JaCarta: Astra Linux Directory 1.5

-
-
-
- -.
- .

:

- Astra Linux Special Edition .10015-01 (1.5)

Astra Linux Special Edition .10015-01 (1.6):
JaCarta: Astra Linux Directory

.pdf

— Astra Linux Smolensk SE 1.5 4.2.0-23-generic, x86_64, :

- JaCarta IDProtect 6.37;
- libccid;
- pcscd;
- libpcsclite1;
- krb5-pkinit;
- libengine-pkcs11-openssl;
- opensc.

— Astra Linux Smolensk SE 1.5 4.2.0-23-generic, x86_64, :

- JaCarta IDProtect 6.37;
- libccid;
- pcscd;
- libpcsclite1;
- krb5-pkinit.

- USB- JaCarta PKI X.509 ALD (Astra Linux Directory).

, ALD , , , .

JaCarta PKI, : libccid, pcscd, libpcsclite1. , IDProtectClient, « ..» –> –> JaCarta –> JaCarta PKI Linux.

- Kerberos ald/kerberos krb5-pkinit . JaCarta PKI, libengine-pkcs11-openssl opensc.

(CA) OpenSSL. OpenSSL — SSL/TLS. RSA, DH, DSA X.509, , CSR CRT.
EXAMPLE.RU. , EXAMPLE.RU, – kdc, – PCclient. , .
.

1. CA mkdir /etc/ssl/CA . .
2. CA:

```
openssl genrsa -out cakey.pem 2048
openssl req -key cakey.pem -new -x509 -days 365 -out cacert.pem
```

. Common name EXAMPLE.RU.

3. KDC:

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

. Common name kdc.

4. . , :

```
export REALM=<_>
export CLIENT=<_>
```

5. pkinit_extensions. , .

6. KDC:

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

7. kdc.pem, kdckey.pem, cacert.pem /var/lib/krb5kdc/

8. /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
```

, .

9. , :

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

-.

, libengine-pkcs11-openssl opensc. , .

, .

! JaCarta PKI . pkcs11-tool:

```
pkcs11-tool --slot 0 --init-token --so-pin 00000000 --label 'JaCarta PKI' --
module /lib64/libASEP11.so
```

:

--slot 0 — . , 0, – 1,2 ..
--init-token – .
--so-pin 00000000 – JaCarta PKI. 00000000
--label 'JaCarta PKI' - .
--module /lib64/libASEP11.so — libASEP11.so. idprotectclient . « ».

:

```
pkcs11-tool --slot 0 --init-pin --so-pin 00000000 --login --pin 11111111 --
module /lib64/libASEP11.so
```

:
--slot 0 — . , 0, – 1,2 ..
--init-pin – - .
--so-pin 00000000 – JaCarta PKI. 00000000
--login –
--pin 11111111 –
--module /lib64/libASEP11.so — libASEP11.so. idprotectclient . « ».

:

```
pkcs11-tool --slot 0 --login --pin 11111111 --keypairgen --key-type rsa:
2048 --id 42 --label “test1 key” --module /lib64/libASEP11.so
```

:
--slot 0 — . , 0, – 1,2 ..
--login --pin 11111111 — , , - «11111111». - , .
--keypairgen --key-type rsa:2048 — , 2048 .

--id 42 — CKA_ID . CKA_ID .

! .

--label “test1 key” — CKA_LABEL . .
--module /lib64/libASEP11.so — libASEP11.so. idprotectclient . « ».

openssl. :

```
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:/lib64/libASEP11.so
OpenSSL> req -engine pkcs11 -new -key 0:42 -keyform engine -out client.req -
subj "/C=RU/ST=Moscow/L=Moscow/O=Aladdin/OU=dev/CN=test1 (!_!)
/emailAddress=test1@mail.com"
OpenSSL>quit
```

-new -key 0:42, 0 — , 42 — CKA_ID .
, , "/C=RU/ST=Moscow/L=Moscow/O=Aladdin/OU=dev/CN=test1 (!_!)/emailAddress=test1@mail.com"

:

```
export REALM=<_>
export CLIENT=<_>
```

:

```
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:

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

:

```
pkcs11-tool --slot 0 --login --pin 11111111 --write-object client.cer --
type 'cert' --label 'Certificate' --id 42 --module /lib64/libASEP11.so
```

:
--slot 0 — . , 0, – 1,2 ..
--login --pin 11111111 — , , «11111111». - , .
--write-object ./client.cer — , .
--type 'cert' — , – .
'cert' --label 'Certificate' — CKA_LABEL . .
--id 42 — CKA_ID . CKA_ID, .
--module /lib64/libASEP11.so — libASEP11.so.

.

/etc/krb5/. /etc/krb5/ CA (cacert.pem) c . kerberos /etc/krb5.conf. [libdefaults] .

```
[libdefaults]
default_realm = EXAMPLE.RU
pkinit_anchors = FILE:/etc/krb5/cacert.pem
pkinit_identities = PKCS11:/lib64/libASEP11.so
```

:

```
kinit <username>
```

- , .
, kerberos , :

```
klist
```

— :

```
kdestroy
```

- , - -.