: Astra Linux Directory

:

- Astra Linux Special Edition .10015-01 (1.7), . 10015-10
- Astra Linux Special Edition .10015-17
- Astra Linux Special Edition .10015-37 (7.7)
- Astra Linux Special Edition .10015-03 (7.6)
- Astra Linux Special Edition .10152-02 (4.7)
- Astra Linux Special Edition .10015-01 (1.6)
- Astra Linux Special Edition .10015-16 . 1
- Astra Linux Special Edition .10015-16 . 2
- Astra Linux Special Edition .10265-01 (8.1)
- Astra Linux Common Edition 2.12

1.

, Astra Linux Directory (ALD):

- : SMARTCARD.ALD;
- :
  - Astra Linux Special Edition 1.6 20190222SE16 (2) ;
  - Astra Linux Directory (ALD) (. Astra Linux Directory (ALD));
  - : kdc;
- :
  - Astra Linux Special Edition 1.6 20190222SE16 (2) ;
  - : client;
- ;
- , ;
- (. Astra Linux).

2. Kerberos

- (ticket) – , , .
- (client) – (,), Kerberos.
- (key distribution center, KDC) – , Kerberos.
- (realm) – , Kerberos, KDC . realm , , .
- (principal) – , Kerberos. root[/instance]@REALM.

3.

Astra Linux:

1. - :
   - libccid;
   - pcscd;
   - libpcsclite1;
   - opensc;
2. Kerberos -:
   - krb5-pkinit;
   - libpam-krb5.

libengine-pkcs11-openssl1.1.

:

```
sudo apt install libccid pcscd libpcsclite1 pcsc-tools opensc krb5-pkinit
libpam-krb5 libengine-pkcs11-openssl1.1
```

- , librtpkcs11ecp.so, — https://www.rutoken.ru/support/download/pkcs/

: librtpkcs11ecp_2.0.2.0-1astra_e2k-8c.deb

:

```
sudo apt install ./librtpkcs11ecp_*.deb
```

"Download is performed unsandboxed"/" ", .

(-) (-) () OpenSSL. OpenSSL — SSL/TLS. RSA, DH, DSA, X.509, , CSR CRT.

:

1. (- CA). . :

   ```
   sudo mkdir /etc/ssl/CA
   ```

2. :

   ```
   cd /etc/ssl/CA
   ```

3. CA, . Common Name . : SMARTCARD.ALD:

   ```
   sudo openssl genrsa -out cakey.pem 2048
   sudo openssl req -key cakey.pem -new -x509 -days 3650 -out cacert.pem
   ```

   -days (- 3650). :

   ```
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.
   -----
   Country Name (2 letter code) [AU]:ru
   State or Province Name (full name) [Some-State]:Moscow
   Locality Name (eg, city) []:Astra Linux
   Organization Name (eg, company) [Internet Widgits Pty Ltd]:Astra Linux
   Organizational Unit Name (eg, section) []:Wiki
   Common Name (e.g. server FQDN or YOUR name) []:SMARTCARD.ALD
   ```

4. KDC, . Common Name kdc. :

   ```
   sudo openssl genrsa -out kdckey.pem 2048
   sudo openssl req -new -out kdc.req -key kdckey.pem
   ```

5. . , :

```
export REALM=SMARTCARD.ALD
export CLIENT=kdc
```

, , :

```
env | grep -E "REALM|CLIENT"
```

6. pkinit_extensions : pkinit_extensions. :

```
[ kdc_cert ]
basicConstraints=CA:FALSE

# Here are some examples of the usage of nsCertType. If it is omitted
keyUsage = nonRepudiation, digitalSignature, keyEncipherment, keyAgreement

#Pkinit EKU
extendedKeyUsage = 1.3.6.1.5.2.3.5

subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer

# Copy subject details

issuerAltName=issuer:copy

# Add id-pkinit-san (pkinit subjectAlternativeName)
subjectAltName=otherName:1.3.6.1.5.2.2;SEQUENCE:kdc_princ_name

[kdc_princ_name]
realm = EXP:0, GeneralString:${ENV::REALM}
principal_name = EXP:1, SEQUENCE:kdc_principal_seq

[kdc_principal_seq]
name_type = EXP:0, INTEGER:1
name_string = EXP:1, SEQUENCE:kdc_principals

[kdc_principals]
princ1 = GeneralString:krbtgt
princ2 = GeneralString:${ENV::REALM}

[ client_cert ]

# These extensions are added when 'ca' signs a request.

basicConstraints=CA:FALSE

keyUsage = digitalSignature, keyEncipherment, keyAgreement

extendedKeyUsage =  1.3.6.1.5.2.3.4
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer


subjectAltName=otherName:1.3.6.1.5.2.2;SEQUENCE:princ_name


# Copy subject details

issuerAltName=issuer:copy

[princ_name]
realm = EXP:0, GeneralString:${ENV::REALM}
principal_name = EXP:1, SEQUENCE:principal_seq

[principal_seq]
name_type = EXP:0, INTEGER:1
name_string = EXP:1, SEQUENCE:principals

[principals]
princ1 = GeneralString:${ENV::CLIENT}
```

7. KDC:

```
sudo -E openssl x509 -req -in kdc.req -CAkey cakey.pem -CA cacert.pem -
out kdc.pem -extfile pkinit_extensions -extensions kdc_cert -
CAcreateserial -days 365
```

8. kdc.pem, kdckey.pem, cacert.pem /var/lib/krb5kdc/:

```
sudo cp kdc.pem kdckey.pem cacert.pem /var/lib/krb5kdc/
```

9. /etc/krb5kdc/kdc.conf, /etc/krb5kdc/kdc.conf, [kdcdefaults] :

```
pkinit_identity = FILE:/var/lib/krb5kdc/kdc.pem,/var/lib/krb5kdc/kdckey.pem
pkinit_anchors = FILE:/var/lib/krb5kdc/cacert.pem
```

, .

10. :

```
sudo systemctl restart krb5-admin-server krb5-kdc
```

4. -.

, .

4.1.

:

1. librtpkcs11ecp.so:

```
find /usr/*(lib|lib64) -name librtpkcs11ecp.so
```

/usr/lib/librtpkcs11ecp.so.

2. , :

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -T
```

```
root@server:/home/u/KDC# pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -T
Available slots:
Slot 0 (0x0): Aktiv Rutoken ECP 00 00
  token label        : AstraLinux
  token manufacturer : Aktiv Co.
  token model        : Rutoken ECP
  token flags        : login required, rng, SO PIN to be changed, token initialized, PIN initialized
  hardware version   : 20.4
  firmware version   : 18.0
  serial num         : 2f996caf
  pin min/max        : 4/32
```

4.2.

. .

pkcs11-tool:

```
pkcs11-tool --slot 0 --init-token --so-pin 87654321 --label 'AstraLinux' --
module /usr/lib/librtpkcs11ecp.so
```

--slot 0 — , . , 0, - 1,2 ..;
--init-token - ;
--so-pin 87654321 - PIN- . 87654321;
--label 'AstraLinux' - ;
--module /usr/lib/librtpkcs11ecp.so — librtpkcs11ecp.so.

```
root@server:/home/u/KDC# pkcs11-tool --slot 0 --init-token --so-pin 87654321 --label 'AstraLinux' --module /usr/lib/librtpkcs11ecp.so
Token successfully initialized
root@server:/home/u/KDC# pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -T
Available slots:
Slot 0 (0x0): Aktiv Rutoken ECP 00 00
  token label        : AstraLinux
  token manufacturer : Aktiv Co.
  token model        : Rutoken ECP
  token flags        : login required, rng, SO PIN to be changed, token initialized, PIN initialized
  hardware version   : 20.4
  firmware version   : 18.0
  serial num         : 2f996caf
  pin min/max        : 4/32
```

4.3. PIN-

PIN- :

```
pkcs11-tool --slot 0 --init-pin --so-pin '87654321' --login --pin
'12345678' --module /usr/lib/librtpkcs11ecp.so
```

--init-pin - PIN- ;
--login - ;
--pin 12345678 - PIN- ;

4.4.

:

```
pkcs11-tool --slot 0 --login --pin 12345678 --keypairgen --key-type rsa:
2048 --id 33 --label "2fa_test1_key" --module /usr/lib/librtpkcs11ecp.so
```

-keypairgen --key-type rsa:2048 — , RSA 2048 ;
--id 33 — CKA_ID . CKA_ID ;
--label “test1 key” — CKA_LABEL() . ;

4.5.

:

```
openssl
```

openssl :

```
OpenSSL> engine dynamic -pre SO_PATH:/usr/lib/x86_64-linux-gnu/engines-1.1/pkcs11.so -pre ID:pkcs11 -pre
LIST_ADD:1 -pre LOAD -pre MODULE_PATH:/usr/lib/librtpkcs11ecp.so
```

```
(dynamic) Dynamic engine loading support
[Success]: SO_PATH:/usr/lib/x86_64-linux-gnu/engines-1.1/pkcs11.so
[Success]: ID:pkcs11
[Success]: LIST_ADD:1
[Success]: LOAD
[Success]: MODULE_PATH:/usr/lib/librtpkcs11ecp.so
Loaded: (pkcs11) pkcs11 engine
```

```
OpenSSL> req -engine pkcs11 -new -key 0:33 -keyform engine -out client.req
```

```
engine "pkcs11" set.
Enter PKCS#11 token PIN for Rutoken ECP <AstraLinux>:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Moscow
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Rusbitech
Organizational Unit Name (eg, section) []: Astra
Common Name (e.g. server FQDN or YOUR name) []:test1 (!__!)
Email Address []: (!__!)

OpenSSL> exit
```

-new -key 0:33, **0**— , **33** — CKA_ID .

Common Name .

4.6.

, (/etc/ssl/CA).

:

```
export REALM=SMARTCARD.ALD
export CLIENT=test1
```

SMARTCARD.ALD -
test1 -

, , :

```
env | grep -E "REALM|CLIENT"
```

:

```
sudo -E openssl x509 -CAkey cakey.pem -CA cacert.pem -req -in client.req -
extensions client_cert -extfile pkinit_extensions -out client.pem -days 365
```

PEM DER:

```
sudo openssl x509 -in client.pem -out client.cer -inform PEM -outform DER
```

:

```
pkcs11-tool --slot 0 --login --pin 12345678 --write-object client.cer --
type 'cert' --label 'test1' --id 33 --module /usr/lib/librtpkcs11ecp.so
```

⚠ **--write-object ./client.cer**— , ;
--type 'cert'— , - ;
'cert' --label 'test1'— CKA_LABEL() . ;

5. .

1. **/etc/krb5/;**
2. **/etc/krb5/ (cacert.pem)** c .
3. Kerberos, /etc/krb5.conf [libdefaults] :

```
[libdefaults]
default_realm = SMARTCARD.ALD
pkinit_anchors = FILE:/etc/krb5/cacert.pem
#
pkinit_identities = PKCS11:/usr/lib/librtpkcs11ecp.so
```

4. :

```
$ kinit
```

PIN- , . , kerberos , :

```
klist
```

:

```
kdestroy
```

⚠ kinit :

```
env KRB5_TRACE=/dev/stdout kinit <_>
```

```
Astra Linux CE 2.12.14 (orel) orel12 tty2
Hint: Num Lock on

orel12 login: test1
AstraLinux                      PIN:

Astra Linux Directory is active with default domain '.smartcard.ald'.

Last login: Wed Jul 10 11:24:04 MSK 2019 on tty2
Creating directory '/ald_home/test1'...
Changing ownership for '/ald_home/test1' (2501:2501)...
Mounting CIFS user home '/ald_home/test1'...
Mounting CIFS user home '/ald_home/test1'...
Execute /etc/ald/ald.session
test1@orel12:~$
```

. Login , Password <PIN >. , , <PIN >:

```
login test1
```

5.1.

pam_krb5.so /etc/pam.d/common-auth pam_krb5.so:

```
# here are the per-package modules (the "Primary" block)
auth    [success=4 default=ignore]      pam_krb5.so minimum_uid=2500 use_pkinit
auth    [success=1 default=ignore]      pam_succeed_if.so quiet user ingroup astra-admin
auth    [success=ignore default=die]    pam_tally.so per_user deny=8
auth    [success=1 default=ignore]      pam_unix.so nullok_secure try_first_pass
# here's the fallback if no module succeeds
```

– try_pkinit — PKCS-11, Kerberos ;

– use_pkinit — PKCS-11, ;

– pkinit_prompt — PKCS-11 .

⚠ pam-auth-update, pkinit .

, , /usr/share/pam-configs/krb5 Auth-Initial .

```
Name: Kerberos authentication
Default: yes
Priority: 704
Conflicts: krb5-openafs
Auth-Type: Primary
Auth:
        [success=end default=ignore]    pam_krb5.so minimum_uid=2500 try_first_pass
Auth-Initial:
        [success=end default=ignore]    pam_krb5.so minimum_uid=2500 use_pkinit
```

. man.

6.

- Kerberos
-
- Kerberos V5 System Administrator's Guide
- https://k5wiki.kerberos.org/wiki/Pkinit_configuration