

ООО Фирма «Инфокрипт»

**Vitamin-TRM**  
**Руководство администратора**

**11485466.72.21.12.191 90**

## Содержание

1	Введение.....	4
1.1	Область применения .....	4
1.2	Краткое описание возможностей системы .....	4
2	Назначение и условия применения .....	5
2.1	Назначение ПО Vitamin .....	5
2.2	Условия применения ПО Vitamin .....	5
3	Установка программного обеспечения Vitamin .....	6
3.1	Подготовка к работе.....	6
3.2	Проверочные действия .....	11
4	Удаление ПО Vitamin.....	16

## Обозначения и сокращения

В настоящем документе используются следующие обозначения и сокращения:

Обозначение	Описание
<b>АРМ</b>	Автоматизированное рабочее место
<b>ВАРМ</b>	Виртуальное автоматизированное рабочее место
<b>ОС</b>	Операционная система
<b>ПО</b>	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 $LIBTPM -0 -l
Using slot 0 with a present token (0x1)
Logging in to "vitamin".
Please enter User PIN:
admin1@sberostest03:~$ █
```

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.

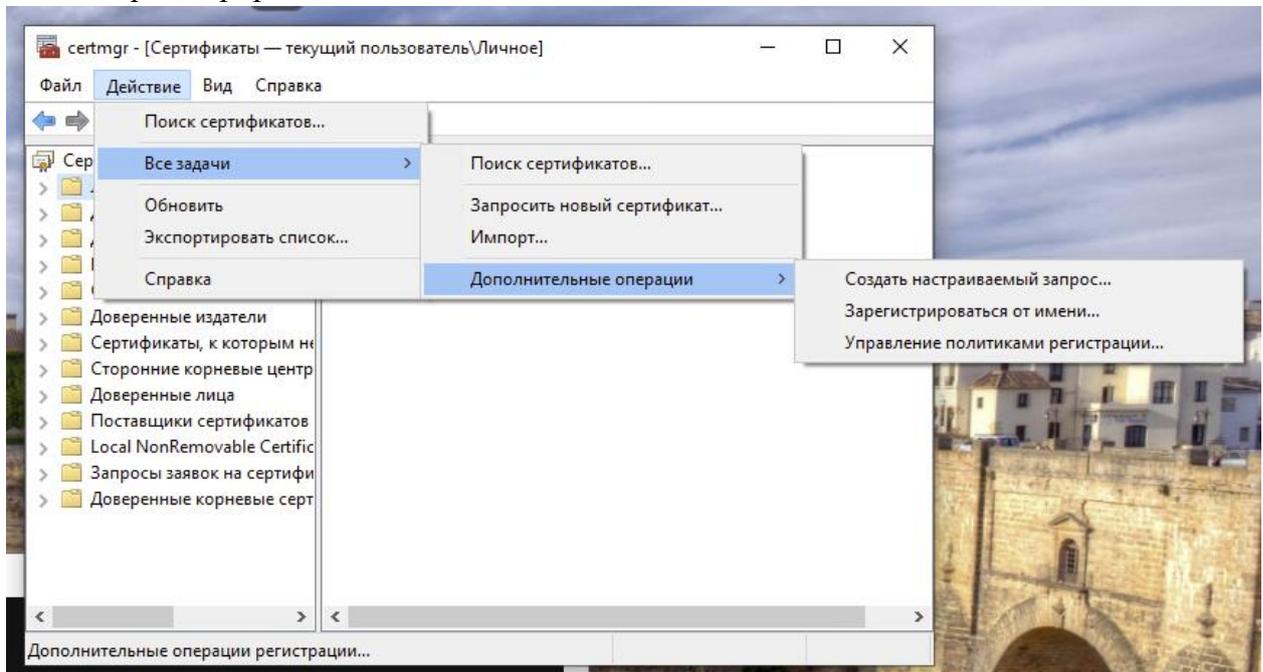
```
(C:\Program Files\Far Manager) - Far 3.0.6575.0 x64 Administrator
C:\Program Files\Far Manager>certutil -scinfo
Диспетчер ресурсов смарт-карт (Microsoft) работает.
Текущее состояние устройства/карты:
Устройства чтения: 1
  0: Infocrypt VSC 00 00
--- Устройство чтения: Infocrypt VSC 00 00
--- Состояние: SCARD_STATE_PRESENT | SCARD_STATE_INUSE
--- Состояние: Карта используется совместно с другим процессом.
--- Карта: Contactless Smart Card
--- ATR:
      3b 80 80 01 01 ;....

=====
Анализ карты в устройстве чтения: Infocrypt VSC 00 00
Microsoft Base Smart Card Crypto Provider: Нет сохраненного набора ключей
Microsoft Smart Card Key Storage Provider: Нет сохраненного набора ключей
-----

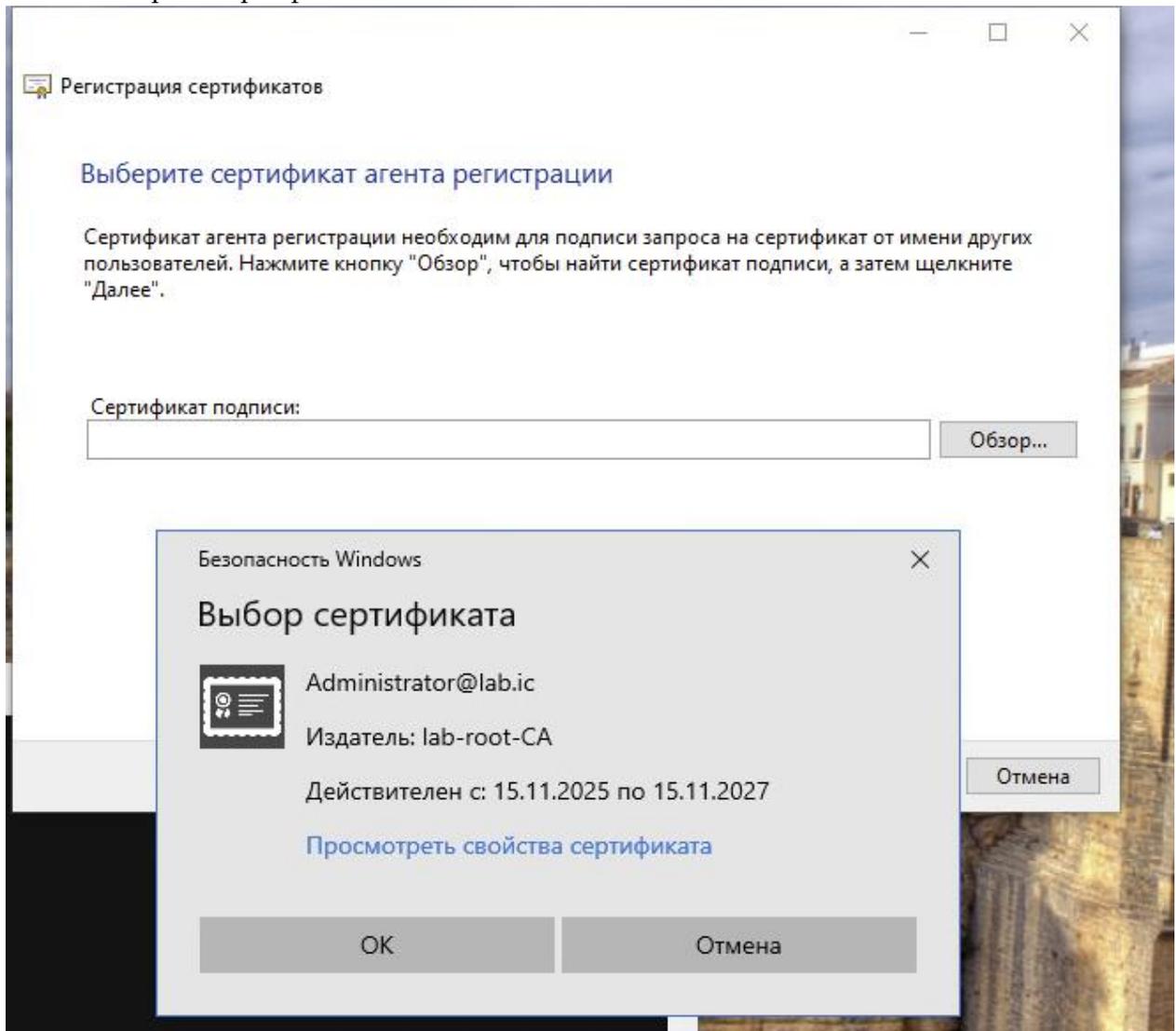
CertUtil: -SCInfo команда НЕ ВЫПОЛНЕНА: 0x80090016 (-2146893802 NTE_BAD_KEYSET)
CertUtil: Набор ключей не существует

C:\Program Files\Far Manager>
1|help 2|UserMn 3|view 4|edit 5|Copy 6|RenMov 7|MkFold 8>Delete 9|ConfMn 10|Quit 11|Plugin 12|Screen
```

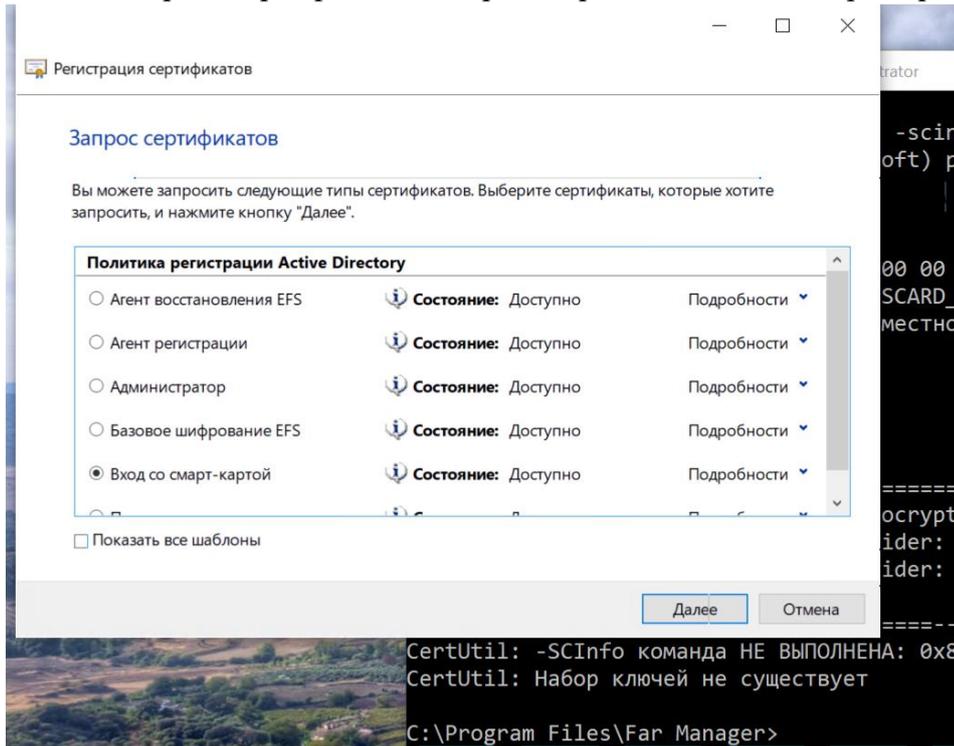
5. Вызвать оснастку certmgr (Win+R -> certmgr.msc). Выбрать пункт «Личное», в меню, «Действие» выбрать «Все задачи» -> «Дополнительные операции» -> «Зарегистрироваться от имени....»



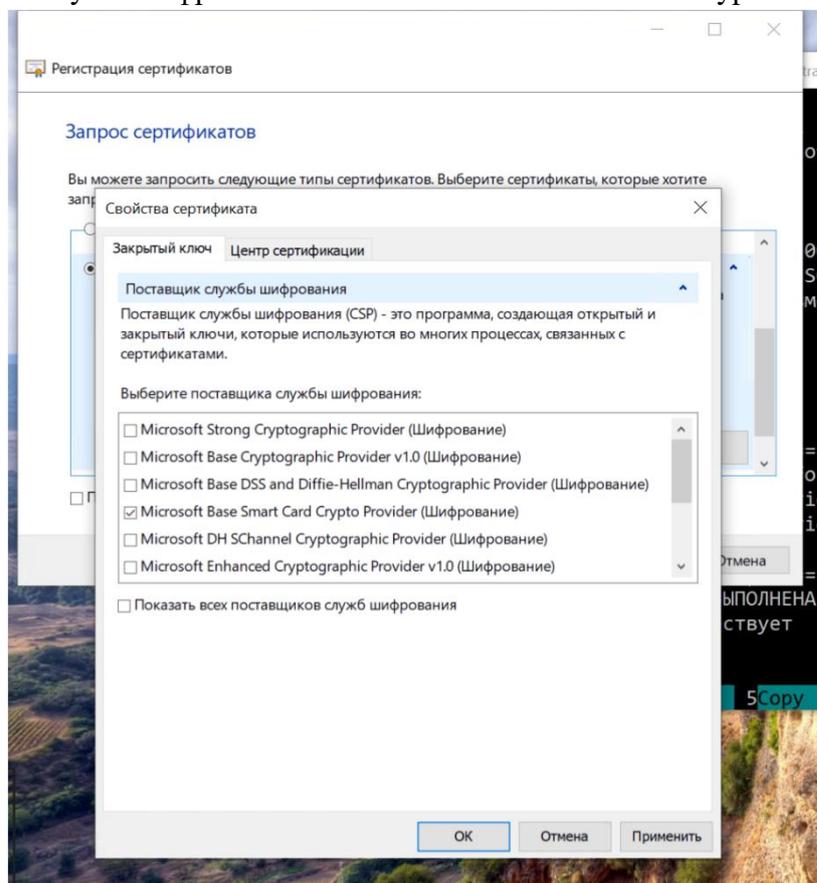
6. В открывшемся окне выбора сертификата агента регистрации нажать кнопку «Обзор» и выбрать сертификат.



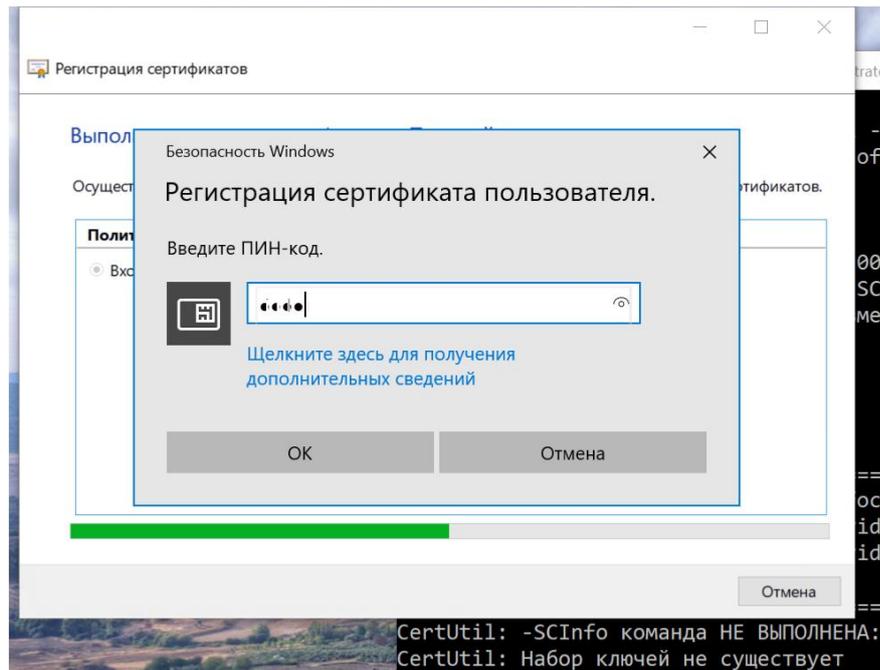
7. Далее в окне запроса сертификатов выбрать вариант «Вход со смарт-картой».



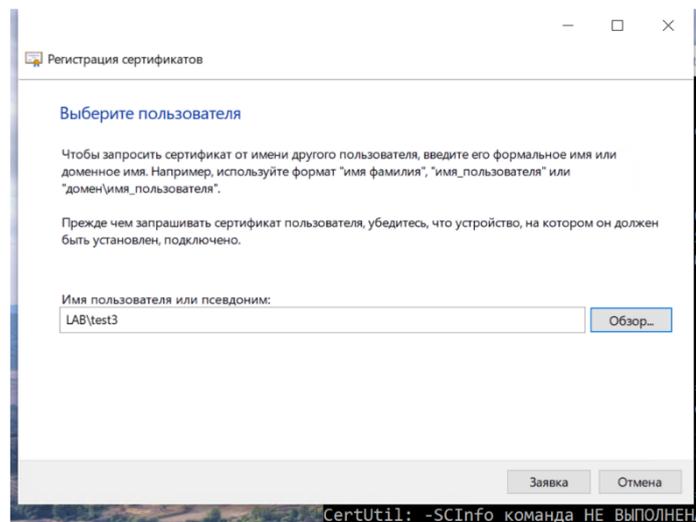
8. В строке «Вход со смарт-картой» нажать поле «Подробнее» и выбрать единственного поставщика служб шифрования: Microsoft Base Smart Card Crypto Provider.



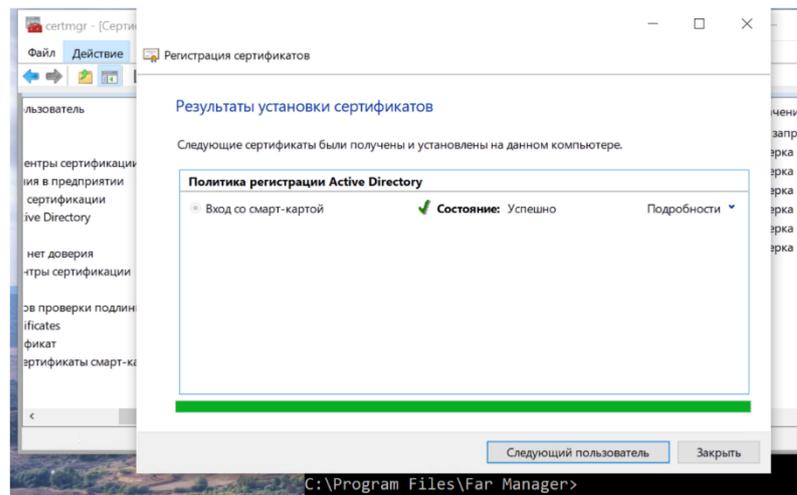
9. При появлении запроса PIN-кода ввести PIN-код, заданный в п. 2.



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.

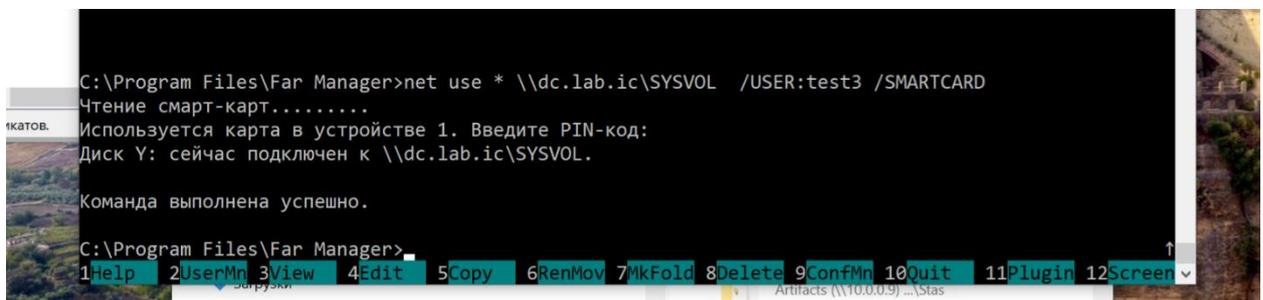


### 3.2 Проверочные действия

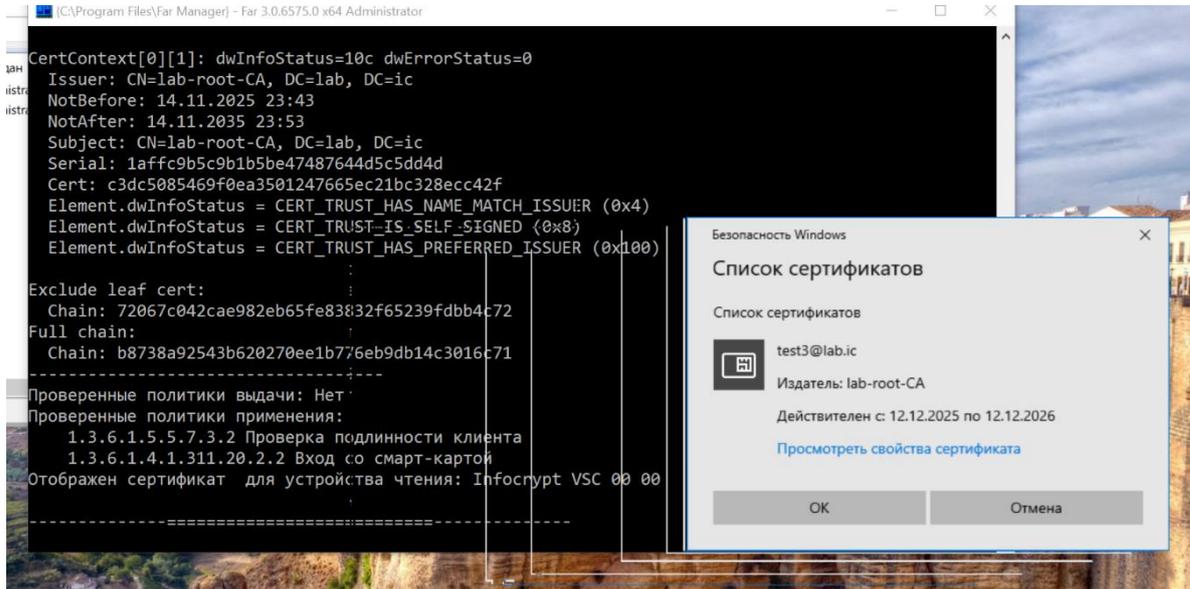
Для того чтобы проверить правильность установки ПО Vitamin, необходимо выполнить следующие действия:

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

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



2. На ВАРМ 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.

```

+ admin1@sberostest03: ~/emu
admin1@sberostest03:~/emu$
admin1@sberostest03:~/emu$
admin1@sberostest03:~/emu$
admin1@sberostest03:~/emu$
admin1@sberostest03:~/emu$ pkcs11-tool --module $LIBTPM -O -l
Using slot 0 with a present token (0x1)
Logging in to "vitamin".
Please enter User PIN:
Public Key Object; RSA 2048 bits
  label:      81 0 INS=47 P1=00 P2=00 LC=08 LE=00

Usage:      encrypt, verify, wrap
Access:     local
uri:        pkcs11:model=SLB9670;manufacturer=Infineon;serial=0000000000000000;token=vitamin;object=
81%200%20INS%3d47%20P1%3d00%20P2%3d00%20LC%3d08%20LE%3d00
;type=public
Private Key Object; RSA
  label:      *\U
  ID:         00
Usage:      decrypt, sign, unwrap
Access:     sensitive, always sensitive, never extractable, local
Allowed mechanisms: RSA-X-509,RSA-PKCS-0AEP,RSA-PKCS,SHA1-RSA-PKCS,SHA256-RSA-PKCS,SHA384-RSA-PKCS,S
HA512-RSA-PKCS,RSA-PKCS-PSS,SHA1-RSA-PKCS-PSS,SHA256-RSA-PKCS-PSS,SHA384-RSA-PKCS-PSS,SHA512-RSA-PKCS-
PSS
  uri:        pkcs11:model=SLB9670;manufacturer=Infineon;serial=0000000000000000;token=vitamin;id=%00;
object=%2a\U;type=private
Certificate Object; type = X.509 cert
  label:      GIDS_CERT_00
  subject:    DN: DC=ic, DC=lab, CN=Users, CN=test3
  serial:     7200000024EAC96EDD5C1F4F0B00000000024
  ID:         00
  uri:        pkcs11:model=SLB9670;manufacturer=Infineon;serial=0000000000000000;token=vitamin;id=%00;
object=GIDS_CERT_00;type=cert
admin1@sberostest03:~/emu$ mc
admin1@sberostest03:~/emu$ █

```

4. Настроить на APM 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 APM проверить аутентификацию через Kerberos, выполнив команды:

```
klist
kinit test3
klist
```

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

прошла успешно.

```

+ admin1@sberostest03: ~
admin1@sberostest03:~$ klist
klist: No credentials cache found (filename: /tmp/krb5cc_1000)
admin1@sberostest03:~$ kinit test3
vitamin                               PIN:
admin1@sberostest03:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: test3@LAB.IC

Valid starting      Expires            Service principal
12.12.2025 00:01:53 12.12.2025 10:01:53  krbtgt/LAB.IC@LAB.IC
        renew until 13.12.2025 00:01:49
admin1@sberostest03:~$ █

```

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

```

admin1@sberostest03:~/emulx_krb5$ kinit=dev/staerr wlfreerdp /v:win10.lab.ic /u:test3 /n:550 /smartcard /smartcard-logout /scale:100 /size:1800x1100
[23:55:40:536] [31567:00007b4f] [WARN][com.freerdp.client.common.cmdline] - [freerdp_client_warn_deprecated]: [deprecated] wlfreerdp3 client has been deprecated
[23:55:40:536] [31567:00007b4f] [WARN][com.freerdp.client.common.cmdline] - [freerdp_client_warn_deprecated]: As replacement there is a SDL3 based client available.
[23:55:40:536] [31567:00007b4f] [WARN][com.freerdp.client.common.cmdline] - [freerdp_client_warn_deprecated]: If you are interested in keeping wlfreerdp3 alive get in touch with the developers
[23:55:40:536] [31567:00007b4f] [WARN][com.freerdp.client.common.cmdline] - [freerdp_client_warn_deprecated]: The project is hosted at https://github.com/freerdp/freerdp and developers hang out in https://matrix.to/#/#FreeRDP:matrix.org?via=matrix.org - don't hesitate to ask some questions. (replies might take some time depending on your timezone)
[23:55:40:721] [31567:00007b4f] [WARN][com.freerdp.crypto] - [verify_cb]: Certificate verification failure 'self-signed certificate (18)' at stack position 0
[23:55:40:721] [31567:00007b4f] [WARN][com.freerdp.crypto] - [verify_cb]: CN = win10.lab.ic
Smartcard-Pin: █

```

## **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

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