Astra Linux Special Edition 1.3 Rutoken ECP ALD

Kerberos-

Related links

http://dev.rutoken.ru/pages/viewpage.action?pageId=3440679
https://help.ubuntu.com/community/Kerberos
: http://k5wiki.kerberos.org/wiki/Pkinit_configuration

```
Key Distribution Center (KDC) -
Admin server -  kerberos.  KDC  admin server
Realm - "",
Principal - ,  .
```

Astra Linux 1.3 x64 ALD

: . .

```
<username> = test1
<realm> = RUSBITECH.RU
<server> = server.rusbitech.ru
```

:

```
libopenct1_0.6.20-1.2_amd64.deb
openct_0.6.20-1.2_amd64.deb
opensc_0.12.2-2_amd64.deb
libp11-2_0.2.8-2_amd64.deb
libengine-pkcs11-openssl_0.1.8-2_amd64.deb
```

Kerberos realm: `RUSBITECH.RU`, `server.rusbitech.ru` (*/etc/hosts*)
: `test1@RUSBITECH.RU`
ald/kerberos `krb5-pkinit`(krb5-pkinit_1.10.1+dfsg-3_amd64.deb, Debian Wheezy):

```
dpkg -i --force-depends krb5-pkinit_1.10.1+dfsg-3_amd64.deb
```

```
$ kinit <username>
...
$ klist
...
$ kdestroy
```

,

```
$ kinit <username>@<realm>
...
$ klist
...
$ kdestroy
```

CA:

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

`Common name test1()`.

KDC:

```
openssl genrsa -out kdckey.pem 2048
```

C

```
openssl req -new -out kdc.req -key kdckey.pem
```

`Common name RUSBITECH.RU`

```
export REALM=RUSBITECH.RU #
export CLIENT=server #
```

pkinit_extensions , .

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

/var/lib/krb5kdc/:

```
kdc.pem
kdckey.pem
cacert.pem
```

preauth .

kdcdefaults :

/etc/krb5kdc/kdc.conf

```
[kdcdefaults]
    kdc_tcp_ports = 88
    pkinit_identity = FILE:/var/lib/krb5kdc/kdc.pem,/var/lib/krb5kdc/kdckey.pem
    pkinit_anchors = FILE:/var/lib/krb5kdc/cacert.pem
[realms]
    AKTIV-TEST = {
        database_name = /var/lib/krb5kdc/principal
        admin_keytab = FILE:/etc/krb5kdc/kadm5.keytab
        acl_file = /etc/krb5kdc/kadm5.acl
        key_stash_file = /etc/krb5kdc/stash
        max_life = 10h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        master_key_type = des3-hmac-sha1
        supported_enctypes = aes256-cts:normal arcfour-hmac:normal des3-hmac-sha1:normal des-cbc-crc:normal des:
normal des:v4 des:norealm des:onlyrealm des:afs3
        default_principal_flags = +preauth
    }
```

preauth

```
kadmin.local$: modprinc +requires_preauth <username>
```

/etc/krb5/

`CA (cacert.pem)` c */etc/krb5/*

```
pkcs15-init --erase-card -p rutoken_ecp
pkcs15-init --create-pkcs15 --so-pin "87654321" --so-puk ""
pkcs15-init --store-pin --label "User PIN" --auth-id 02 --pin
"12345678" --puk "" --so-pin "87654321" --finalize
```

ID!

```
pkcs15-init -G rsa/2048 --auth-id 02 --id 42 --label "testuser's key" --public-key-label "testuser's public key"
```

...

```
openssl
OpenSSL> engine dynamic -pre SO_PATH:/usr/lib/ssl/engines/engine_pkcs11.so -pre ID:pkcs11 -pre LIST_ADD:1 -pre LOAD -pre MODULE_PATH:opensc-pkcs11.so
```

:

```
(dynamic) Dynamic engine loading support
[Success]: SO_PATH:/usr/lib/openssl/engines/engine_pkcs11.so
[Success]: ID:pkcs11
[Success]: LIST_ADD:1
[Success]: LOAD
[Success]: MODULE_PATH:opensc-pkcs11.so
Loaded: (pkcs11) pkcs11 engine
```

```
OpenSSL> req -engine pkcs11 -new -key 1:42 -keyform engine -out client.req -subj "/C=RU/ST=Moscow/L=Moscow/O=Aktiv/OU=dev/CN=testuser (!_!)/emailAddress=testuser@mail.com"
```

:

```
engine "pkcs11" set.
PKCS#11 token PIN:
```

```
OpenSSL> quit
```

(client.req) CA:

```
export REALM=RUSBITECH.RU #
export CLIENT=testuser #
openssl x509 -CAkey cakey.pem -CA cacert.pem -req -in client.req -extensions client_cert -extfile pkinit_extensions -out client.pem
```

kdc:

```
/etc/init.d/krb5-admin-server restart
/etc/init.d/krb5-kdc restart
```

(client.pem) /etc/krb5/ <

```
pkcs15-init --store-certificate client.pem --auth-id 02 --id 42 --format pem
```

client.pem !

kerberos

/etc/krb5.conf

```
[libdefaults]
default_realm = RUSBITECH.RU
pkinit_anchors = FILE:/etc/krb5/cacert.pem
#
# pkinit_identities = FILE:/etc/krb5/client.pem,/etc/krb5/clientkey.pem
#
pkinit_identities = PKCS11:/usr/lib/x86_64-linux-gnu/opensc-pkcs11.so
```

```
$ kinit <username>
```