ООО Фирма «Инфокрипт»

Vitamin-TPM
Руководство администратора

11485466.72.21.12.191 90

2026

Содержание

Обозначения и сокращения

В настоящем документе используются следующие обозначения и сокращения:

Обозначение	**Описание**
АРМ	Автоматизированное рабочее место
ВАРМ	Виртуальное автоматизированное рабочее место
ОС	Операционная система
ПО	Программное обеспечение

1 Введение

1.1 Область применения

Настоящий документ содержит описание основных возможностей и процесса установки программного обеспечения Vitamin-TPM (далее Vitamin).

Документ предназначен для системного администратора.

1.2 Краткое описание возможностей системы

ПО Vitamin обеспечивает аутентификацию в ВАРМ под управлением ОС Windows с помощью виртуальной смарт-карты (VSC), использующей в качестве защищённого хранилища ключей модуль TPM 2, установленный в АРМ пользователя под управлением ОС SberOS. Аутентификация производится с помощью решения Termidesk VDI по протоколу RDP.

ПО Vitamin предназначено для работы в автоматическом режиме. Вмешательство пользователя не требуется.

2 Назначение и условия применения

2.1 Назначение ПО Vitamin

ПО Vitamin представляет собой драйвер виртуальных смарт-карт на базе безопасного хранилища предназначено для обеспечения аутентификации в ВАРМ под управлением ОС Windows с помощью виртуальной смарт-карты, использующей в качестве защищённого хранилища ключей модуль TPM 2, установленный в АРМ пользователя под управлением ОС SberOS.

2.2 Условия применения ПО Vitamin

Клиентская часть ПО Vitamin устанавливается на компьютеры, удовлетворяющие следующим аппаратным и программным требованиям:

- На АРМ должен быть установлен модуль TPM 2.
- АРМ должно работать под управлением операционной системы SberOS.
- На АРМ должно быть установлено ПО Termidesk.
- ВАРМ должно работать под управлением операционной системы Windows.
- На ВАРМ должно быть установлено ПО Termidesk.

3 Установка программного обеспечения Vitamin

Для того чтобы установить клиентскую часть ПО Vitamin на АРМ под управлением операционной системы SberOS, необходимо выполнить команду:

```
sudo dpkg -i ./vitamintpm-card_0.10_amd64.deb
```

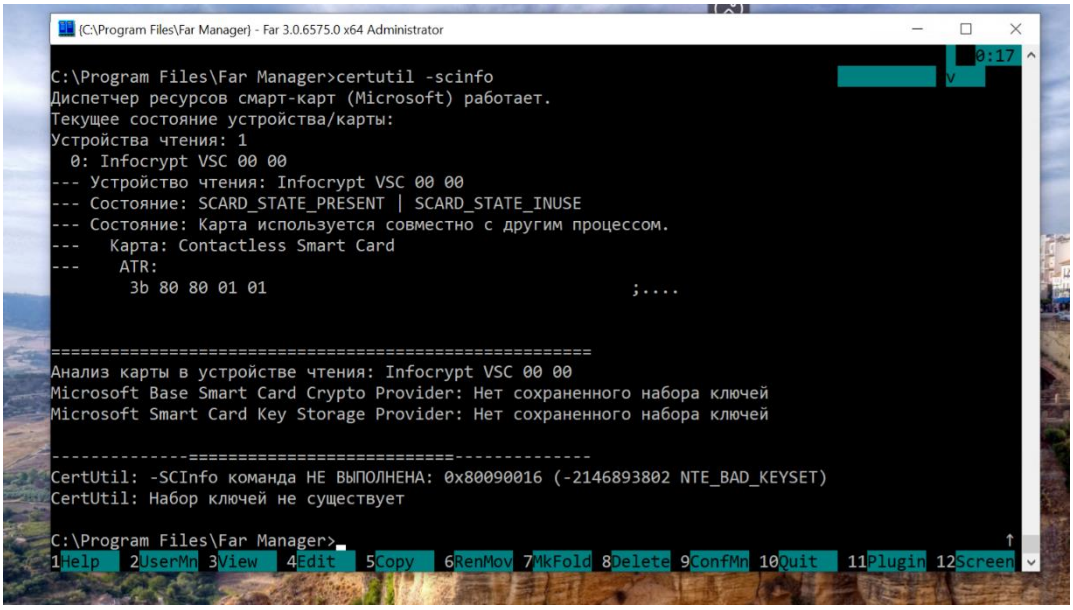
3.1 Подготовка к работе

Для подготовки к работе необходимо выполнить следующие действия:

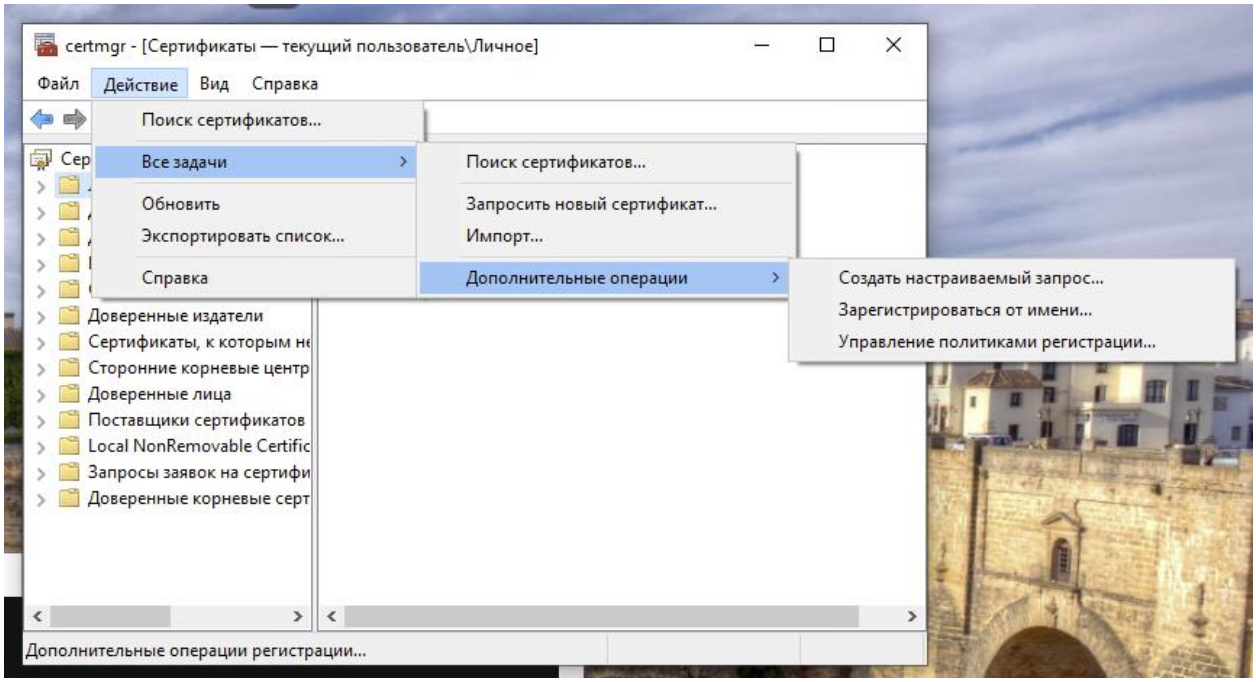
1. На ВАРМ под управлением ОС Windows завести в домене пользователя (например, test3).
2. На АРМ под управлением ОС SberOS проинициализировать модуль TPM 2 с помощью утилиты tpm2_ptool. Создать токен с PIN-кодом.

```
admin1@sberostest03:~$
admin1@sberostest03:~$ tpm2_ptool addtoken --pid=1 --sopin=1234 --userpin=1111 --label=vitamin
admin1@sberostest03:~$ tpm2_ptool addtoken listtokens --pid=1
usage: tpm2_ptool addtoken [-h] --pid PID --sopin SOPIN --userpin USERPIN --label LABEL
                           [--hierarchy-auth HIERARCHY_AUTH] [--path PATH]
tpm2_ptool addtoken: error: the following arguments are required: --sopin, --userpin, --label
admin1@sberostest03:~$ tpm2_ptool listtokens --pid=1
- id: 1
  label: vitamin

admin1@sberostest03:~$ pkcs11-tool --module $LIBTPM -O -l
Using slot 0 with a present token (0x1)
Logging in to "vitamin".
Please enter User PIN:
admin1@sberostest03:~$
```

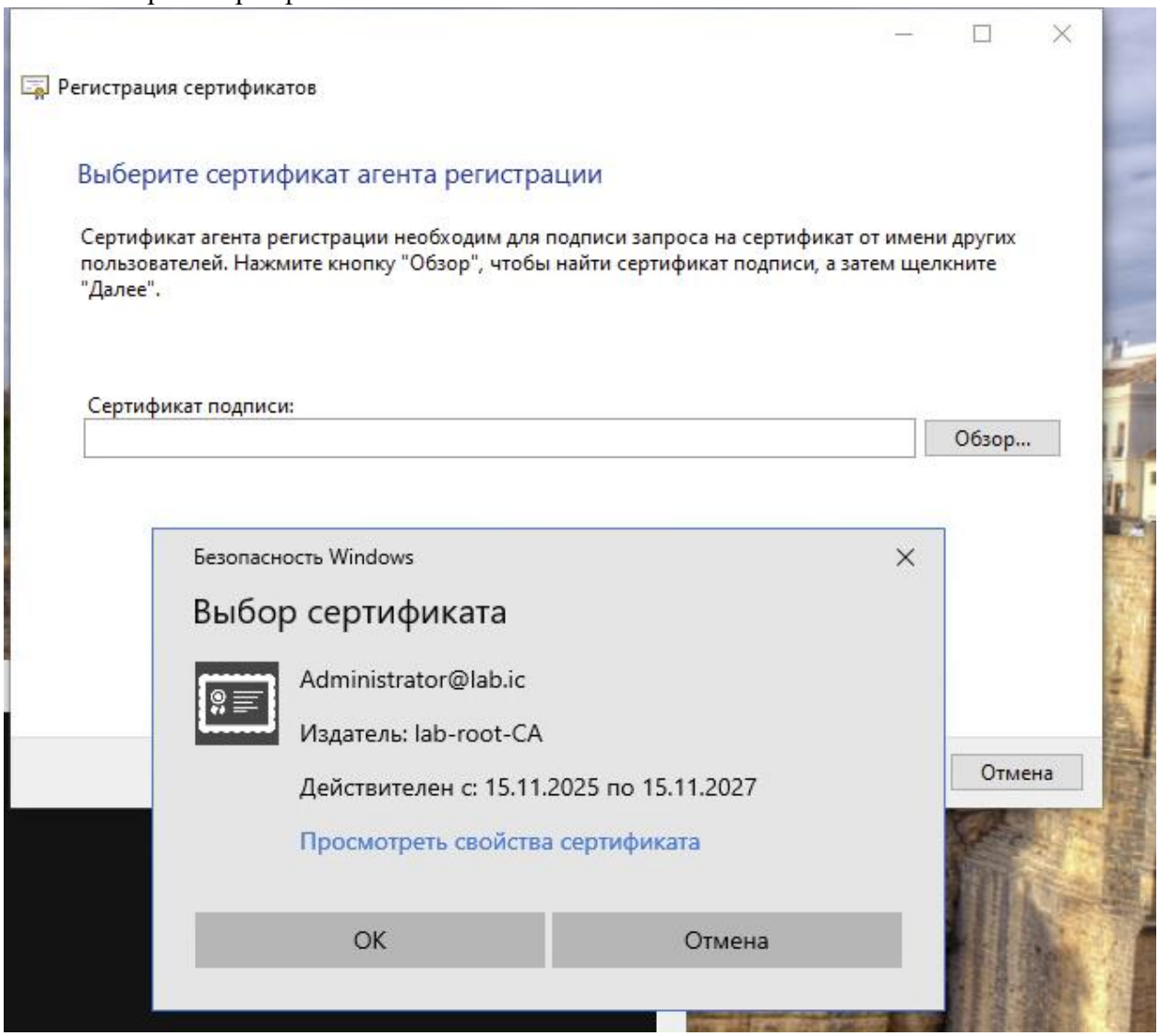
3. С АРМ от имени пользователя Администратор с помощью логина и пароля аутентифицироваться на ВАРМ по протоколу RDP.
4. С помощью команды `certutil -scinfo` удостовериться в наличии виртуальной карты и в отсутствии на ней каких-либо ключей и сертификатов.



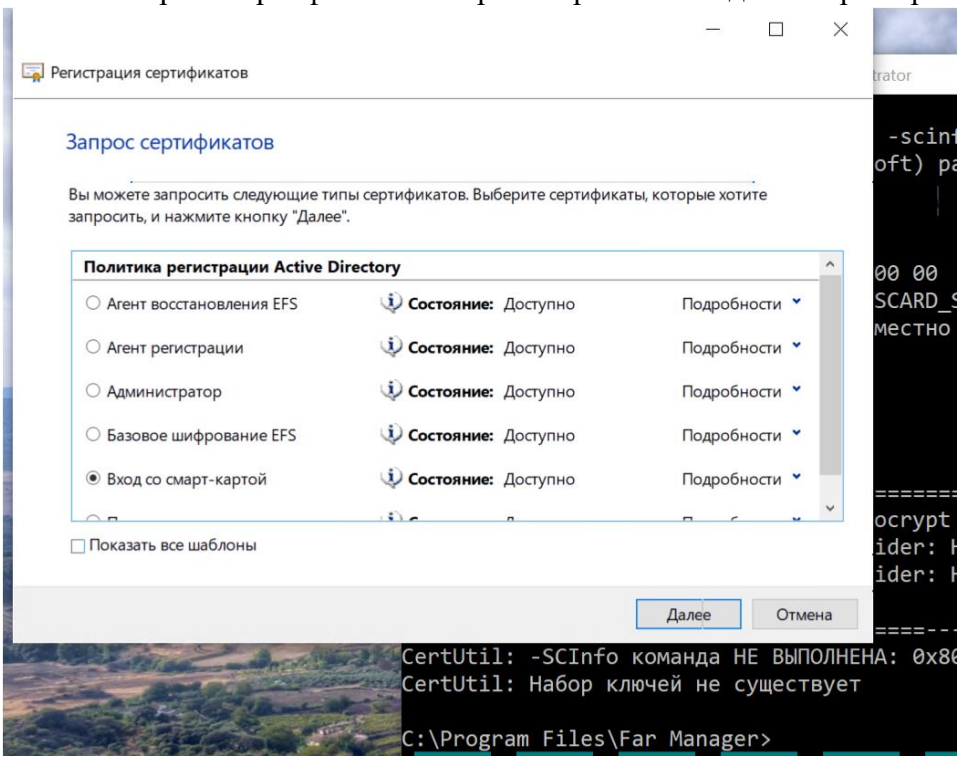
5. Вызвать оснастку certmgr (Win+R -> certmgr.msc). Выбрать пункт «Личное», в меню, «Действие» выбрать «Все задачи» -> «Дополнительные операции» -> «Зарегистрироваться от имени....»



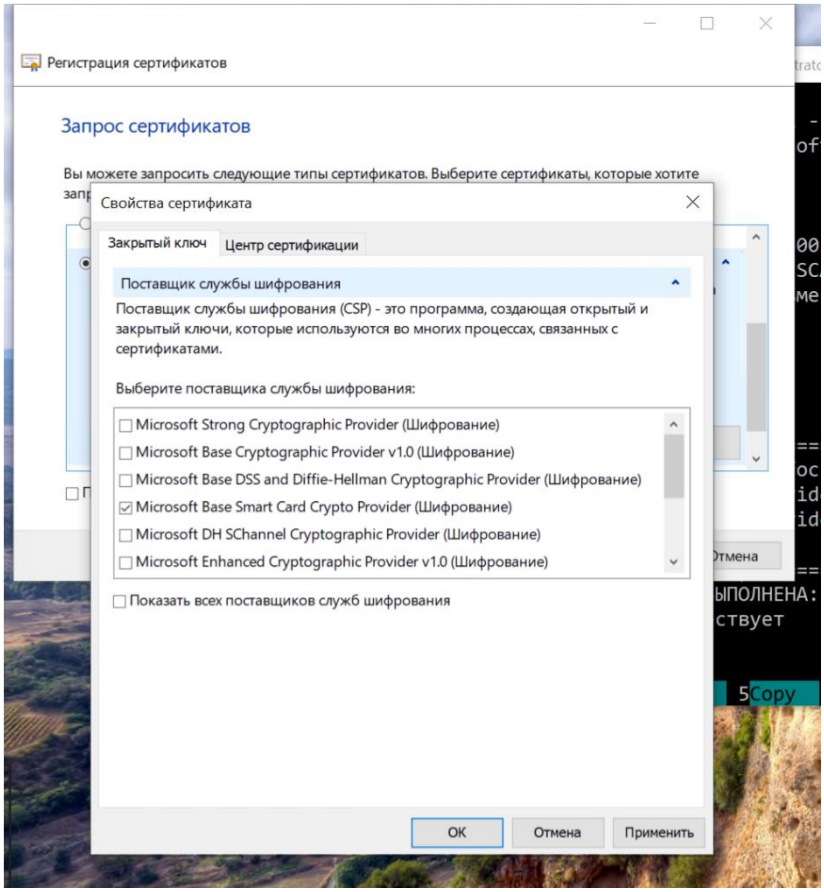
6. В открывшемся окне выбора сертификата агента регистрации нажать кнопку «Обзор» и выбрать сертификат.



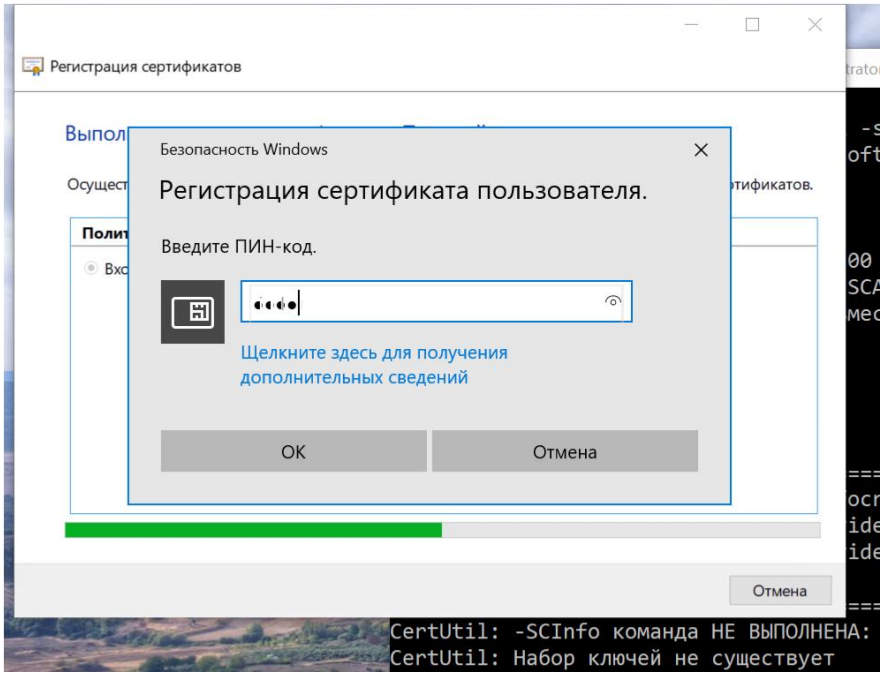
7. Далее в окне запроса сертификатов выбрать вариант «Вход со смарт-картой».



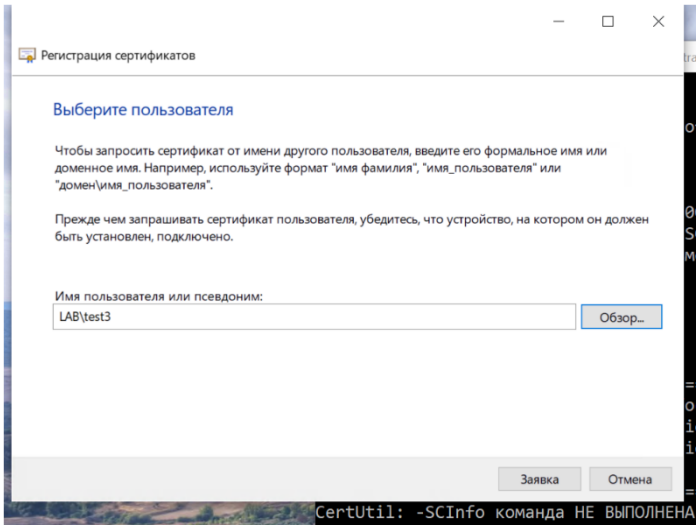
8. В строке «Вход со смарт-картой нажать поле «Подробности» и выбрать единственного поставщика служб шифрования: Microsoft Base Smart Card Crypto Provider.



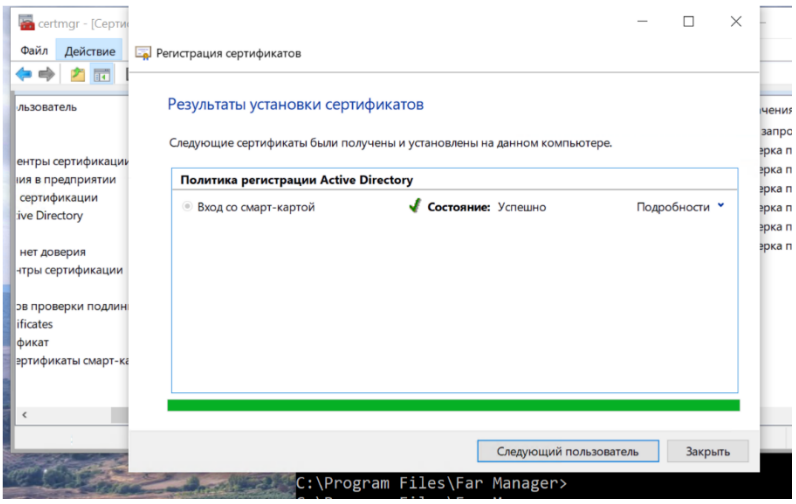
9. При появлении запроса PIN-кода ввести PIN-код, заданный в п. 2.



10. В окне выбора пользователя и ввести «домен\имя пользователя», для пользователя созданного в п. 1, или нажать кнопку «Обзор» и выбрать имя пользователя. Затем нажать кнопку «Заявка».



11. Убедиться, что появилось сообщение о создании сертификата на смарт-карте.

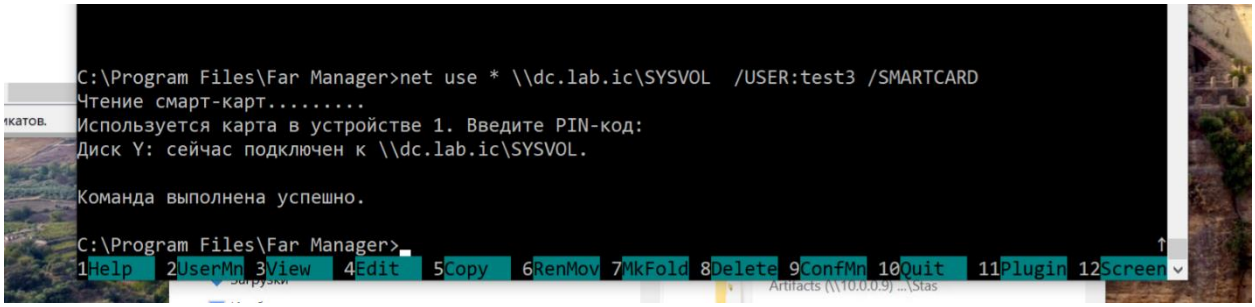


3.2 Проверочные действия

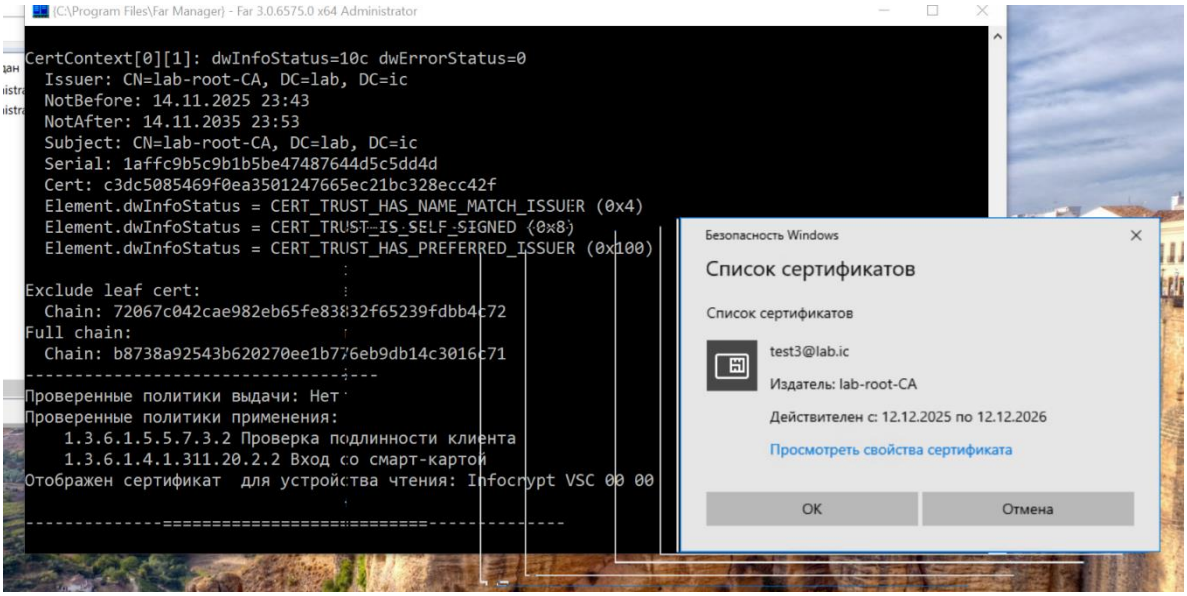
Для того чтобы проверить правильность установки ПО Vitamin, необходимо выполнить следующие действия:

1. На ААРМ под управлением ОС Windows убедиться, что смарт-карта работоспособна, выполнив команду

```
Net use * имя_ресурса /USER:test3 /SMARTCARD
```



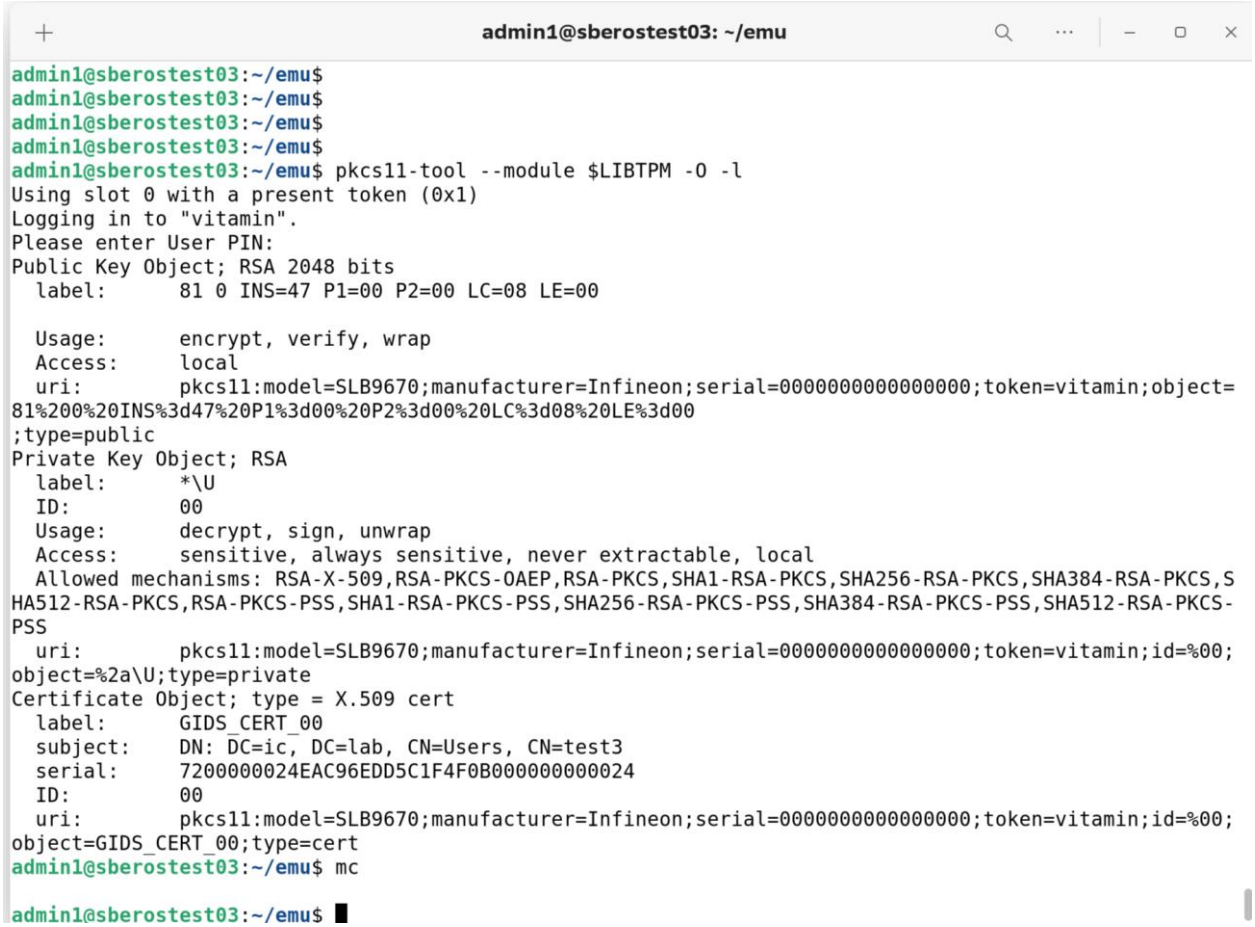
2. На АРМ удостовериться, что на виртуальной карте появился сертификат с нужными свойствами, выполнив команду `certutil -scinfo`.



3. На АРМ под управлением ОС SberOS с помощью утилиты

`pkcs11-tool -O -l`

удостовериться, что появились закрытый и открытый ключи, а также сертификат пользователя. Наличие у открытого ключа полей Access: never extractable , always sensitive означает, что ключ хранится в модуле TPM 2. Поле DN в сертификате соответствует имени пользователя, для которого был выпущен сертификат.



4. Настроить на АРМ протокол Kerberos, задав в файле /etc/krb5.conf следующие параметры:

```
[libdefaults]
default_realm = LAB.IC
        pkinit_kdc_hostname = dc.lab.ic
        pkinit_identities = PKCS11:/usr/lib/x86-64-linux-gnu/pkcs11/libtpm2_pkcs11.so
        pkinit_anchors = FILE:/etc/labroot.crt
        pkinit_eku_checking = kpServerAuth

# The following krb5.conf variables are only for MIT Kerberos.
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true
      rdns = false

# The following libdefaults parameters are only for Heimdal Kerberos.
        fcc-mit-ticketflags = true
udp_preference_limit = 0

[realms]
        LAB.IC = {
            kdc = dc.lab.ic
            master_kdc = dc.lab.ic
            admin_server = dc.lab.ic
            default_domain = lab.ic
            pkinit_identities = PKCS11:/usr/lib/x86_64-linux-gnu/pkcs11/libtpm2_pkcs11.so
            pkinit_anchors = FILE:/etc/labroot.crt
        }
        LAB = {
            kdc = dc.lab.ic
            maater_kdc = dc.lab.ic
            admin_server = dc.lab.ic
            default_domain = lab.ic
            pkinit_identities = PKCS11:/usr/lib/x86_64-linux-gnu/pkcs11/libtpm2_pkcs11.so
            pkinit_anchors = FILE:/etc/labroot.crt
        }

[domain_realm]
        lab.ic = LAB.IC
        .lab.ic = LAB.IC
```

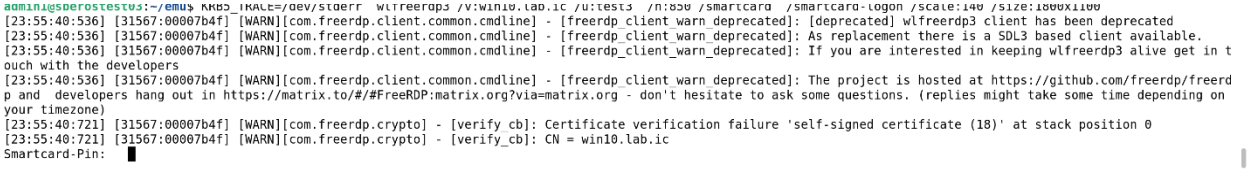
5. На АРМ проверить аутентификацию через Kerberos, выполнив команды:

```
klist

kinit test3

klist
```

Отсутствие ошибок и появление тикета в выводе klist означает, что аутентификация

прошла успешно.

6. Перегрузить АРМ. Аутентифицироваться через RDP-клиент Termidesk в ВАРМ Windows от имени пользователя test3 с помощью смарт-карты, введя PIN-код при соответствующем запросе RDP-клиента.



4 Удаление ПО Vitamin

Для того чтобы удалить ПО Vitamin на АРМ под управлением операционной системы SberOS, необходимо выполнить команду

```
sudo dpkg -r vitamintpm-card_0.10_amd64
```

Лист регистрации изменений

№№ п/п	Дата	Описание изменения, основание для внесения изменения	Автор
1			
2			
3			