

Настройка двухфакторной аутентификации в домене Windows AD

Служба обеспечения совместимости <gost@basealt.ru>, Константин Белаш

Version 1.3, 07.10.2022

Оглавление

1. Общая информация	1
2. Базовая конфигурация стенда	2
2.1. Общие требования к стенду	2
2.2. Требования к токенам и смарт-картам	2
2.3. Требования к сертификату пользователя домена Windows AD	2
2.4. Информация о пользователях домена	3
2.5. Проверка работы ПК клиента в домене Windows AD	3
3. Установка и настройка ПО для работы с токенами	5
3.1. Настройка Polkit	5
3.2. Проверка работы PC/SC интерфейса	6
3.3. Проверка работы библиотек вендоров PKCS#11	7
3.3.1. ESMART Token	7
3.3.2. Rutoken ECP	7
3.3.3. JaCarta-2 SE	8
4. Настраиваем PKINIT на клиенте	9
4.1. Настройка и проверка Kerberos	9
4.1.1. Рутокен ECP	10
4.1.2. ESMART Token	10
4.1.3. JaCarta-2 SE	10
4.1.4. Отладка Kerberos	11
4.2. Настройка sssd	11
4.2.1. p11_child. Проверка работы sssd с токенами	11
4.2.1.1. Рутокен ECP	11
4.2.1.2. ESMART Token	12
4.2.1.3. JaCarta-2 SE	12
4.2.2. sssd.conf. Настройка службы sssd	12
5. Проверяем 2ФА в текстовой консоли	14
5.1. Рутокен ECP	14
5.2. ESMART Token	14
5.3. JaCarta-2 SE	14
6. Проверяем 2ФА в графическом сеансе	16
6.1. Рутокен ECP	16
6.2. ESMART Token	19
6.3. JaCarta-2 SE	23
7. Проверка отзыва сертификата	28
8. Отладка sssd	29
9. Полезные ссылки	30

1. Общая информация

Настоящий документ можно считать практическим руководством для конечного пользователя с методическими рекомендациями по контролю за успешностью выполнения настройки.

Из этого документа станет понятно, как настроить двухфакторную аутентификацию (2ФА) в домене Windows AD (Active Directory), где в качестве клиента выступает ОС «Альт Рабочая станция (К) 10», а в качестве контроллера домена используется ОС Microsoft Windows Server 2012R или 2019.

В процессе настройки и тестирования мы убедимся, что токены, содержащие криптографическую информацию, позволяют зарегистрироваться в домене при корректном вводе PIN-кода, без дополнительных способов аутентификации (например, ввода пароля), а также убедиться в обратном, что при вводе некорректного PIN-кода в аутентификации будет отказано. Также в аутентификации будет отказано, если сертификат отозван Удостоверяющим Центром (УЦ).

Под криптографической информацией на токене здесь явно подразумеваются: сертификат пользователя, выданный УЦ, открытый и закрытый ключи пользователя.

С теоретической информацией по доменной двухфакторной аутентификации можно ознакомиться в документе «Двухфакторная аутентификация в доменной инфраструктуре ОС Альт. Общая информация.».

2. Базовая конфигурация стенда

2.1. Общие требования к стенду

Стенд будет состоять из контроллера домена Windows AD и ПК клиента домена.

Стенд должен удовлетворять следующим условиям:

- ПК клиента должен быть введён в домен Windows AD
- На контроллере домена должны быть заведены учётные записи пользователей домена
- Для домена Windows AD настроен Удостоверяющий центр (УЦ)
- В УЦ для контроллера домена Windows AD выпущен сертификат KDC (key distribution center)
- В УЦ для пользователей домена Windows AD выпущены сертификаты
- Сертификаты пользователей хранятся на токене или смарт-карте
- В домене Windows AD работает служба проверки сертификатов OCSP
- OCSP служба должна поддерживать «Nonce requests» (использование одноразового кода в запросе, <https://ru.wikipedia.org/wiki/OCSP>)

2.2. Требования к токенам и смарт-картам

Используются токены и смарт-карты, имеющие следующие характеристики:

- токены (смарт-карты) аппаратно выполняют криптографические функции (без использования программного криптопровайдера)
- закрытый ключ, сгенерированный на токене, не может быть экспортирован
- мультислотовые токены (например JaCarta-2 SE) имеют уникальные метки для каждого слота

Токены, используемые в настоящем руководстве: **Rutoken ECP**, **JaCarta-2 SE**, **ESMART Token**.

2.3. Требования к сертификату пользователя домена Windows AD

- закрытый ключ для сертификата должен быть сгенерирован на токене
- сертификат должен содержать ключ (EKU, Extended Key Usage), который позволяет использовать сертификат для аутентификации клиента - **clientAuth** (TLS Web Client Authentication, OID 1.3.6.1.5.5.7.3.2)
- сертификат должен содержать альтернативное имя субъекта (SAN, Subject Alternative Name), в котором указано имя субъекта-пользователя (UPN)
- сертификат должен иметь данные о ресурсе, где будет проверяться валидность сертификата (OCSP служба)

- сертификат должен также находиться в профиле пользователя, в базе LDAP

2.4. Информация о пользователях домена

Для токенов **Rutoken ECP**, **JaCarta-2 SE**, **ESMART Token** в домене были созданы соответствующие пользователи:

- `rt_win`: Rutoken ECP
- `jc_win`: JaCarta-2 SE
- `es_win`: ESMART Token

2.5. Проверка работы ПК клиента в домене Windows AD

Вводим ОС Альт Рабочая станция в домен:

- если используется ОС Альт Рабочая станция К — <https://docs.altlinux.org/ru-RU/index.html#alt-kworkstation>, п. «Ввод рабочей станции в домен Active Directory»
- если используется ОС Альт Рабочая станция — <https://docs.altlinux.org/ru-RU/index.html#alt-workstation>, п. «Ввод рабочей станции в домен Active Directory»

Заходим на ПК клиента с доменной учётной записью и проверяем получение билета Kerberos:

```
rt_win@alt-p10 Рабочий стол $ klist
Ticket cache: KEYRING:persistent:53801602:krb_ccache_jYX1Bzy
Default principal: rt_win@TEST5.ALT

Valid starting      Expires            Service principal
17.06.2022 15:16:55  18.06.2022 01:16:55  krbtgt/TEST5.ALT@TEST5.ALT
    renew until 24.06.2022 15:16:55
```

```
alt-p10 ~ # net ads testjoin
Join is OK
```

```
alt-p10 ~ # net ads info
LDAP server: 10.33.33.200
LDAP server name: w12r2-vm340.test5.alt
Realm: TEST5.ALT
Bind Path: dc=TEST,dc=ALT
LDAP port: 389
Server time: Пт, 17 июн 2022 15:20:25 MSK
KDC server: 10.33.33.200
Server time offset: 0
```

Last machine account password change: Пт, 17 июн 2022 15:15:42 MSK

```
alt-p10 ~ # getent passwd rt_win  
rt_win:*:53801602:53800513:rt_win:/home/TEST5.ALT/rt_win:/bin/bash
```

3. Установка и настройка ПО для работы с токенами

Настройка выполняется на обновлённой пакетной базе и последнем ядре из репозитория:

```
$ su-
# apt-get update
# apt-get dist-upgrade
# update-kernel
# reboot
```

Для работы с токенами необходимо установить следующие пакеты:

```
# apt-get install librtpkcs11esp libjcpkcs11 isbc-pkcs11 \
  opencsc pcsc-lite-ccid pcsc-lite pcsc-tools gnutls-utils \
  libp11 libp11-kit
```

- **librtpkcs11esp**, **libjcpkcs11**, **isbc-pkcs11** — библиотеки PKCS#11 вендоров токенов: Актив, Аладдин и ISBC, соответственно;
- **opencsc**, **pcsc-lite-ccid**, **pcsc-lite**, **pcsc-tools**, **gnutls-utils** — утилиты и библиотеки, необходимые для обеспечения работы интерфейсов PC/SC(+CCID) и PKCS#11;
- **libp11** — библиотека для работы с токенами в openssl (openssl engine);
- **libp11-kit** — прокси-библиотека для работы с библиотеками вендоров токенов по протоколу PKCS#11.

Если каких-то пакетов в репозитории нет или с ними выявлены проблемы, необходимо установить их с сайта производителя:

- Актив Рутокен (librtpkcs11esp): <https://www.rutoken.ru/support/download/pkcs/>
- Аладдин JaCarta (libjcpkcs11-2): https://www.aladdin-rd.ru/support/downloads/jacarta_client (а для x86_64 теперь ещё и в составе «Единого Клиента JaCarta»)
- ISBC ESMART (libisbc_pkcs11_main): <https://esmart.ru/download/>

3.1. Настройка Polkit

По умолчанию Policy Kit позволяет работать с токенами только в активном сеансе (после входа в ОС) и только локальному пользователю. Чтобы можно было работать с токенами на этапе логина доменных пользователей, необходимо поменять все запреты ">no<" на разрешения ">yes<" в файле `/usr/share/polkit-1/actions/org.debian.pcsc-lite.policy`.

```
# sed -iE 's:>no<:>yes<:' /usr/share/polkit-1/actions/org.debian.pcsc-lite.policy
```

В итоге конфигурационный файл polkit примет следующий вид:

```
# cat /usr/share/polkit-1/actions/org.debian.pcsc-lite.policy
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE policyconfig PUBLIC
  "-//freedesktop//DTD PolicyKit Policy Configuration 1.0//EN"
  "http://www.freedesktop.org/standards/PolicyKit/1.0/policyconfig.dtd">
<policyconfig>
  <vendor>The PCSC-Lite Project</vendor>
  <vendor_url>https://pcsc-lite.apdu.fr/</vendor_url>
  <!-- <icon_name>smart-card</icon_name> -->
  <action id="org.debian.pcsc-lite.access_pcsc">
    <description>Access to the PC/SC daemon</description>
    <message>Authentication is required to access the PC/SC daemon</message>
    <defaults>
      <allow_any>yes</allow_any>
      <allow_inactive>yes</allow_inactive>
      <allow_active>yes</allow_active>
    </defaults>
  </action>
  <action id="org.debian.pcsc-lite.access_card">
    <description>Access to the smart card</description>
    <message>Authentication is required to access the smart card</message>
    <defaults>
      <allow_any>yes</allow_any>
      <allow_inactive>yes</allow_inactive>
      <allow_active>yes</allow_active>
    </defaults>
  </action>
</policyconfig>
```

3.2. Проверка работы PC/SC интерфейса

Работу интерфейса PC/SC обеспечивает служба **pcscd.service**, которая запускается через одноимённый сокет — **pcscd.socket**.

Включаем **pcscd.socket**:

```
# systemctl enable --now pcscd.socket
Created symlink /etc/systemd/system/sockets.target.wants/pcscd.socket →
/lib/systemd/system/pcscd.socket.
```

Убеждаемся, что токен виден в выводе утилиты **pcsc_scan**, запущенной с правами пользователя, и однозначно определяется его модель:

```
$ pcsc_scan -r
Using reader plug'n play mechanism
```



```
Scanning present readers...
0: Aktiv Rutoken ECP 00 00
1: ESMART Token GOST [ESMART Token] 01 00
2: Aladdin R.D. JaCarta 02 00
```

Если в выводе команды `pcsc_scan -r` вы не видите токенов, то для решения этого вопроса обратитесь к документу «Методика тестирования токенов» (доступна по запросу в службу обеспечения совместимости).

3.3. Проверка работы библиотек вендоров PKCS#11

Библиотеки PKCS#11 являются основой для работы с токенами и будут использоваться всеми компонентами, участвующими в 2ФА. В общем виде работа с библиотеками вендоров токенов выглядит следующим образом:

```
$ pkcs11-tool --module путь_до_библиотеки_вендора --list-token-slots
```

Если в выводе команды `pcsc_scan -r` вы не видите токенов, то для решения этого вопроса обратитесь к документу «Методика тестирования токенов» (доступна по запросу в службу обеспечения совместимости).

3.3.1. ESMART Token

```
$ pkcs11-tool --module /usr/lib64/libisbc_pkcs11_main.so --list-token-slots
Available slots:
Slot 0 (0x1): ESMART Token GOST [ESMART Token] 00 00
  token label      : esmart_64
  token manufacturer : ISBC
  token model      : ESMART Token
  token flags      : login required, rng, token initialized, PIN initialized
  hardware version : 0.0
  firmware version : 2.4
  serial num       : 206F6060C102
  pin min/max     : 4/8
```

3.3.2. Rutoken ECP

```
$ pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so --list-token-slots
Available slots:
Slot 0 (0x1): Aktiv Rutoken ECP 01 00
  token label      : RuTokenECP
  token manufacturer : Aktiv Co.
  token model      : Rutoken ECP
  token flags      : login required, rng, SO PIN to be changed, token initialized,
  PIN initialized, user PIN to be changed
  hardware version : 20.5
```

```
firmware version : 23.2
serial num       : 3ce96775
pin min/max     : 6/32
```

3.3.3. JaCarta-2 SE

```
$ pkcs11-tool --module /usr/lib64/libjcpkcs11-2.so --list-token-slots
Available slots:
Slot 0 (0x1ffff): Aladdin R.D. JaCarta 02 00
  token label       : STANDART.SE
  token manufacturer : Aladdin R.D.
  token model       : JaCarta GOST 2.0
  token flags       : login required, rng, token initialized, PIN initialized, other
  flags=0x800
  hardware version  : 1.0
  firmware version  : 2.55
  serial num        : 6082023848937678
  pin min/max       : 6/32
Slot 1 (0x2ffff): Aladdin R.D. JaCarta 02 00
  token label       : jacarta-slot-laser
  token manufacturer : Aladdin R.D.
  token model       : JaCarta Laser
  token flags       : login required, token initialized, PIN initialized
  hardware version  : 1.0
  firmware version  : 1.0
  serial num        : 6082023848937678
  pin min/max       : 4/10
```

4. Настраиваем PKINIT на клиенте

4.1. Настройка и проверка Kerberos

Копируем сертификат УЦ на ПК доменного пользователя, в каталог `/etc/pki/tls/certs` (сертификат УЦ предварительно экспортирован в общий каталог `//win19/sysvol/` на контроллере домена как `ca.cer`).

```
alt-p10 ~ # smbclient //w12r2-vm340/sysvol/ -U Администратор
Enter TEST\Администратор's password:
Try "help" to get a list of possible commands.
smb: \> get ca.cer /etc/pki/tls/certs/cacert.pem
```

Добавляем в конфигурационный файл Kerberos (`/etc/krb5.conf`), в секцию `[realms]`, следующее содержимое:

```
[realms]
TEST5.ALT = {
    pkinit_anchors = FILE:/etc/pki/tls/certs/cacert.pem
    pkinit_kdc_hostname = w12r2-vm340.test5.alt
    pkinit_eku_checking = kpServerAuth
    pkinit_cert_match = <ISSUER>.*test-W12R2-VM340-CA
}
```

`pkinit_anchors` — путь к сертификату УЦ

`pkinit_kdc_hostname` — DNS имя контроллера домена

`pkinit_eku_checking` — будет ли проверяться наличие расширенного использования ключа (EKU, Extended key usage). В данном случае в сертификате контроллера домена проверятся наличие EKU, которое предназначено для аутентификации на стороне сервера

`pkinit_cert_match` — фильтр выбора сертификата (если их на токене несколько). В данном случае выбираем сертификат, строка издателя которого оканчивается именем контроллера домена (`test-W12R2-VM340-CA`)

Итоговый конфигурационный файл Kerberos:

```
alt-p10 ~ # cat /etc/krb5.conf | grep -viE '(\#|\$)'
```

```
includedir /etc/krb5.conf.d/
[logging]
[libdefaults]
default_realm = TEST5.ALT
dns_lookup_kdc = true
dns_lookup_realm = false
ticket_lifetime = 24h
```

```

renew_lifetime = 7d
forwardable = true
rdns = false
default_ccache_name = KEYRING:persistent:%{uid}
[realms]
TEST5.ALT = {
    pkinit_anchors = FILE:/etc/pki/tls/certs/cacert.pem
    pkinit_kdc_hostname = w12r2-vm340.test5.alt
    pkinit_eku_checking = kpServerAuth
    pkinit_cert_match = <ISSUER>.*test-W12R2-VM340-CA
}
[domain_realm]

```

Далее проверяем получение билета Kerberos.

4.1.1. Рутокен ECP

```

user@alt-p10 ~ $ kinit -X X509_user_identity=PKCS11:librtpkcs11ecp.so rt_win
RuTokenECP PIN:
user@alt-p10 ~ $ klist
Ticket cache: KEYRING:persistent:500:500
Default principal: rt_win@TEST5.ALT

Valid starting Expires Service principal
20.06.2022 19:32:54 21.06.2022 05:32:54 krbtgt/TEST5.ALT@TEST5.ALT
renew until 27.06.2022 19:32:46

```

4.1.2. ESMART Token

```

user@alt-p10 ~ $ kinit -X X509_user_identity=PKCS11:libisbc_pkcs11_main.so es_win
esmart_64 PIN:
user@alt-p10 ~ $ klist
Ticket cache: KEYRING:persistent:500:krb_ccache_iXXI94
Default principal: es_win@TEST5.ALT

Valid starting Expires Service principal
20.06.2022 19:33:36 21.06.2022 05:33:36 krbtgt/TEST5.ALT@TEST5.ALT
renew until 27.06.2022 19:33:26

```

4.1.3. JaCarta-2 SE

Здесь необходимо дополнительно указать метку слота, так как токен мультислотовый.

```

user@alt-p10 ~ $ kinit \
-X X509_user_identity='PKCS11:libjcpkcs11-2.so:token=jacarta-slot-laser' jc_win
jacarta-slot-laser PIN:
user@alt-p10 ~ $ klist

```

```
Ticket cache: KEYRING:persistent:500:krb_ccache_ppoB6Qg
Default principal: jc_win@TEST5.ALT
```

```
Valid starting      Expires            Service principal
20.06.2022 19:34:46 21.06.2022 05:34:46 krbtgt/TEST5.ALT@TEST5.ALT
    renew until 27.06.2022 19:34:26
```

4.1.4. Отладка Kerberos

Если при проверке Kerberos возникают ошибки, то для более полной информации по процессу PKINIT добавьте опцию вывода отладочной информации в консоль — **KRB5_TRACE=/dev/stdout**. Команда получения билета Kerberos с отладкой:

```
user@alt-p10 ~ $ KRB5_TRACE=/dev/stdout \
  kinit \
  -X X509_user_identity='PKCS11:libjcpkcs11-2.so:token=jakarta-slot-laser' jc_win
```

4.2. Настройка sssd

После ввода ПК клиента в домен Windows AD за аутентификацию отвечает служба **sss**. Утилита **p11_child**, входящая в состав пакета **sss**, обеспечивает доступ к сертификату на токене.

4.2.1. p11_child. Проверка работы sssd с токенами

Убедимся, что служба sssd видит сертификат на токене.

4.2.1.1. Рутокен ЕСП

```
user@alt-p10 ~ $ /usr/libexec/sss/p11_child \
  --ca_db=/etc/pki/tls/certs/cacert.pem --pre
RuTokenЕСP
/usr/lib64/pkcs11/librtpkcs11esp.so
6C652D52545F4A435F45535F323034382D63633831343231332D653232302D34362D30353632355F45
le-RT_JC_ES_2048-cc814213-e220-46-05625_E
MIIGozCCBYugAwIBAgITJwAAAA1nYbE+RFds5wAAAAADTANBgkqhkiG9w0BAQsFADBjMRMwEQYKCZImiZP...
0y0AxXzGs4Ex/slygrEGCA03MJuN3k=
```

- **RuTokenЕСP** — метка (label) токена
- **/usr/lib64/pkcs11/librtpkcs11esp.so** — библиотека вендора, которая подходит для данного токена
- **6C652D52545F4A435F45535F323034382D63633831343231332D653232302D34362D30353632355F45** — идентификатор (id) сертификата
- **le-RT_JC_ES_2048-cc814213-e220-46-05625_E** — метка (label) сертификата

- `MIIGozCCBY...A03MJuN3k=` — сертификат (вывод сокращён)

4.2.1.2. ESMART Token

```
user@alt-p10 ~ $ /usr/libexec/sss/p11_child \  
  --ca_db=/etc/pki/tls/certs/cacert.pem --pre  
esmart_64  
/usr/lib64/pkcs11/libisbc_pkcs11_main.so  
6C652D52545F4A435F45535F323034382D66316462616564382D313563642D34332D3038343637  
le-RT_JC_ES_2048-f1dbaed8-15cd-43-08467  
MIIGozCCBYugAwIBAgITJwAAAA+7dZWQmcP+kAAAAAADzANBgkqhkiG9w0BAQsFADBJMRMwEQYKCZImiZP...  
gqCa6bWgGnqxgCQqpV7ld0N3IzFmTI=
```

4.2.1.3. JaCarta-2 SE

Для проверки работы службы `sss` с токеном JaCarta-2 SE необходимо дополнительно указать слот. Сделать это можно при помощи схемы `pkcs11:<URI>`, которая поддерживается в `sss`. С полным перечнем параметров `pkcs11:<URI>` можно ознакомиться в RFC7512 (<https://datatracker.ietf.org/doc/html/rfc7512#section-2.1>).

Создадим символическую ссылку в каталоге `/usr/lib64/pkcs11/` на библиотеку `libjck2.so` (чтобы не было ошибок с первым слотом JaCarta GOST 2.0; исправлено с версии 2.7.4-alt6 пакета `libjckpkcs11`):

```
alt-p10 ~ # cd /usr/lib64/pkcs11/  
alt-p10 pkcs11 # ln -s ../libjck2.so .
```

```
user@alt-p10 ~ $ /usr/libexec/sss/p11_child \  
  --ca_db=/etc/pki/tls/certs/cacert.pem --pre --uri=pkcs11:token=jacarta-slot-laser  
jacarta-slot-laser  
/usr/lib64/pkcs11/libjckPKCS11-2.so  
6C652D52545F4A435F45535F323034382D39333561643039332D653866662D34632D3237373131  
le-RT_JC_ES_2048-935ad093-e8ff-4c-27711  
MIIGozCCBYugAwIBAgITJwAAAA4vyUvSfio0vAAAAAADzANBgkqhkiG9w0BAQsFADBJMRMwEQYKCZImiZP...  
P26XcAxrMgfjft53PYqC30uk+W7S7Q=
```

4.2.2. sssd.conf. Настройка службы sssd

Добавим в секцию `[pam]` следующие параметры для 2ФА по сертификатам:

```
[pam]  
pam_cert_auth = True  
pam_p11_allowed_services = +mate-screensaver, +lightdm, +kf5-screenlocker, +sddm  
pam_cert_db_path = /etc/pki/tls/certs/cacert.pem
```

- `pam_cert_auth` — определяем, что следует проводить аутентификацию по сертификату
- `pam_p11_allowed_services` — определяем, каким службам sssd предоставит доступ к сертификату на токене
- `pam_cert_db_path` — указываем расположение сертификата УЦ

Так как аутентификация по токену занимает больше времени чем по паролю (поиск сертификата на токене, проверка сертификата по протоколу OCSP и т.п.) необходимо увеличить таймауты для Kerberos и для p11_child. Добавим следующие параметры:

```
[domain/test5.alt]
...
krb5_auth_timeout = 60
[pam]
...
p11_child_timeout = 60
```

В итоге конфигурационный файл sssd примет следующий вид:

```
alt-p10 ~ # cat /etc/sss/sss.conf | grep -viE '(^#|^$|^;)'
[sss]
config_file_version = 2
services = nss, pam
user = _sss
domains = TEST5.ALT
[nss]
[pam]
pam_cert_auth = True
pam_p11_allowed_services = +mate-screensaver, +lightdm, +kf5-screenlocker, +sddm
pam_cert_db_path = /etc/pki/tls/certs/cacert.pem
p11_child_timeout = 60
[domain/TEST5.ALT]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad
default_shell = /bin/bash
fallback_homedir = /home/%d/%u
debug_level = 0
ad_gpo_ignore_unreadable = true
ad_gpo_access_control = permissive
krb5_auth_timeout = 60
```

После изменения конфигурации перезапустим службу, очистив при этом кеш sssd:

```
alt-p10 ~ # systemctl stop sssd && sss_cache -E && systemctl start sssd
```

5. Проверяем 2ФА в текстовой консоли

При аутентификации по сертификату на токене, до приглашения ввести пароль ожидается приглашение ввода PIN-кода. Если PIN-код верный, аутентификация должна пройти успешно, иначе — отказ. При успешной аутентификации выдаётся действующий билет Kerberos.

5.1. Рутокен ЕСР

```
alt-p10 login: rt_win
PIN for RuTokenECP:
Last login: Mon Jun 20 17:17:59 MSK 2022 on ttyS0
rt_win@alt-p10 ~ $ klist
Ticket cache: KEYRING:persistent:53804102:krb_ccache_XCL4NK0
Default principal: rt_win@TEST5.ALT

Valid starting          Expires                Service principal
21.06.2022 18:42:57    22.06.2022 04:42:57    krbtgt/TEST5.ALT@TEST5.ALT
        renew until 28.06.2022 18:42:54
```

5.2. ESMART Token

```
alt-p10 login: es_win
PIN for esmart_64:
Last login: Mon Jun 20 17:26:23 MSK 2022 on ttyS0
es_win@alt-p10 ~ $ klist
Ticket cache: KEYRING:persistent:53804104:krb_ccache_LPmR1a1
Default principal: es_win@TEST5.ALT

Valid starting          Expires                Service principal
21.06.2022 18:44:02    22.06.2022 04:44:02    krbtgt/TEST5.ALT@TEST5.ALT
        renew until 28.06.2022 18:43:57
```

5.3. JaCarta-2 SE

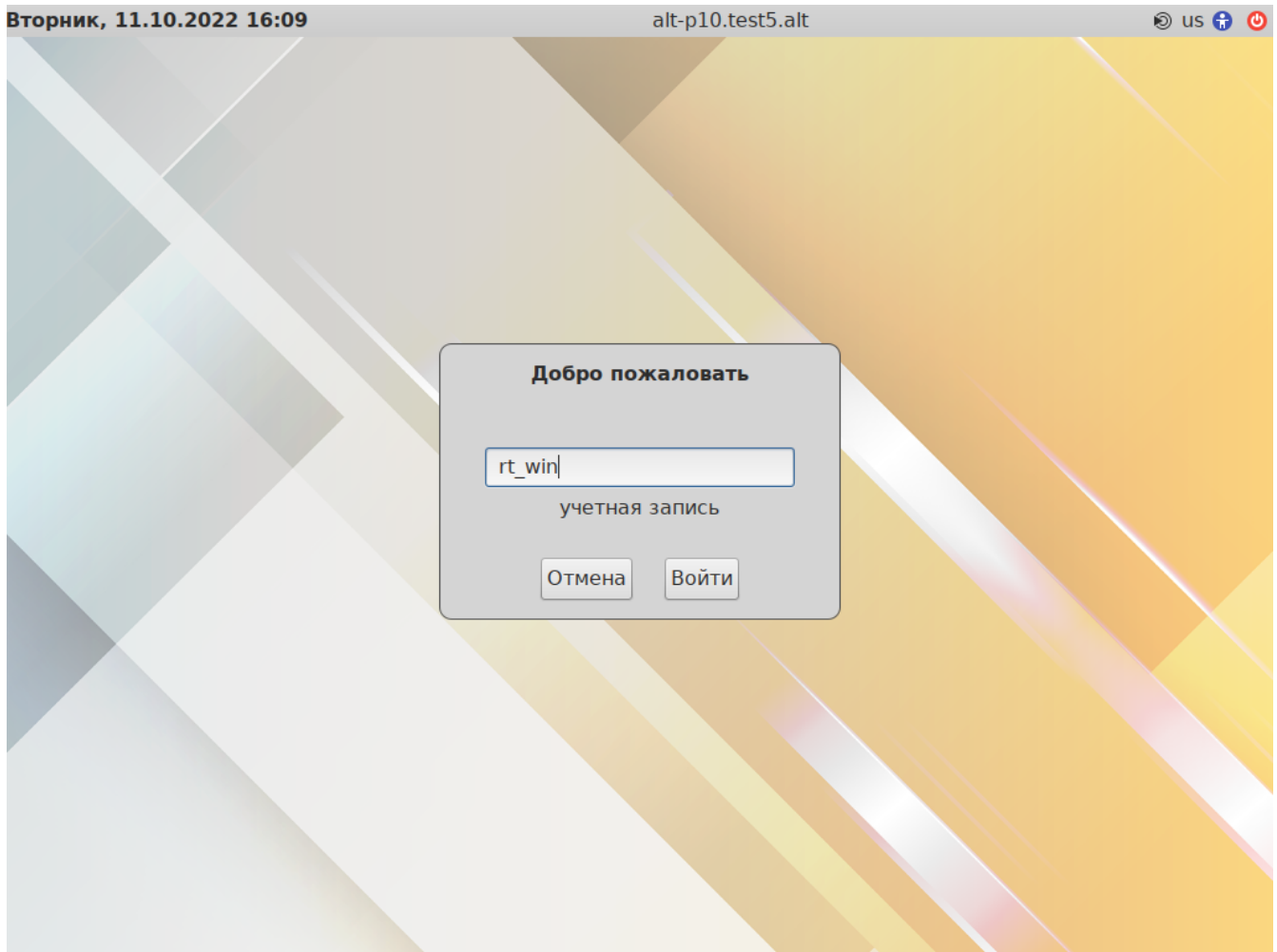
Для проверки работы службы sssd с токеном JaCarta-2 SE необходимо дополнительно указать слот. Добавьте параметр `p11_uri=pkcs11:token=jacarta-slot-laser` в секцию `[ram]` и перезапустите службу `sss`.

```
alt-p10 login: jc_win
PIN for jacarta-slot-laser:
jc_win@alt-p10 ~ $ klist
Ticket cache: KEYRING:persistent:53804103:krb_ccache_VrG194p
Default principal: jc_win@TEST5.ALT
```


Valid starting	Expires	Service principal
21.06.2022 19:38:42	22.06.2022 05:38:42	krbtgt/TEST5.ALT@TEST5.ALT
renew until	28.06.2022 19:38:29	

6. Проверяем 2ФА в графическом сеансе

6.1. Рутокен ЕСР

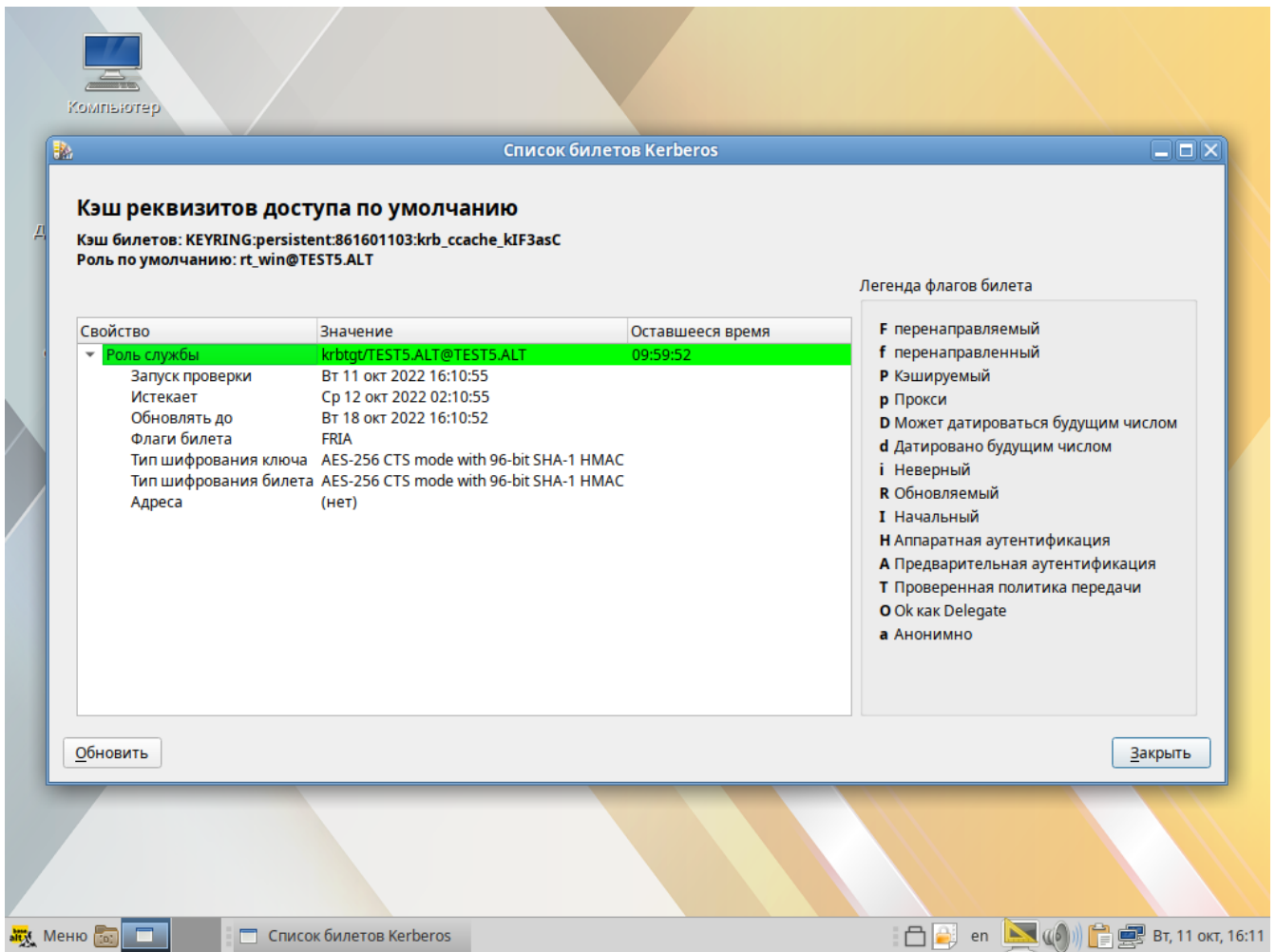


Добро пожаловать

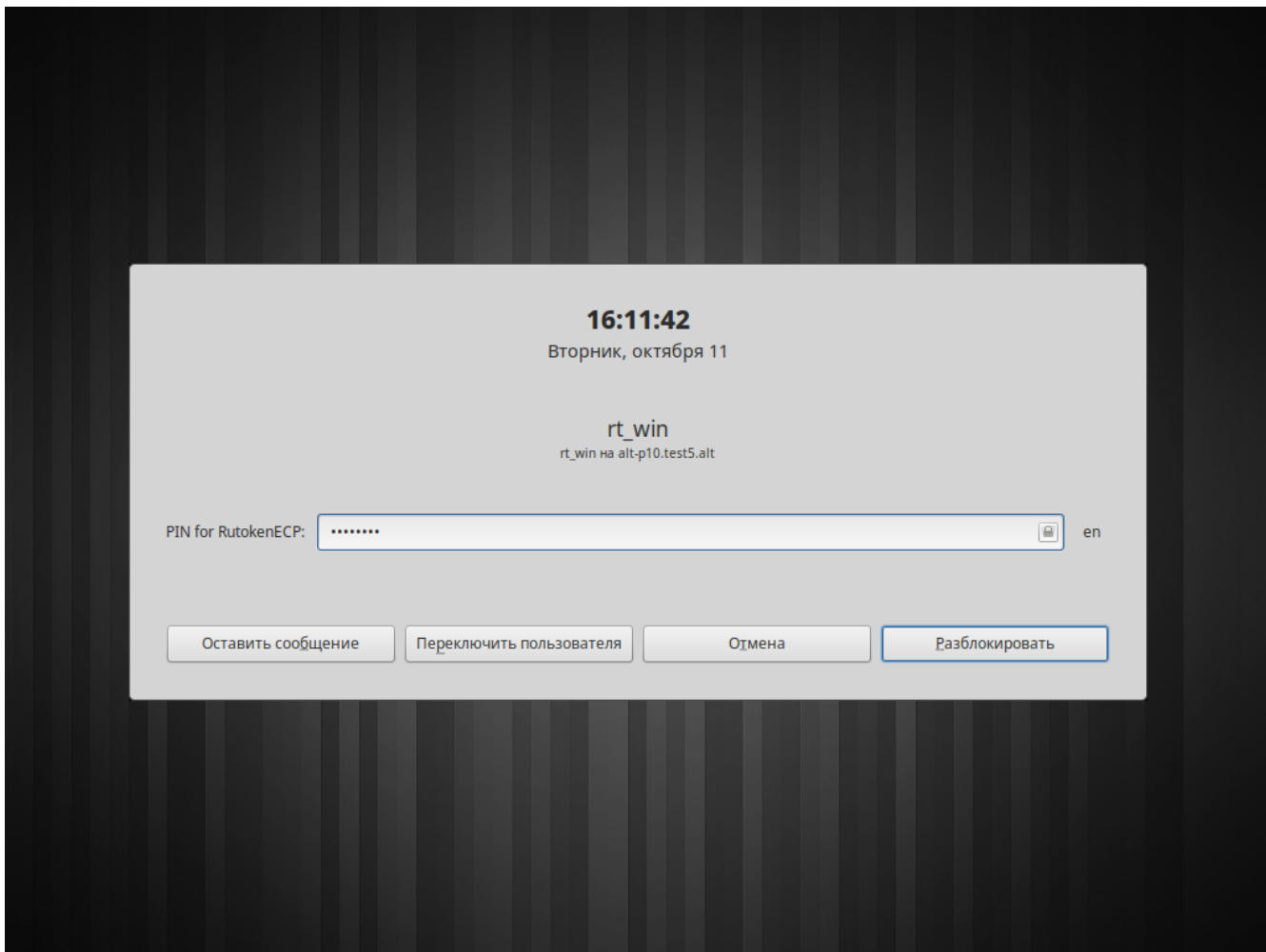
PIN for RutokenECP

Отмена

Войти



Разблокировка графического сеанса MATE по сертификату:




6.2. ESMART Token

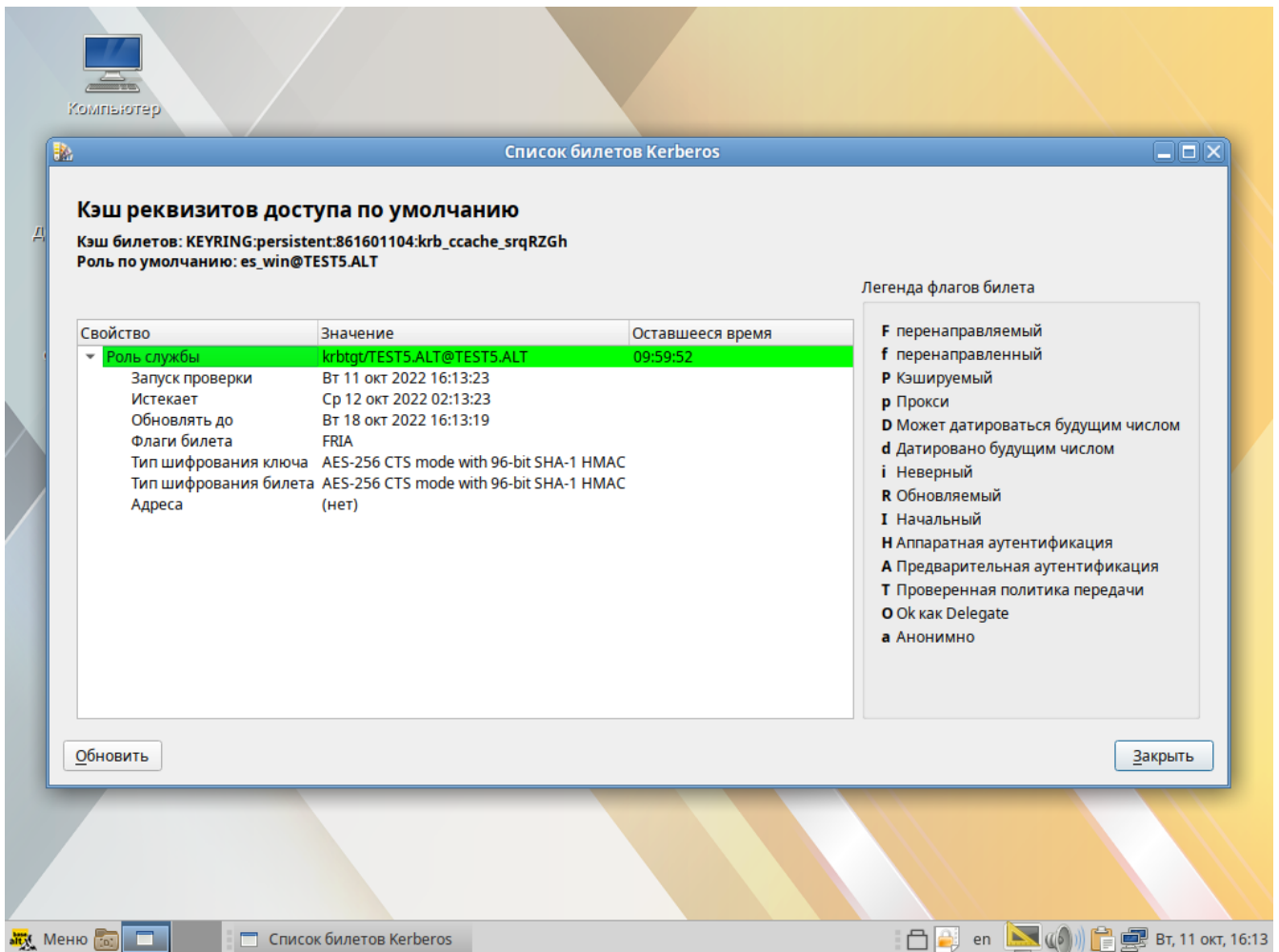
Добро пожаловать

учетная запись

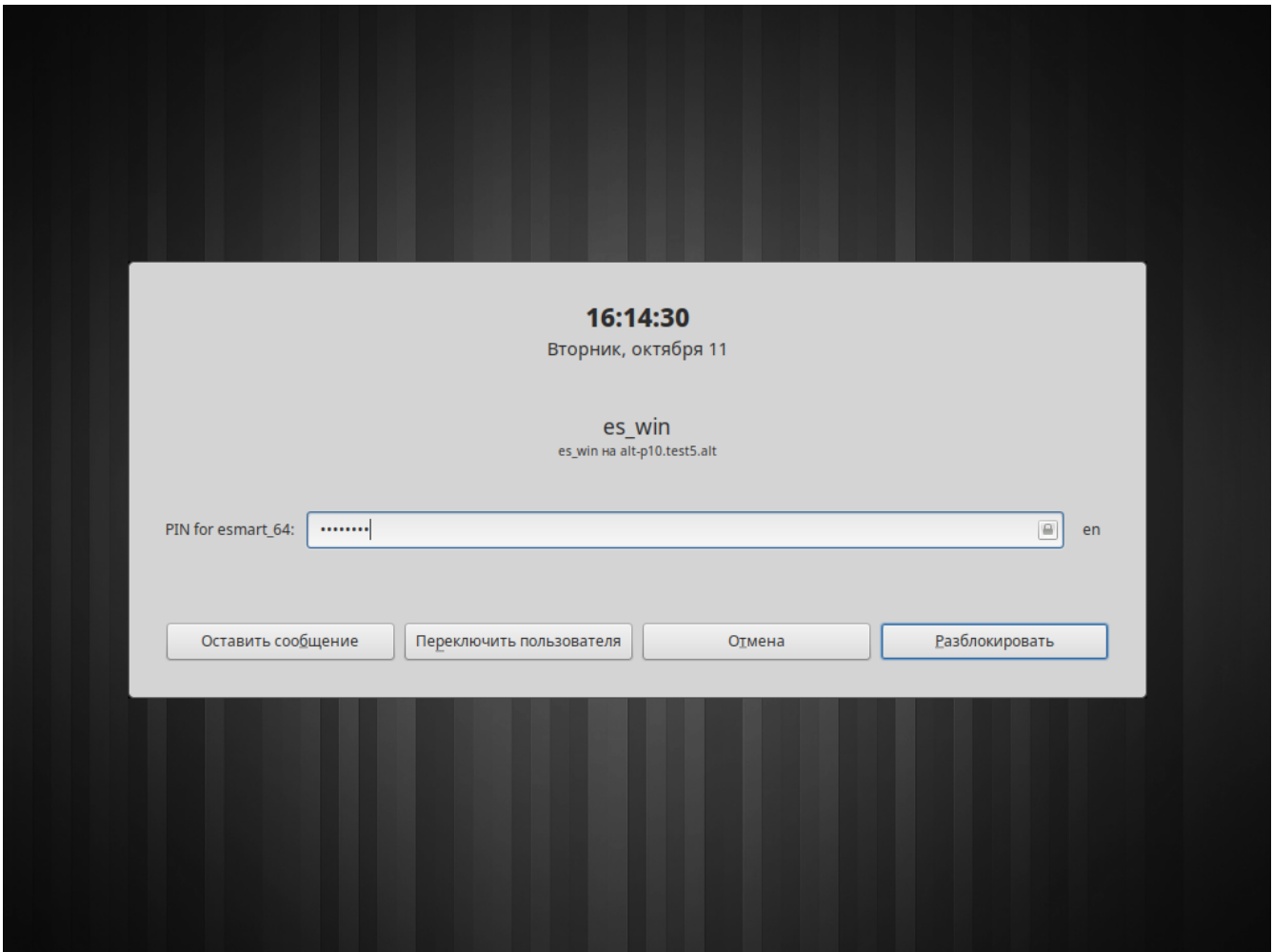
Добро пожаловать

.....| 

PIN for esmart_64



Разблокировка графического сеанса MATE по сертификату:




6.3. JaCarta-2 SE

Для проверки работы sssd с токеном JaCarta-2 SE необходимо дополнительно указать слот. Добавьте параметр `p11_uri=pkcs11:token=jacarta-slot-laser` в секцию `[ram]` и перезапустите службу `sss`.

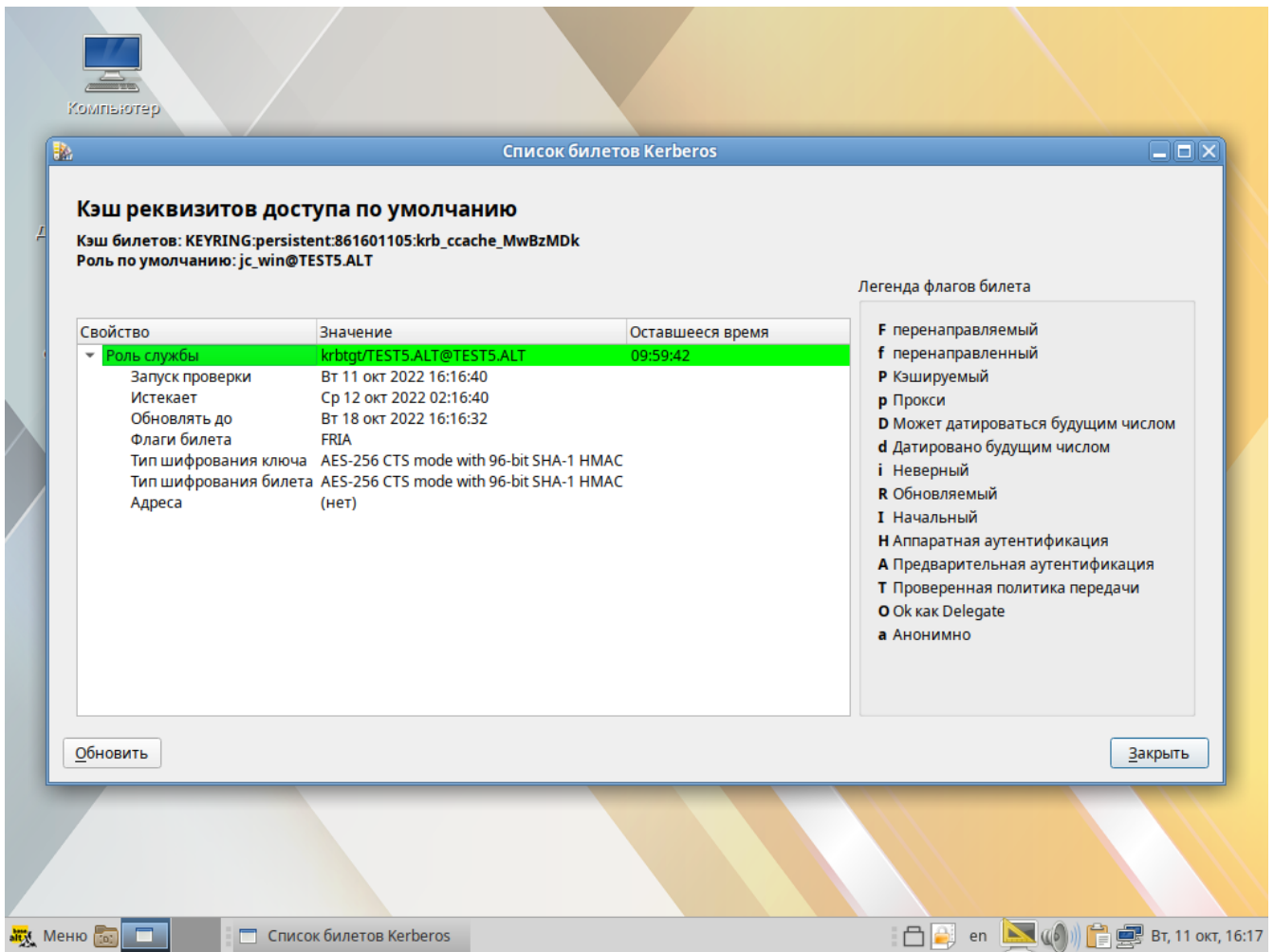
Добро пожаловать

учетная запись

Добро пожаловать

.....| 

PIN for jacarta-slot-laser



Разблокировка графического сеанса МАТЕ по сертификату:

16:17:49

Вторник, октября 11

jc_win

jc_win на alt-p10.test5.alt

PIN for jacarta-slot-laser:



en

Оставить сообщение

Переключить пользователя

Отмена

Разблокировать

7. Проверка отзыва сертификата

Отзываем сертификат на контроллере домена Windows AD. Для примера отзываем сертификат пользователя `rt_win`.

Проверяем 2ФА в консоли:

```
alt-p10 login: rt_win
Password:
```

Так как сертификат отозван, то запроса пин-кода нет.

Увидеть это можно в `/var/log/sssd/p11_child.log`:

```
...
* (2022-06-22 19:47:15): [p11_child[3763>> [read_certs] (0x4000): found cert[le-
RT_JC_ES_2048-cc814213-e220-46-05625_E][DC=alt/DC=test/CN=Users/CN=rt_win]
* (2022-06-22 19:47:15): [p11_child[3763>> [do_ocsp] (0x4000): Using OCSP URL
[http://w12r2-vm340.test5.alt/ocsp].
* (2022-06-22 19:47:15): [p11_child[3763>> [do_ocsp] (0x4000): Nonce in OCSP
response is the same as the one used in the request.
* (2022-06-22 19:47:15): [p11_child[3763>> [do_ocsp] (0x0020): OCSP check failed
with [1][revoked].
...
(2022-06-22 19:47:15): [p11_child[3763>> [read_certs] (0x0040): Certificate [le-
RT_JC_ES_2048-cc814213-e220-46-05625_E][DC=alt/DC=test/CN=Users/CN=rt_win] not valid,
skipping.
```

8. Отладка sssd

Если аутентификация по токену не работает как ожидается, то для более полной информации по этому процессу добавьте опцию вывода отладочной информации в файлы логов службы sssd. Логи службы sssd находятся в директории `/var/log/sss`. Добавление опции вывода отладочной информации необходимо добавить в те секции конфигурационного файла `sss.conf`, которые необходимо исследовать. Выглядеть это может, примерно, так:

```
[domain/test5.alt]
debug_level = 8
...
[sss]
debug_level = 8
...
[nss]
[ssh]
[sudo]
[pam]
debug_level = 8
...
```

`debug_level = 8` — уровень отладки при котором выводятся содержимое внутренних переменных функций sssd.

Более подробно об уровнях отладки см. `man sss.conf`.

9. Полезные ссылки

- https://sssd.io/design-pages/certmaps_for_LDAP_AD_file.html
- https://sssd.io/design-pages/smartcard_authentication_testing_with_ad.html
- <https://sssd.io/design-pages/smartcards.html>
- https://sssd.io/design-pages/smartcard_authentication_require.html
- https://k5wiki.kerberos.org/wiki/Pkinit_configuration
- <https://web.mit.edu/kerberos/krb5-devel/doc/admin/pkinit.html>
- <https://dev.rutoken.ru/pages/viewpage.action?pageId=57149225&src=contextnavpagetreemode>
- <https://dev.rutoken.ru/pages/viewpage.action?pageId=57148831&src=contextnavpagetreemode>
- <https://www.sysadmins.lv/blog-ru/ocsp-chast-1.aspx>
- <https://www.sysadmins.lv/blog-ru/ocsp-chast-2.aspx>