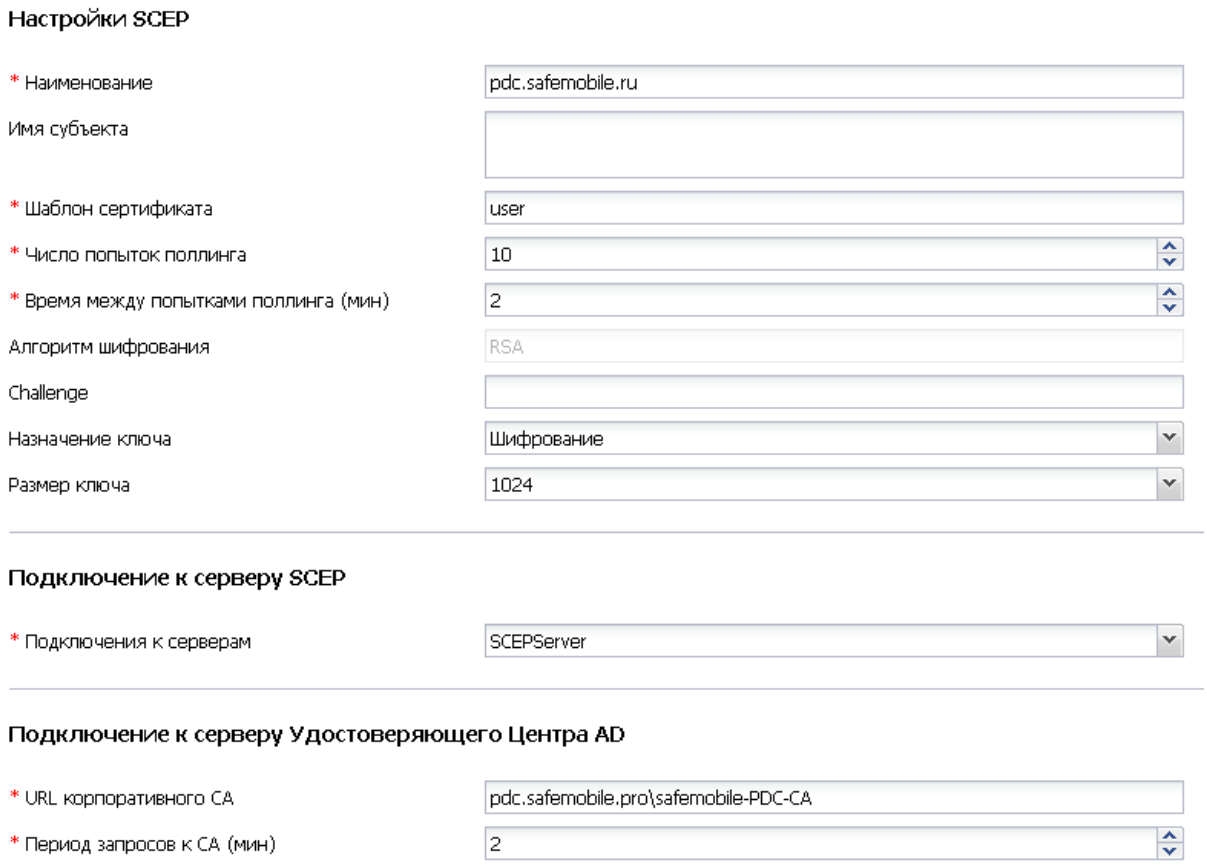
1. При использовании самоподписанных сертификатов на URL-ах сервера SafeMobile, вразделе «Серверные сертификаты» загрузить https-сертификат, который будет проверяться Клиентом при обращении к серверу на порт 8082



2. При использовании самоподписанных сертификатов на URL-ах сервера SafeMobile, в разделе «Подключение к серверам» настроить URL подключения к SCEP-серверу и назначить ему ранее загруженный сертификат.



3. В разделе «Настройки SCEP» задать параметры сервера



В указанном примере кроме наименования достаточно заменить содержимое полей Наименование, Шаблон сертификата(наименование шаблона УЦ, к которому будет обращаться сервер, см. п.п. В.11 ниже), URL корпоративного CA.

4. В разделе «Профили» создать профиль «Точка доступа WiFi 802.1X Android»

Тип	Точка доступа WiFi 802.1X Android
* Наименование	SNT-EAP
Описание	
Примечание	Профиль работает на устройствах Samsung при наличии у монитор а привилегий KNOX и Device Owner, либо KNOX и Device Admin. На прочих устройствах необходимы привилегии Device Owner. С верси и Android 11 при выборе типа безопасности - Enterprise, необходим
* Имя точки доступа (SSID)	SNT-EAP
* Скрытая сеть	Нет
* Выполнить попытку автоматического подключения	Да
* Тип безопасности	Enterprise
* Пароль	Не задано
* Тип EAP	TLS
* Учётные данные (клиентский сертификат или настройки SCEP)	pdc.safemobile.pro
Сертификат удостоверяющего центра WiFi сети	Не задано
Имя пользователя	{{employee.exchange.emp_email_domain}}\{{employee.exchange.emp
Пароль пользователя	Не задано
* Вторая фаза аутентификации	Не задано
Псевдоним, используемый вместо имени пользователя в первой фазе PEAP	Не задано

заполнив своими значениями поля Имя точки доступа и Учетные данные(выбрать из списка).
И назначить профиль на целевые устройства.

5. У Сотрудника должны быть заполнены поля «E-mail Домен» и «E-mail Логин», по этим данным происходит запрос сертификата в УЦ.

* Фамилия:	QA
* Имя:	Tests
Отчество:	
Должность:	-
E-Mail Домен:	user02
E-Mail Логин:	safemobile.pro
E-Mail:	

Подготовка компьютера для агента регистрации

Регистрационный агент представляет собой Windows сервис, который должен устанавливаться на компьютер с ОС Windows в инфраструктуре заказчика.

Ссылка на дистрибутив агента регистрации: https://owncloud.niisokb.ru/s/uaARjJsi7z9IXyx

Для инсталляции Агента регистрации необходимо выполнить следующие действия:

B.1 Установка Агента регистрации должна производиться на компьютер, включенный в тот же домен, что и сервер CA.

B.2 Все действия должны выполняться от имени доменного администратора.

B.3 Скачать и установить пакет **.NET Framework 4.7.2,** если данный пакет еще не был установлен.

B.4 Скачать и установить Агент регистрации. Файл **«SafeMobileEnrollmentAgentSetup.msi»** входит в комплект ПО для установки «UEM SafeMobile» по требованию заказчика.

B.5 Создать доменного пользователя, от имени которого будет запускаться служба Агента регистрации.

B.6 Добавить пользователя в группу **CERTSVC_DCOM_ACCESS** или Certificate Service DCOM Access, на контролере домена или на любом компьютере домена с установленным RSAT.

B.7 На компьютере с установленным Агентом регистрации следует выполнить следующие действия:

B.7.1.1 Запустить оснастку Services (mmc.exe services.msc).

B.7.1.2 В параметрах службы агента регистрации **SafeMobile EnrollmentSrv** настроить вход в систему от имени созданного пользователя.

B.8 В каталоге установки агента регистрации (обычно C:\Program Files (x86)\NIISOKB\SafeMobile Enrollment Agent) настроить параметры подключения к CA и БД в файле conf.yml:

```
# SafeMobile database connection settings
ca:
pdc.safemobile.pro\safemobile-PDC-CA
enrollmentTemplate: EnrollmentAgent
db:
type: postgresql
user: sphone
password: 111
host: 10.11.12.13
port: 5432
name: sphone
```

B.9 Адрес удостоверяющего центра можно посмотреть в файле C:\Windows\System32\certsrv\certdat.inc (переменная sServerConfig) на сервере CA.

B.10 На сервере CA в оснастке mmc Component Services выбрать свойства компонента: Console root -> Component Services -> Computers -> My computer -> DCOM config -> CertSrv request. В закладке Security в свойствах Launch and Activation permissions выбрать Customize -> Edit. Убедится, что доменной группе CERTSVC_DCOM_ACCESS или Certificate Service DCOM Access разрешены права: Remote Launch и Remote Activation. Для свойства Access Permissions группе CERTSVC_DCOM_ACCESS или Certificate Service DCOM Access должны быть разрешены права Remote Access.

B.11 На сервере CA в оснастке **mmc Certificate Templates** выбрать шаблон **User**(или любой другой, созданный для wi-fi), в закладке **Security** задать для пользователя службы агента регистрации разрешения: **Read** и **Enroll**.

B.12 На сервере CA в оснастке **mmc Certificate Templates** выбрать шаблон **Enrollment Agent,** в закладке **Security** задать для пользователя службы агента регистрации разрешения: **Read** и **Enroll**.

B.13 На сервере CA в оснастке **mmc Certification Authority** в каталог **Certificate Templates** добавить шаблон **Enrollment agent**, если еще не добавлен.

B.13.1 Проверить доступность CA можно следующим образом:

B.13.1.1 Запустить интерпретатор командной строки от имени созданного пользователя. Например, **runas /user:имя пользователя@домен cmd.**

B.13.1.2 В командном интерпретаторе набрать: **certutil -ping -config "<Адрес удостоверяющего центра>".**

B.13.1.3 Если настройки выполнены правильно, то будет результат: **CertUtil: -ping — command completed successfully.**

B.14 На компьютере агента регистрации запустить сервис **SafeMobileEnrollmentSrv.**

B.15 Перейти в системный журнал событий компьютера агента регистрации и убедиться, что в ветке: **Event viewer -> Windows Logs -> Application** нет событий ошибок от источника **SafeMobile Enrollment Agent**