НИИ СОКБ
ЦЕНТР РАЗРАБОТКИ

КОМПЛЕКСНАЯ ЦИФРОВАЯ МУЛЬТИПЛАТФОРМА УПРАВЛЕНИЯ МОБИЛЬНЫМИ СРЕДСТВАМИ КОММУНИКАЦИЙ

РУКОВОДСТВО ПО УСТАНОВКЕ SCEP

SAFEMOBILE

Москва

2023

Установка серверного компонента.

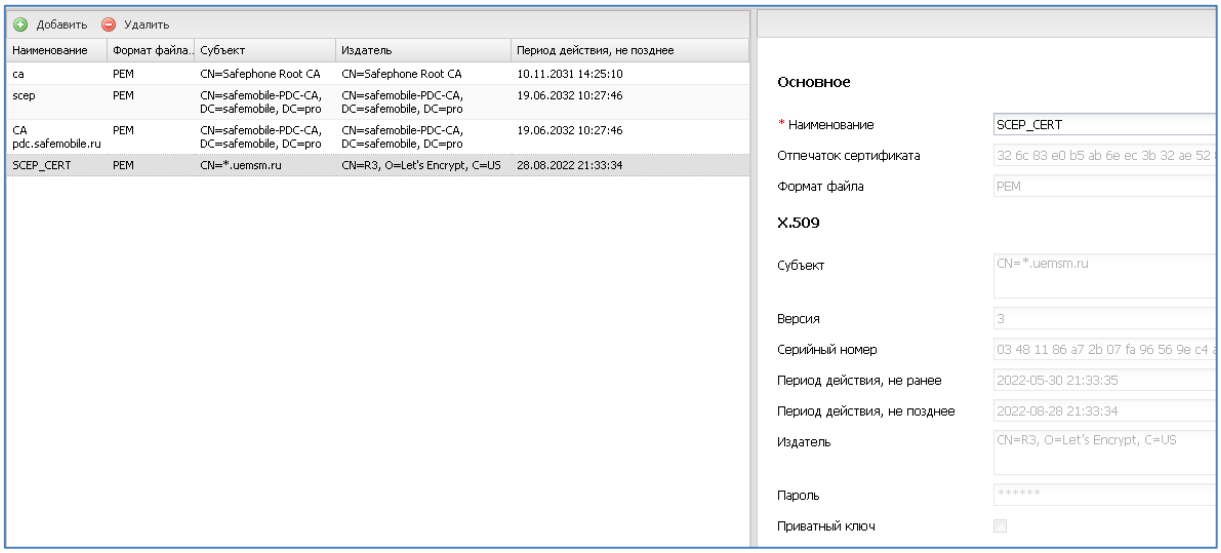
На ВМ, предназначенной для SCEP-сервера, при прохождении мастера первоначальной настройки setup.sh, следует выбрать:

```
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.

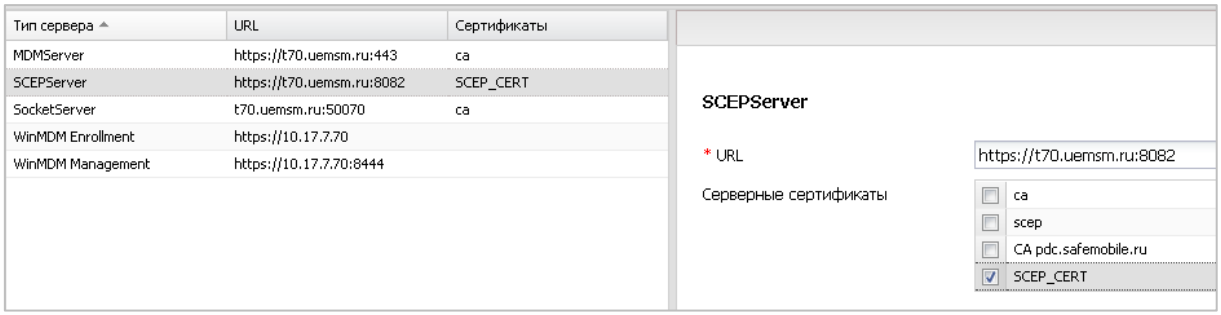
Настройка в АРМ администратора

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



Раздел «Серверные сертификаты»

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.



Раздел «Подключение к серверам»

3. В разделе «Настройки SCEP» задать настройки для сервера. (см. «Настройки SCEP»)

4. При настройке профилей Wi-Fi следует использовать настройки SCEP, вместо клиентского сертификата (к 01.12 также Exchange аккаунта и VPN IKEv2 для iOS).

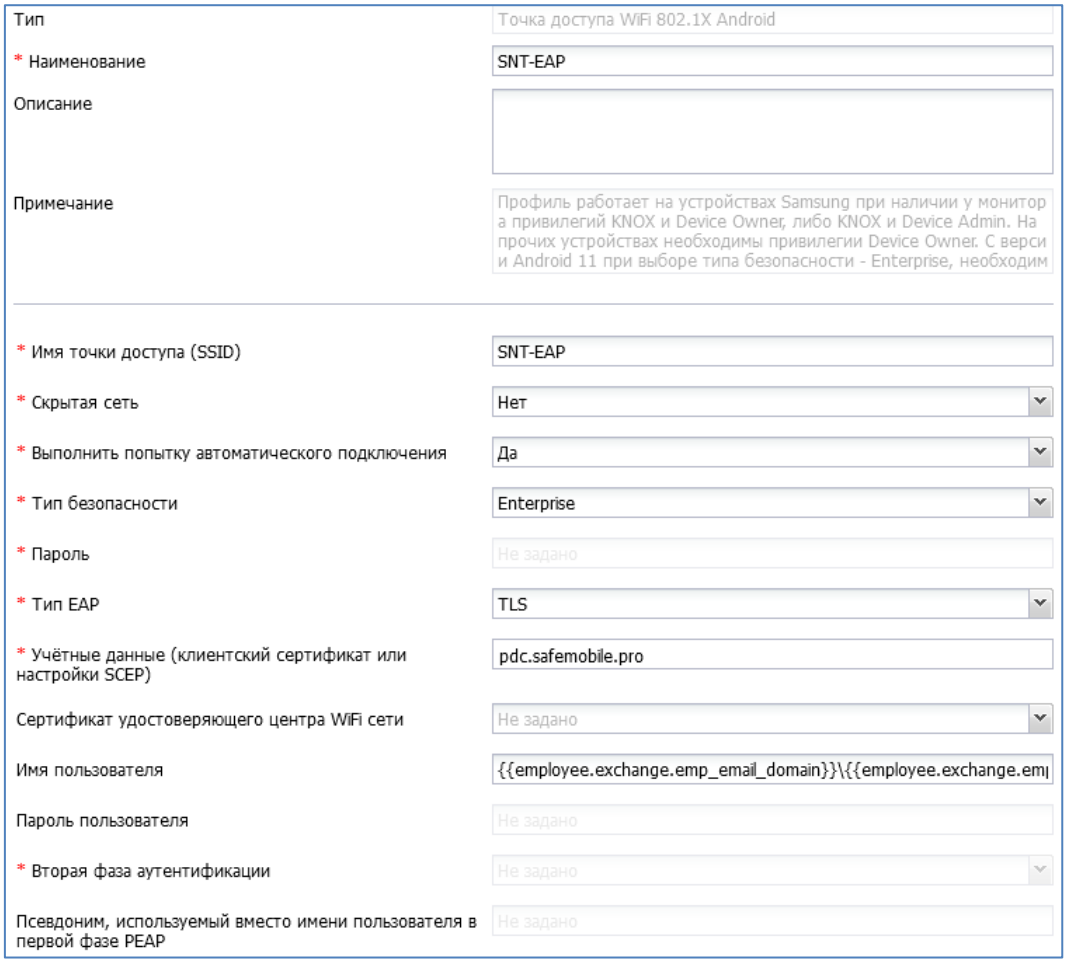
Пример:

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

Заполнить своими значениями поля:

- *Имя точки доступа*
- *Учетные данные (выбрать из списка).*

И назначить профиль на целевые устройства.

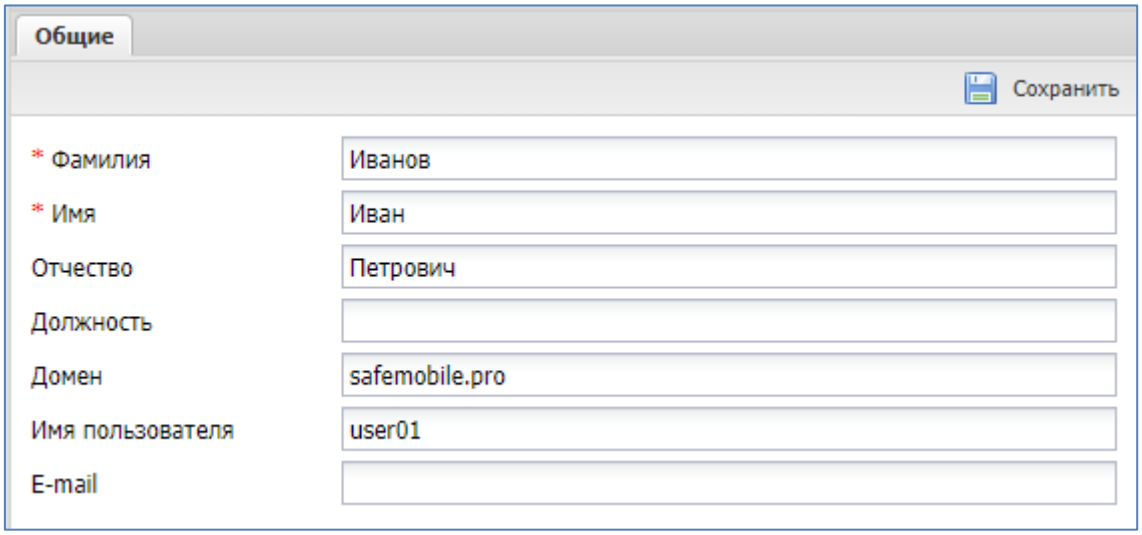


Создание профиля - тип «Точка доступа WiFi 802.1X Android»

5. У Сотрудника должны быть заполнены поля:

- E-mail Домен
- E-mail Логин»

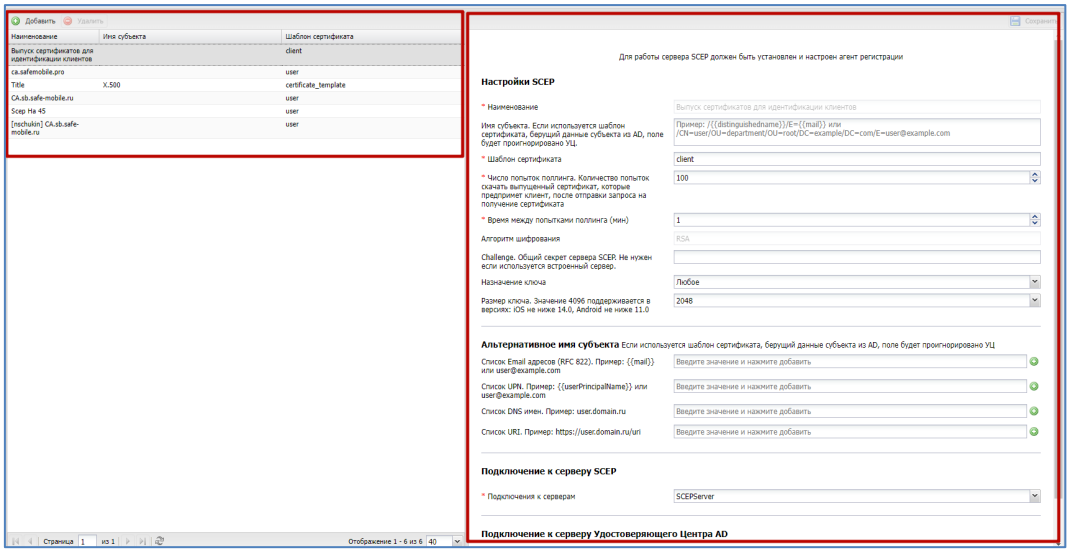
По этим данным происходит запрос сертификата в УЦ.



Настройки сотрудника, в разделе «Сотрудники»

Настройки SCEP

Раздел **«Настройки SCEP»** предназначен для учёта и распространения клиентских сертификатов с настраиваемыми параметрами посредством SCEP в соответствии с рисунком 2.123.



Окно «Настройки SCEP»

В таблице с перечнем сертификатов отображаются следующие столбцы:

- Наименование – наименование сертификата (по умолчанию, отображается в таблице);
- Имя субъекта – формат сертификата (по умолчанию, отображается в таблице);
- Шаблон сертификата – шаблон используемого сертификата (по умолчанию, отображается в таблице).

В правой части рабочего экрана отображаются настройки, выбранной в таблице настройки SCEP и состоят из следующих полей данных:

- **Настройки SCEP:**
  - **Наименование** – наименование настройки;
  - **Имя субъекта. Если используется шаблон сертификата, берущий данные субъекта из AD, поле будет проигнорировано УЦ**.
    - Это отличительное имя (DN), содержащее идентифицирующую информацию об объекте, которому выдан сертификат. Имя субъекта может быть создано из стандартных компонентов каталога LDAP, таких как общие имена и организационные подразделения. Эти компоненты

определены в X.500. Поле не заполняется, если данные пользователя берутся из AD (см. примечание).

Пример:

/CN=user/OU=department/OU=root/DC=example/DC=com/E=user@example.com.

В имени субъекта могут быть использованы следующие подстановки:

1. /{{distinguishedname}} - специальная подстановка (начинается с "/"), которую нужно использовать чтобы подставить полное имя пользователя.
2. {{mail}} - подстановка адреса электронной почты.

Пример использования подстановок:

/{{distinguishedname}}/E={{mail}};

- **Шаблон сертификата** – шаблон сертификата, по которому будут выпускаться сертификаты для устройств (должен быть заранее создать в AD);
- **Число попыток поллинга. Количество попыток скачать выпущенный сертификат, которые предпримет клиент, после отправки запроса на получение сертификата.** В зависимости от настроек, УЦ может выписывать сертификат не сразу, а после подтверждения администратором УЦ;
- **Время между попытками поллинга (мин)** - интервал времени между обращениями монитора за готовым сертификатом;
- **Алгоритм шифрования** – RSA (всегда);
- **Challenge. Общий секрет сервера SCEP. Не нужен если используется встроенный сервер**;
- **Назначение ключа** – доступны значения:
  - Шифрование, Подпись, Любое;
- **Размер ключа. Значение 4096 поддерживается в версиях: iOS не ниже 14.0, Android не ниже 11.0**;

- **Альтернативное имя субъекта:**
  - **Список Email адресов (RFC 822). Пример: {{mail}} или user@example.com**– один и более email адресов (не заполняется, если данные пользователя берутся из AD (см. примечание);
  - **Список UPN. Пример: {{userPrincipalName}} или user@example.com**–

один и более UserPrincipalName (не заполняется, если данные пользователя берутся из AD (см. примечание);

- **Список DNS имен. Пример: user.domain.ru**– один и более DNS (не заполняется, если данные пользователя берутся из AD (см. примечание);
- **Список URI. Пример: https://user.domain.ru/uri** – один и более Uniform Resource Identifier (не заполняется, если данные пользователя берутся из AD (см. примечание));

- **Подключение к серверу SCEP:**
  - Подключения к серверам – выбор из списка серверов SCEP;

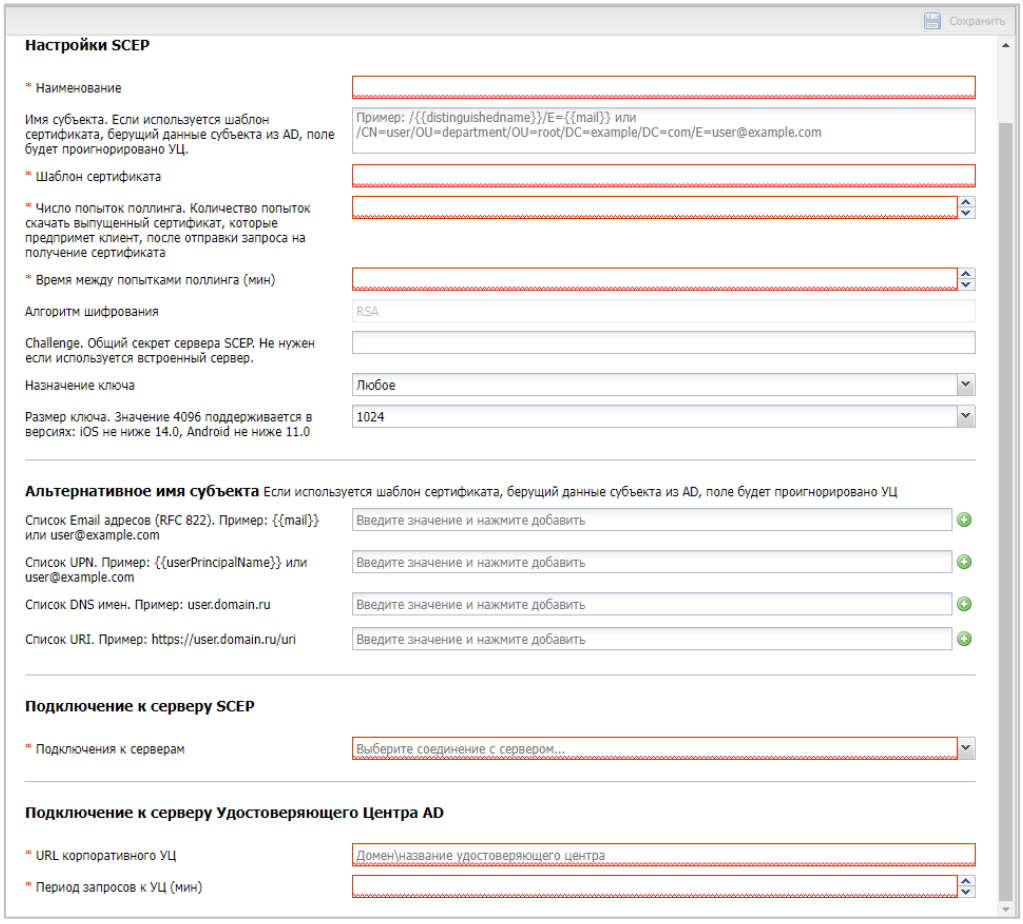
- **Подключение к серверу Удостоверяющего Центр AD:**
  - URL корпоративного УЦ – адрес расположения корпоративного УЦ;
  - Период запросов к УЦ (мин) – задается в минутах.

Примечание.

- *В свойствах «шаблона сертификата» в УЦ должен быть указан источник данных пользователя: AD или запрос сертификата. Если в шаблоне указано, что брать данные следует из AD, то все, что введено в полях SN и SAN игнорируется и берется из AD. Если же указано брать из запроса сертификата, то нужно, чтобы в запросе было заполнено хотя бы одно из полей: SN или SAN иначе УЦ вернет ошибку создания сертификата.*
- *В поле «Имя субъекта» и полях блока «Альтернативное имя субъекта» допускается использование всех подстановок, указанных в «Руководстве администратора» 2.6.8.2 Настройка параметров профиля.*

Добавление новой настройки SCEP

1. Перейти в раздел «Настройки SCEP»
2. Нажать кнопку «Добавить» в панели инструментов верхней части окна. Затем заполнить форму в правой части окна.



Форма с настройками SCEP

3. После заполнения формы нажать кнопку «Сохранить» и новые настройки SCEP отобразится в таблице.

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:

1. Установка Агента регистрации должна производиться на компьютер, включенный в тот же домен, что и сервер CA.
2. Все действия должны выполняться от имени доменного администратора.
3. Скачать и установить пакет **.NET Framework 4.7.2,** если данный пакет еще не был установлен.
4. Скачать и установить Агент регистрации. Файл **«SafeMobileEnrollmentAgentSetup.msi»** входит в комплект ПО для установки «UEM SafeMobile» по требованию заказчика.
5. Создать доменного пользователя, от имени которого будет запускаться служба Агента регистрации.
6. Добавить пользователя в группу **CERTSVC_DCOM_ACCESS** или Certificate Service DCOM Access, на контролере домена или на любом компьютере домена с установленным RSAT.
7. На компьютере с установленным Агентом регистрации следует выполнить следующие действия:
    - Запустить оснастку Services (mmc.exe services.msc).
    - В параметрах службы агента регистрации **SafeMobile EnrollmentSrv** настроить вход в систему от имени созданного пользователя.
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: user #template certificate for enrollment
```

```
db:
type: postgresql
user: sphone
password: 111
host: 10.11.12.1
port: 5432
name: sphone # "database name" for posgresql
```

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

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.

11. 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**.

12. На сервере CA в оснастке **mmc Certification Authority** в каталог **Certificate Templates** добавить шаблон **Enrollment agent**, если еще не добавлен.
    Проверить доступность CA можно следующим образом:

    - Запустить интерпретатор командной строки от имени созданного пользователя. Например, **runas /user:имя пользователя@домен cmd.**
    - В командном интерпретаторе набрать: **certutil -ping -config "<Адрес удостоверяющего центра>".**
    - Если настройки выполнены правильно, то будет результат: **CertUtil: -ping — command completed successfully.**

13. На компьютере агента регистрации запустить сервис **SafeMobileEnrollmentSrv.**

14. 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**

Взаимодействие SCEP клиента и сервера

1. Клиент запрашивает у сервера SCEP “сертификат CA”. Этот сертификат используется для защиты ключей шифрования CSR внутри SCEP запросов (см. ниже). Поскольку наш сервер SCEP расшифровывает запросы, то “сертификат CA” (в терминах протокола SCEP) – это сертификат сервера SCEP. Это специальный, практически вечный сертификат, который лежит на сервере SCEP. Использование срочных сертификатов или сертификатов внешних УЦ в качестве “сертификата CA” на сервере SCEP не предусматривается.

2. Клиент может проверить хэш сертификата CA. В структуре профиля SCEP для iOS для этого есть поле CAFingerprint. Мы этой возможностью не пользуемся, потому что мы сами отправляем устройству сертификат нашего сервера. Если клиент по каким-то причинам получит другой сертификат, наш сервер SCEP просто не сможет расшифровать его запрос.

3. Клиент генерирует ключевую пару и CSR.

4. Клиент формирует SCEP запрос. Клиент подписывает тело SCEP запроса:
    - Сертификатом из CSR, если запрашивается новый сертификат.
    - Действующим сертификатом, если запрашивается новый сертификат, когда текущий ещё действует (перевыпуск сертификата
5. Внутри тела SCEP запроса передаётся зашифрованный блок данных, в котором передаётся CSR вместе с challenge. Также внутри тела SCEP запроса передаётся ключ для расшифровки зашифрованного блока данных. Этот ключ зашифрован публичным ключом из “сертификата CA” (в нашем случае – сертификатом сервера SCEP).

6. Сервер в ответ на запрос клиента может вернуть один из трёх ответов:
    - **Reject**. Ошибка:
        - Неправильный размер ключа. Ошибку может вернуть CA, если размер в запросе не соответствует размеру в шаблоне.
        - Неправильный challenge. Ошибку возвращает сервер SCEP, если запрос пришёл с challenge, который ему неизвестен. Это событие не пишется в БД.

Его актуально передавать в syslog.

- CA не может проверить запрос. В оригинале The CA could not validate the request. Скорее всего возвращается сервером SCEP, если ему пришёл не SCEP запрос.
- SCEP запрос подписан сертификатом, которому CA не доверяет. Ошибка возникает, если старый сертификат клиента отозван, клиент об этом ещё не знает, формирует запрос на перевыпуск сертификата и подписывает его старым (уже отозванным) сертификатом.
- CA не может авторизовать атрибуты запроса. Например, доменного пользователя заблокировали или отключили.

- **Pending**. Сертификат ещё не выпущен. Для клиента этот ответ означает, что нужно подождать и обратиться к серверу повторно через время поллинга.
- **Success**. Сертификат выпущен. В этом случае сертификат возвращается в теле ответа на SCEP запрос.

7. Если сертификат сервера SCEP истекает, в протоколе заложена возможность выпуска shadow сертификата. Срок действия shadow сертификата начинается с момента истечения текущего сертификата. Клиенты могут использовать shadow сертификат для генерации новых клиентских сертификатов, которые можно будет использовать, когда shadow сертификат станет основным. Для нас это не актуально, потому что сертификат сервера SCEP (сертификат “CA”) у нас условно вечный.

Особенности реализации в SafeMobile

1. SCEP запросы формируются мобильными устройствами iOS и Android. Приватный ключ, относящийся к CSR и сертификату, не покидает мобильное устройство.

2. SCEP сервер принимает и расшифровывает SCEP запросы, после чего сохраняет CSR в базу данных. Далее регистрационный агент во внутренней сети выгружает CSR и обращается в CA по DCOM. Инфраструктура заказчика не знает ничего про наш SCEP. Для неё весь процесс выглядит как выпуск сертификатов сервисной учётной записью по DCOM.

3. Для авторизации при обращении к серверу SCEP используются случайные challenge. SafeMobile генерирует для каждого устройства случайный уникальный 128-битный challenge.

Список подстановок

В качестве значений строковых параметров можно использовать подстановки.

Подстановки – строки специального вида, вместо которых перед применением подставляются персонифицированные данные.

В каждом строковом параметре допускается использование одной или нескольких подстановок.

Ключ подстановки в тексте должен начинаться с префикса "{{" без кавычек, а заканчиваться постфиксом "}}" без кавычек.
Например, для того чтобы значение параметра содержало домен\логин пользователя, нужно указать следующую строку:
{{employee.exchange.emp_email_domain}}\{{employee.exchange.emp_email_login}}

Список ключей подстановок:

- {{employee.surname}} - фамилия сотрудника.
- {{employee.name}} - имя сотрудника.
- {{employee.patronymic}} - отчество сотрудника.
- {{employee.exchange.emp_email}} - email сотрудника.
- {{employee.exchange.emp_email_login}} - логин сотрудника.
- {{employee.exchange.emp_email_domain}} - домен сотрудника.
- {{noncompliance_rule.name}} - наименование правила несоответствия.
- Импортированные атрибуты из AD:
  - {{userPrincipalName}}
  - {{sAMAccountName}}
  - {{displayName}}
  - {{mail}}
  - {{title}}
  - {{company}}
  - {{sn}}
  - {{givenName}}
  - {{middleName}}
  - {{objectGuid}}

Примечание.

- *Подстановки могут быть использованы только в полях ввода типа «Строка» или «Массив строк». В настройках SCEP, подстановки могут быть использованы в следующих полях данных:*
  - *Имя субъекта*
  - *Email адрес (RFC 822)*
  - *UPN*
  - *DNS имя*
  - *URI имя*
- *При отсутствии значения подстановки в необязательном для заполнения поле ввода, подстановка заменяется на пустую строку удаляется поля ввода, после чего поле ввода обрабатывается как валидное.*

Известные проблемы и способы их решения

Ошибка: Enrollment Agent certificate not found

Проблема возникает, когда из хранилища сертификатов удаляют еще действующий сертификат агента регистрации.

При появлении ошибки: Enrollment Agent certificate not found

Необходимо выполнить действия:

1. На компьютере, на котором располагается «Регистрационный агент» (далее РА), найти в реестре ветку:
   Computer\HKEY_USERS\S-1-5-21-XXXXXXXXXX-XXXXXXXX-XXXXXXXXXX-XXXX\Software\NIISOKB\SafePhone Enrollment Agent
   Искать нужно по названию папки SafePhone Enrollment Agent.
2. В этой ветке удалить все подкаталоги.
3. Сделать рестарт РА, после чего РА заново запросит сертификаты.
4. Если ошибка воспроизведется прислать нам содержимое этой ветки реестра.