

ЗАО «АВЕСТ»

**Простой протокол регистрации сертификата,
реализация Авест (Av Simple Certificate Enrollment
Protocol).**

Инструкция по настройке

Простой протокол регистрации сертификата, реализация Авест (Av Simple Certificate Enrollment Protocol) Инструкция по настройке.

Оглавление

Аннотация	2
Начальные условия.....	2
Действия по настройке сервиса AvSCEP.....	4
1. Генерация сертификата для сервиса AvSCEP.....	4
2. Установка и настройка ApacheTomcat.....	4
3. Организация рабочего места пользователя	5
Получение пользовательского сертификата средствами сервиса AvSCEP	7
Окончательная схема взаимодействия пользователя с ИОК.....	10

Аннотация

Этот документ описывает процесс настройки Инфраструктуры открытых ключей (ИОК) для реализации возможности получения клиентского сертификата средствами простого протокола регистрации сертификатов (AvSCEP).

Начальные условия

Данная инструкция предполагает, что ИОК развёрнута и функционирует (см. Рис. 1):

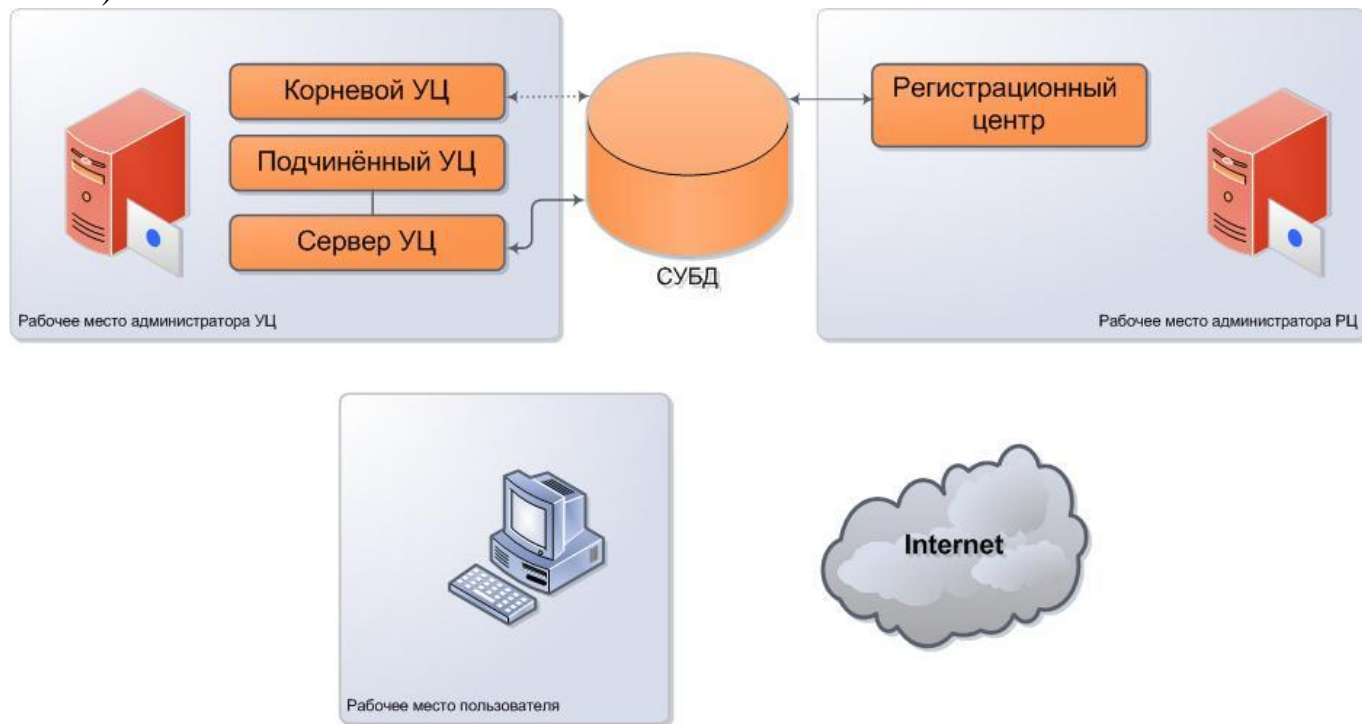


Рис. 1 Инфраструктура открытых ключей

Набор компонентов ИОК и их расположение может варьироваться в зависимости от нужд информационной системы, эксплуатирующей данную инфраструктуру. В нашем примере мы рассматриваем схему с наиболее полным числом компонентов:

1. Корневой удостоверяющий центр (далее – КУЦ).
2. Подчинённый удостоверяющий центр(далее – ПУЦ). В реальности ПУЦ может быть несколько. Количество ПУЦ регулируется нуждами и географией информационной системы.
3. Сервер автоматической обработки запросов от центров регистрации (поставляется в составе программного обеспечения (далее – ПО) «Центра цифровых сертификатов АВЕСТ» (AvCA).
4. Регистрационный центр (далее – РЦ), в полномочия администратора РЦ входит ручная регистрация поступающих запросов на сертификаты и обязательная проверка данных в запросе перед отправкой на автоматическую обработку в ПУЦ. В реальности РЦ может быть несколько. Количество РЦ регулируется нуждами и географией информационной системы.
5. СУБД. Требования к СУБД подробно описаны в Руководстве оператора ПК AvCA. В рассматриваемом примере все объекты инфраструктуры подключаются к одной СУБД под разными пользователями.

6. Рабочее место пользователя размещается локально (без связи с СУБД) и оборудовано ПО программный комплекс «Комплект Абонента АВЕСТ» (AvUCK).

Сервис AvSCEP получает запросы на сертификат от пользователей по протоколу SCEP и помещает в базу данных УЦ или РЦ в зависимости от того, какой из компонентов системы проводит первичную идентификацию абонентов в системе. Сервис AvSCEP не предназначен для автоматической выдачи сертификатов, он – удобное средство для оперативной доставки запросов от пользователя в органы регистрации запросов.

Действия по настройке сервиса AvSCEP

1. Генерация сертификата для сервиса AvSCEP

Требуется выпустить в Удостоверяющем центре сертификат по шаблону «Сертификат сервиса AvSCEP» (ServiceAvSCEP.tpl).

Перед тем как выпускать сертификат, нужно скопировать файл ServiceAvSCEP.tpl (поставляется вместе с ПО AvSCEP) в папку с установленным ПО Удостоверяющий центр, для того, чтобы получить возможность выбрать этот шаблон при выпуске сертификата.

Процесс выпуска сертификата по выбранному шаблону подробно описан в руководстве оператора «Программный комплекс «Центр цифровых сертификатов Авест» п. 8.2.

2. Установка и настройка ApacheTomcat

Устанавливаемая версия ApacheTomcat 6.0.28. Установку можно пройти по умолчанию. В корень каталога с установленным ApacheTomcat нужно поместить файлы *server.log.xml* и *avscep.properties* (поставляется вместе с ПО AvSCEP). В каталог *webapp* поместить файл *AvScep.war* (поставляется вместе с ПО AvSCEP).

В файл *avscep.properties* нужно внести информацию о сертификате сервиса AvSCEP и настроить подключение к базе данных:

- **store_type** – тип носителя, на котором находится контейнер с личным ключом сервиса AvSCEP.
- **key_id** – идентификатор ключа субъекта. Вносится без пробелов. Узнать и скопировать keyID можно из свойств сертификата при просмотре (см. Рис. 2):

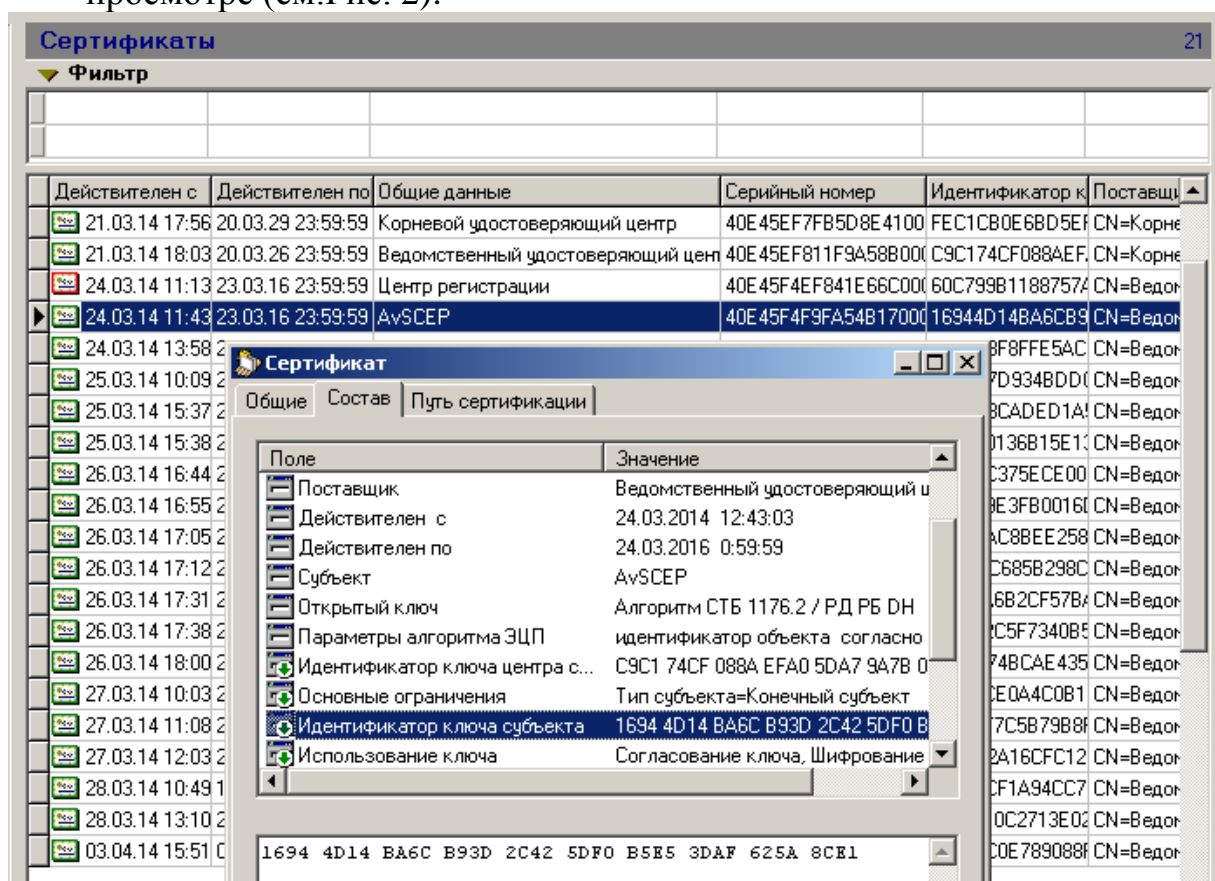


Рис. 2 Идентификатор ключа субъекта

- **container_name** – имя контейнера с личным ключом от сертификата службы AvSCEP.
- **container_password** – пароль к контейнеру с личным ключом от сертификата сервиса AvSCEP. Задаётся для того, чтобы обеспечить возможность автоматической работы сервиса. Пароль хранится в открытом виде, поэтому требуется ответственно подходить к защите рабочего места, на котором работает сервис AvSCEP.
- **crystore_driver** – подключение к базе данных (Oracle или MySQL).
- **crystore_url** – путь подключения к базе данных. Требуется указать тип базы данных, постоянный IP-адрес или DNS-имя хоста, на котором располагается база, имя базы данных. Например, для БД BankCertDB на MySQL, располагающейся во внутренней сети по адресу 10.0.0.150 строка будет выглядеть так:
`crystore_url=jdbc:mysql://10.0.0.150/BankCertDB?characterEncoding=cp1251`
- **crystore_user** – имя пользователя БД. Нужно указать имя существующего пользователя ИОК, в базу которого первоначально будут поступать запросы на сертификат. В нашем примере – это Регистрационный центр (далее – РЦ), если в ИОК РЦ отсутствует, то можно организовать сервис AvSCEP на базе Удостоверяющего центра (далее – УЦ).
- **crystore_password** – пароль пользователя БД.

После внесения всех изменений нужно сохранить файл *avscep.properties* и перезапустить ApacheTomcat.

Инфраструктура открытых ключей примет следующий вид (см. Рис. 3):

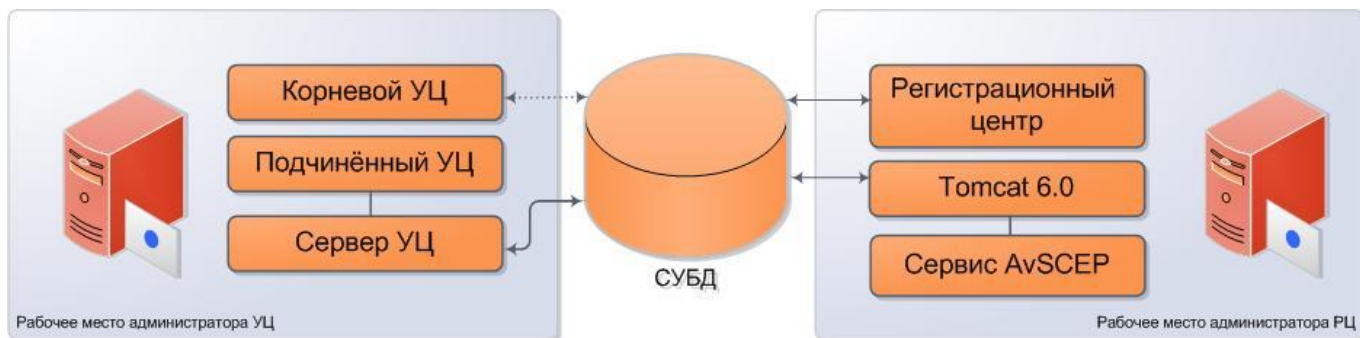


Рис. 3 Инфраструктура открытых ключей с сервисом AvSCEP

3. Организация рабочего места пользователя

Для того, чтобы иметь возможность отправить запрос в Центр регистрации (Удостоверяющий центр) на рабочем месте пользователя должен быть установлен Персональный менеджер сертификатов Авест AvPCM (далее – менеджер) версии не ниже 3.3.6.

В файл *AvCmMsg.ini*, который находится в каталоге с установленным менеджером, нужно внести секцию, по которой будет происходить соединение с сервисом AvSCEP. Это будет IP-адрес или DNS-имя хоста, на котором располагается ApacheTomcat. В нашем случае, эта секция будет выглядеть так:

```
[SCEP]
URL=http://srv03AvRA:8080/AvScep/avpkiclient
BasicAuthentication=False
ProxyPassword=
ProxyPort=
ProxyServer=
ProxyUsername=
```

В случае, если на рабочем месте организован доступ к интернету через прокси, то значение Basic Authentication нужно изменить на true и остальные параметры заполнить актуальными значениями (адрес прокси сервера, порт, имя пользователя и пароль).

После внесения изменений в настроечный файл *AvCmMsg.ini* нужно сохранить его.

Можно настроить менеджер сертификатов на отправку запроса в ЦР (УЦ) сразу после генерации запроса. Для этого нужно в желаемый шаблон, который находится также в каталоге с установленным менеджером, добавить приводившуюся выше секцию.

Получение пользовательского сертификата средствами сервиса AvSCEP

Процедура создания запроса средствами менеджера подробно описана в руководстве оператора AvPCMV п.6.1.

После создания запроса на сертификат, пользователь получает возможность автоматически отправить запрос на сертификат в сервис AvSCEP (см.Рис.4). Не обязательно сразу запускать мастер удалённой регистрации запроса. Функционал регистрации будет доступен в контекстном меню нового запроса.

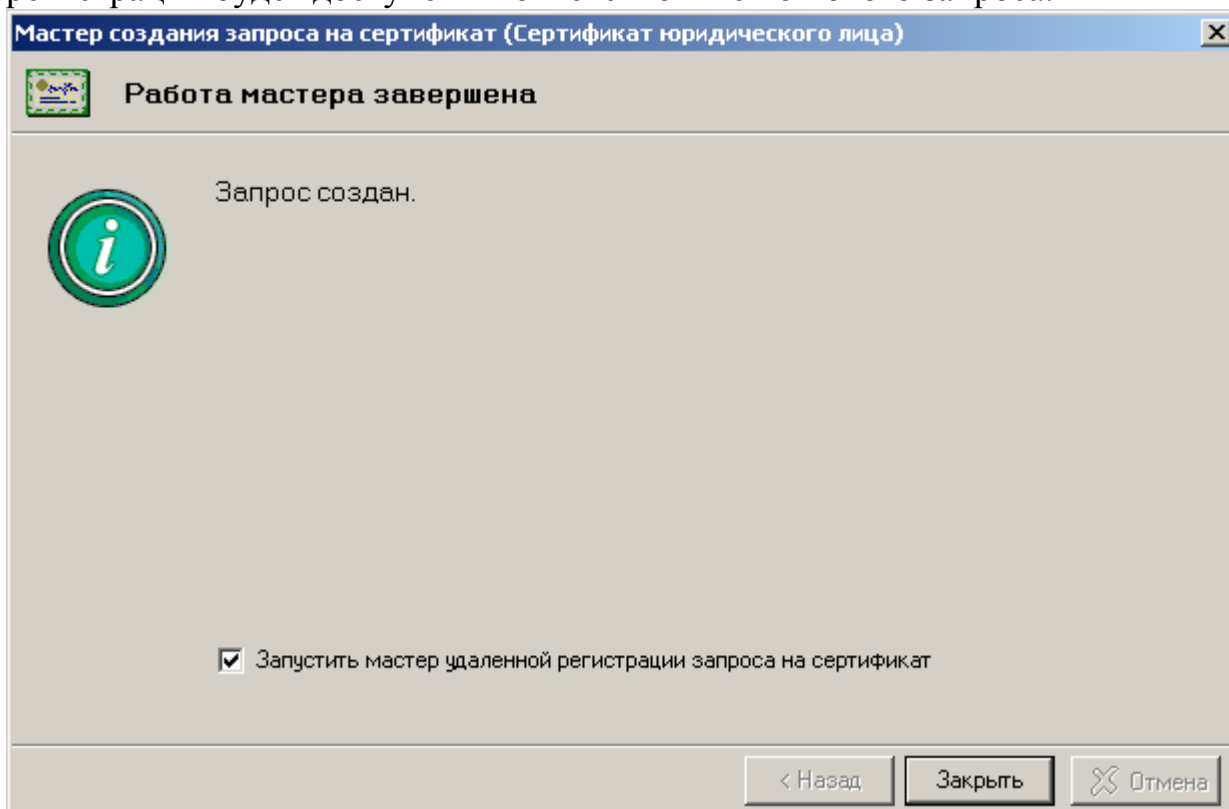


Рис.4 запуск мастера удалённой регистрации запроса

После создания запроса на сертификат он помещается в справочник «Запросы на сертификат» — «Новые» (смРис. 5).

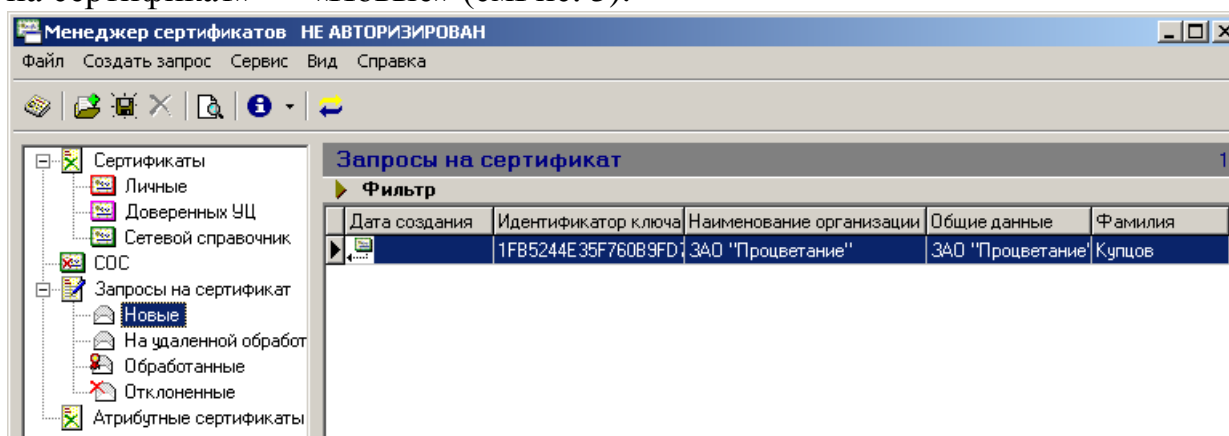


Рис. 5 Новый запрос на сертификат

После отправки перемещается в справочник «Запросы на сертификат» — «На удалённой обработке». Запросы, успешно прошедшие обработку, хранятся в справочнике «Запросы на сертификат» — «Обработанные», причём, вызвав просмотр обработанного запроса можно увидеть сертификат, выданный по этому запросу (см. Рис.6):

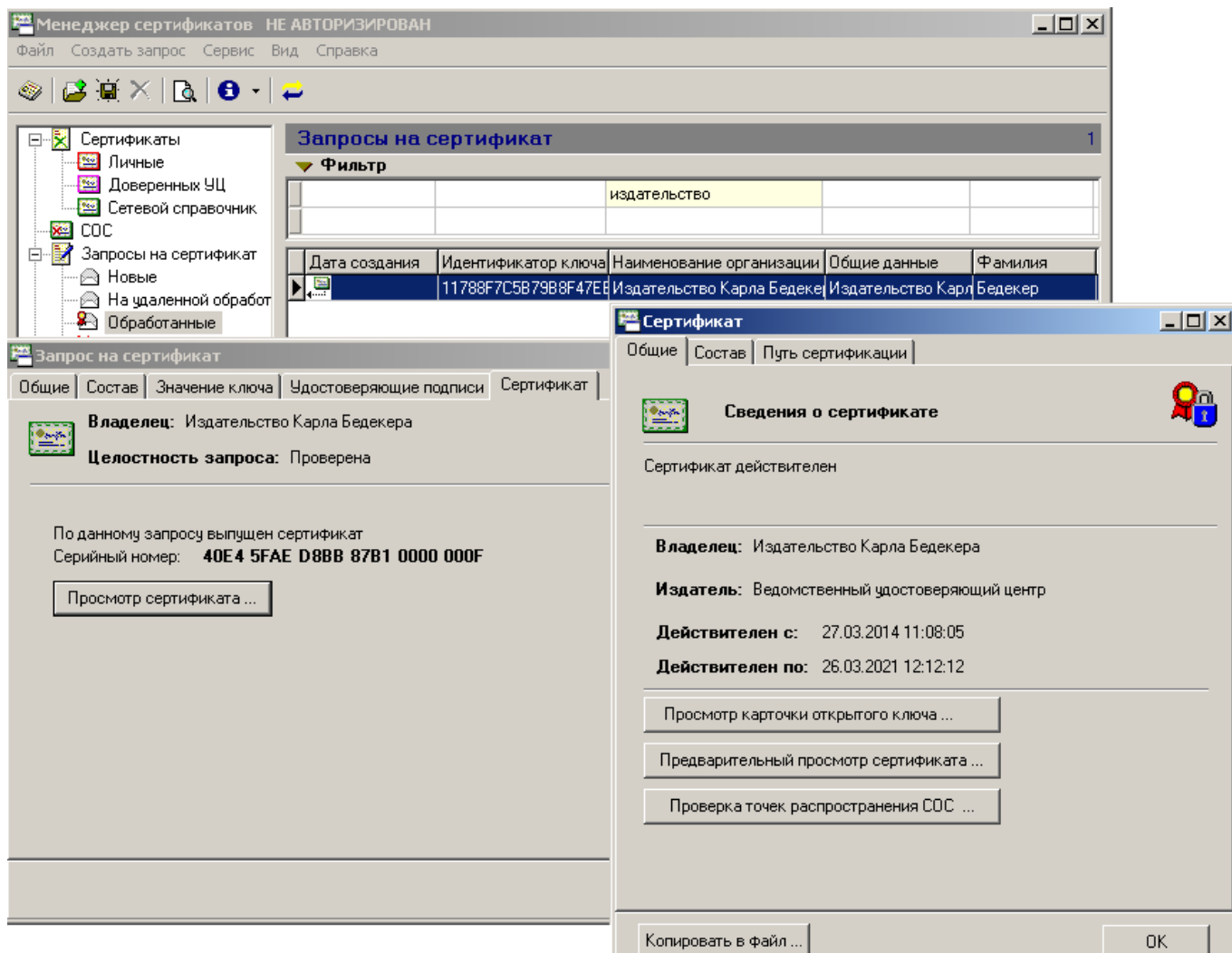


Рис.6 Просмотр сертификата

Запросы на сертификат, обработку которых отклонил ЦР или УЦ по какой-либо причине, хранятся в справочнике «Запросы на сертификат» — «Отклонённые».

Если сертификат отправлен на обработку, то проверить состояние можно из меню «Проверить статус сертификата» (см. Рис. 7):

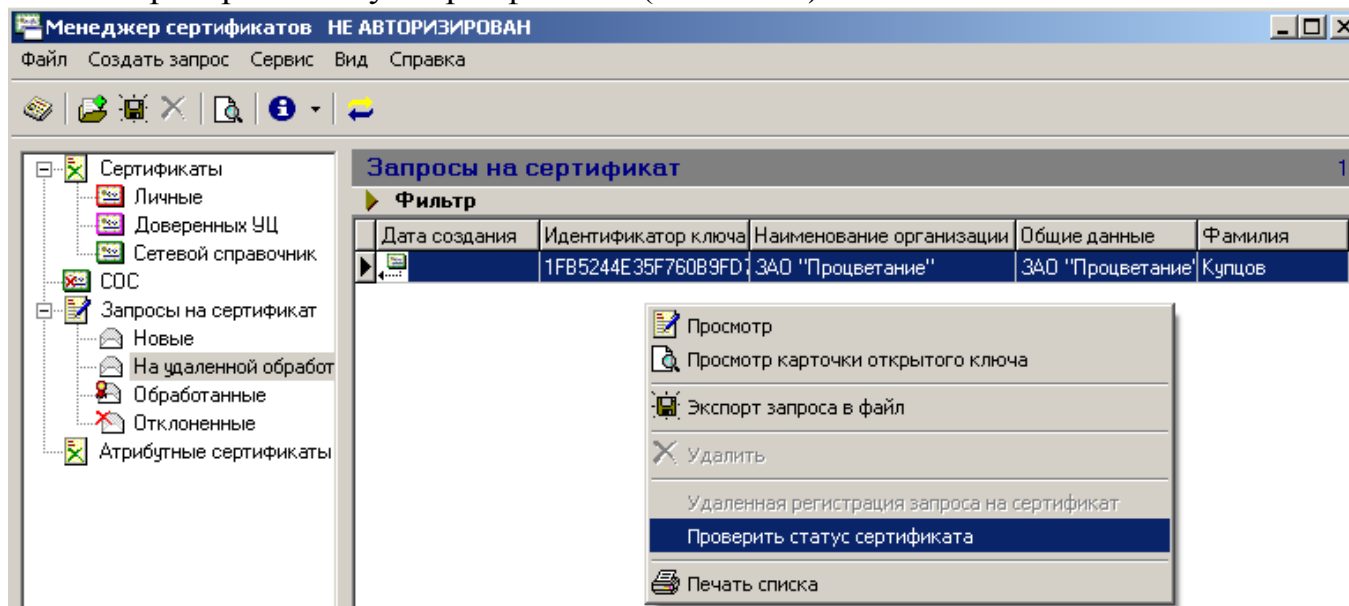


Рис. 7 Проверка статуса сертификата

После выполнения проверки становится понятно в каком состоянии запрос.

Он может находиться в состоянии ожидания ручного утверждения администратором ЦР или УЦ либо сертификат по запросу уже выпущен. В первом случае пользователь может ещё раз проверить статус при нажатии на кнопку «Повторить запрос». Во втором случае пользователю предоставляется возможность сразу же проимпортировать полученный сертификат (и всю цепочку сертификатов издателей) в своё локальное хранилище сертификатов (см.Рис. 8):

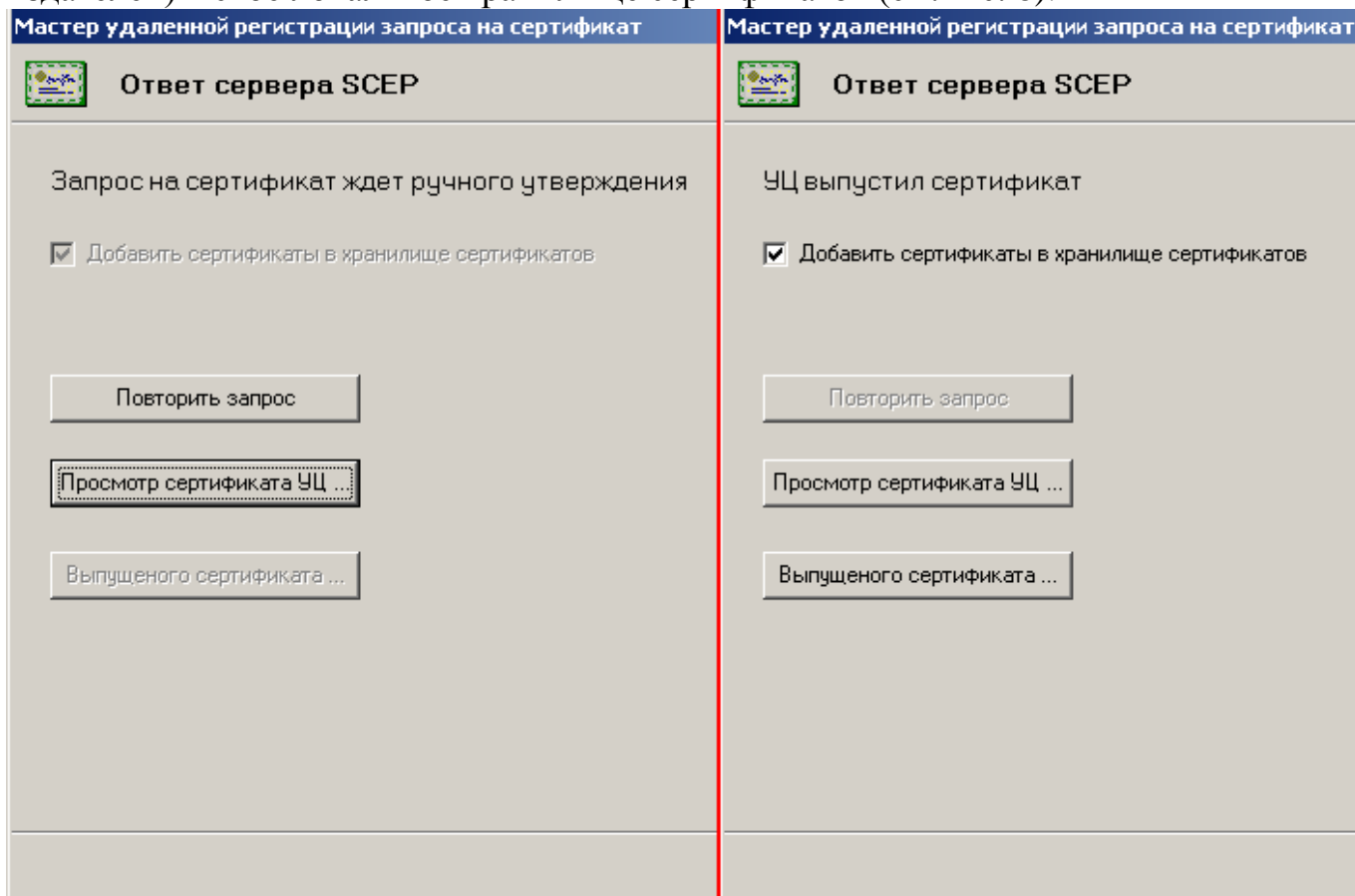


Рис. 8 Статус обрабатываемого запроса

Таким образом, пройдя удалённую регистрацию запроса на сертификат с помощью сервиса AvSCEP и проимпортировав полученные сертификаты в соответствующее хранилище, пользователь получает возможность стать полноценным участником ИОК.

Текущая реализация сервиса AvSCEP предполагает, что пользователь получает списки отозванных сертификатов (далее СОС) с помощью какого-нибудь другого сервиса ИОК. Например, точка распространения СОС может присутствовать в сертификате либо пользователь может собственноручно скачать свежие СОС из открытых источников, куда их своевременно публикует УЦ, а также настроить «Контроль точек распространения СОС» средствами менеджера (подробнее о настройке «Контроля точек распространения СОС» можно узнать в Руководстве оператора AvPCM п. 6.14.3)

Окончательная схема взаимодействия пользователя с ИОК

Окончательная схема взаимодействия пользователя с ИОК для получения сертификата средствами сервиса AvSCEP представлена на Рис.9:

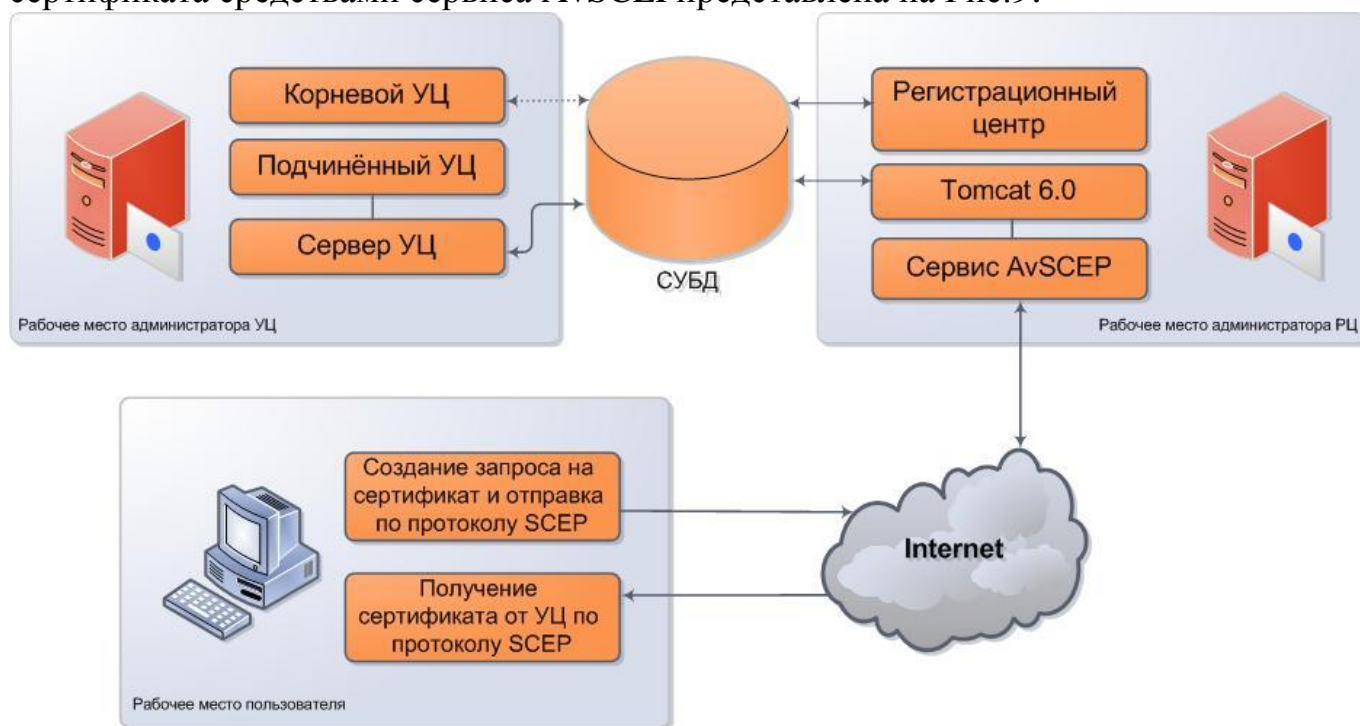


Рис.9 схема взаимодействия пользователя с ИОК