ГАЗИНФОРМ СЕРВИС

Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4»

Руководство администратора безопасности

Часть 4. Настройка подсистемы управления токенами, ЦС DogTag

Санкт-Петербург, 2024

Аннотация

В документе содержатся сведения о настройке подсистемы управления жизненным циклом токенов средства защиты информации от несанкционированного доступа «Блокхост-Сеть 4» при взаимодействии с центром сертификации DogTag и сервисом каталогов FreeIPA, а также сведения о настройке сертификатов, необходимых для функционирования подсистемы.

Содержание

Введение

Подсистема управления жизненным циклом токенов предназначена для управления носителями пользователей на протяжении всего жизненного цикла.

Для настройки и установки подсистемы управления жизненным циклом токенов в существующей иерархической структуре уже должны быть развернуты следующие компоненты:

– корневой центр сертификации;

– служба каталогов FreeIPA совместно с центром сертификации DogTag.

Знаки, расположенные на полях руководства, указывают на примечания.

Степени важности примечаний:

Важная информация
Указания, требующие особого внимания.

Дополнительная информация
Указания, позволяющие упростить работу с подсистемой.

1 Подсистема жизненного цикла токенов

Подсистема предназначена для управления устройствами аутентификации пользователей на протяжении всего жизненного цикла и обеспечивает учет токенов в системе, управление токенами и аудит в течении всего жизненного цикла.

Подсистема жизненного цикла токенов поддерживает управление токенами перечисленными в таблице 1.1.

Таблица 1.1 – Поддерживаемые подсистемой токены

Носитель	**Производитель**	**Наименование носителя**	
		поддерживаемые ОС Windows	**поддерживаемые ОС Linux**
eToken	ЗАО «АЛАДДИН Р.Д.»	eToken Pro, eToken Pro (Java), eToken ГОСТ, eToken NG-FLASH, eToken NG-FLASH (Java), eToken NG-OTP, eToken NG-OTP (Java), eToken GT (Java), eToken PRO (Java) SC, eToken PRO SC	
SafeNet eToken	ООО «Сертифицированные информационные системы»	SafeNet eToken 5100, SafeNet eToken 5105, SafeNet eToken 5200, SafeNet eToken 5205, SafeNet eToken 7200, SafeNet eToken 7300, SafeNet eToken 4100	
Рутокен	ЗАО «Актив Софт»	Рутокен, Рутокен S, Рутокен Lite, Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен ЭЦП 2.0 Flash, Рутокен ЭЦП 3.0	Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен ЭЦП 2.0 Flash, Рутокен ЭЦП 3.0
JaCarta	ЗАО «АЛАДДИН Р.Д.»	JaCarta-2, JaCarta PKI, JaCarta PRO	JaCarta-2, JaCarta PKI, JaCarta PRO
eSmart Token	ООО «Интеллектуальные системы управления бизнесом»	eSmart Token	eSmart Token

Для работы с сертификатами на токене в подсистеме жизненного цикла СЗИ от НСД «Блокхост-Сеть 4» необходимо выполнить определенные настройки центра сертификации и в самой подсистеме жизненного цикла токенов.

2 Настройки на сервисе каталогов FreeIPA/центре сертификации Dogtag

2.1 Создание сервисной учетной записи

Для первоначальной настройки подсистемы жизненного цикла токенов необходимо создать сервисную учетную запись (агента регистрации), обладающую достаточными правами для создания сертификата и входящую в группу издателей сертификатов сервиса каталогов FreeIPA.

Для создания сервисной учетной записи (например, ***serviceCA***) необходимо выполнить следующие действия:

1) Создать базу данных сертификатов:

```
mkdir /root/nss
certutil -N -d /root/nss
```

После выполнения команды ввести пароль доступа к базе сертификатов и повторить его.

2) Импортировать сертификат CA Агента для доступа к службе выдающего ЦС:

```
pk12util -i /root/ca-agent.p12 -d /root/nss
```

3) Для проверки доступа выполнить команду для вывода списка сертификатов в созданной базе:

```
certutil -L -d /root/nss
```

В результате выполнения команды отобразится список, содержащий сертификат CA Агента.

4) Провести проверку подключения к службе выдающего ЦС с запросом списка профилей сертификатов:

```
sudo pki -d /root/nss/ -n ipa-ca-agent ca-profile-find
```

5) Создать новую сервисную учетную запись от имени пользователя, обладающего правами администратора с помощью команды:

```
sudo pki –d /root/nss/ -n ipa-ca-agent ca-user-add <имя учетной записи> --fullName "псевдоним учетной записи"
```

```
user@alt9cafreeipa ~ $ sudo pki -d /root/nss/ -n ipa-ca-agent ca-user-add serviceCA --fullName “CA Агент”
[sudo] password for user:
Enter password for Internal Key Storage Token
----------------------
Added user "serviceCA"
----------------------
  User ID: serviceCA
  Full name: CA Агент
user@alt9cafreeipa ~ $
```

Рисунок 2.1 – Создание сервисной учетной записи

6) Добавить созданную сервисную учетную запись в группу издателей сертификатов Certificate Manager Agents с помощью команды:

```
sudo pki -d /root/nss/ -n ipa-ca-agent ca-group-member-add "Certificate Manager Agents" <имя учетной записи>
```

```
user@alt9cafreeipa ~ $ sudo pki -d /root/nss/ -n ipa-ca-agent ca-group-member-add "Certificate Manager Agents" serviceCA
[sudo] password for user:
Enter password for Internal Key Storage Token

----------------------------
Added group member "serviceCA"
----------------------------
  User: serviceCA
user@alt9cafreeipa ~ $
```

Рисунок 2.2 – Добавление сервисной учетной записи в группу издателей сертификатов

2.2 Создание сертификата агента регистрации

Для выпуска пользовательских сертификатов на токене необходим сертификат агента регистрации. В этом случае администратор может обращаться к центру сертификации DogTag для выпуска сертификатов пользователям сервиса каталогов FreeIPA.

Для создания сертификата сервисной учетной записи необходимо выполнить следующие действия:

1) Создать запрос на сертификат агента регистрации от имени пользователя, обладающего правами администратора с помощью команды:

```
sudo pki -d /root/nss/ -c <пароль администратора ЦС> client-cert-request uid=<имя УЗ CA Агента> --profile CustomUserCert
```

или

```
sudo pki -d /root/nss/ -c <пароль администратора ЦС> client-cert-request cn=<имя УЗ CA Агента>,E=<имя УЗ CA Агента>@<CANAME UPPER CASE> --profile CustomUserCert
```

2) Используя данные запроса сертификата *«Request ID»* выполнить создание сертификата агента регистрации с помощью команды:

```
sudo pki -d /root/nss/ -n ipa-ca-agent ca-cert-request-review <request ID> --action approve
```

```
user@alt9cafreeipa ~ $ sudo pki -d /root/nss/ -n ipa-ca-agent ca-cert-request-review 162 --action approve
[sudo] password for user:
Enter password for Internal Key Storage Token

WARNING: The --action option has been deprecated. Use the following command instead:
WARNING:   $ pki ca-cert-request-<action> <request ID>
-------------------------------
Approved certificate request 162
-------------------------------
  Request ID: 162
  Type: enrollment
  Request Status: complete
  Operation Result: success
  Certificate ID: 0x51
user@alt9cafreeipa ~ $
```

Рисунок 2.3 – Создание сертификата агента регистрации

3) Используя данные выпуска сертификата *«Certificate ID»* выполнить назначение сертификата сервисной учетной записи с помощью команды:

```
sudo pki -d /root/nss/ -n ipa-ca-agent ca-user-cert-add <имя учетной записи> --serial <certificate ID>
```

```
user@alt9cafreeipa ~ $ sudo pki -d /root/nss/ -n ipa-ca-agent ca-user-cert-add serviceCA --serial 0x51
[sudo] password for user:
Enter password for Internal Key Storage Token

-----------------------------------------------------------------------------------------------
Added certificate "2;81;CN=freeipa.local,O=FREEIPA.LOCAL;E=serviceCA@FREEIPA.LOCAL,CN=serviceCA"
-----------------------------------------------------------------------------------------------
  Cert ID: 2;81;CN=freeipa.local,O=FREEIPA.LOCAL;E=serviceCA@FREEIPA.LOCAL,CN=serviceCA
  Version: 2
  Serial Number: 0x51
  Issuer: CN=freeipa.local,O=FREEIPA.LOCAL
  Subject: E=serviceCA@FREEIPA.LOCAL,CN=serviceCA
user@alt9cafreeipa ~ $
```

Рисунок 2.4 – Назначение сертификата учетной записи агента регистрации

4) Выполнить импорт сертификата сервисной учетной записи в базу данных ЦС с помощью команды:

```
sudo pki -d /root/nss/ -c <пароль администратора ЦС> client-cert-import <имя учетной записи> --serial <certificate ID>
```

```
user@alt9cafreeipa ~ $ sudo pki -d /root/nss/ -c Gazprom09 client-cert-import serviceCA --serial 0x51
[sudo] password for user:
Imported certificate "serviceCA"
WARNING: Notice: Trust flag u is set automatically if the private key is present.
user@alt9cafreeipa ~ $
```

Рисунок 2.5 – Импорт сертификата учетной записи агента регистрации

5) Выполнить экспорт сертификата и закрытого ключа сервисной учетной записи в файл с помощью команды:

```
sudo pki -d /root/nss/ -c <пароль администратора ЦС> client-cert-show <имя учетной записи> --pkcs12 <имя файла ключей агента регистрации>.p12 --pkcs12-password <пароль к файлу ключей агента регистрации>
```

```
user@alt9cafreeipa ~ $ sudo pki -d /root/nss/ -c Gazprom09 client-cert-show serviceCA --pkcs12 serviceCA.p12 --pkcs12-password Gazprom09
[sudo] password for user:
user@alt9cafreeipa ~ $ ls
 freeipa    serviceCA.p12   Документы   Загрузки   Общедоступные   'Рабочий стол'
user@alt9cafreeipa ~ $
```

Рисунок 2.6 – Экспорт сертификата учетной записи агента регистрации

2.3 Создание профиля для выпуска сертификата пользователя

Для выпуска сертификатов на токене пользователей сервиса каталогов FreeIPA необходимо создать профиль пользователя.

Для создания профиля для выпуска сертификата пользователя необходимо выполнить следующие действия:

1) Вывести список всех доступных пользователей с помощью команды

```
sudo pki -d /root/nss/ -n ipa-ca-agent ca-profile-find
```

и найти профиль с идентификатором *CustomUserCert*.

```
user@alt9cafreeipa ~ $ sudo pki -d /root/nss/ -n ipa-ca-agent ca-profile-find
[sudo] password for user:
Enter password for Internal Key Storage Token

-----------------
93 entries matched
-----------------
  Profile ID: acmeServerCert
  Name: ACME Server Certificate Enrollment
  Description: This certificate profile is for enrolling server certificates via ACME protocol.

  Profile ID: caCMCserverCert
  Name: Server Certificate Enrollment using CMC
  Description: This certificate profile is for enrolling server certificates using CMC.

  Profile ID: caCMCECserverCert
  Name: Server Certificate wth ECC keys Enrollment using CMC
  Description: This certificate profile is for enrolling server certificates with ECC keys using CMC.

  Profile ID: CustomUserCert
  Name: Custom Manual User Dual-Use Certificate Enrollment
  Description: This certificate profile is for enrolling user certificates.
```

Рисунок 2.7 – Список всех доступных профилей

2) Выгрузить найденный профиль в файл с помощью команды:

```
sudo pki -d /root/nss/ -n ipa-ca-agent ca-profile-show <идентификатор профиля> --raw --output <имя файла>.cfg
```

```
user@alt9cafreeipa ~ $ sudo pki -d /root/nss/ -n ipa-ca-agent ca-profile-show CustomUserCert --raw --output CustomUserCert.cfg
[sudo] password for user:
Enter password for Internal Key Storage Token

-----------------------------------------------
Saved profile CustomUserCert to CustomUserCert.cfg
-----------------------------------------------
user@alt9cafreeipa ~ $
```

Рисунок 2.8 – Сохранение профиля в файл

3) Просмотреть выгруженный профиль можно по команде:

```
sudo pluma <имя файла>.cfg
```

CustomUserCert.cfg

```
1 auth.class_id=
2 classId=caEnrollImpl
3 desc=This certificate profile is for enrolling user certificates.
4 enable=true
5 enableBy=admin
6 input.i1.class_id=keyGenInputImpl
7 input.i2.class_id=subjectNameInputImpl
8 input.i3.class_id=submitterInfoInputImpl
9 input.list=i1,i2
10 name=Custom Manual User Dual-Use Certificate Enrollment
11 output.list=o1
12 output.o1.class_id=certOutputImpl
13 policyset.list=userCertSet
14 policyset.userCertSet.1.constraint.class_id=subjectNameConstraintImpl
15 policyset.userCertSet.1.constraint.name=Subject Name Constraint
16 policyset.userCertSet.1.constraint.params.accept=true
17 policyset.userCertSet.1.constraint.params.pattern=^E=[^,]+,CN=.*$
18 policyset.userCertSet.1.default.class_id=userSubjectNameDefaultImpl
19 policyset.userCertSet.1.default.name=Subject Name Default
20 policyset.userCertSet.1.default.params.name=
21 policyset.userCertSet.10.constraint.class_id=renewGracePeriodConstraintImpl
22 policyset.userCertSet.10.constraint.name=Renewal Grace Period Constraint
23 policyset.userCertSet.10.constraint.params.renewal.graceAfter=30
```

Рисунок 2.9 – Просмотр профиля в редакторе

4) При необходимости отредактировать выгруженный профиль:

– если необходимо включить в профиль информацию о точках распространения CRL добавьте следующую секцию:

При изменении обратите внимание на указание правильного адреса сервера и пути, указанного в настройках сервера.

```
policyset.userCertSet.11.constraint.class_id=noConstraintImpl
policyset.userCertSet.11.constraint.name=No Constraint
policyset.userCertSet.11.default.class_id=crlDistributionPointsExtDefaultImpl
policyset.userCertSet.11.default.name=CRL Distribution Points Extension Default
policyset.userCertSet.11.default.params.crlDistPointsCritical=false
policyset.userCertSet.11.default.params.crlDistPointsEnable_0=true
policyset.userCertSet.11.default.params.crlDistPointsIssuerName_0=
policyset.userCertSet.11.default.params.crlDistPointsIssuerType_0=
policyset.userCertSet.11.default.params.crlDistPointsPointName_0=http:// <FQDN-имя сервера выдающего ЦС>/ipa/crl/MasterCRL.bin
```

```
policyset.userCertSet.11.default.params.crlDistPointsPointType_0=URIName
policyset.userCertSet.11.default.params.crlDistPointsReasons_0=
```

– если необходимо изменить в профиле информацию о сроке действия сертификата отредактируйте следующую секцию:

```
policyset.userCertSet.2.constraint.params.range=1100
policyset.userCertSet.2.default.params.range=1000
```

5) После внесения изменений, переименовать профиль в параметре *profileId* (рисунок 2.10).

```
 1 auth.class_id=
 2 classId=caEnrollImpl
 3 desc=This certificate profile is for enrolling user certificates for 1 year.
 4 enable=true
 5 enableBy=admin
 6 input.i1.class_id=keyGenInputImpl
 7 input.i2.class_id=subjectNameInputImpl
 8 input.i3.class_id=submitterInfoInputImpl
 9 input.list=i1,i2
10 name=Custom Manual User Dual-Use Certificate Enrollment 1 Year
11 output.list=o1
12 output.o1.class_id=certOutputImpl
13 policyset.list=userCertSet
14 policyset.userCertSet.1.constraint.class_id=subjectNameConstraintImpl
15 policyset.userCertSet.1.constraint.name=Subject Name Constraint
103 policyset.userCertSet.8.default.params.subjAltExtPattern_0=(UTF8String)1.3.6.1.4.1.311.20.2.
104 policyset.userCertSet.8.default.params.subjAltExtPattern_1=$request.sn_e$
105 policyset.userCertSet.8.default.params.subjAltExtType_0=RFC822Name
106 policyset.userCertSet.8.default.params.subjAltExtType_1=OtherName
107 policyset.userCertSet.8.default.params.subjAltNameExtCritical=false
108 policyset.userCertSet.8.default.params.subjAltNameNumGNs=2
109 policyset.userCertSet.9.constraint.class_id=signingAlgConstraintImpl
110 policyset.userCertSet.9.constraint.name=No Constraint
111 policyset.userCertSet.-
    9.constraint.params.signingAlgsAllowed=SHA1withRSA,SHA256withRSA,SHA512withRSA,SHA1withEC,SH
    PSS,SHA384withRSA/PSS,SHA512withRSA/PSS
112 policyset.userCertSet.9.default.class_id=signingAlgDefaultImpl
113 policyset.userCertSet.9.default.name=Signing Alg
114 policyset.userCertSet.9.default.params.signingAlg=-
115 policyset.userCertSet.list=1,10,2,3,4,5,6,7,8,9
116 profileId=CustomUserCert1Year
```

Рисунок 2.10 – Изменение идентификатора профиля в редакторе

6) Выполнить загрузку измененного профиля в базу данных с помощью команды:

```
sudo pki -d /root/nss/ -n ipa-ca-agent ca-profile-add <имя профиля>.cfg --raw
```

```
user@alt9cafreeipa ~ $ sudo pki -d /root/nss/ -n ipa-ca-agent ca-profile-add CustomUserCertYear1.cfg --raw
Enter password for Internal Key Storage Token

#Thu Mar 17 10:58:38 MSK 2022
policyset.userCertSet.7.constraint.class_id=noConstraintImpl
policyset.userCertSet.6.constraint.params.keyUsageNonRepudiation=true
policyset.userCertSet.8.default.params.subjAltExtType_0=RFC822Name
policyset.userCertSet.5.default.params.authInfoAccessCritical=false
policyset.userCertSet.6.default.params.keyUsageNonRepudiation=true
policyset.userCertSet.9.default.name=Signing Alg
policyset.userCertSet.6.constraint.name=Key Usage Extension Constraint
policyset.userCertSet.1.default.params.name=
policyset.userCertSet.6.default.params.keyUsageDataEncipherment=false
--------------------------------
Added profile CustomUserCertYear1
--------------------------------
user@alt9cafreeipa ~ $
```

Рисунок 2.11 – Загрузка измененного профиля в базу данных

7) Выполнить активацию измененного профиля с помощью команды:

```
sudo pki -d /root/nss/ -n ipa-ca-agent ca-profile-enable <идентификатор профиля>
```

```
user@alt9cafreeipa ~ $ sudo pki -d /root/nss/ -n ipa-ca-agent ca-profile-enable CustomUserCertYear1
[sudo] password for user:
Enter password for Internal Key Storage Token

-----------------------------------
Enabled profile "CustomUserCertYear1"
-----------------------------------
user@alt9cafreeipa ~ $
```

Рисунок 2.12 – Активация измененного профиля

3 Настройки на сервере «Блокхост-Сеть»

3.1 Установка сертификата агента регистрации

Установка сертификата агента регистрации осуществляется на рабочее место администратора безопасности с установленной серверной версией средства защиты от несанкционированного доступа «Блокхост-Сеть 4» для возможности выпуска сертификатов пользователей.

Для сервера «Блокхост-Сеть» под управлением ОС Linux не требуется экспорт и установка сертификата агента регистрации на сервере «Блокхост-Сеть».

3.1.1 Экспорт сертификата агента регистрации

Для экспорта сертификата агента регистрации выполните следующие действия:

1) На рабочей станции с установленным центром сертификации DogTag найти сертификат агента регистрации с помощью команды:

```
sudo ls
```

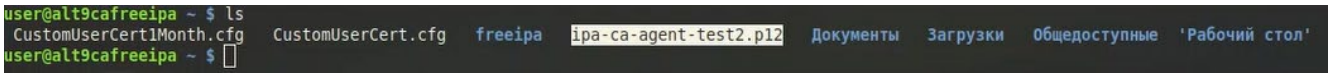


Рисунок 3.1 – Поиск сертификатов

2) Скопировать данный сертификат в каталог пользователя с помощью команды:

```
sudo cp <имя сертификата> ~
```

3) Записать сертификат на переносное устройство для установки на рабочее место администратора безопасности с установленной серверной версией средства защиты от несанкционированного доступа «Блокхост-Сеть 4».

3.1.2 Установка сертификата агента регистрации на сервер под управлением ОС Windows

Для установки сертификата агента регистрации выполните следующие действия:

1) С помощью мастера импорта сертификатов установить сертификат в личное хранилище текущего пользователя (рисунок 3.2).

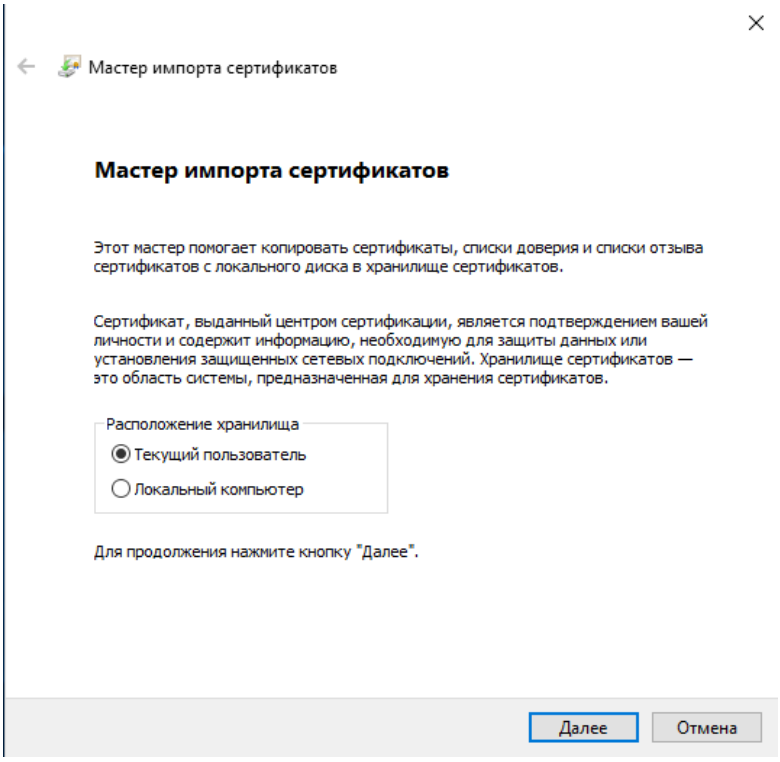


Рисунок 3.2 – Установка сертификата в хранилище пользователя

2) Указать пароль, заданный при экспорте сертификата (рисунок 3.3).

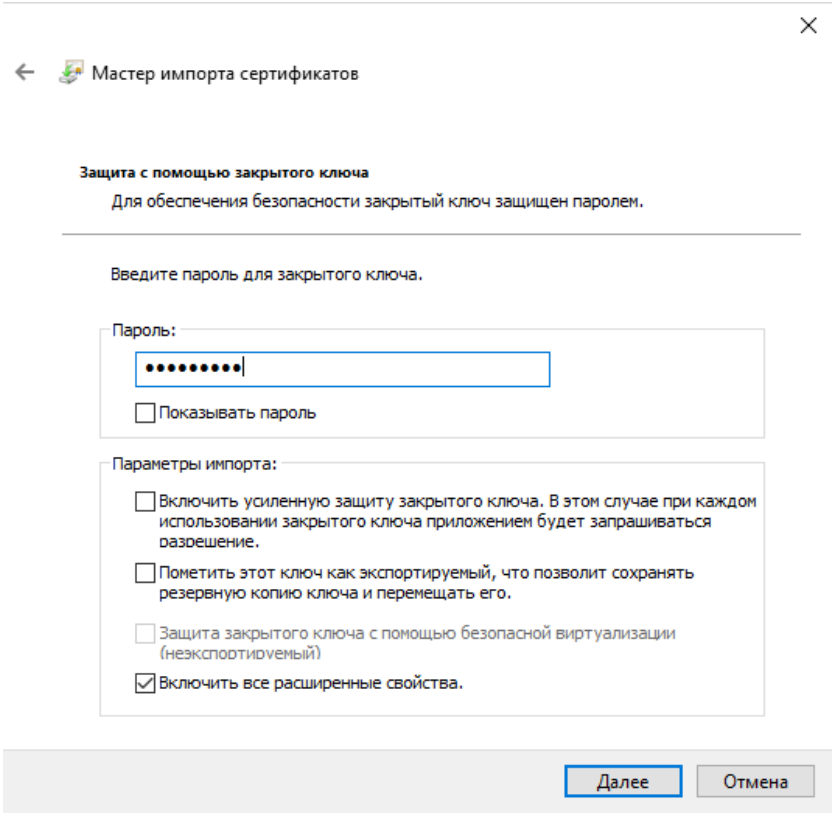


Рисунок 3.3 – Ввод пароля при импорте сертификата в хранилище

3) Выбрать хранилище сертификатов «Личные» (рисунок 3.4).

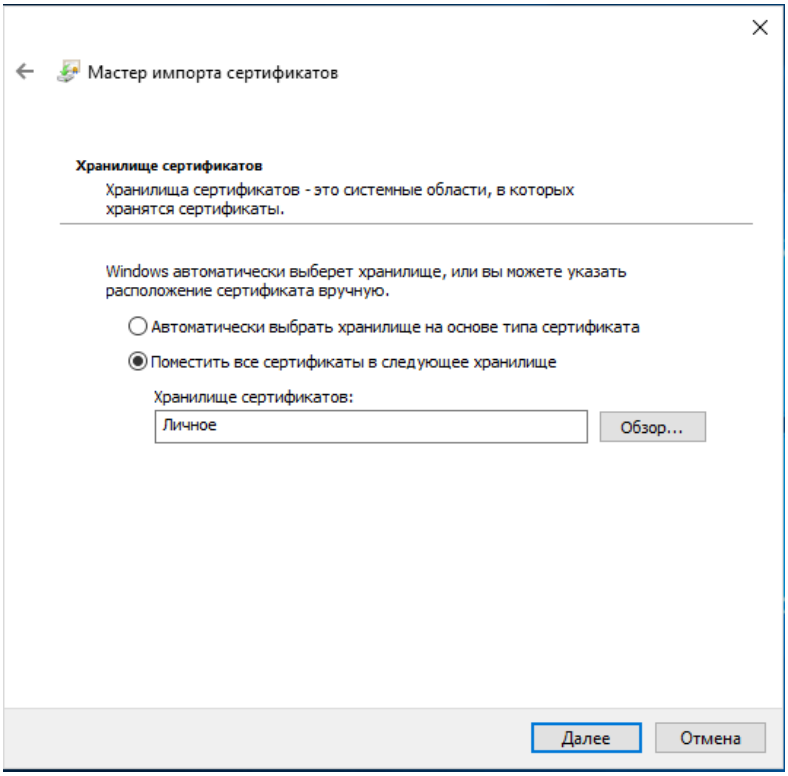


Рисунок 3.4 – Выбор хранилища при импорте сертификата

4) Перейти в директорию *C:\\Windows\System32\drivers\etc* и в файле *hosts* указать доменное имя центра сертификации:

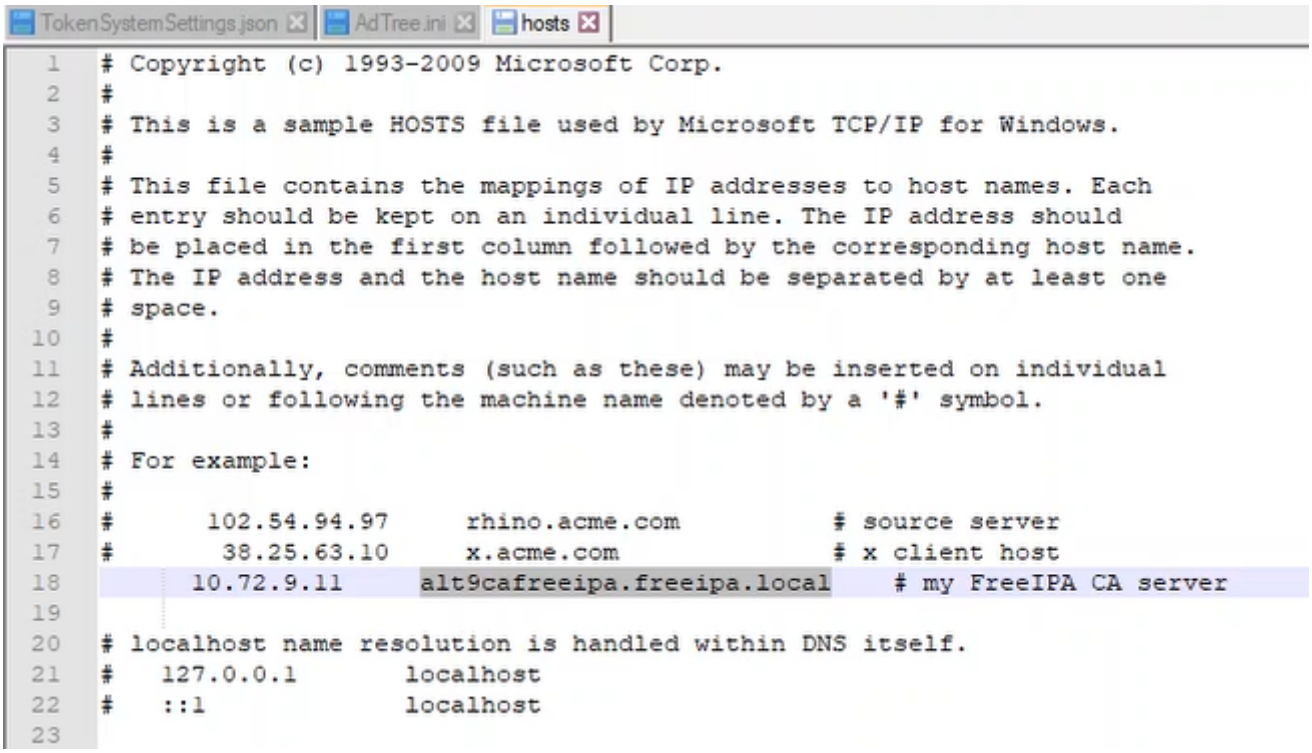


Рисунок 3.5 – Добавление центра сертификации в файл *hosts*

5) Проверить доступность центра сертификации:

```
ping alt9cafreeipa.freeipa.local
```

3.2 Установка доверенного корневого сертификата и промежуточного сертификата

Для корректного построения цепочки сертификации для пользовательского сертификата, выпущенного центром сертификации DogTag необходимо на рабочее место администратора безопасности с установленной серверной версией средства защиты от несанкционированного доступа «Блокхост-Сеть 4» выполнить установку промежуточного и доверенного корневого сертификатов.

3.2.1 Экспорт доверенного корневого сертификата и промежуточного сертификата

Для экспорта промежуточного и доверенного корневого сертификатов выполните следующие действия:

1) На рабочей станции с установленным центром сертификации DogTag найти сертификаты *ipa.cer* и *root.cer* (рисунок 3.6) с помощью команды:

```
sudo ls /root/
```

```
user@alt9cafreeipa ~ $ sudo ls /root/
[sudo] password for user:
ca-agent.p12  cacert.p12  ipa.cer  ipa.csr  kracert.p12  nss  root.cer  root.crl  tmp
```

Рисунок 3.6 – Поиск сертификатов

2) Скопировать данные сертификаты в каталог пользователя с помощью команды:

```
sudo cp /root/<имя сертификата>.cer ~
```

```
user@alt9cafreeipa ~ $ sudo cp /root/ipa.cer ~
user@alt9cafreeipa ~ $ sudo cp /root/root.cer ~
```

Рисунок 3.7 – Копирование сертификатов в каталог пользователя

3) При необходимости сменить владельца сертификатов с помощью команды

```
sudo chown user:user <имя сертификата>.cer
```

```
user@alt9cafreeipa ~ $ sudo chown user:user ipa.cer
user@alt9cafreeipa ~ $ sudo chown user:user root.cer
```

Рисунок 3.8 – Смена владельца сертификатов

4) Записать на переносное устройство для установки промежуточного и доверенного корневого сертификата на рабочее место администратора безопасности с установленной серверной версией средства защиты от несанкционированного доступа «Блокхост-Сеть 4».

3.2.2 Установка доверенного корневого сертификата и промежуточного сертификата на сервер под управлением ОС Windows

Для установки доверенного корневого сертификата и промежуточного сертификата выполните следующие действия:

1) С помощью мастера импорта сертификатов установить сертификаты в хранилище локального компьютера (рисунок 3.9).

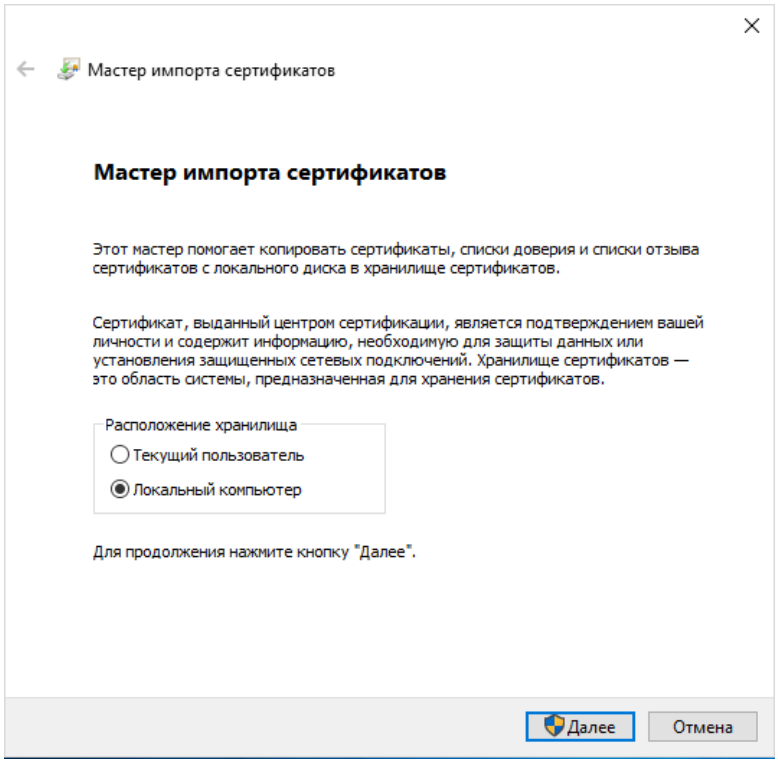


Рисунок 3.9 – Установка сертификата в хранилище пользователя

2) Выбрать хранилище сертификатов «Доверенные корневые центры сертификации» для корневого сертификата *root.cer* и «Промежуточные центры сертификации» для сертификата *ipa.cer* (рисунок 3.10).

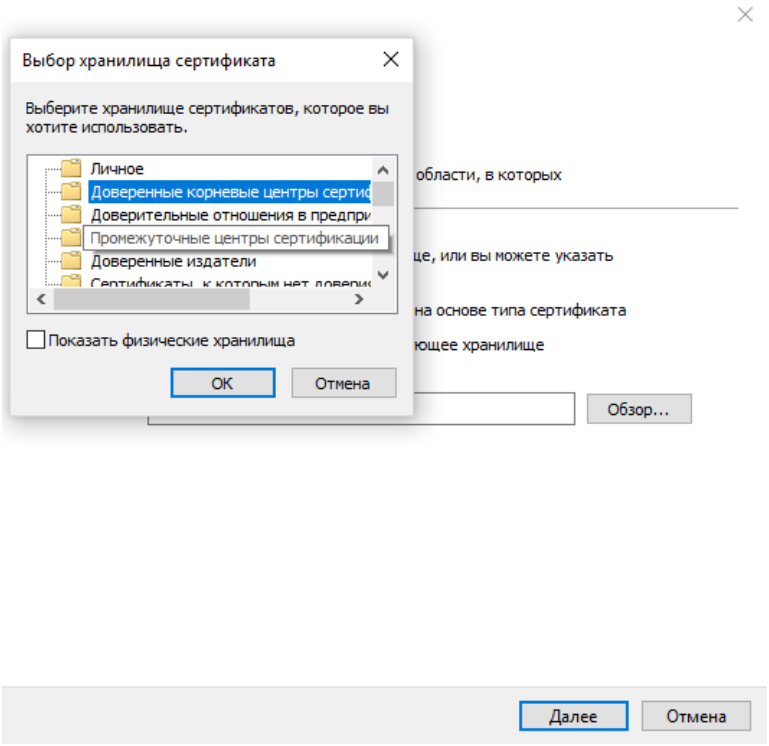


Рисунок 3.10 – Выбор хранилища при импорте сертификата

3.2.3 Установка доверенного корневого сертификата и промежуточного сертификата на сервер под управлением ОС Linux

Для установки доверенного корневого сертификата и промежуточного сертификата выполните следующие действия:

1) Установить «КриптоПро CSP» с помощью *deb* или *rpm* пакета в соответствии с версией ОС Linux (скачать «КриптоПро CSP» можно по ссылке https://www.cryptopro.ru/products/csp).

2) Перейти в директорию установки архива «КриптоПро CSP» и выполнить распаковку архива с помощью команды:

```
tar -xvf <название архива>
```

3) Перейти в директорию распаковки командой:

```
cd <название папки>
```

4) Выполнить запуск установочного скрипта командой:

```
sudo ./install.sh или sudo bash install.sh

sudo ./install_gui.sh или sudo bash install_gui.sh
```

5) Выполнить установку доверенного корневого сертификата и промежуточного

сертификата:

```
/opt/cprocsp/bin/amd64/certmgr -inst -store root -file /home/user/root.cer
/opt/cprocsp/bin/amd64/certmgr -inst -store root -file /home/user/ipa.cer
```

3.3 Создание профилей в настройках подсистемы

Для корректной работы подсистемы управления жизненным циклом токенов по выпуску сертификатов необходимо создать профиль для выпуска сертификата в настройках подсистемы управления жизненным циклом токенов.

Откройте консоль администрирования Блокхост-Сеть и перейдите в раздел ***Настройки*** → ***Выпуск сертификатов*** по кнопке (рисунок 3.11).

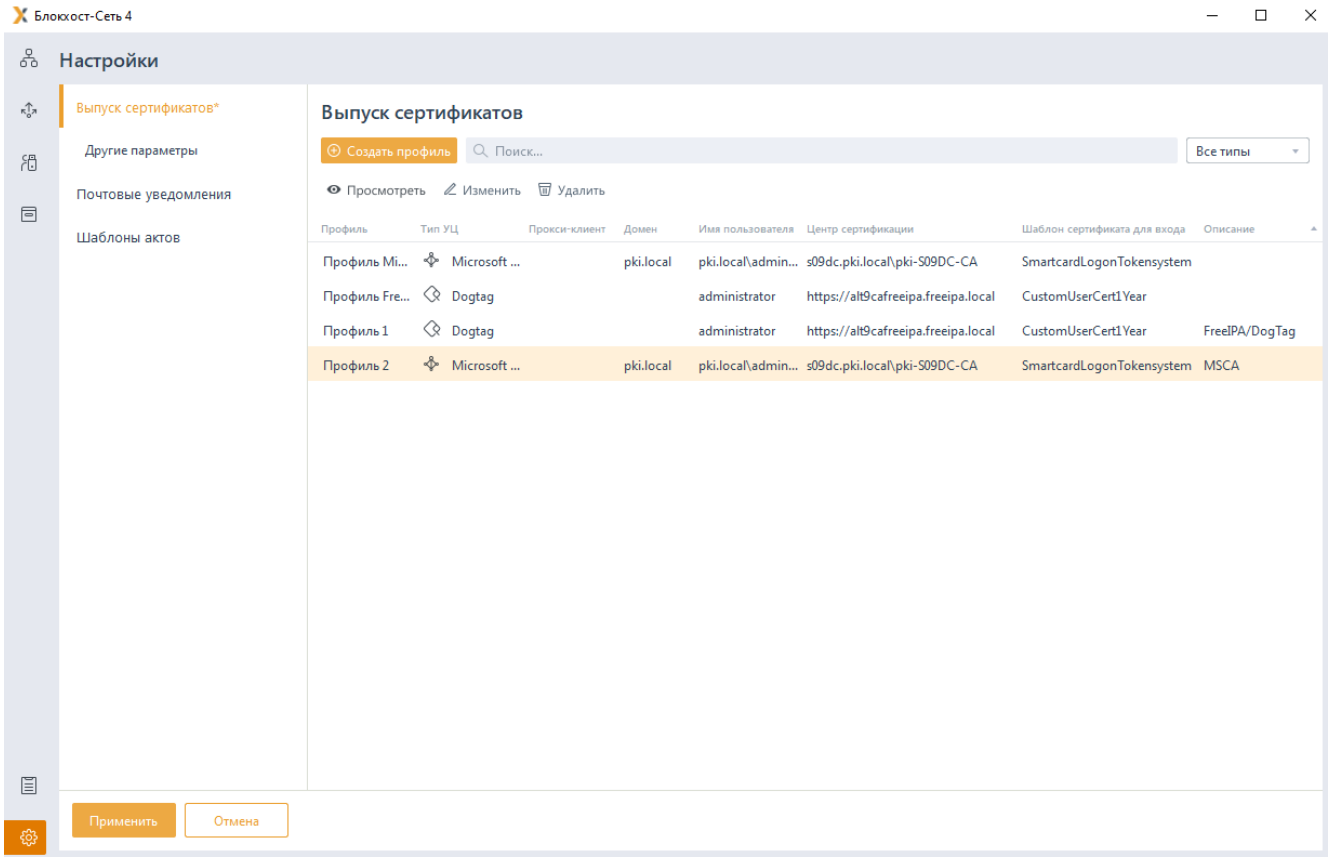


Рисунок 3.11 – Раздел ***Настройки***

Для каждого созданного профиля в окне ***Выпуск сертификатов*** отображается информация:

– *Профиль* – наименование профиля;

– *Тип УЦ* – центр сертификации выпускающий сертификат (Microsoft CA/DogTag);

– *Прокси-клиент* – клиентская рабочая станция, выбранная для взаимодействия с центром сертификации;

– *Домен* – наименование домена;

– *Имя пользователя* – наименование сервисной учетной записи;
– *Центр сертификации* – адрес центра сертификации;
– *Шаблон сертификата* – шаблон сертификата для входа;
– *Описание* – подробное описание профиля.

При необходимости, любой из созданных профилей возможно изменить или удалить с помощью соответствующих кнопок в верхней части вкладки (рисунок 3.11).

3.3.1 Создание профиля FreeIPA/DogTag

Для создания профиля по выпуску сертификатов центра сертификации DogTag нажмите на кнопку Создать профиль и выберите ***FreeIPA/DogTag*** (рисунок 3.12).

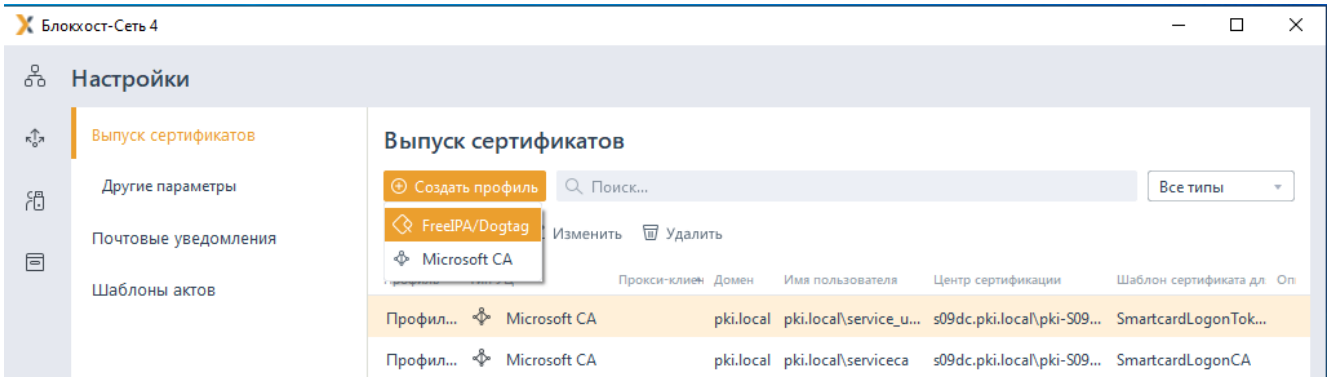


Рисунок 3.12 – Выбор центра сертификации

В появившемся окне (рисунок 3.13) введите наименование профиля, его описание, при необходимости, и параметры сервисной учетной записи (имя пользователя и пароль) в соответствующих полях.

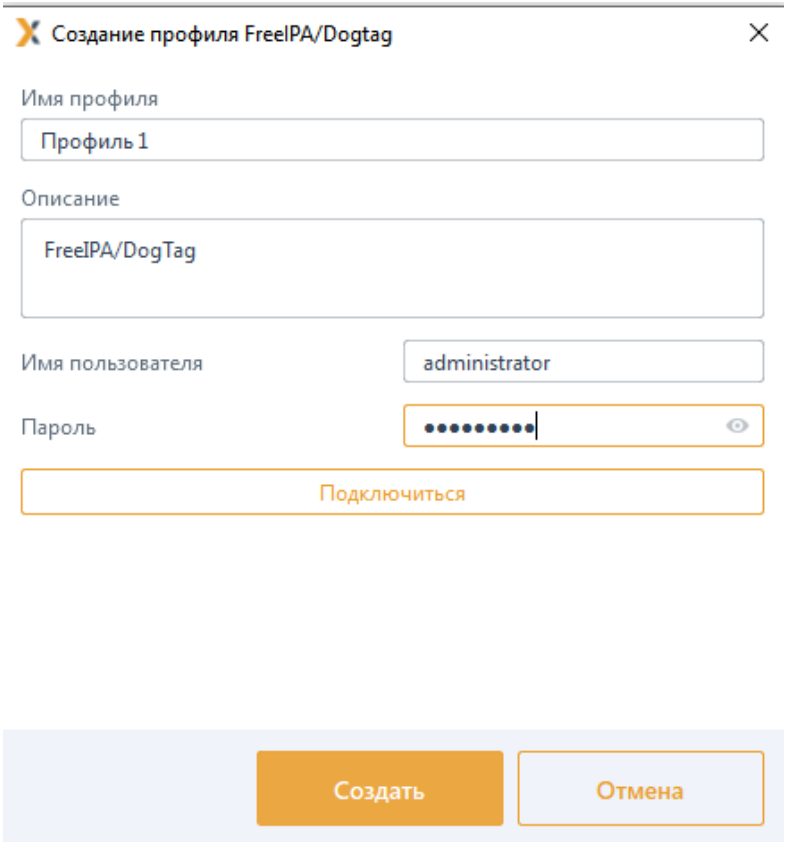


Рисунок 3.13 – Создание профиля FreeIPA/DogTag

Нажмите кнопку ***Подключиться*** (рисунок 3.13).

При возникновении ошибки при подключении убедитесь, что для вводимой сервисной учетной записи или для группы, в которую учетная запись входит, правилами клиентской политики безопасности не установлен запрет на аутентификацию ОС (подробное описание приведено в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 1. Управление политиками»).

После успешного подключения добавьте адрес центра сертификации в поле ***Центр сертификации*** и по кнопке ***Выбрать сертификат Enrollment agent*** укажите путь к сертификату агента регистрации, дающий право выпускать пользовательские сертификаты, установленный в личное хранилище оснастки **Сертификаты.** (рисунок 3.14).

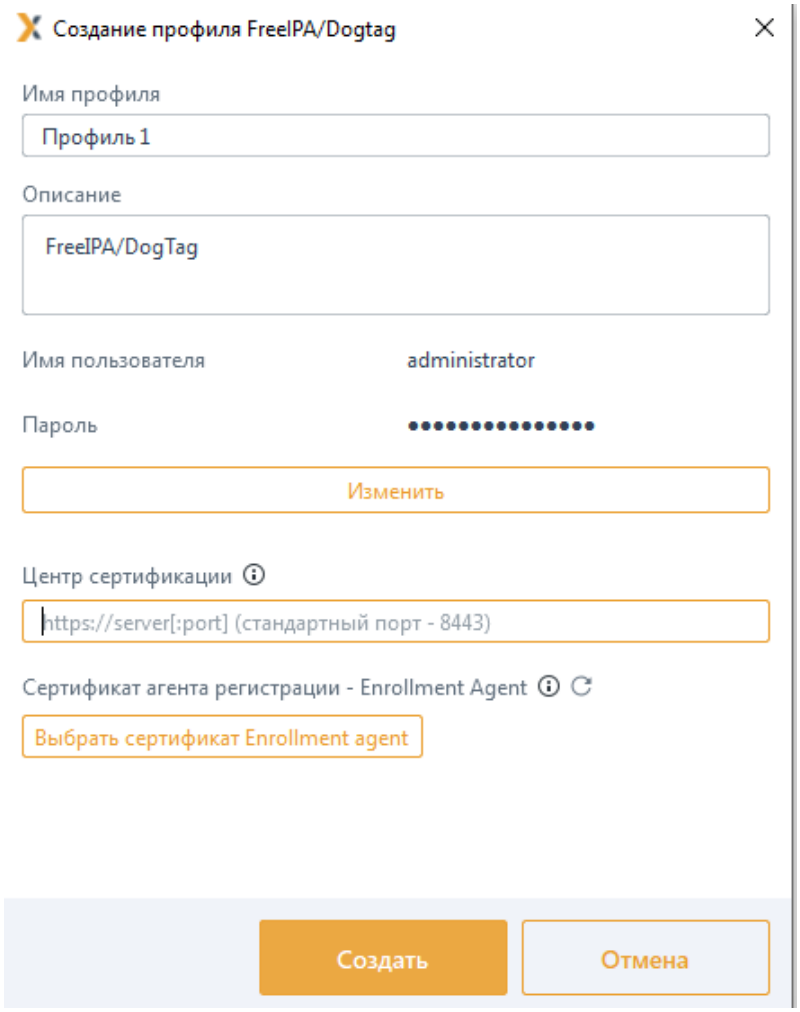


Рисунок 3.14 – Ввод центра сертификации и выбор сертификата агента регистрации

В поле ***Шаблон сертификата для входа*** (рисунок 3.15) выберите из списка шаблон сертификата пользователя, созданный в центре регистрации (например, ***CustomUserCert1Year***, созданный в разделе ***Создание профиля для выпуска сертификата пользователя***) и нажмите ***Применить***.

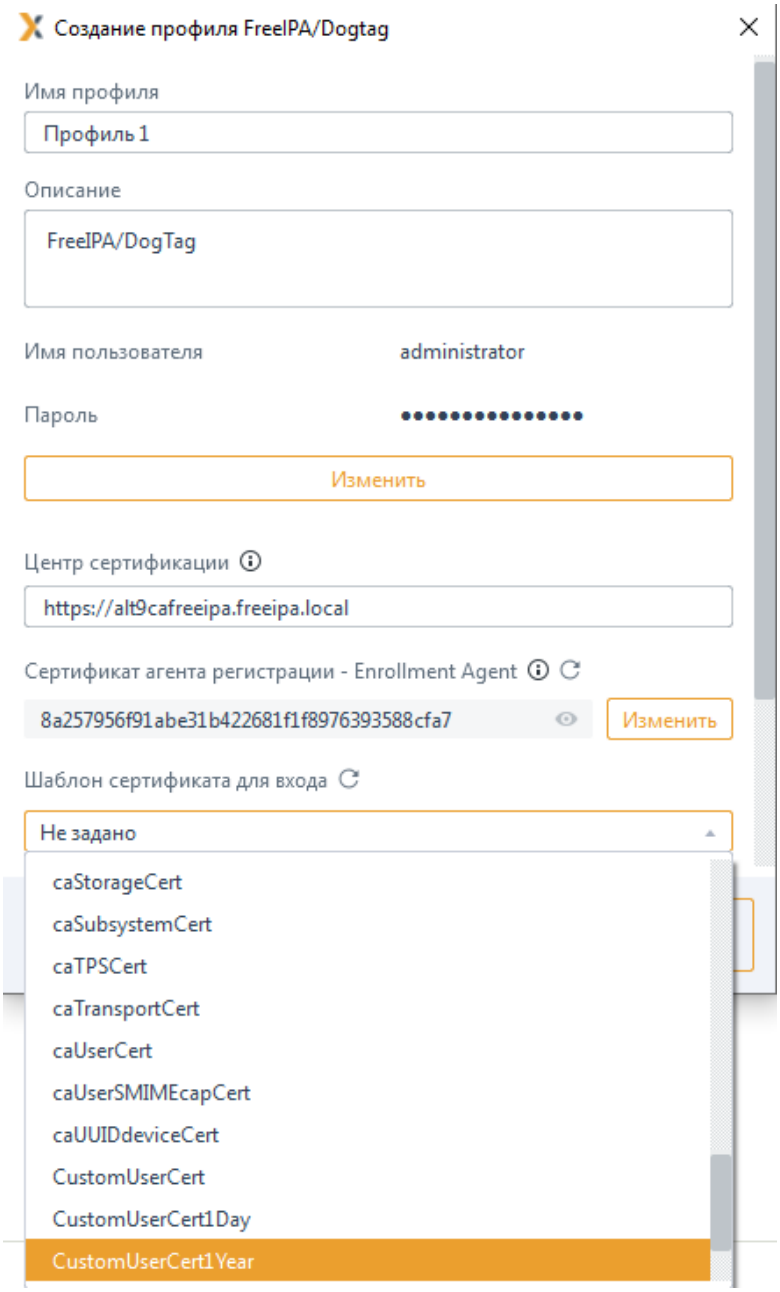


Рисунок 3.15 – Выбор шаблона сертификата для входа

После нажатия кнопки ***Создать*** профиль отобразится в списке и будет доступен к выбору при выпуске токена пользователю для входа по сертификату (рисунок 3.16).

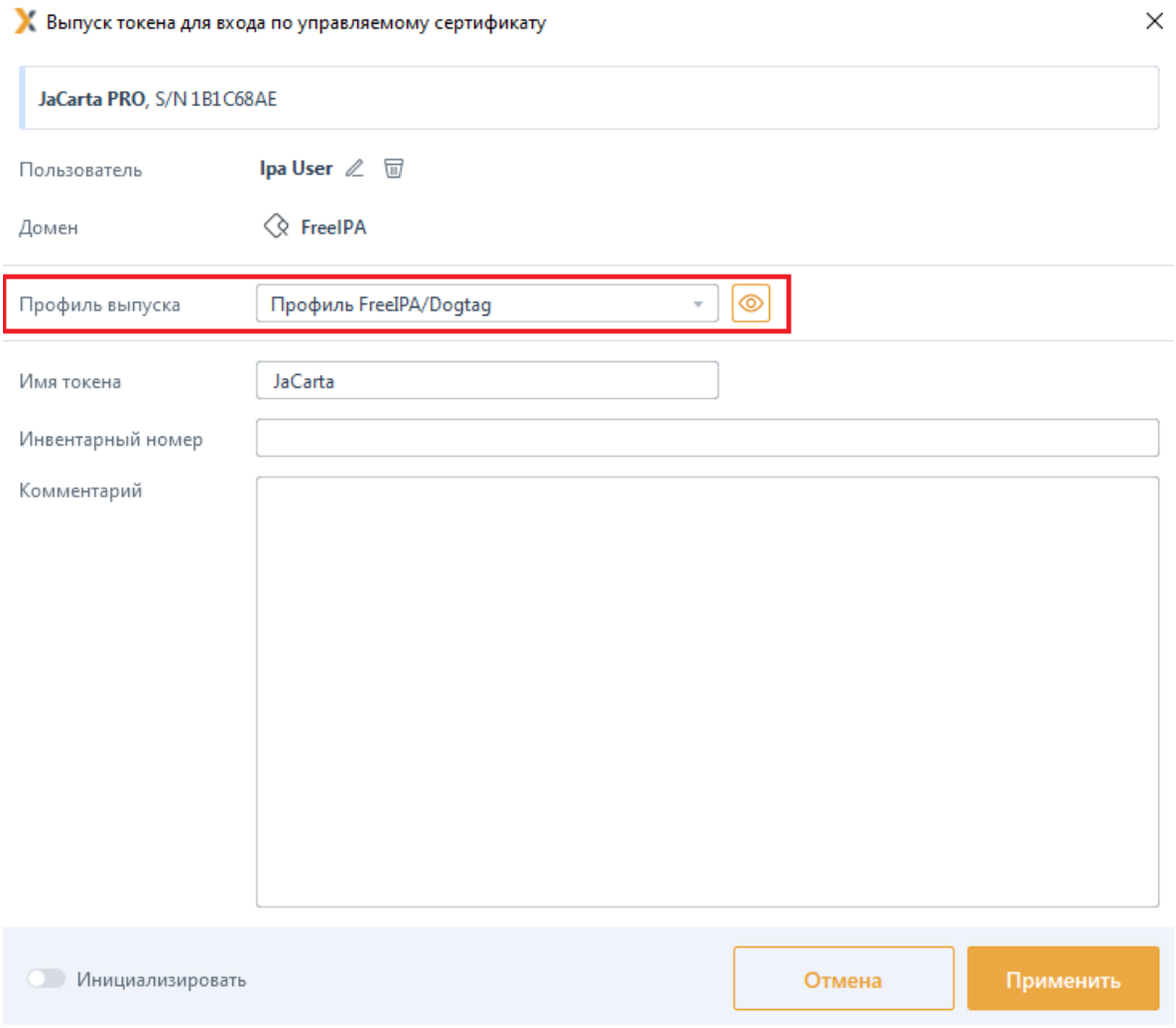


Рисунок 3.16 – Отображение профиля при выпуске токена

4 Особенности при выпуске токена средствами подсистемы

При выпуске токена средствами подсистемы жизненного цикла токенов, с записью на него сертификата для входа пользователя или при использовании токена для входа по паролю, на токен записывается информация служебного характера (рисунок 4.1).

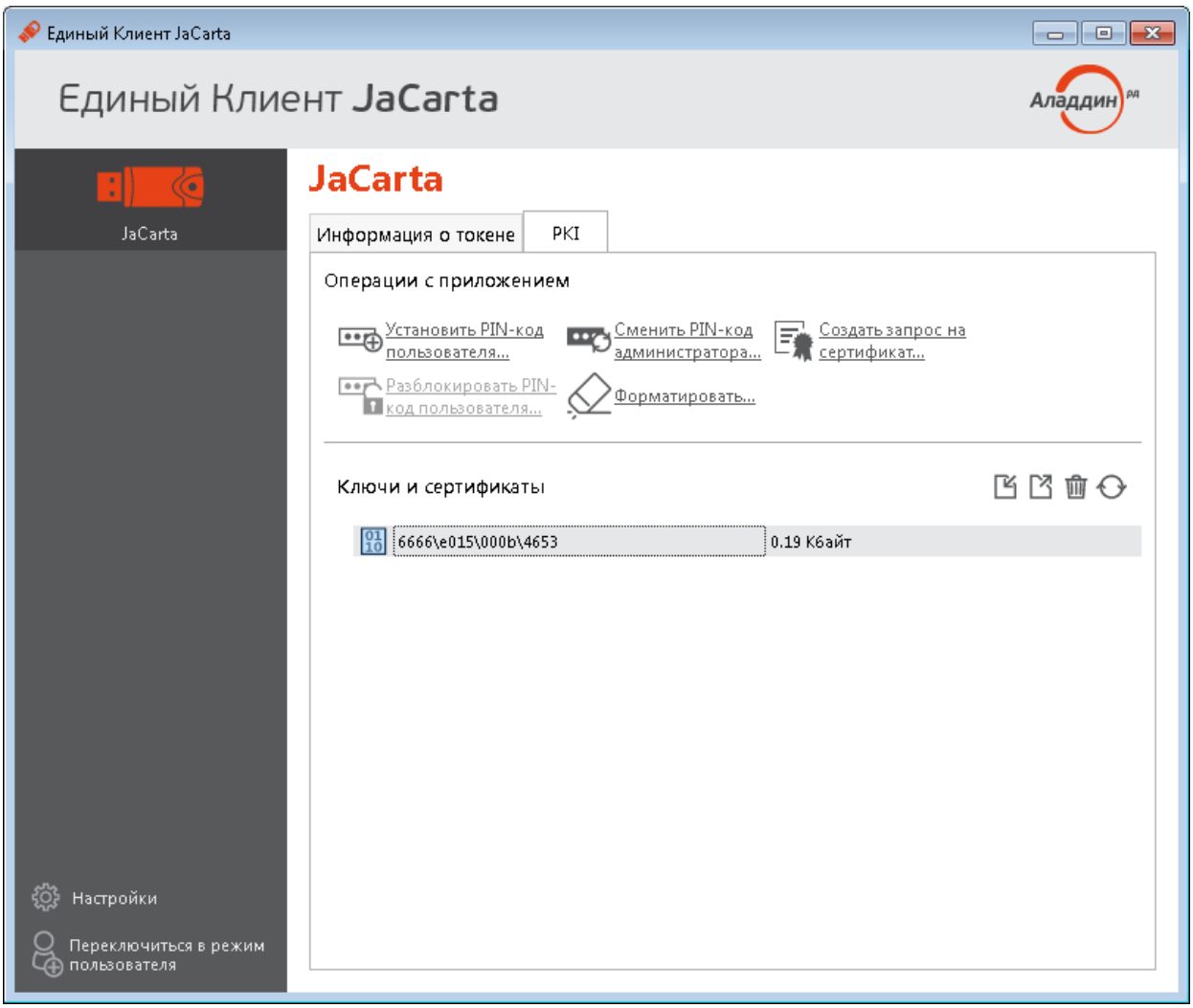


Рисунок 4.1 – Запись служебной информации при выпуске токена

Служебная информация на токене не подлежит удалению или редактированию. Указанные действия приведут к некорректной работе подсистемы с используемым токеном, и ошибкам при выполнении операций с ним.

Дальнейшие действия администратора по работе с подсистемой управления жизненным циклом токенов описаны в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 5. Управление токенами».

5 Настройка входа по сертификатам ЦС DogTag в ОС Linux

Перед выполнением настроек входа по сертификатам на рабочие станции под управлением ОС семейства Linux необходимо убедиться, что клиентская рабочая станция входит в домен FreeIPA, и что на рабочей станции установлена клиентская часть СЗИ от НСД «Блокхост-Сеть 4».

Установка клиентской части СЗИ на рабочие станции под управлением ОС семейства Linux описана в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство по инсталляции в ОС Linux».

5.1 Приоритет проверок средств аутентификации при входе

При входе пользователя в ОС семейства Linux действует следующая очередность проверок предъявляемых пользователем средств аутентификации по убыванию приоритета: вход по сертификату, вход по БВПП, вход по паролю:

1) При предъявлении пользователем токена, в первую очередь выполняется проверка на наличие на устройстве сертификата для входа:

   если сертификат для входа присутствует на токене (вне зависимости от истечения срока действия сертификата, наличия возможности безопасного входа по паролю), будет осуществлена попытка входа по сертификату.

2) При отсутствии на предъявляемом токене сертификата для входа, выполняется проверка на наличие на устройстве возможности безопасного входа по паролю:

   если безопасный вход по паролю возможен для пользователя, будет осуществлена попытка входа по паролю на токене.

3) В случае невозможности входа по сертификату и по паролю на токене, пользователь может воспользоваться входом по паролю без предъявления токена, при этом предъявляемое для входа устройство необходимо извлечь.

5.2 Ввод рабочей станции ОС Linux в домен FreeIPA

5.2.1 Ввод рабочей станции под управлением ОС Альт в домен FreeIPA

Перед вводом рабочей станции в домен, необходимо предварительно убедиться в **правильности настроек сети** (домен и все вводимые в него рабочие станции находятся в одной виртуальной подсети) и **в отсутствии расхождения по времени** между доменом и рабочей станцией, которая вводится в домен.

Ввод рабочей станции под управлением ОС Альт в домен FreeIPA может быть выполнен только одним способом с использованием инструментария sssd.

Подробное описание ввода в домен FreeIPA рабочей станции под управлением ОС Альт доступно на сайте справочного центра Альт https://www.altlinux.org/FreeIPA.

Для ввода в домен рабочей станции в ОС Альт необходимо последовательно выполнить следующие действия:

1) Скачать и установить все необходимые для работы пакеты:

```
sudo apt-get install task-auth-ad-sssd samba-client sssd-ad
sudo apt-get install task-auth-freeipa
```

2) Если используется домен, оканчивающийся на «.local», сразу выполнить следующую команду:

```
sudo chkconfig avahi-daemon off
sudo reboot
```

3) Задать имя клиентского компьютера следующей командой:

```
hostnamectl set-hostname <имя клиентского компьютера в нижнем регистре>.freeipa.local
```

при этом, имя клиентского компьютера обязательно должно содержать ***freeipa.local***.

4) В файле /etc/hosts указать:

```
10.72.9.11    alt9cafreeipa.freeipa.local alt9cafreeipa
10.72.9.11    freeipa.local
```

5) В *Центре управления системой* перейти в раздел ***Пользователи*** → ***Аутентификация***, выбрать пункт ***Домен FreeIPA*** и заполнить поля (рисунок 5.1).

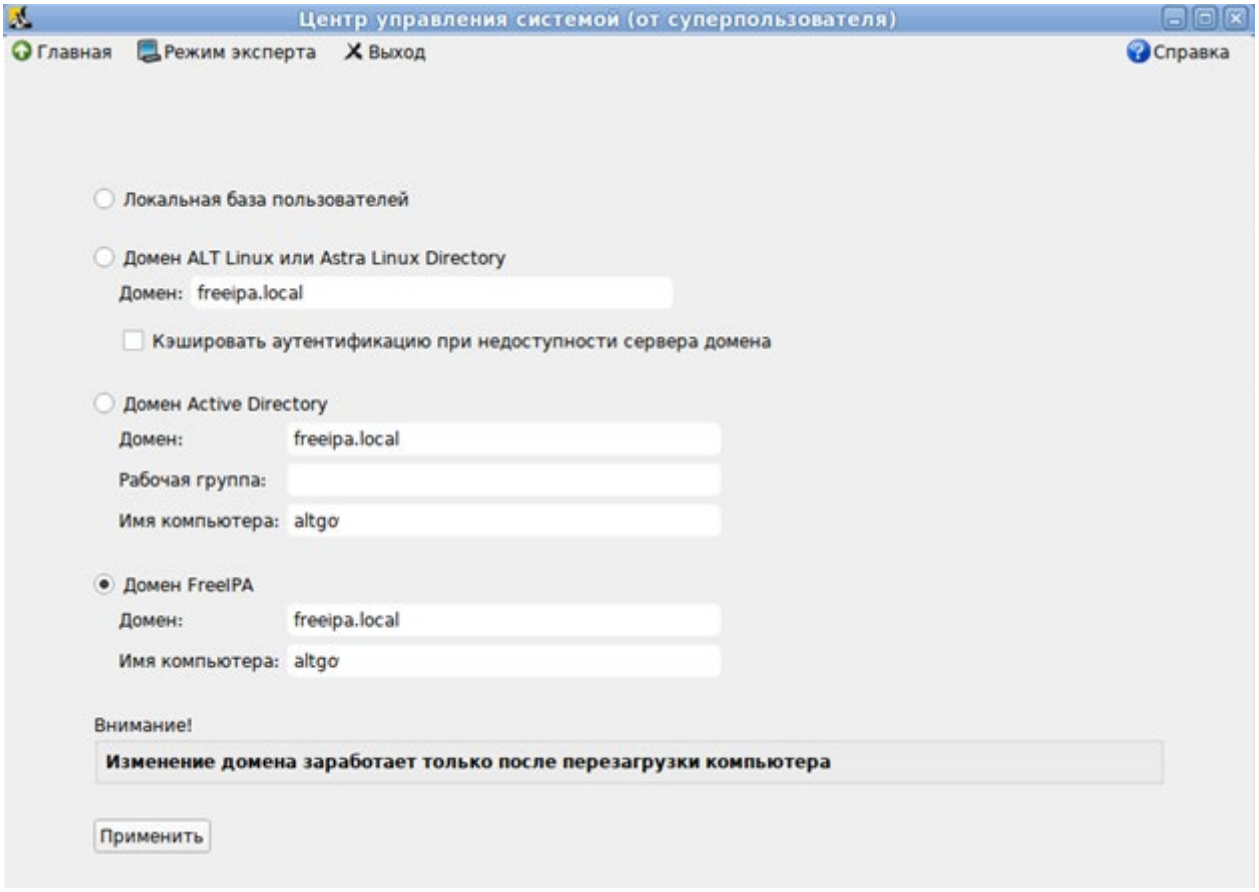


Рисунок 5.1 – Заполнение полей для ввода в домен FreeIPA

6) Нажать кнопку ***Применить***.

5.2.2 Ввод рабочей станции под управлением ОС Astra Linux в домен FreeIPA

Перед вводом рабочей станции в домен, необходимо предварительно убедиться в **правильности настроек сети** (домен и все вводимые в него рабочие станции находятся в одной виртуальной подсети) и **в отсутствии расхождения по времени** между доменом и рабочей станцией, которая вводится в домен.

Подробное описание ввода в домен FreeIPA рабочей станции под управлением ОС Astra Linux доступно на сайте справочного центра Astra Linux https://wiki.astralinux.ru/pages/viewpage.action?pageId=60359750.

Для ввода в домен рабочей станции в ОС Astra Linux необходимо последовательно выполнить следующие действия:

1) Задать имя клиентского компьютера следующей командой:

```
hostnamectl set-hostname <имя клиентского компьютера в нижнем регистре>.freeipa.local
```

при этом, имя клиентского компьютера обязательно должно содержать ***freeipa.local***.

2) В файле /etc/hosts указать:

```
127.0.1.1    <имя клиентского компьютера в нижнем регистре>.freeipa.local pc34
10.72.9.11    alt9cafreeipa.freeipa.local alt9cafreeipa
10.72.9.11    freeipa.local
```

3) Проверить доступность клиентского компьютера командой:

```
ping alt9cafreeipa.freeipa.local
```

4) Установить графический инструмент **fly-admin-freeipa-client** для ввода рабочей станции в домен:

```
sudo apt install fly-admin-freeipa-client
```

5) После установки пакет будет доступен в графическом меню ***Пуск → Панель управления → Сеть → Настройка FreeIPA client Fly***.

6) Для ввода рабочей станции в ОС Astra Linux в домен Active Directory необходимо выполнить запуск инструмента, указать имя домена, имя и пароль администратора и нажать кнопку ***Подключиться.***

5.2.3 Ввод рабочей станции под управлением РЕД ОС в домен FreeIPA

Перед вводом рабочей станции в домен, необходимо предварительно убедиться в **правильности настроек сети** (домен и все вводимые в него рабочие станции находятся в одной виртуальной подсети) и **в отсутствии расхождения по времени** между доменом и рабочей станцией, которая вводится в домен.

Подробное описание ввода в домен FreeIPA рабочей станции под управлением РЕД ОС доступно на сайте справочного центра РЕД ОС https://redos.red-soft.ru/base/arm/arm-domen/redos-in-ipa/.

Для ввода в домен рабочей станции в РЕД ОС необходимо последовательно выполнить следующие действия:

1) Отключить SELINUX в файле **/etc/selinux/config**:

```
SELINUX=disabled
```

После изменения перезагрузить ОС.

2) Задать имя клиентского компьютера следующей командой:

```
hostnamectl set-hostname <Имя компьютера>.<домен>
```

при этом, если домен **freeipa.local**, то имя клиентского компьютера обязательно должно содержать **client.freeipa.local**.

3) В файле /etc/hosts указать:

```
10.72.9.11    <Имя компьютера>.<домен> <Имя компьютера>
10.72.9.11    <домен>
```

4) Проверить доступность клиентского компьютера командой:

```
ping <Имя компьютера>.<домен>
```

5) Установить ipa-client:

```
dnf -y install ipa-client
```

6) Присоединить клиента к домену IPA:

```
ipa-client-install --domain freeipa.local --server alt9cafreeipa.freeipa.local --force-join
--mkhomedir
```

7) Согласитесь, введя *yes*, для продолжения с фиксированными значениями:

```
Proceed with fixed values and no DNS discovery? [no]:
```

8) Нажмите *Enter* в следующем сообщении:

```
Do you want to configure chrony with NTP server or pool address? [no]:
```

9) Согласитесь с продолжением настройки системы:

```
Client hostname: redos2.freeipa.local
Realm: FREEIPA.LOCAL
DNS Domain: freeipa.local
IPA Server: alt9cafreeipa.freeipa.local
BaseDN: dc=freeipa,dc=local

Continue to configure the system with these values? [no]:
```

10) Введите имя администратора (возможно использовать администратора по умолчанию IPA, который был создан при установке сервера) и пароль администратора:

```
User authorized to enroll computers: admin
```

11) При успешной установке появится сообщение:

```
Client configuration complete.
The ipa-client-install command was successful
```

5.3 Порядок настройки для входа по сертификатам в ОС Linux

Для возможности аутентификации пользователя на клиентской рабочей станции под управлением СЗИ от НСД «Блокхост-Сеть 4» с использованием цифрового сертификата в ОС Linux необходимо выполнить следующие действия на клиентской рабочей станции:

1) Установить корневые сертификаты домена FreeIPA.

2) Запустить задачу по настройке входа по сертификату через подсистему развертывания.

5.3.1 Экспорт корневого сертификата FreeIPA

Для установки промежуточного и доверенного корневого сертификатов необходимо выполнить следующие действия:

1) На рабочей станции с установленным центром сертификации DogTag с помощью команды

```
sudo ls /root/
```

найти сертификаты *ipa.cer* и *root.cer* (рисунок 5.2).

```
user@alt9cafreeipa ~ $ sudo ls /root/
[sudo] password for user:
ca-agent.p12  cacert.p12  ipa.cer  ipa.csr  kracert.p12  nss  root.cer  root.crl  tmp
```

Рисунок 5.2 – Поиск сертификатов

2) Скопировать данные сертификаты в каталог пользователя с помощью команды:

```
sudo cp /root/<имя сертификата>.cer
```

```
user@alt9cafreeipa ~ $ sudo cp /root/ipa.cer ~
user@alt9cafreeipa ~ $ sudo cp /root/root.cer ~
```

Рисунок 5.3 – Копирование сертификатов в каталог пользователя

3) При необходимости сменить владельца сертификатов с помощью команды

```
sudo chown user:user <имя сертификата>.cer:
```

```
user@alt9cafreeipa ~ $ sudo chown user:user ipa.cer
user@alt9cafreeipa ~ $ sudo chown user:user root.cer
```

Рисунок 5.4 – Смена владельца сертификатов

4) Записать сертификаты на переносное устройство для установки на клиентской рабочей станции.

5) На клиентской рабочей станции под управлением СЗИ от НСД «Блокхост-Сеть 4»

для удобства настройки сделать из файлов *ipa.cer* и *root.cer* один общий файл *ca.pem*:

```
cat ipa.cer > ca.pem

cat root.cer >> ca.pem
```

6) Для сохранения сертификатов создайте каталог */etc/certs/:*

```
sudo mkdir /etc/certs
```

7) Скопируйте в каталог */etc/certs/* сертификат центра сертификации (*ca.pem*):

```
sudo cp /<директория хранения сертификата> /etc/certs
```

5.3.2 Запуск задачи по настройке входа по сертификату через подсистему развертывания

Для создания задачи по настройке входа по сертификату на клиентских рабочих станциях откройте консоль управления Блокхост-Сеть перейдите по кнопке во вкладку ***Задачи***, раскройте меню создания задач по кнопке и выберите пункт ***Настройка входа по сертификатам*** (рисунок 5.5).

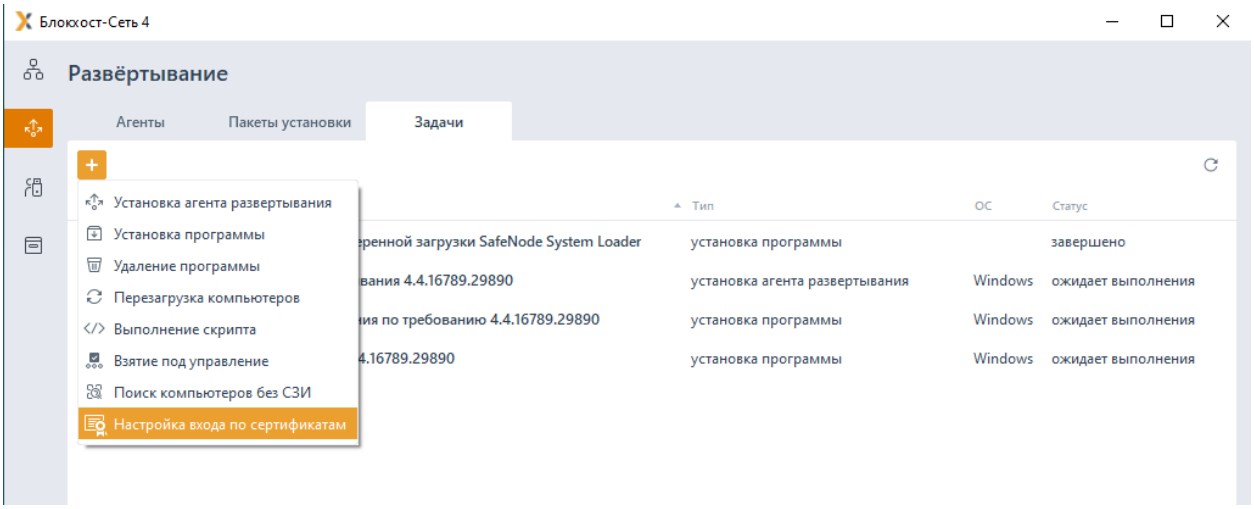


Рисунок 5.5 – Выбор задачи настройки входа по сертификатам

В открывшемся окне создания задачи настройки входа по сертификатам (рисунок 5.6) нажмите кнопку Выбрать для перехода к окну выбора домена.

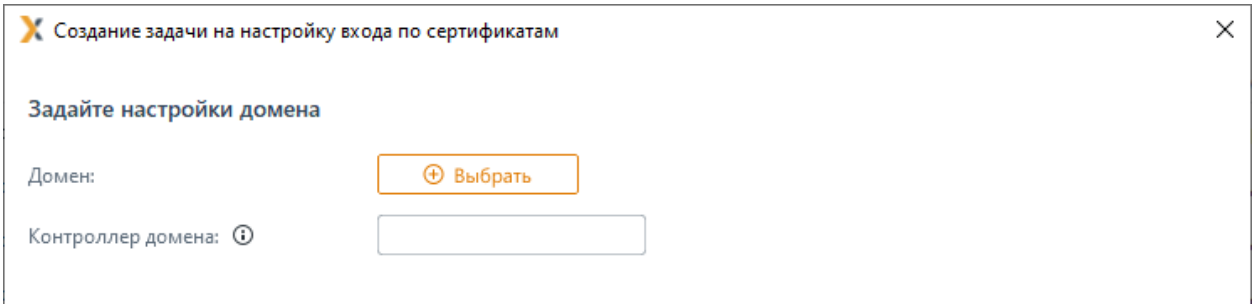
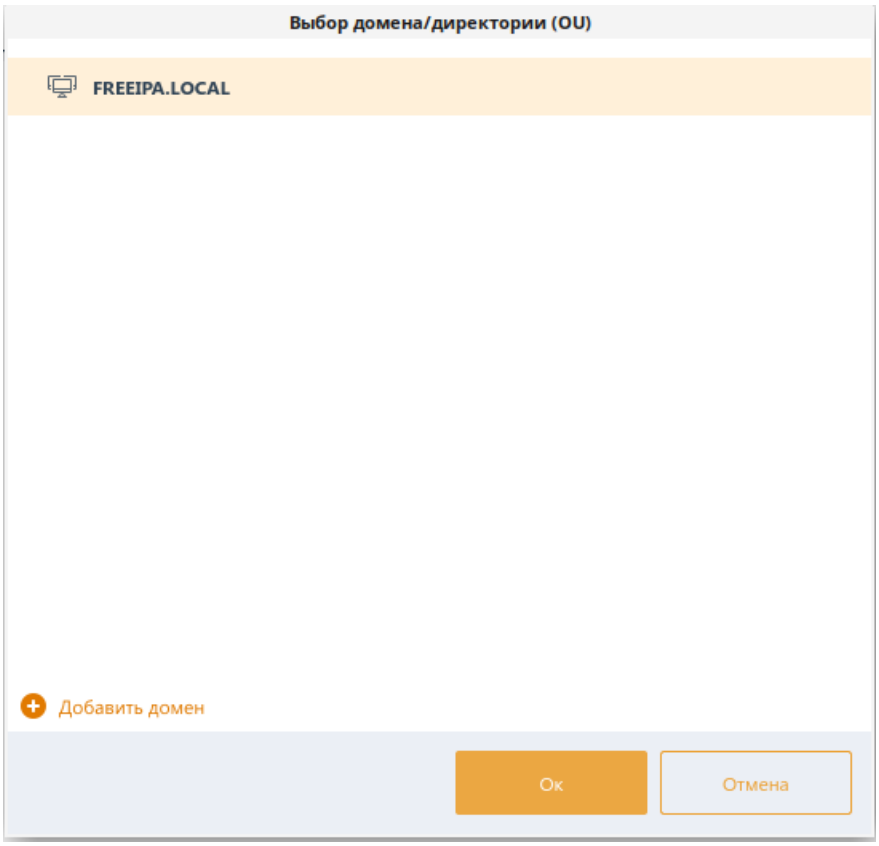
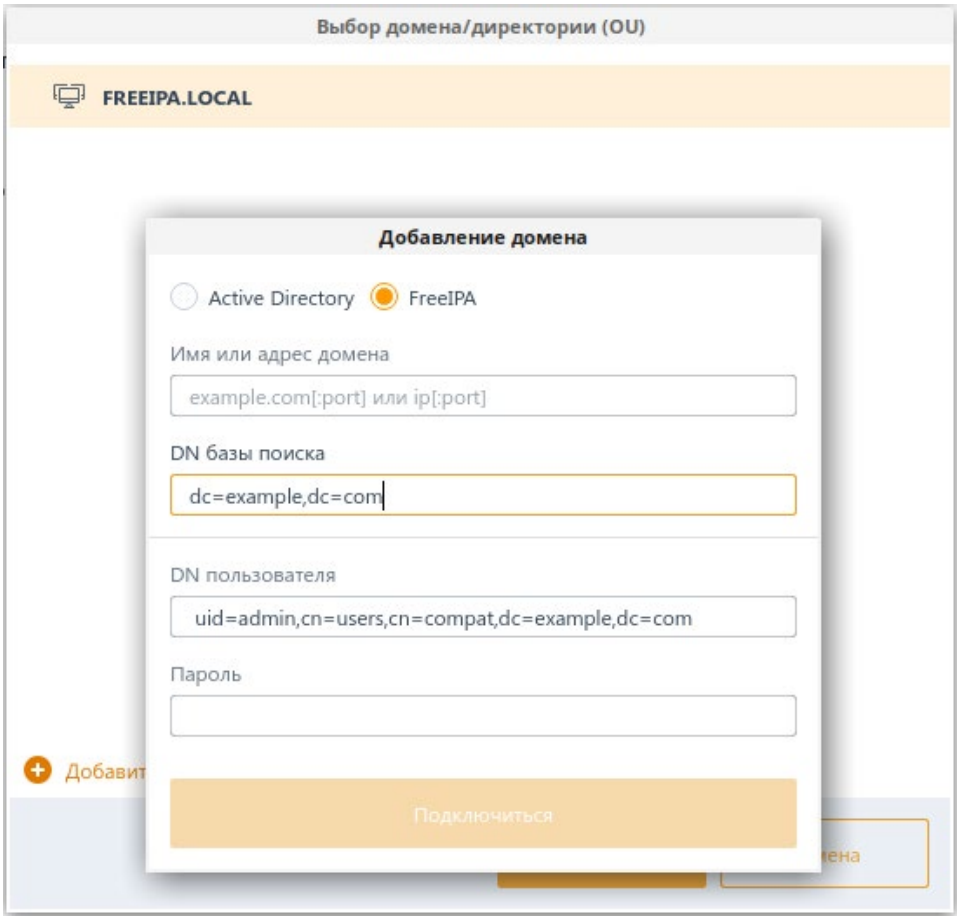


Рисунок 5.6 – Задание настроек домена

Выберите нужный домен (рисунок 5.7 а) или, при отсутствии необходимого домена в списке, добавьте его по ссылке Добавить домен (рисунок 5.7 б) и нажмите ***ОК***.



а)



б)

Рисунок 5.7 – Выбор домена

Домены во вкладке ***Домены*** подразделяются на:

– *системные* домены, которые добавляются в список доменов автоматически. Подключение к системному домену (при раскрытии дерева или по двойному щелчку) происходит из-под текущей учетной записи или, в случае неудачи, запрашивается логин/пароль для подключения.

– *пользовательские* домены, которые добавляются по кнопке Добавить домен. При подключении к пользовательскому домену всегда запрашивается логин/пароль для подключения (попытка подключения из-под текущей учетной записи не выполняется).

После выбора домена нажмите кнопку ***Далее*** (рисунок 5.8).

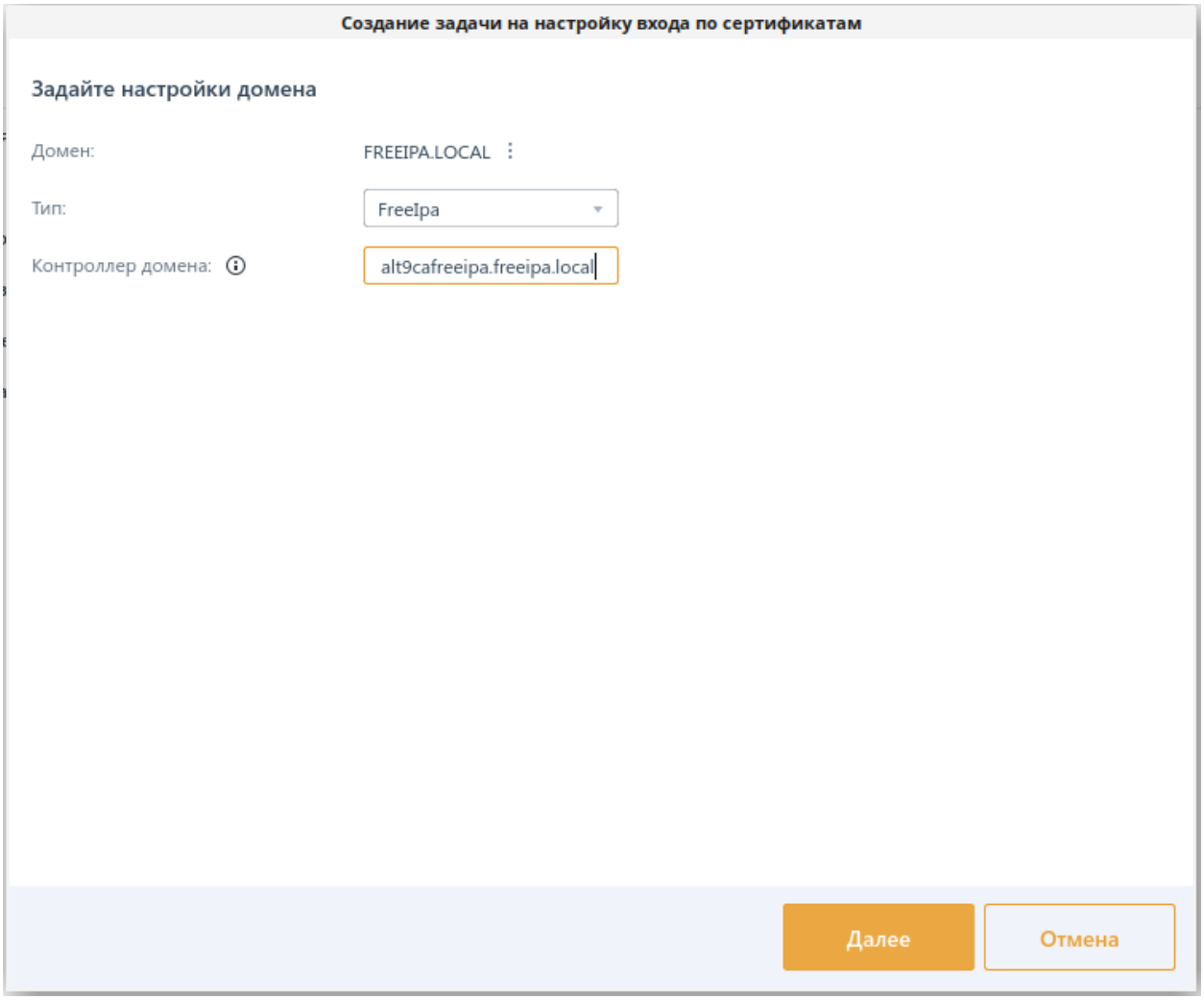


Рисунок 5.8 – Отображение выбранного домена

Выберите в списке те рабочие станции, на которых необходимо выполнить настройку входа по сертификатам, и нажмите кнопку ***Далее*** (рисунок Рисунок 5.9).

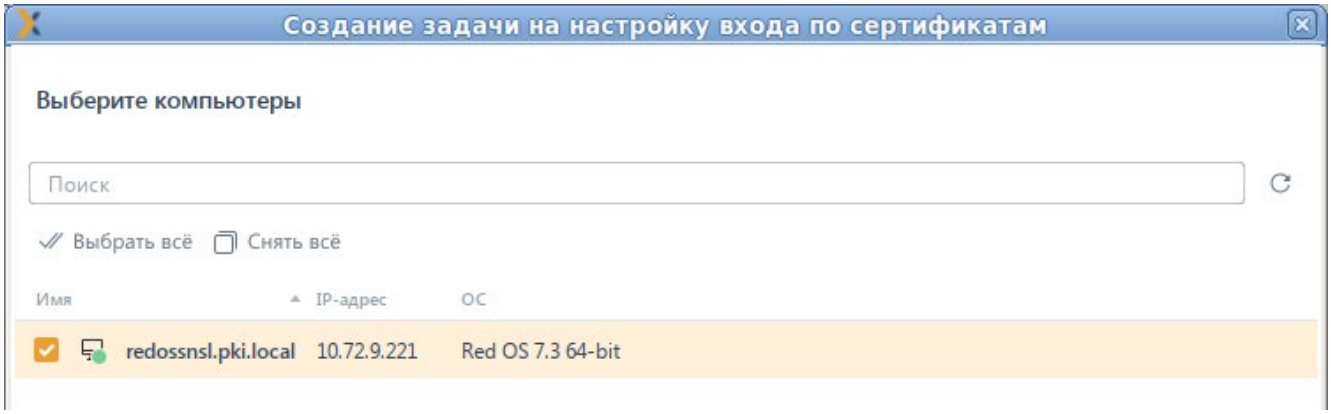
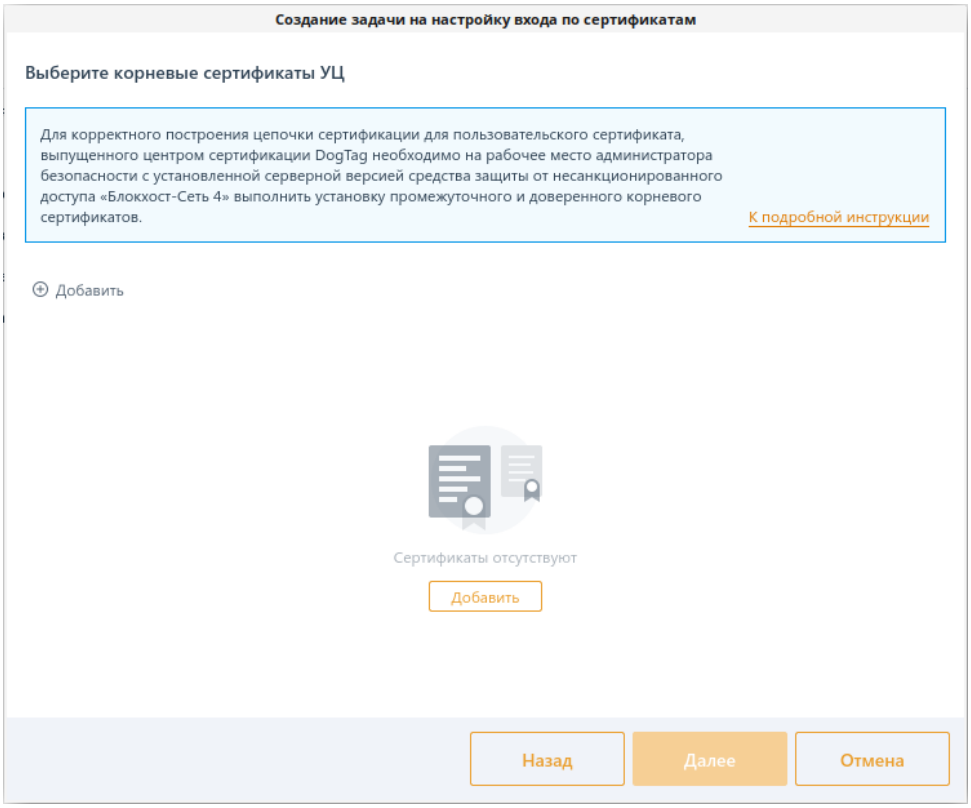


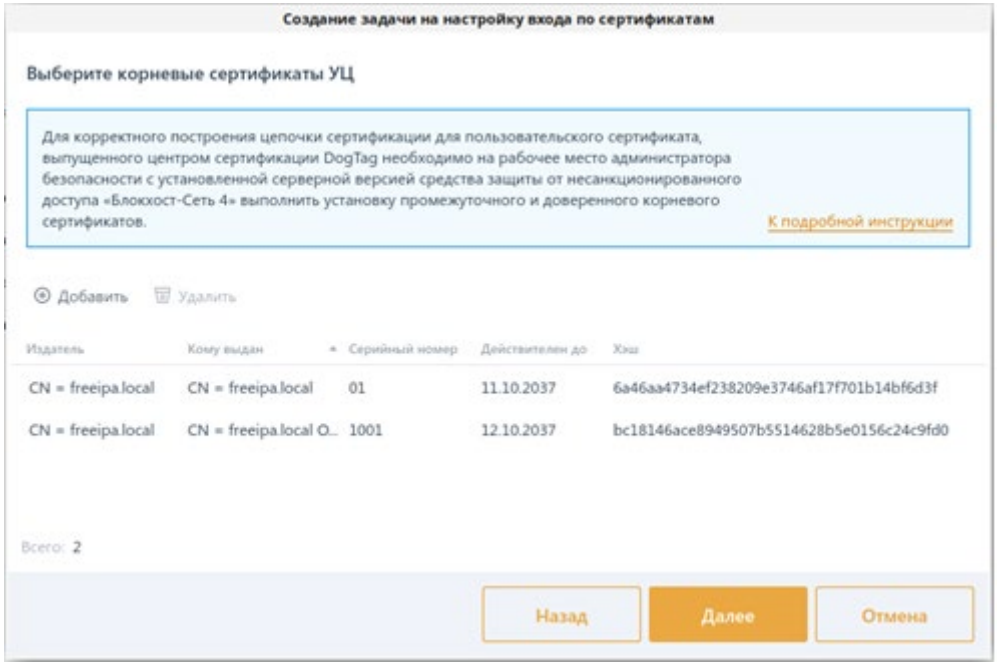
Рисунок 5.9 – Выбор рабочих станций

В следующем окне (рисунок 5.10 а) по кнопке ***Добавить*** добавьте корневой сертификат ЦС DogTag (экспорт подробно описан в разделе ***«Экспорт корневого сертификата***

FreeIPA/DogTag в ОС Linux»). При необходимости воспользуйтесь инструкцией по установке корневого сертификата, доступной по кнопке ***К подробной инструкции*** (рисунок 5.10 б).



а)

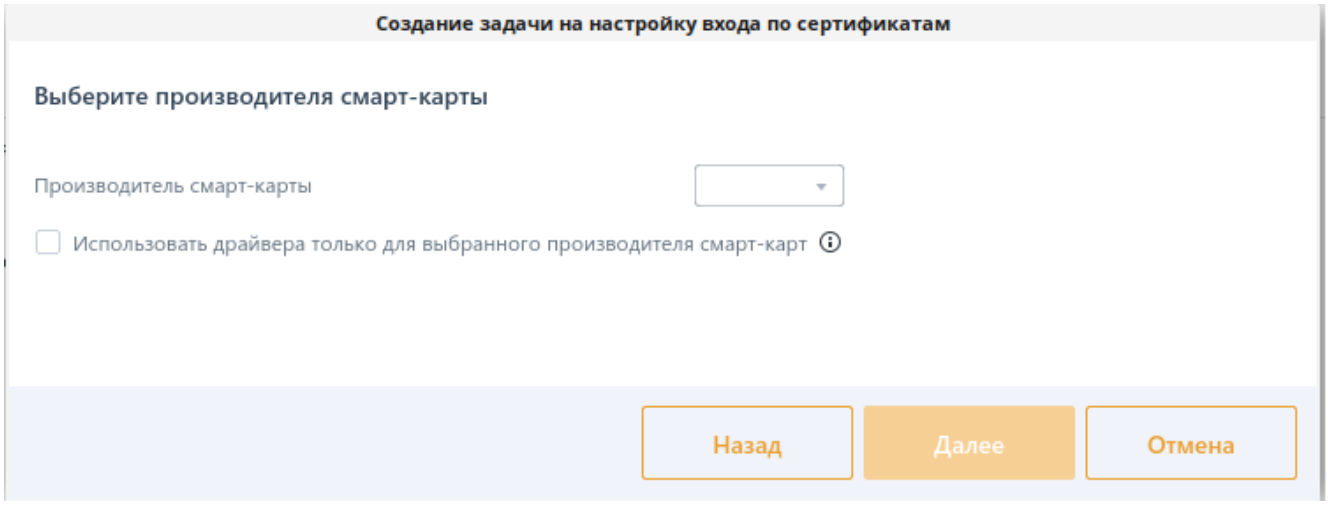


б)

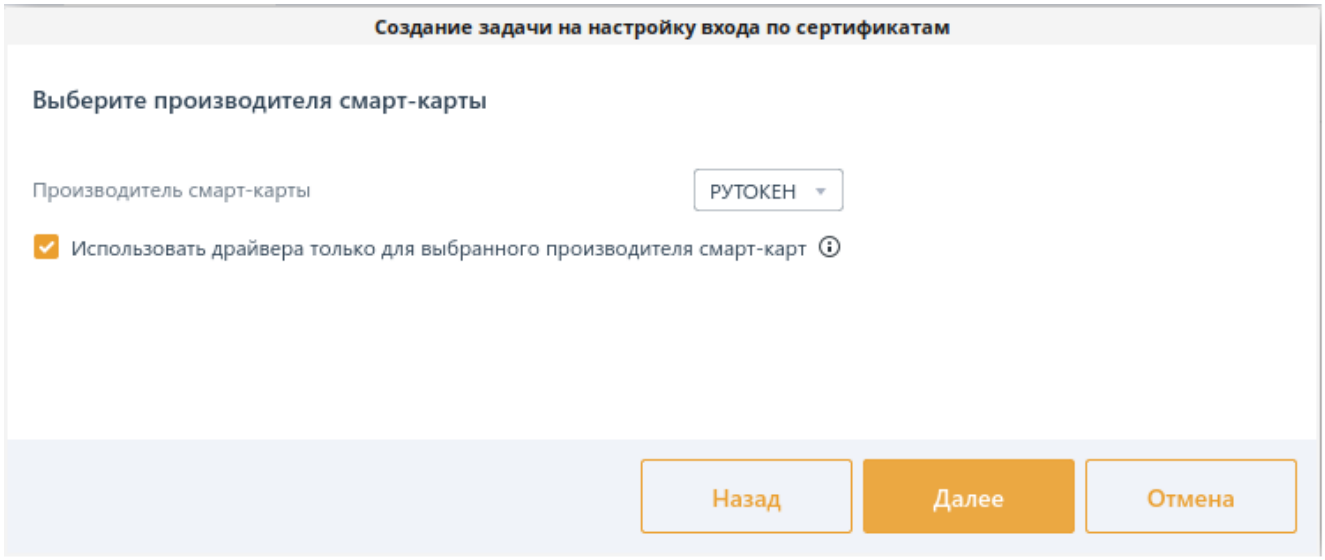
Рисунок 5.10 – Добавление корневого сертификата

В следующем окне выберите из списка производителя смарт-карты для которого будет выполняться настройка входа по сертификатам (рисунок 5.11).

При настройке двухфакторной аутентификации драйвера смарт-карты могут конфликтовать с драйверами других производителей в том числе и системными. Это может привести к невозможности входа с использованием сертификата. Рекомендуется выполнять настройку с установленным параметром ***Использовать драйвера только для выбранного производителя смарт-карты*** (рисунок 5.11 б).



а)



б)

Рисунок 5.11 – Выбор производителя смарт-карты

Задайте параметры планировщика запуска задачи (подробнее в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора. Часть 2. Развертывание и аудит» в

пункте ***«Указание параметров планировщика задачи по установке агента»***), определите интервалы времени выполнения задачи (рисунок 5.12) и нажмите кнопку ***Далее*** для продолжения создания задачи по настройке входа по сертификатам.

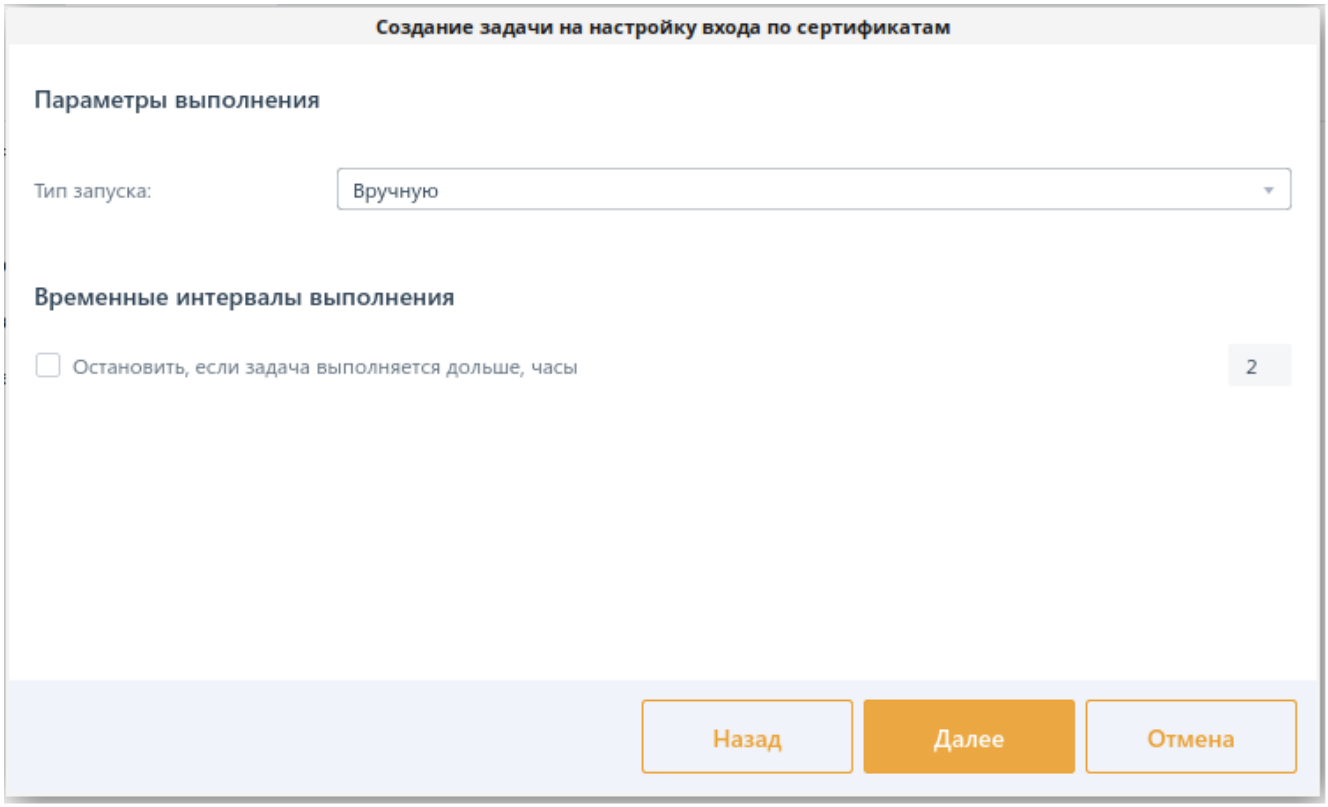


Рисунок 5.12 – Определение параметров планировщика и временных интервалов выполнения задачи

Введите имя создаваемой задачи и нажмите кнопку ***Создать***.

В результате во вкладке ***Задачи*** будет создана новая задача по настройке входа по сертификатам с заданными в ходе работы мастера создания задачи параметрами.

В зависимости от установленных параметров планировщика запуск задачи будет осуществлен автоматически или вручную.

Для запуска задачи вручную выделите нужную задачу в списке и нажмите в меню кнопку ▷ Запустить или нажмите кнопку ***Запустить*** в открывшейся панели справа (подробнее в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора. Часть 2. Развертывание и аудит» в пункте ***«Запуск задачи»***).

В результате выполнения задачи по настройке входа по сертификатам на всех указанных в списке рабочих станциях будет настроен вход по сертификатам для выбранного производителя смарт-карт.

Перечень сокращений

CA	–	Certification Authority (удостоверяющий центр)
НСД	–	Несанкционированный доступ
ОС	–	Операционная система
СЗИ	–	Средство защиты информации